Configuring the Nortel Networks Remote Access Concentrators and the DMS-10 for Remote Access.

Author: John Picavage (email: johnp@nortelnetworks.com)

1.0 Introduction

The Nortel Networks RAC8000 and RAC5399 are Remote Access Concentrators which provide remote access to the Internet. The RACs provides modem as well as ISDN access between the circuit switched network and an Internet service Provider Point of Presence (POP). The RACs interfaces to the DMS-10 through a T1 (DS-1) 1.544Mbps facility, using either T1 (A/B robbed bit signalling) or ISDN PRI format. The RAC provides 2 T1 ports with 48 digital modems capable of V.34/V.90, X2, K56, or ISDN using V120, PPP of MLPP.

The Bay Networks RAC8000 and RAC5399 are similar devices and run essentially the same software. The RAC8000 is 19 inch small rack mount unit which supports two T1 ports and has a single LAN output. The RAC 5399 is a plug in unit, “blade”, which resides in a System 5000 Multi Service shelf. While the two units are physically different they are functionally identical.

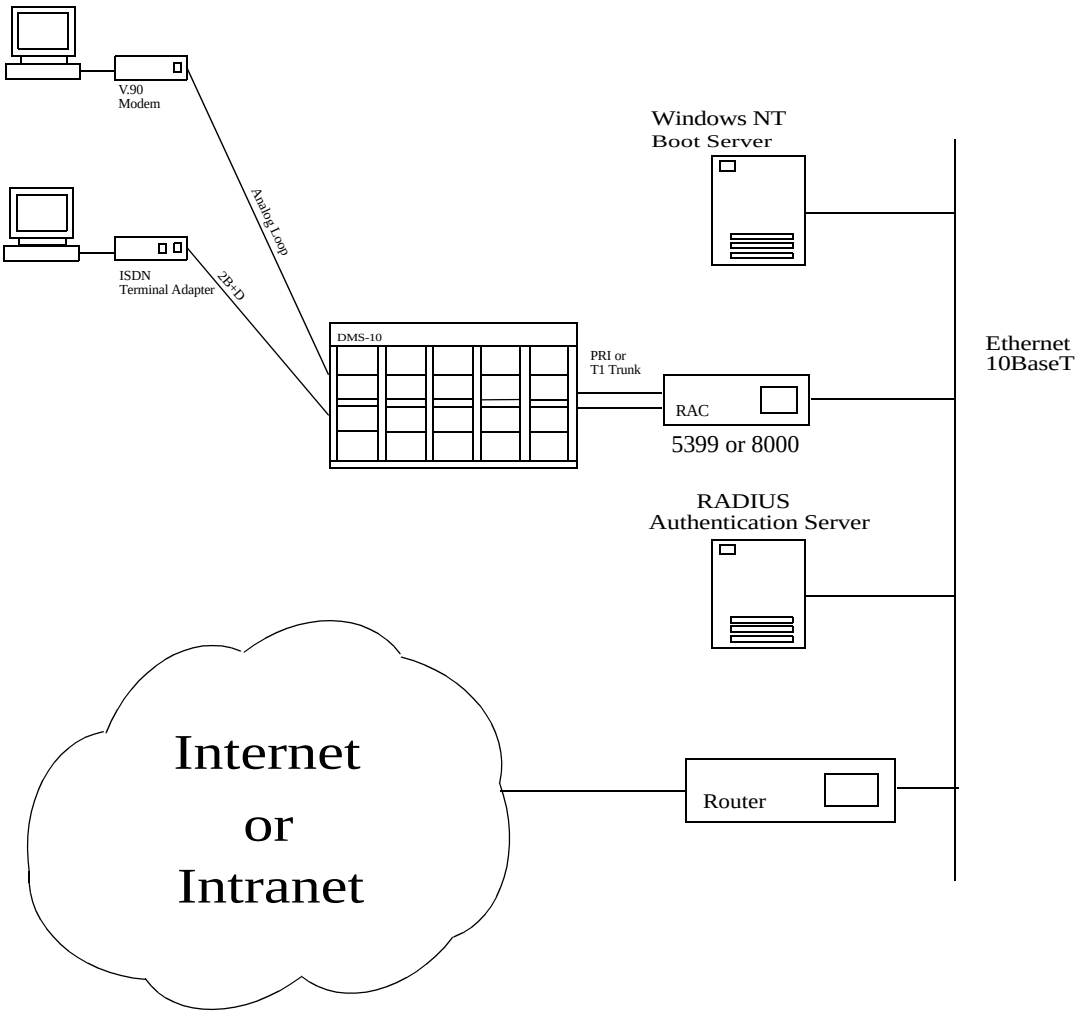
With the phenomenal growth of the Internet application such as work at home, telecom-muting, SOHO, etc, the RAC fills a need for remote network access through the DMS-10. The RAC product fit nicely modem based servers and the high capacity CVX1800.

