RAS 2000 Release 3.0

Release Notes

COMPUTONE
Corporation

Computone Corporation
1060 Windward Ridge Parkway
Suite 100
Alpharetta, GA 30005-3992
U.S.A.

Disclaimer: Computone Corporation ("Computone") makes no representations or warranties with respect to the contents hereof, and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Computone reserves the right to revise this publication and make changes from time to time to the contents hereof, without obligation of Computone to notify any person of such revisions or changes.

Support Information: If you require technical support, contact your Computone dealer or Computone Technical Support. The Computone Technical Support staff can be reached by phone at the following numbers, from 8:30 a.m. to 8:00 p.m. Eastern time, Monday through Friday:

(800) 241-3946 ext. 2002
(770) 625-0000 ext. 2002
(770) 625-0013 (FAX

Technical Support can be contacted by email at the Internet address **`support@computone.com`**

Release Notes, RAS 2000, Release 3.0 P/N: 0-13091, Rev.B

Contents

RELEASE NOTES

RAS 2000 Release 3.0

The purpose of this release is to add three new features:

- Web based configuration
- Secure shell server functionality
- DHCP support.

The web server provides the ability to change most configuration items via a web browser. This has been tested on Microsoft's Internet Explorer 5.0 and on Netscape's Navigator version 4.5.

The secure shell provides end-to-end encryption of shell sessions. It uses a port of OpenSSH version 1.5 in conjunction with cryptographic software. The implementation supports server key lengths up to 2048 bits, however because of the extraordinary load on the processor, limit the key sizes to 1024 bits. There are two builds of the kernel available: US and International. The secure shell is only available with the US kernel build.

When booting up without a configured IP address, the RAS 2000 polls three services for a configuration: BOOTP, RARP, and DHCP. The first server to respond wins the R2000's attention.

Secure Shell

Encryption of data can take on many forms, some more secure than others. Some of the earliest forms of encryption included smoke signals and Morse code. A bit more sophisticated were the schemes where each character of the alphabet was replaced by some other letter - scramblers. In all these cases, the sender and the recipient of a message had to agree upon the encryption algorithm and the key being used prior to sending the message. So, how does the sender inform the recipient, in a secure fashion, of the encryption method and keys used? The answer is in the sections following.

Encryption Key Generation

Mathematical algorithms use very large prime numbers to derive encryption and decryption keys.

Table 1 Encryption Key Types

Key Type	**Definition**	**Advantage**	**Disadvantage**
Symmetric	When the key used to decrypt the message is the same as the key used to encrypt the message, the key is said to be "symmetric".	They are fast. Encryption and decryption can be accomplished very quickly when compared to asymmetric keys.	Both the sender and the recipient must agree ahead of time on a specific key.
Asymmetric	Some algorithms derive separate encryption and decryption keys. These are said to be "asymmetric" and are also know as public/private key pairs or RSA keys.	The advantage of asymmetric keys is that you can publish one of them as your "public key" and keep the other one private. Thus someone wanting to send you a message encrypts the message with your public key, knowing that only the person with the private key namely you, can decrypt it. The reverse can also be used to send a message. If a recipient can decrypt a message using your public key, then the message must have originated and been encrypted by someone with the private key.	The disadvantage of asymmetric keys is that they are extremely math intensive and thus require lots of CPU time.

The secure shell, in accordance with the OpenSSH version 1.5 specification, uses both asymmetric and symmetric keys. Specifically, it generates two separate asymmetric key pairs which are defined as:

Table 2 **Secure Shell Asymmetric Key Pairs**

Key	Definition
host key	The host key is generated one time and is good for the life of the machine. As such, it gets stored in an area of flash that can neither be saved nor restored.
server key	The server key is generated at run time, is stored in memory, and is never used more than one hour (configurable).

When a client connects to the secure shell server in the RAS 2000, the server sends its version information to the client. If the client doesn't like the version information, it disconnects and perhaps informs the user. If the server version i acceptable to the client, the client then sends its version information to the server. Again, if the server finds this unacceptable, it disconnects.

