RELEASE NOTES

SUPERSTACK® II REMOTE ACCESS SYSTEM 1500

RELEASE 2.0

These Release Notes contain information that does not appear in the SuperStack® II Remote Access System 1500 (RAS 1500), Release 2.0 documentation. It includes the following:

Visit the RAS 1500 Web Site (http://www.3com.com/ras1500) for the latest RAS 1500 product information, code, and documentation. On this this site, you will also find a link to the 3Com Knowledgebase where you will find useful product tips and information posted by other RAS 1500 users.

ISDN Assistance

For assistance with ISDN services in the U.S., call the 3Com Access Plus hot line, 1-800-343-3266.

When a similar service is available in Canada, information will be posted on the 3Com Support Web Site (http://support.3com.com).

For assistance with ISDN services in Latin America, contact your local phone company.

Part No. 1.024.2320 Rev BA
January, 2000

New Features

The following are new features in this release:

Web Configuration Interface

The Web Configuration Interface or Web Configurator is a browser-based application for configuring features of your SuperStack® II Remote Access System1500. This new tool provides a platform-independent solution to set up your unit and only requires that you run a browser (such as, Netscape Navigator or Microsoft Internet Explorer) that supports HTML 4.0, or higher, JavaScript, and style sheets on your PC or UNIX workstation. Details for setting up basic features of your RAS 1500 are described in the *SuperStack® II Remote Access System 1500 Quick Setup Guide* that is packaged with your system. You can also find this guide by clicking on "Documentation" on the Release 2.0 Resource CD.

Primary Rate Access Unit (PAU)

The Primary Rate Access Unit (PAU) is an ISDN PRI T1 or E1 access unit that connects to your Router Unit via a STACKNET™. Once the units are connected to the base unit, the system serves as one network entity, managed as one device, by a single network management application.

Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP), acting as a server, proxy, or relay is a new component for this release. The RAS 1500 can serve as the central DHCP server for both LAN-based and remote users. In addition, it can "proxy" or "relay" IP address requests to another central server. This feature simplifies network administration and enhances the mobility of both remote and local users. The three DHCP scenarios are described below:

- **Server** - Acting as a DHCP server, the RAS 1500 receives and processes requests for IP information from dial-in clients and provides the IP information directly back to the client.
- **Proxy** - Acting as a DHCP proxy, the RAS 1500 initiates a DHCP requests to a DHCP server on behalf of a DHCP dial-in client. The DHCP server receives and processes the request and sends the IP information back to the dial-in client via the RAS 1500.
- **Relay** - Acting as a DHCP relay, the RAS 1500 passes on a request for IP information from LAN clients through a LAN-to-LAN connection to a DHCP server.

PPP Over Serial WAN Port

This release of the RAS 1500 supports a PPP connection over a leased line on its serial port. A leased line is a dedicated line between two sites and is a permanently installed rather than a dialed up connection. PPP over the

WAN port can connect to another RAS 1500 or any compatible device that supports PPP. PPP over leased line offers the following benefits:

- Constant connection. Once the connection between the sites is established, the link does not come down unless you issue a command to do so.
- Simple configuration. To prepare a RAS 1500 for leased-line PPP requires little configuration.
- Fast. The RAS 1500 supports speeds of 2.048 Mbps.

Installation and Upgrade Information

The following is installation and upgrade information in this release:

Primary Rate Access Unit (PAU) Firmware Upgrade

The Primary Rate Access Unit (PAU) is delivered with firmware pre-installed. If you upgrade to future releases of the firmware, be aware of the following information:

After issuing the download command for PAU firmware upgrade, **`download pau_image pau_x.dmf from server <tftp server ip address> command sdl_start`**, do not enter anything, even though the RAS 1500 prompt is visible from the console. The PAU code is being written to flash. Wait until the message, **`"PAU is Operational,"`** is displayed. This takes approximately 15 minutes. When the PAU is operational message is displayed, it is safe to issue commands from the console.