This document is meant to augment the information provided in the DMS-10 NTP’s and the RAC documentation. The product respective documentation should be obtained and understood before configuring the RAC8000 or RAC5399. A Windows NT is assumed to be available for supporting the RAC. Installing a Windows NT Server requires a understanding beyond the scope of this document. A sufficient understanding of the process of installing Windows NT is assumed. This document is meant to highlight pitfalls that were discovered is lab setups to demonstrate this White Paper. In the DMS-10 lab a RAC was configured to accept calls from both a DSI PRI and a DCM Trunk interface. A NT workstation was configured running the RAC boot software, Event Logging, and RADIUS security. Analog modem V.90 and V.34 as well as ISDN BRI calls were demonstrated on both interfaces.

2.0 Applications

Probably the most common application for a Remote Access Server is dial in access for a Internet Service Provider. In this case the RAS provides an intelligent termination between the circuit switched public network and the packet switched internet. Figure 1 shows a typical configuration of a RAC interfacing with a DMS-10. The RAC has two WAN ports which can be either ISDN PRI or T1 A/B signaling type. The output of the RAC is 10Base-T Ethernet which is connected to the IP network via a router.

FIGURE 1. Typical Co Internet application



The RAC provides only a limited security for the incoming calls. It is recommended that a RADIUS (Remote Access Dial In User Service) Security be set up to control access to the customers network. Another option is to use Bay's Access Control Protocol security using Windows NT or a UNIX server. In either case these devices provide excellent security allowing a central data base for controlling access as well as logging access. RADIUS is recommended since it is considered an industry standard for dial in security.

In order to download the operating software into the RAC, a Windows NT PC will provide the required file service. The RAC will boot off it's own image if necessary, but it is recommended that a external server be provided so that the software can be upgraded when required. The RAC can also use a UNIX device running TFTP for a boot device. The UNIX solution will not be covered in this document.

3.0 Administration

Initial configuration of the RAC must be done using a serial terminal connected to the serial port on the back of the RAC. The unit comes without a IP address or Subnet mask. In order for it to communicate on the network and boot, a IP address will need to be assigned along with appropriate Subnet mask. If the device is to be booted off a external device the boot devices address will need to be entered using this ROM monitor. If there is no boot device available and the RAC is to be booted from its self, then “self” must be set.

Once the basic info has been established and the RAC is booted, the other parameters must be loaded into the unit. The other parameters involve setting up the WAN (T1 parameters), IP address for the ports, Security, Name Servers, etc. Administration can be accomplished using the Command Line Interface (CLI) off the serial port or a telnet session to the RAC, once the IP address has been set up. The unit can also be programmed using a Browser based JAVA program. This requires special browser software to be installed on a NT or UNIX server. The device can also be set up using the NA utility which can be installed in Windows NT. NA allows a line by line, like CLI, session to be set up or a config file which can be edited and then downloaded to the EEPROM on the RAC. Using NA allow you to configure several RAC using a single config file edited slightly for each device if necessary. Only CLI will be covered in this white paper since it is the native setup language.

Once the RAC has been configured it will need to be rebooted to set the changes into its operating system. If changes from the default settings on the WANs are made the unit will need to be booted from a server to install the proper driver software.

4.0 Security

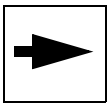
Dial Access should never be deployed with out a high level of security. The RADIUS security server is the recommended security. The RADIUS server is a workstation which is connected to the network being accessed, it does not have to be co-located with the RAS. The RADIUS server then acts as a central point to administering dial up access. Its basic job is to provide authorization for username and password and set access attributes. The RADIUS server also can administer levels of access which includes type of access, IP address assignment for the port, number of B-channels allowed for MLPP, as well as other attributes. Anyone providing dial access should seriously consider providing a RADIUS server.

5.0 Configuration

5.1 Introduction Windows NT setup

Windows NT provides a reasonably easy to use graphics interface to setup and support the RAC. Windows NT also provides a solution to download the RAC with its software. While the RAC is capable of downloading a software image from itself. Providing a external server allows the device to be upgraded easily. In addition if any of the WAN ports are

changed from T1 inband signaling to ISDN PRI signaling the WAN ports will need to be loaded from a server, such as a windows NT, to change their personality. The NT Server also serves to provide a repository for log messages coming from the RAC using its built in event logging. The Windows NT server keeps configuration files, using NA, with all the configuration information for the RAC. This allows the NT Server to download all the settings for the RAC. This will allow a unit to be replaced with another RAC if maintenance is required in addition it allows other units to be “cloned” with the same or modified information

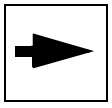


Note: The Windows NT Server must have a NTFS formatted disk for the Bay Remote Access tools to install.