Once the server and client have accepted each other's version:

1. The server sends the client the public portion of its host key followed by the public portion of its server key, still in plain text. Also contained in this message are the encryption algorithms supported by the server.
2. The client generates a random 128-bit number that becomes the session key, which is a symmetric key.
3. The client selects from an encryption method supplied by the server and encrypts this choice along with the session key using both the public host key and the public server key supplied by the server and sends the encrypted message to the server. Since the private portions of these keys are known only to the server, only the server can decrypt it to obtain the session key.
4. From this point on, all data in this session is encrypted using the session key before being sent to the other party. This session key lasts only as long as the session. Therefore, if the client were to disconnect and reconnect, it would generate a different session key.
5. User authentication takes place next. The only authentication methods supported by the RAS 2000 is Local and RADIUS. Local authentication takes place against the locally defined user file. RADIUS authentication takes place on a RADIUS server.

■ End of Procedure

Key Size and Security

The host key size and the server key size are paramount in determining how secure the keys are. The following is important to remember.

Table 3 Key Size and Security

Key Type	Strong Security	Weak Security	Notes
Symmetric	128 bit	40 bits	
Asymmetric (Host & Server)	1024 bits	512 bit	It is recommended configuring the host key to be 1024 bits and the server key to be 768 bits. Since the session key is generated by the client, it is suggested that you configure your client (if possible) to generate a 128-bit key. The RAS 2000 supports up to 2048-bit host and server keys. The practicality of keys larger than that decreased substantially while CPU requirements increased exponentially. Additionally, if you are going to secure a RAS 2000, be sure to disable the web configuration (httpd) and the insecure shell (telnetd).

Secure Shell Configuration

The RAS 2000 is shipped configured to have the web server running, as well as telnetd and sshd. However, sshd refuses to run until a host key has been generated, a process that must be started manually. Before generating a host key, however, you must configure the secure shell parameters.

Configuring Secure Shell Parameters

To begin the secure shell parameter configuration process:

1. Do one of the following. Either telnet into the RAS 2000, or connect a serial terminal (or terminal emulator) to the console port (usually port 0).
2. From a shell prompt, run the `apps` command to display a list of applications and their current enabled or disabled status.

NOTE: If you wish to secure your RAS 2000, it is suggested that you disable httpd and telnetd and enable sshd. If you wish to leave your RAS 2000 unsecured, it is suggested that you disable sshd. For the time being, leave httpd and telnetd enabled so that if something goes wrong during the configuration process you are able to telnet in to fix it.

3. Enable the sshd applications with the following command:

```
apps set sshd enable
```

4. Run `ssh` and the ssh parameters are displayed:

Table 4 ssh Parameters

Parameter	Definition
hostkey	Number of bits that are used to generate the host key.
serverkey	Number of bits that are used to generate a server key.
authgrace	Number of seconds that a user has to successfully authenticate before being cut off.
regen	Defines the usable life span of a server key in seconds.
port	Defines the TCP port on which sshd listens for connection requests.
authmethod	Defines the method by which users are authenticated. Possible values are “local”, “radius”, or “both”. In the latter case, the local user file is checked first, then RADIUS.
allowroot	Either allow or disallow a user to login as root.

5. Set the parameters as desired using one or more commands of the form:

```
ssh set <paramName> <value>
```

For more help, type in `help ssh`.

6. Save these configuration parameters to flash so that they are used the next time the machine is booted. Saving to a TFTPhost is fine as well, as long as the system is configured to fetch its configuration from thatsame TFTP host. To save, type:

```
save
```

or

```
save <hostname> <filename>
```

All the configuration parameters are now set.

■ End of Procedure

Generating a Host Ke

Once you have configured the secure shell parameters it is time to generate a host key. Use the following procedure:

1. Type `sshd gen`

Typical times for a 1024-bit key range from 21 seconds to 4 minutes. The host key is saved to a section of non-volatile memory that is not considered part of the system's configuration and, thus, is not included in saves and restores. Therefore, it is safe to save or restore your configurationvia TFTP.

CAUTION: It is strongly recommended erasing the host key prior to selling the machine, shipping it back for RMA, or otherwise releasing the machine fro your possession. An additional argument to `sshd` has been added to help you keep your system secure in the event you should ship it somewhere. This command is

```
sshd erase
```

This erases the host key from non-volatile memory.

During the RMA process, Computone can not guarantee the security of your machine, nor the security of your host key. Furthermore, Computone can not guarantee that you'll get the same machine you sent us; it could have a different engine card.