Operational Information

The following is operational information in this release:

Idle Timeout for LAN-to-LAN Configuration

The idle timeout default for LAN-to-LAN in the Web Configurator is 0 (or no timeout).This default value cannot be changed in the Web Configurator. If you want to change the idle timeout, and we recommend you do, you *must* use the CLI. The command is as follows:

```
Set user <user name> Idle_timeout <idle timeout value>
```

IMPORTANT: *Please be aware that if you do not change the idle timeout default value, which is set at 0, on-demand configurations will* ***not*** *timeout. This means that you could incur costly telco charges. Therefore, we recommend that you change this default from the CLI.*

NT NOS Application

Before loading the RAS 1500 NT NOS Authentication application, be sure to uninstall any previous versions of this or the AccessBuilder NOS Authentication application that may have been used previously.

Use the following steps to install and configure NOS authentication software on the Windows NT station:

1. Insert the RAS 1500 Resource CD into the Windows NT station.
2. Select Install Software from the Main Menu.
3. Select NT NOS Security. The setup program will be executed.
4. From the Windows NT desktop, click *Start*, then *Programs*, then *RAS 1500 Security Client*, then *Enable Authentication*.
5. Follow the directions to enable the service on the NT platform. This ensures the service starts each time the machine is rebooted.
6. By default the NOS program is installed to authenticate users without regard to time differences between the RAS 1500 and the NT system running NT Security Client. If you do wish to use the NT Security Client to check timestamps between the RAS 1500 and the NT system, change the default time of 0 to 15 minutes.
7. On the NT system, go to Start, Programs, RAS 1500 Security Client and select Security Client Config. The encryption key is a password exchanged between the NT system and the RAS 1500. 3Com recommends you do not change this. If you do, you must change the secret password on the RAS 1500 the Web Configurator or the CLI with the following command:

   ```
   set authentication secondary_secret [password]
   ```

8. By default, there is no timestamp checking (0). To check timestamps between the RAS 1500 and the server, enter the allowable time difference, for example, 15.
9. It is very important to set the date, time, and time zone correctly on the RAS 1500 when using the timestamp check feature of NT Security Client. To do this, through the Web Configurator click Date & Time/Timezone

10 Under the selection pulldown menu, select Timezone and select your time zone. Click Apply to enable these settings.

11 Click Daylight Savings Time, if applicable. Enter the appropriate time information, if daylight-saving applies to your configuration. Click Apply to enable those settings.

12 Click Date&Time/Timezone. Under the selection pulldown menu, select Date&Time. Select the appropriate date and time information. Click Apply to enable these settings.

The RAS 1500 does not support MS-CHAP authentication with Windows NT NOS authentication.

Users must logon locally to allow the user to use Windows NT security with the RAS 1500. For example, follow these steps:

1 Log on to the NT Server as Administrator.

2 Open the Administrative Tools Program Group.

3 Double-click the User Manager for Domains Program Group icon. The User Manager screen appears.

4 Click the single or multiple users you want to assign remote-access rights.

5 In the User Rights from *Policies* list, select "logon locally."

6 Click *OK*.

The table below shows NT event viewer messages that help when troubleshooting the RAS 1500.

Table 1 Event Viewer Messages

Message ID	Message
1	Security Service installed successfully
2	Security Service disabled
3	Security Service enabled successfully with encryption key *(key)*
4	Security Service stopped
5	User successfully authenticated *user* RAS 1500 *IP Address*
6	User failed to authenticate *user* RAS 1500 *IP Address*

Extra Blank Faceplate Packed with the PAU

For this release of the software, an I/O card does not have to be present in the Router Unit (however, if one is installed it must be installed in rm0/slot:1). Although you do not have to install an I/O card in the Router Unit, it is recommended that you cover the blank slot so that no slots are left exposed. An extra face plate is provided when you purchase a PAU. This face plate should be used to cover this empty slot in your Router Unit. It can be easily attached to the unit by using the panel screws that are provided.