Before setting up a PC for use with the Bay Networks software it must first be configured to use the NTFS disk file format. The Bay software requires that NTFS be installed. The file format FAT16 is not compatible. It should also be upgraded to service pack 3. The current version (Release 6) of “Remote Access Tools for Windows NT” will not load with Service Pack 4, be sure and check with Bay Networks on compatibility prior to installing Service Pack 4.

The NT server will also need to be a Domain Controller in order for “Remote Access Tools for Windows NT” to load and work properly.

.



Note: The Windows NT server must be the Domain Controller to run **the Bay NT software.**

The Windows NT device can also be used as the RADIUS server using BaySecure software. This product provides a solid easy to setup software package. The Baysecure Radius software allows administering user names and passwords, as well as establishing and maintaining attributes.

5.2 RADIUS Server

The BaySecure RADIUS software is very easy to setup. The software loads and automatically starts the services. Once loaded it is simply a matter of choosing the Remote Annex product from Bay RAC8000 or 5399 as the Remote Access Server as the client type.

5.2.1 Radius Configuration

When setting up users there are several options. If you are not going to have the RADIUS control and allocate the IP addresses you will need to set up the address pool for the RAC.

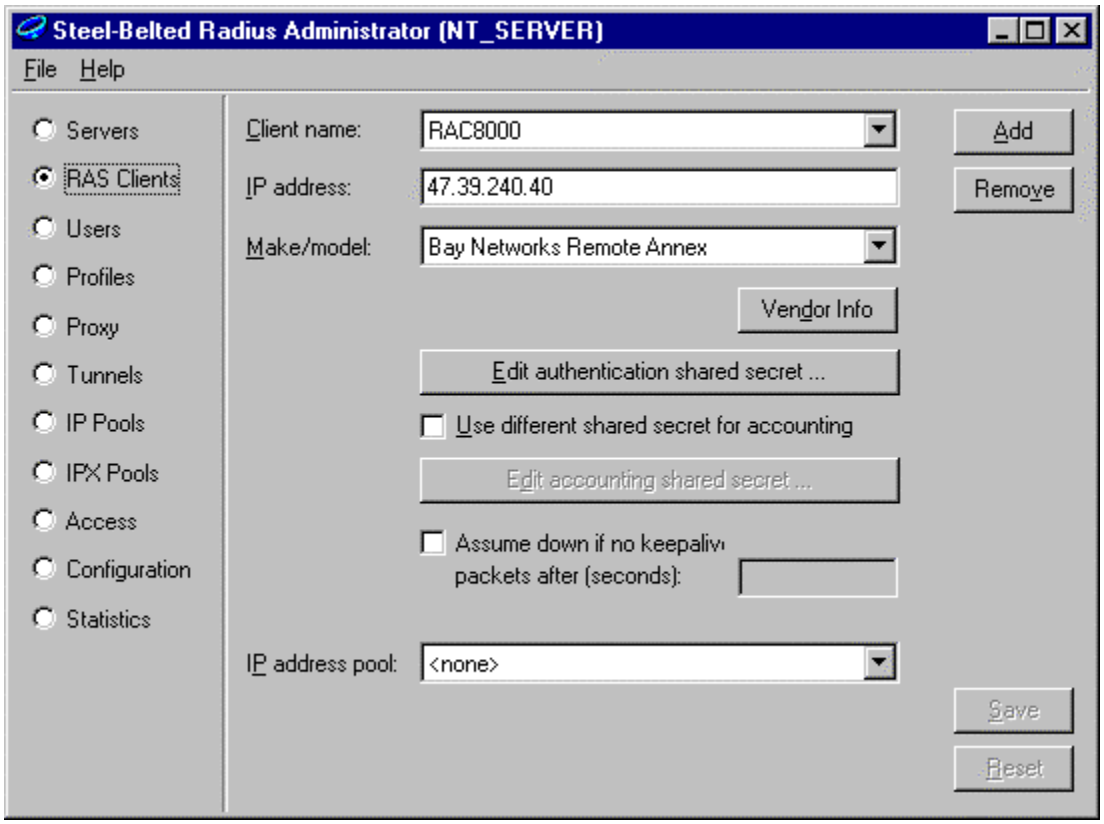
Once you decide if you are going to assign IP addresses using RADIUS or not, then you can start to add users. If the users are going to be allowed to use MLPP and bundle a second B-Channel you will need to set the Port Limit in the outgoing message to “2”. If you are going to have the RADIUS server control access to the RAC, such as for logging into CLI over telnet, a user with no attributes should be set up for this account.

