RELEASE NOTES

SUPERSTACK® II REMOTE ACCESS SYSTEM 1500

RELEASE 2.5

These Release Notes contain information for Release 2.5 of the SuperStack® II Remote Access System 1500 (RAS 1500). 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 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 Integrated Services Digital Network (ISDN) services in the U.S., call the 3Com Access Plus hot line, 1-800-367-3869.

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 CA
June 2000

New Features

The following are new features in this release:

MSCHAP Version 1 and MSCHAP Version 2

RAS 1500 includes support for local, Remote Authentication Dial In User Services (RADIUS) and NT NOS authentication. In addition to Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) support, Release 2.5 adds MSCHAP Versions 1 and 2 for local and RADIUS authentication. Versions 1 and 2 are separate protocols and are incompatible with each other. Therefore, you must set Point To Point (PPP) Receive Authentication using *either* Version 1 or Version 2 of MSCHAP.

You may set PPP Receive Authentication through the Web Configuration Interface. From the main, browser-based Web Configuration Interface page, click *Authentication* under the **Administration** menu. The selections for MSCHAPV1 or MSCHAPV2 are under the **PPP Authentication Type** pulldown menu.

You may also set PPP Receive Authentication through the Command Line Interface (CLI). The CLI command to set PPP Receive Authentication using *either* Version 1 or Version 2 is as follows:

```
SET PPP RECEIVE_AUTHENTICATION [ANY CHAP MSCHAPV1 MSCHAPV2
NONE PAP]
```

Note the use of "any" in the above CLI command example. If you previously set any scripts using "either" (which was specified in the CLI command for Version 2.0), you will need to change "either" to "any" in the script.

Full Duplex Ethernet

Ethernet now has full duplex functionality. Full duplex is typically implemented between two endpoints. Both endpoints of the full duplex link *must* operate in full duplex mode in order for full duplex to be fully operational. If both endpoints are not set for full duplex functionality, performance may degrade. The CLI command to set full duplex or half is as follows:

```
SET ETHERNET DUPLEX_MODE [FULL_DUPLEX HALF_DUPLEX]
```

Auto-negotiation is not supported on the Ethernet port. Therefore, when you set full duplex while connected through a switch on the Ethernet port, make sure you manually set the switch to full duplex mode.

File Compression

Release 2.5 includes improved file compression for internal file storage, increasing the amount of free space on the flash of the Router Unit. This allows for larger configuration files stored locally on the flash, and reduces the frequency of RAS 1500 going into 'Flash Compaction' mode. This feature is automatic and you don't have to do anything to implement it.

TCP PAT

Release 2.5 includes support for Port Address Translation (PAT) over the WAN interface. Transmission Control Protocol (TCP) PAT sets a static address mapping translation for a connection and associates a user name with that connection. TCP PAT translates TCP port numbers and user IP addresses on the private network and maps these addresses to a single ISP-assigned address.

You can set PAT through the Web Configuration Interface. From the main browser-based Web Configuration Interface page, click *Select NAT/PAT Configuration* under the **Network** menu, choose PAT and supply the following parameters:

- User name
- TCP Public Port
- TCP Private Port
- TCP Private IP Address

You can also set PAT using CLI. The CLI command for adding TCP PAT over the WAN interface is as follows:

```
ADD PAT TCP USER <USER_NAME>
```

This command should be followed sequentially by the following sub commands. See the table below for definitions of the parameters.

```
PRIVATE_ADDRESS <IP_ADDRESS>
PRIVATE_PORT <NUMBER>
PUBLIC_PORT <NUMBER>
```

Parameter	Description
<USER_ NAME>	Unique name you assign to the connection that you want to configure for static TCP PAT. Limit: 32 ASCII characters.
PRIVATE_ADDRESS	The source IP address of the user on the private network.

Parameter	Description
PRIVATE_PORT	The source port number on the private network from which TCP packets are transferred.
PUBLIC_PORT	The destination port number of the ISP-assigned IP address on the public network.