2. Once the host key generation is complete, reboot the machine with the following command:

```
shutdown now
```

This assures that the new configuration takes effect. Depending on the size of your server key, it may take a few minutes after a reboot for sshd to become ready. Recall that it requires both a host key and a server key, and that the server key is generated at runtime.

3. Start your ssh client and connect to the RAS 2000. Depending on the client it may or may not ask for your user name, though it should always ask for your password. After logging in you should see a shell prompt.

4. To complete securing your RAS 2000, it is recommended that httpd and telnetd be disabled. This can be accomplished from a shell prompt with the following command:

```
apps set httpd disable

apps set telnetd disable
```

5. Save this configuration to flash and/or a TFTP server:

```
save
```

6. Reboot the RAS 2000 using the following command to ensure these two services are NOT running:

```
shutdown now
```

■ End of Procedure

Configuration Flash Remapping

In prior releases, the configuration flash memory was divided into two sections and this left no room to store the host key. In this release, the configuration flash has been reorganized to allow room for the host key to be stored.

Since the capability of running a new kernel from netboot exists, reorganizing the configuration flash must be delayed until the new kernel is actually loaded from flash. Here's the reasoning:

- The old kernel does not recognize the new configuration layout. Therefore, a long as the old kernel exists in flash, the configuration flash can not be reorganized to the new mapping. If the machine were to reboot to the old kernel, it must be able to understand the layout of the configuration flash.
- If the new kernel is netbooted it recognizes the old configuration flash layout and uses it and *maintains* that layout when saving configuration information to flash. Additionally, it disables all secure shell functions since there's no place to store a host key in the old layout.
- If the new kernel is saved to flash, the configuration flash layout is reorganized the next time the machine is booted from flash. This makes room for the host key and allows secure shell functionality.

Once the new kernel is saved to flash and the configuration flash layout reorganized, that machine can not netboot an old kernel and expect that old kernel to understand the new layout. If downgrading to an old kernel is required, see the section, *Downgrading the Kernel*.

DHCP (Dynamic Host Configuration

Release 3.0 of the RAS 2000 introduces a limited implementation of DHCP (see section ***Release 3.0.4***). The limitation to the use of DHCP is that the RAS 2000 continues to use an assigned IP address even though, perhaps, the lease on the address has long since expired. This is due to the fact that the RAS 2000 can not change the IP address of the ethernet interface on-the-fly.

In most cases, this is not a problem because the unit attempts to renew its lease on an address as dictated by parameters provided by the DHCP server, usually half the duration of the lease. If the DHCP server can not be contacted for lease renewal, the RAS 2000 waits half the remaining duration of the lease and tries the renewal process again. If the lease period expires, the RAS 2000 continue renewal attempts every 30 minutes.

It is recommended that an IP address be reserved in the DHCP server for each RAS 2000 it serves. This assures that the address is issued to no other node on the network.

Known Bugs

Updating the Kernel

The RAS 2000, as shipped, comes with the latest released kernel installed. However, latency in our distribution channels could mean that by the time you receive your RAS 2000, a more recent kernel is available. Computone tries to make bug fixes and additional features available at least once each quarter. Kernel files are posted on Computone's FTP site in the ***/pub/Products/ras2000*** directory. Be sure to check this occasionally

Use the following procedure to install a new kernel:

1. Download the desired kernel version from Computone's FTP site. Be sure to use the BINARY transfer mode.
2. Place the file in your TFTP server's directory.
3. Log in as root on the RAS 2000 PowerRack.
4. Save the current configuration to a TFTP host. If you later choose to reinstall the old kernel, you'll need to restore your configuration from this saved copy. When naming the file in which the configuration is stored, also include the version of the kernel under which it was saved.

```
save <hostname> <configFileName>
```

You now have a choice of either running the new kernel, saving it to flash, or both. **If you want to run the new kernel without saving it to flash memory** (preserving your existing kernel), enter the command:

```
netboot host filename
```

where “host” is the name or IP address of the TFTP server on which the file is stored, and “filename” is the name of the file as it's stored on that server.

5. **To save the new kernel to flash**, overwriting your existing kernel, enter the command:

```
netboot -s host filename
```

6. **To both save and execute the new kernel**, enter the command:

```
netboot -sr host filename
```

Attention Beta Testers: If you are upgrading from a release or beta version prior to 2.3, you also have to perform the upgrade as a two-step process. First, netboot the kernel without saving it to flash (first example above). Second, `netboot -sb` to save the kernel and the bootstrap loader into flash (second example above). Upgrading from kernel 2.3 does not require the -b command line switch.