The following examples are not meant to replace the BaySecure setup documentation. Their purpose is to provide a guide to easily get started setting up a RAC, for any difficulties the manual should be consulted. Note: the figures are for a Funk software “Steel Belted RADIUS” which is repackaged as a BaySecure.

5.2.1.1 Choosing the RAC

Once the RADIUS software has been installed the type of RAS Client needs to be selected. In this case it will be a RAC8000, see figure 2. The RAS client is added by choosing ADD New RAS Client and assigning its name, IP address, and model number. The IP address pool can be assigned here or it can be assigned in the actual user profile attribute.

FIGURE 2. RAS Client Setup

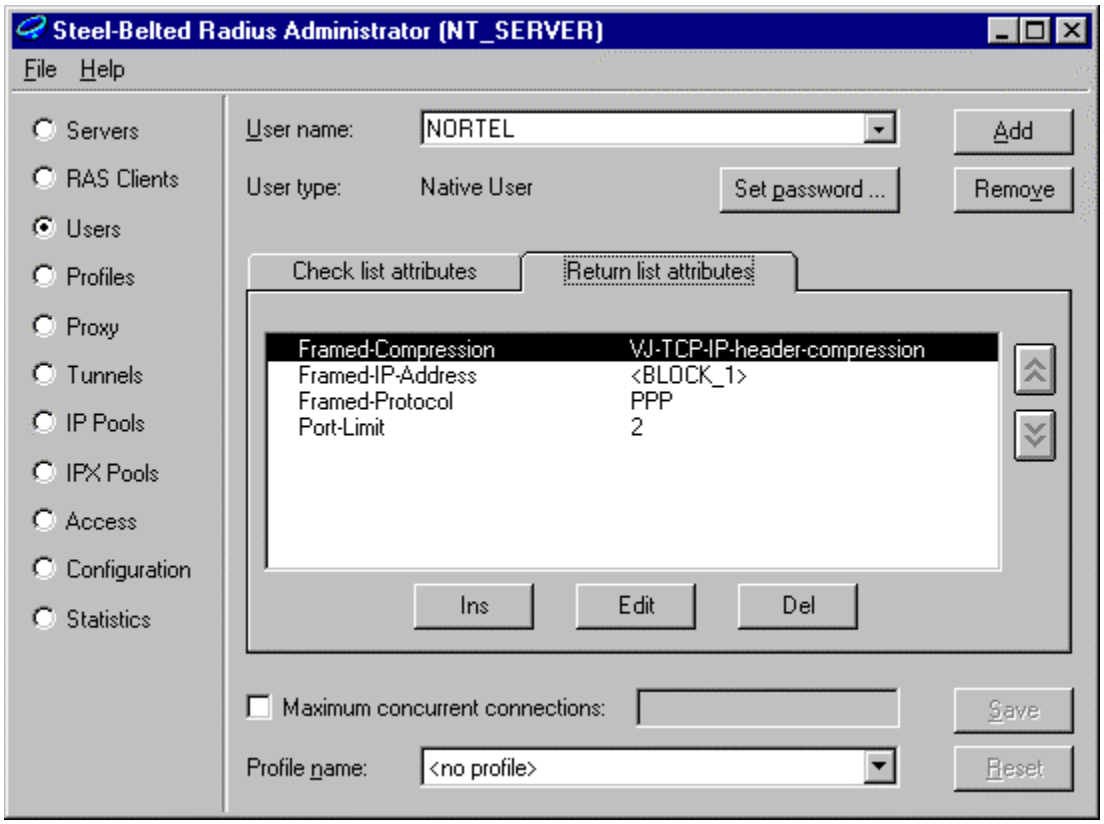


5.3 Assigning a User

A user profile is assigned by going into the Users Menu and adding a new user. In Figure 3, I have shown a typical user. Setting the Return List Attributes you define the attributes that are set back to the RAS following a authentication from the RAS. The Return list tells the RAC that:

- Van Jacobson IP header compression is allowed
- IP address is to be assigned from BLOCK_1 - Block 1 contains a list of sequential IP address that are allocated for use.
- The supported framed protocol is PPP.
- Port Limit - Setting the Port Limit to 2 allows MLPP to be performed on this connection with a bundle of 2 channels.