PAU Delete Command

Remove the STACKNET cable from the PAU before issuing a delete command.

set imodem interface command in the CLI for the PAU

There is an undocumented **`set imodem interface`** command for saving modem configurations on the PAU that is not displayed in the section entitled, "**Set Commands**" in Chapter 4 of the *SuperStack® II Remote Access System 1500 System Reference Guide*. Enter the following command to save your PAU modem configuration:

```
set imodem interface <PAU interface name> at at&S
```

Restoring Router Unit to Factory Defaults

When the Router Unit is restored to factory defaults, the IP address and manage user(s) will be deleted. To begin using your RAS 1500, you must reassign an IP address, either through the IP Wizard available from the 2.0 Resource CD if you are a PC user, or through the CLI Quick Setup if you are a UNIX user. Refer to the *SuperStack® II Remote Access System 1500 Quick Setup Guide* for details on setting an IP address for your RAS 1500.

Once you have reassigned an IP address for your RAS 1500, use the default user name "**Admin**" and the default password "**Password**" when you configure features through the Web Configurator. You are prompted to enter this user name and password when you select the first feature, from the menu of features, that you want to configure. Both the default user name and password will be overwritten once you set your own unique manager user name and password. The user name must be between 1 and 32 alphanumeric, nonblank characters and is case-sensitive. The password must be between 1 and 15 characters and is not case-sensitive.

List Connections Command in the CLI

Sometimes a **`list connections`** command from the CLI (Command Line Interface) will scroll information. If this occurs, press <CTRL-C> to refresh the screen.

Using Fractional PRI

If you are using fractional PRI, obtain from your telco, information on the PRI line and the channels that are associated with that line. Configure a specific modem group to include only those PRI members. Do not use modem group all.

Creating A Network Service

Creating a network service automatically creates a modem group with the same name as the network service. This could cause a problem if a modem group already exists with the same name. The modem group will be overwritten with new information.

Refreshing Web Configuration Interface Data

In order to ensure data between device and web browser is synchronized, refresh the data in your web browser by clicking the reload or refresh button. Do not leave the browser open on the desktop. When configuration is complete exit out of the browser session.

Configuring Users

To properly change a user's configuration, follow these general steps:

1. From the Web Configuration Interface, telnet to the CLI in the Router Unit.
2. Disable the user.
3. Make the changes to the user's configuration.
4. Enable the user.

For example, to set an existing user, "john," as a "network" type, enter the following commands in the CLI:

1 **disable user john**

A message appears.

2 **set user john type network**

3 **enable user john**

Installing 3CDaemon and Adobe Acrobat from the 2.0 Source CD

Before you install freeware applications, such as 3CDaemon and Adobe Acrobat, from the 2.0 Resource CD, you *must* disable any antivirus software that is running on your system (i.e., Norton Utilities). If you do not, your system may fail and you may receive an operational failure message, "ISSET_SE". If after you disable antivirus software you still receive an "ISSET_SE" after installing your freeware, go to the Microsoft Support Web page and search on "ISSET_SE" for installation problems.

North American Switch Types for ISDN BRI calls

In rare situations, ISDN BRI calls using North American switch types, may connect and then immediately disconnect. If this happens, while using this release, issue the following commands for each of your BRI ISDN interfaces on the Router Unit or Port Expansion Module (PEM):

```
set switched interface rm0/slot:1/mod:1 at at*B3=0
set switched interface rm0/slot:1/mod:2 at at*B3=0
set switched interface rm0/slot:1/mod:3 at at*B3=0
set switched interface rm0/slot:1/mod:4 at at*B3=0
set switched interface rm0/slot:2/mod:1 at at*B3=0
set switched interface rm0/slot:2/mod:2 at at*B3=0
set switched interface rm0/slot:2/mod:3 at at*B3=0
set switched interface rm0/slot:2/mod:4 at at*B3=0
```