UDP PAT Release 2.5 includes support for User Data Protocol (UDP) PAT over the WAN interface. UDP PAT sets a static address mapping translation for a connection and associates a user name with that connection. UDP PAT translates UDP port numbers and user addresses on the private network and maps these addresses to a single ISP-assigned address by changing the source IP port number and IP address.

You can set UDP PAT through the Web Configuration Interface. From the main, browser-based Web Configuration Interface page, click *Select NAT/PAT Configuration* under the **Network** menu, choose PAT and supply the following parameters:

- User name
- UDP Public Port
- UDP Private Port
- UDP Private IP Address

You can also set UDP PAT using CLI. The CLI command for adding UDP PAT over the WAN interface is as follows:

```
ADD PAT UDP USER <USER_NAME>
```

This command should be followed sequentially by the following sub commands. See the table below for definitions of the parameters.

```
PRIVATE_ADDRESS <IP_ADDRESS>
PRIVATE_PORT <NUMBER>
PUBLIC_PORT <NUMBER>
```

Parameter	Description
<USER_ NAME>	Unique name you assign to the connection that you want to configure for static UDP PAT. Limit: 32 ASCII characters.
PRIVATE_ADDRESS	The source IP address of the user on the private network.
PRIVATE_PORT	The source port number on the private network from which UDP packets are transferred.

Parameter	Description
PUBLIC_PORT	The destination port number of the ISP-assigned IP address on the public network.
PUBLIC_PORT	The port number of the single ISP-assigned IP address on the public network.

Note: *PAT can only be used when the ISP has provided only one IP address. This one IP address will dynamically change with each new connection.*

Dynamic NAT

Release 2.5 includes support for Dynamic Network Address Translation (NAT) over the WAN interface. Dynamic NAT configures and associates a name with a specific number of ISP-assigned addresses.

You can set Dynamic NAT through the Web Configuration Interface. From the main, browser-based Web Configuration Interface page, click *Select NAT/PAT Configuration* under the **Network** menu, choose NAT and supply the following parameters:

- User name
- Starting IP Address
- Number of Addresses
- Subnet Mask

You can also set Dynamic NAT using CLI. The CLI command for adding Dynamic NAT over the WAN interface is as follows:

```
ADD NAT DYNAMIC USER <USER_NAME>
```

This command should be followed sequentially by the following sub commands. See the table below for definitions of the parameters.

```
COUNT <NUMBER OF ADDRESSES>
PUBLIC_POOL_START<IP_ADDRESS>
```

Parameter	Description
<USER_ NAME>	Unique name that you want to assign the connection that uses Dynamic NAT to map ISP-assigned addresses to connections on the private network. Limit: 32 ASCII characters.
COUNT	Total number of ISP-assigned addresses starting with the public_pool_start address that is used by the RAS 1500 for Dynamic NAT mapping.

Parameter	Description
PUBLIC_POOL_START	The first of the contiguous range of IP addresses assigned by Dynamic NAT mapping.

Below is an example of Dynamic NAT.

The command,

```
ADD NAT DYNAMIC USER NATD COUNT 4 PUBLIC_POOL_START 2.2.2.2
```

sets (the count of) **"4"** consecutive ISP-assigned addresses beginning with the ISP-assigned address **"2.2.2.2"** to use for Dynamic NAT. In this case, the range includes the ISP-assigned addresses, "2.2.2.2", "2.2.2.3", "2.2.2.4", and "2.2.2.5". **"NATD"** represents the name that is assigned for the connection for this configured range.

Each time a user connects to the public network, Dynamic NAT translates the IP address from that user on the private network and maps it to the first available public IP address from the contiguous range of ISP-assigned addresses that you configured by using this command. The RAS 1500 maintains a table of active IP addresses on the public network mapped to user IP addresses on the private network for the connection. Once the connection to the public network is closed, the information in the table is dropped and this IP address is free for the next connection. Each time a user connects to the public network, the next available address from the contiguous range is assigned, and a new table of mapped addresses is established by the RAS 1500.