FIGURE 3. A Typical Dial In User

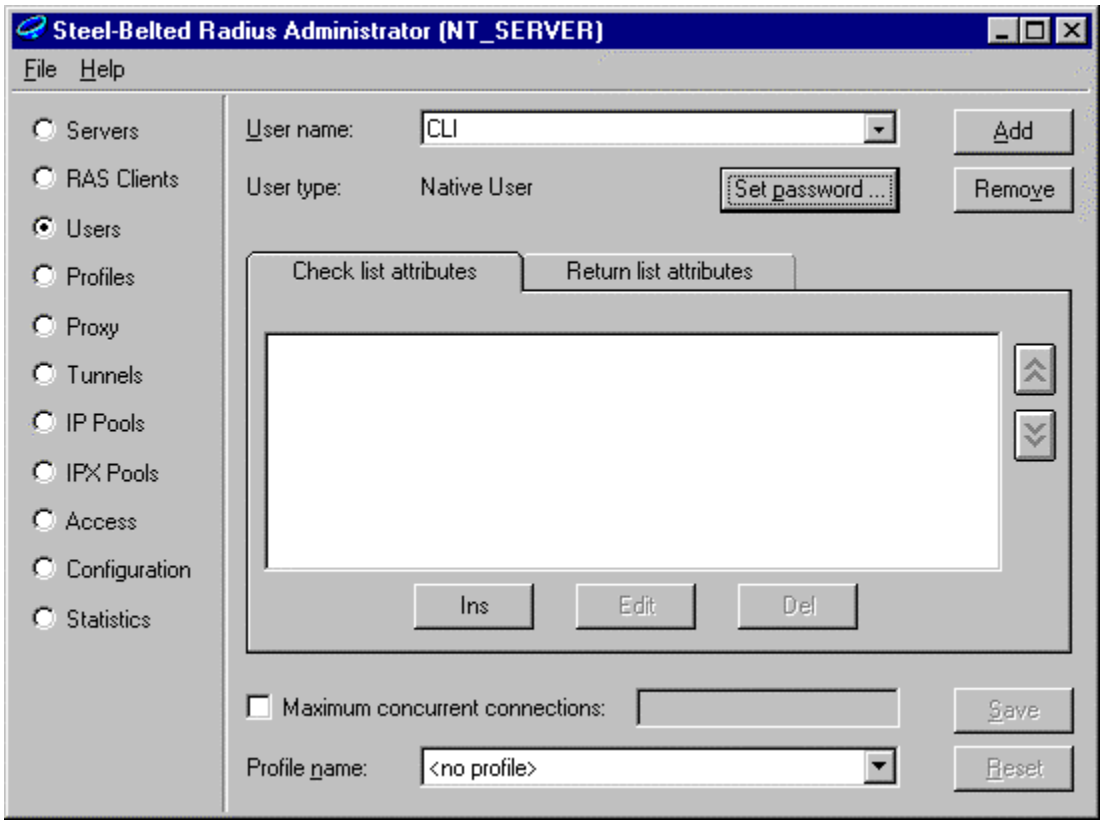


Since the RADIUS server will most likely be used to provide security for accessing the Command Line Interface, an example is included for a typical user for CLI. In the case of Figure 4 the user is CLI and no attributes should be included in the profile.

When a user accesses the RAC from either telnet or the console monitor the RAC will request a authentication from the RADIUS server to insure the user is authorized. The profile in Figure 4 will be tested and the results returned to the RAC. If the username and

password match the assignment the user will be able to gain access. No attributes need to be set.