■ End of Procedure

Downgrading the Kernel

For discussion purposes, it is assumed that you have version 3.0 saved to the kernel flash, configuration flash has been reorganized, and that for some reason you wish to install a previous version of the kernel. It is also assumed that you've downloaded the desired kernel image fro our ftp site and that you've stored this kernel on a TFTP site.

Use the following procedure to load an older kernel version:

1. Connect a serial terminal or terminal emulator to the console port (usually port 0).
2. Save your current configuration to a TFTP host using the following command.

```
save <hostname> <filename>
```

3. Load and save the old kernel to flash using the following command.

```
netboot -sr <hostname> <kernelImageName>
```

This will also reboot the machine once the save is complete.

4. The system comes up and is able to read the IP address and MAC address out of the configuration. However, since previous versions do not know how to read the entire configuration from the new layout, it is guaranteed to be inaccurate. Therefore, it is necessary to restore the configuration that was saved when you upgraded to the current release. Use the following command:

```
restore <hostname> <configFileName>
```

5. Save the restored configuration to flash and reboot the machine to assure all aspects of this configuration are effective. Type the following:

```
save

shutdown now
```

■End of Procedure

Still Need Help

Computone's technical support staff is only a phone call or e-mail away:

1-800-241-3946 or support@computone.com.

Release 3.0.4

The following table outlines the changes, additions, and corrections comprising Release 3.0.4 of the RAS 2000.

Table 5 Release 3.0.4 Description

Feature		Description
ssh	Added	Non-administrative users can now use ssh.
	Added	Commands can now be executed from ssh using standard command-line executable shell comands, such as: ***Ssh -l user_name ip_address*** Example: **`ssh -1 root 10.1.1.10`** ***Ssh -l user_name -t ip_address command*** Example: **`ssh -l root -t 10.1.1.10 menu`**
DHCP	Changed	DHCP now accepts host name, subnet mask, gateway, name server, and merit dump file. The merit dump file may contain the name of a configuratio file to load from a given TFTP server. The TFTP server can be specified in the DHCP setup.)
BOOT	Added	Added ***admin forcebootp*** command to force a bootp/dhcp request.
	Changed	Modified boot sequence. The RAS 2000 now issues two bootp requests, then two DHCP requests if a bootp server does not respond.
TFTP	Added	NVRAM parameters are now patched with bootp/dhcp network info when downloading a config file from a TFTP server.
Global Connections	Added	The Global Connections funtion was added to the HTML menu selections.
	Added	***tip*** added to connections list under tables/Global Connections/Command. **NOTE**: User connections are incomplete, but will be completed next release.

Release 3.0.5

Release 3.0.5 of the RAS 2000 adds the following means of restoring factory defaults. You can restore to factory defaults by:

1. Connecting a terminal to port 0, at 9600 baud, 8-bit characters, no parity, and 1 stop bit.
2. Pressing the ESC key while the RAS 2000 is booting (at power-up or after a "shutdown" command).

This feature was present in the PowerRack product, and is in addition to the "pin-hole" method of restoring factory defaults already present.

Release 3.0.6

Release 3.0.6 of the RAS 2000 adds the following changes:

- Fixed message bug in “save hostname configfile”.
- Allows hang-up port ptsxx to work on ssh sessions.
- Added command line option to tip to allow changing the exit character. Command line: tip -x portnum, where ‘x’ is the character (default is ‘.’).
- Added xmodem suppoort to send/receive configuration files via serial port. Works with Hyperterm only.
- Ssh commands can now be executed directly (e.g. **ssh -l root 160.77.25.89 ps**).
- Tip exits if it’s parent shell dies.
- Added tip command to issue a break. (~%b).
- Modified radius handling to allow null service type.
- Fixed tip to handle incoming breaks.
- Added admin allowtelnet and allowssh commands to allow non-root users to telnet/ssh.
- Added tipmenu login type.
- Tip and tipmenu terminate if the incoming connection (telnet, ssh, or serial port) is disconnected.
- Tip can now be used whether or not the port is set as a modem port (i.e. set port modem yes/no). If the port is set to modem yes, tip will exit when carrier is lost. If the port is set to modem no, tip will not exit when carrier is lost or detected.