Static NAT

Release 2.5 includes support for Static NAT over the WAN interface. Static NAT configures, and associates a name to, a mapping between and IP address on the private network to a *specific* ISP-assigned address on the public network that uses Static NAT.

You can set Static NAT through the Web Configuration Interface. From the main, browser-based Web Configuration Interface page, click *Select NAT/PAT Configuration* under the **Network** menu, choose NAT and supply the following parameters:

- User name
- Public IP Address
- Private IP Address

You can also set Static NAT using CLI. The CLI command for adding Static NAT over the WAN interface is as follows:

```
ADD NAT STATIC USER <USER_NAME>
```

This command should be followed sequentially by the following sub commands. See the table below for definitions of the parameters.

```
PRIVATE_ADDRESS <IP_ADDRESS>
PUBLIC_ADDRESS <IP_ADDRESS>
```

Parameter	Description
<USER_ NAME>	Unique name that you want to assign the connection that uses Static NAT to map a specific ISP-assigned address to a specific address on the private network.
PRIVATE_ADDRESS	The network address of the host on the private network that is designated a specific, static public IP address. This address is always used when connecting to the public network.
PUBLIC_ADDRESS	The public network IP address from the contiguous range assigned by the ISP, that is reserved for, and always maps to, the IP address on the private network configured for Static NAT.

Below is an example of Static NAT.

The command,

```
ADD NAT STATIC USER NATS PRIVATE ADDRESS 1.1.1.1 PUBLIC
ADDRESS 2.2.2.2
```

statically assigns the private address 1.1.1.1 to the ISP-assigned addresses address **“2.2.2.2”** to for Static NAT and names this mapping that uses Static NAT, **“NATS”**. In this case, 1.1.1.1 **always** connects to 2.2.2.2. In this example, **“NATS”** is the name given to the mapping between the IP address on the private network and ISP-assigned address on the public network configured for this Static NAT.

Each time the IP address on the private network, “1.1.1.1” connects to the public network, Static NAT translates the IP address and connects it to the static assigned addresses, “2.2.2.2”. The RAS 1500 maintains a table of active mappings between IP addresses on the private network mapped to statically assigned IP addresses on the public network.

NAT can only be used when the ISP has provided more than one IP address. The first and last in the contiguous range of ISP-assigned

addresses are "broadcast" addresses and are not available for NAT. The second address in the contiguous range is reserved for the RAS 1500 and also is not available for NAT.

*Both Dynamic and Static NAT can be used simultaneously, **however** individual users connecting to the public network must be configured for **either** dynamic or static NAT. In addition, the IP addresses of users configured for either NAT type, must be **consecutive** addresses at the **beginning** or **end** of the series of addresses in the subnet on the private network.*

GSM Release 2.5 includes support for callback to Global Systems for Mobile Communications (GSM) devices, at the prevailing GSM data rate.

Operational Information

The following operational information is associated with this release:

Closing A Telnet Issue Resolved

Closing a Telnet session by clicking the box in the top right corner of the window will now properly close the session.

Lingering User Sessions Have Been Eliminated

Faulty handling of certain dial in client disconnects has been corrected. The symptoms for this problem include:

- User sessions which no longer exist, remain in the session list.
- Disconnected users appear active.
- Apparently random rebooting of the RAS1500. Rebooting of the unit was caused by the loss of memory, due to the accumulation of inactive user sessions.

Timing Out Prematurely During Dial-Out Resolved

Certain situations in which dialing out from the RAS1500 would time-out prematurely while waiting for the other side to answer, have been corrected.

Adding a User

When you add a user from the LAN-to-LAN page, to use Frame Relay over the WAN port, the Permanent Virtual Circuit (PVC) that is created will have the name that is entered in the "Incoming User Name" field. In the Shared ISP page, it will be the "ISP Name".