FIGURE 4. Command Line Interface User



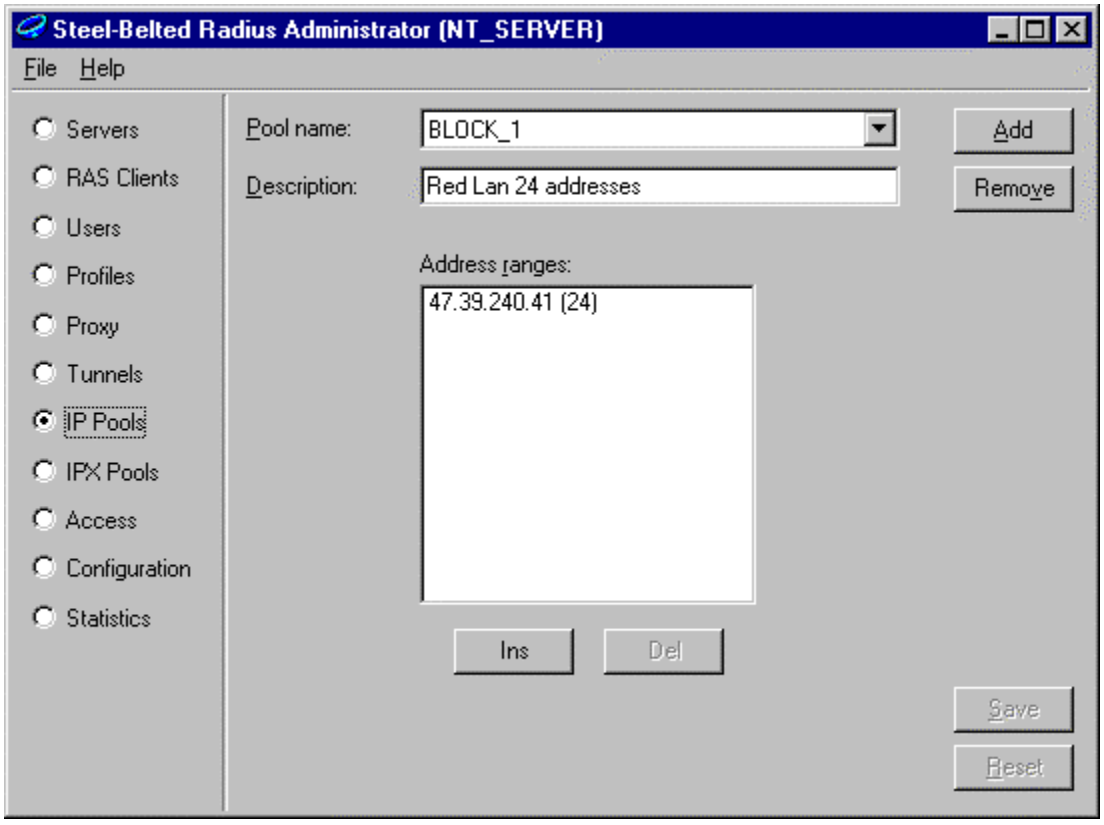
5.3.1 IP Pools

Setting up IP pools is not required if the RAS has IP addresses assigned per “B channel”. (This is an option on the RAC WAN setup). In order to conserve IP addresses or to assign specific blocks of IP addresses to user this function can be administered by the RADIUS server.

The setup is easy to do using the IP pools option in the RADIUS Administrator. First a block name will need to be assigned as in Figure 4. This is performed using the ADD button. Once named a optional description can be added. The address range is defined as a origin address with a count of the number in the sequence. Several address origins and counts can be added to the pool.

IP pools can also be assigned in the RAS Client setup, figure 2. Assigning them in the RAS Client menu will use that pool for the whole RAS, not specific users as shown in figure 3.

FIGURE 5. IP pools



5.4 DMS-10 Setup Introduction

The preferred method of interfacing to a RAC is using ISDN PRI for the WAN interface. PRI allows a 64KB channel to interface to the RAC. Additionally, using PRI allows provides much quicker call setup since PRI uses the D channel signalling. If PRI cannot be deployed, normal T1 trunking can be used for the interface. The only significant limitation will be that the connection bandwidth will be limited to 56Kbs. ISDN calls will still terminate to the RAC and MLPP is also supported with both interfaces. MLPP is only supported on ISDN originating calls. If you will be using standard T1 trunking and have customers using BRI ISDN, make sure your customer base is aware of the 56Kbs limitation. Using 56Kbs limits the number of ISDN terminal adapters available. Not all vendors support ISDN at 56Kbs.

Setting up either PRI or T1 trunking are quite similar. In each case a Trunk Group will need to be defined, a Route will need to be setup and the number for your RAC will need to be intercepted or translated.

5.4.1 T1 Trunk TG setup

The trunk setup for normal inband trunks is straight forward. The RAC does not require any directory number to be sent to the unit. It is recommended that no numbers be delivered to the RAC.

Set up a Trunk group (overlay TG) similar to one below:

```
TYP  TG
   NUM  72
   TGTP OUT
   SIGT INB
   64NC NO
   PKTP DTRK
   SITE BASE
   TGDP DATA   < DATA sets the Trunk Loss to 0DB 412.10 and above.
   RMB  YES
   STPL WINK
   TRNS MF
   SDTM 5 SEC
   GDTI 768 MSEC
   IDLE MOST
   DTSI 0
   SYNC NO
   ANI  YES
   ASTR OFHK
   ATMO CONN
   2RID NO
   EOAT NO
   ATIC NO
   HIT  5 SEC
   4XCD NO
   TRK  CAPB PE  03 5 05 01
        CAPB PE  03 5 05 02
        CAPB PE  03 5 05 03
        CAPB PE  03 5 05 04
                 .....
                 .....
        CAPB PE  03 5 05 24
```

In overlay trunk (TRK) set the TGDP option to DATA. Note that this is a new trunk padding, DATA, it available in 412.10 and is patchable in generics 411.20, 411.10, and 410.10. The DATA padding sets the pads in both directions to 0DB for all calls. This is required if you want to terminate ISDN calls to the RAS using inband signalling and it will help with 56Kbs V.90 calls. While V.90 calls will tolerate some loss padding, they do not tolerate multiple pads well. If DATA is not available use DIOD.

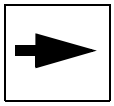
Setting up the Route is also straight forward. Below is an example of a Route set for a RAC:

```
   ROUT 72
```

```
ALTR OVFL
TYPE EAS
UPGR NONE
CTYP NONE
TG   72
CHG  YES
OPR  NO
SDCN NOCO
COS  NONE
DEL  7    <= No digits need to be sent to the RAC
APFX NONE
CNTL ETHR
OVLP NO
PGNC NO
```

There is no need to send digits to the RAC. It is capable of auto-detecting the protocol being terminated on it, for example ISDN 56Kbs bsor Modem, and PPP, MLPP. Some other RAS devices need a special DN or a prefix (APFX) to indicate the protocol expected for the termination. In some instances you may want to override his capability for special CLI manual regarding “Session Parameter Blocks” or SPBs.

If you expect to send digits to the RAC you will need to set the “dnis” parameter in the RAC WAN configuration. The “dnis” parameter sets the RAC to expect digits to be sent to the trunk on a seizure. If “dnis” set to zero and numbers are sent, you will likely get a “TRK018” from the DMS-10. This is because the RAC will not wait for the digits and will answer before the DMS-10 is done sending the digits.



Note: If digits are being sent to the RAC on a A/B bit Trunk, the WAN “dnis” parameter on the RAC must be set with the number of digits. Otherwise the RAC will answer before the number is sent resulting in a DMS-10 “TRK018”.

Once the Trunk Group and Route are set. The the chosen DN will need to be set to terminate on the trunk group. This can be done by either translating or by intercepting the DN and sending it to a screen with the route to the trunk group.

5.4.2 ISDN PRI LTG Setup

PRI setup is nearly identical to setting up a DCM trunk. PRI requires you to set up a Line Trunk Group (LTG) which is automatically done in overlay PRI when the PRI is assigned. Below is an example of a typical LTG for a RAC.

```
TYP  LTG
NUM  2
APPL PRI
TGTP OUT
```

```
SITE BASE
RMB  NO
TRK  CAPB CE  01 1 04 1 01
     CAPB CE  01 1 04 1 02
     CAPB CE  01 1 04 1 03
     CAPB CE  01 1 04 1 04
          ...
          ...
     CAPB CE  01 1 04 1 23
```

With the LTG assigned a Route will need to be added to the LTG. This is done as in the DCM example in Overlay ROUT. Below is an example of a ROUT in this case rout 601.

```
ROUT 601
ALTR BUSY
TYPE PRI
CTYP NONE
CHG  YES
LTG  2
DEL  0
APFX NONE
PGNC YES
```

5.5 Introduction RAC 8000 Setup

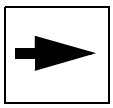
Once the RAC has been mounted in its frame and it has been powered up according to the documentation provided with the unit. A terminal device, such as a PC running Hyperterminal or equivalent must be used to setup the device. It is adviseable to start a log session when making changes so a record can be made.

This description is intended to provide a focused approach to setting up the RAC to work with a DMS-10. It is not to replace the appropriate documentation supplied by Bay Networks. The Author has made an attempt to layout the important commands in a manner that they can be more easily understood based on his experience. It makes no attempt to set up all the extensive features available on the RAC, just to provide the basic features for internet access off a DMS-10.

5.5.1 Command Line Interface

The Command Line Interface, CLI, should be understood prior to any setting up of parameters since its navigation is required. Figure 6 shows a overview of the Command Line interface on the RAC. There are two entry points to the monitor. The initial entry point is through the console serial port of the RAC. The second entry point in through telnet over the ethernet port. Initially the RAC must be setup using the serial console port to set up the IP address, subnet mask and boot addresses if applicable.

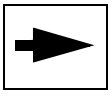
Figure 6 illustrates the entry points to the various levels of the CLI monitor. Each level provides different functions.



Note: The command line help is available at each level of CLI by typing “help” or “?”.

The ROM monitor provides the basic IP setup to configure the ethernet interface. In order to get into the “boot” monitor it is necessary to put the RAC into a setup mode using a front panel pushbutton. Refer to Bay documentation for this. The boot monitor allows basic testing of the device prior to booting. In the ROM monitor the IP address must be set along with the subnet mask and boot IP address if the RAC is to be booted off a network device. If the RAC is to be “stand alone” the boot sequence will need to be modified so it boots off of itself and does not try to boot off of the network. In order to leave ROM monitor a boot must be executed from the command line. This causes the RAC to load it operation code.