Deleting a Datalink

If you want to delete a datalink on the WAN interface, you should do it through the CLI using the following commands:

```
RAS1500>DISABLE DATALINK <FRAME_RELAY | PPP> INTERFACE
rm0/wan:1

RAS1500>DELETE DATALINK <FRAME_RELAY | PPP> INTERFACE
rm0/wan:1
```

Deleting a Frame Relay PVC

If you want to delete a Frame Relay PVC, you should do it through the CLI using the following command:

```
RAS1500>DISABLE USER <USERNAME ASSOCIATED WITH THE PVC>
RAS1500>DISABLE FRAME_RELAY PVC <PVC NAME>
RAS1500>DELETE FRAME_RELAY PVC <PVC NAME>
```

Modifying DLCI

The Digital (Data) Link Connection Identifier (DLCI) of a Frame Relay user, cannot be modified directly from the LAN-to-LAN and Shared ISP pages of the RAS 1500 Web Configurator. To modify the DLCI, you must use the CLI.

Perform the following steps to change the DLCI:

a) Go to the CLI and delete the existing PVC and the user using the following CLI commands:

```
RAS1500>DISABLE USER <USERNAME>
RAS1500>DISABLE FRAME_RELAY PVC <PVC NAME>
RAS1500>DELETE USER <USERNAME>
RAS1500>DELETE FRAME_RELAY PVC <PVC NAME>
```

b) Through the Web Configurator, add an entry in the LAN-to-LAN or the Shared ISP page depending on your requirements, with the new DLCI. This will add a PVC with the new DLCI.

Changing Datalink

RAS1500 allows you to have one datalink on the WAN interface, either PPP or Frame Relay. You cannot modify a Frame Relay user to PPP Leased Line or vice versa, in the modify mode in the LAN-to-LAN and Shared ISP pages of the RAS 1500 Web Configurator. (The same holds true if you want to change the datalink on the WAN interface from Frame Relay to Leased Line or vice versa). To change the Datalink, you must use CLI.

Perform the following steps to change a Datalink:

a) Go to the CLI and delete the user.

If you are changing from Frame Relay to PPP Leased Line, use the following CLI commands:

```
RAS1500>DISABLE USER <USERNAME>
RAS1500>DISABLE FRAME_RELAY PVC <PVC NAME>
RAS1500>DISABLE DATALINK FRAME_RELAY INTERFACE rm0/wan:1
RAS1500>DELETE USER <USERNAME>
RAS1500>DELETE FRAME_RELAY PVC <PVC NAME>
RAS1500>DELETE DATALINK FRAME_RELAY INTERFACE rm0/wan:1
```

If you are changing from PPP Leased Line to Frame Relay, use the following CLI commands:

```
RAS1500>DISABLE USER <USERNAME>
```

```
RAS1500>DISABLE DATALINK PPP INTERFACE rm0/wan:1
RAS1500>DELETE USER <USERNAME>
RAS1500>DELETE DATALINK PPP INTERFACE rm0/wan:1
```

b) You may add a new entry in the LAN-to-LAN or the Shared ISP, through the Web Configurator, based on your needs.

Frame Relay Local Management Interface

The Local Management Interface (LMI) is a set of enhancements to the basic Frame Relay specification. It is supported by the RAS 1500 and set ON to ANSI T1.617 Annex –D by default.

However, make sure that your Frame-Relay service provider supports this feature.

Some Frame-Relay providers require you to turn this feature OFF.

To disable LMI on your WAN port, use the following command at the CLI prompt

```
: SET FRAME_RELAY ON INTERFACE RM0/WAN:1 MANAGEMENT_TYPE
NO_LMI
```

About LMI: LMI virtual circuit status messages provide communication and synchronization between Frame Relay DTE and DCE devices. These messages are used to periodically report on the status of PVCs, preventing data from being sent into *black holes* (that is, over PVCs that no longer exist).

The LMI global addressing extension gives Frame Relay DLCI values global rather than local significance. DLCI values become DTE addresses that are unique in the Frame Relay WAN.