Once the Boot has been performed using the serial port the Console Monitor becomes available. The entry point is the “`Console:`” monitor prompt. Type CLI to enter the CLI monitor. CLI as shown in Figure 1 has several levels. If security has been enabled, which is discussed later, a user and password will be needed. The first level indicated by the “annex:” prompt provides only basic function. In order to move to where changes can be made the operator must login as Super User (SU). The initial password is the IP address assigned to the RAC in the ROM monitor. Once logged in the password should be updated to a more secure choice. The Super User CLI indicated by the “annex#” prompt provides a much larger choice of function. Figure 6 only shows a subset of the most useful commands.

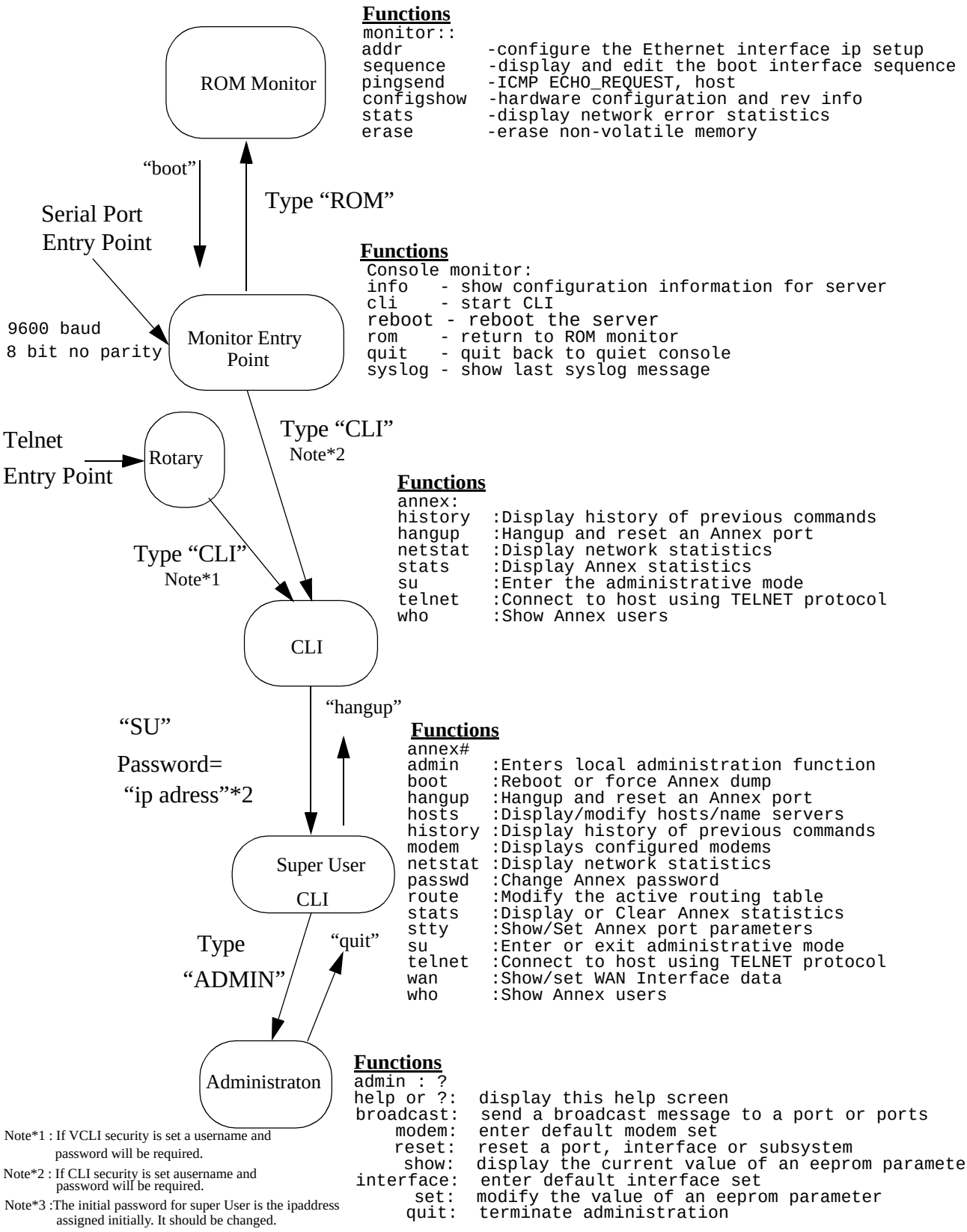


Note: The default prompt is “annex”. It can be set to other strings in the prompt definitions.

The actual setup of the WANs and other important functions are handled in the Admin portion of CLI. This level is selected by typing “admin”, once logged in as super user. This will invoke the “admin:’ prompt to be displayed. At this level the commands deal with setting, showing and resetting devices. Things which can be set, reset or shown are, port, annex, wan, interface or modem. It is a good idea to show an interface prior to making any changes since it will provide a guideline for the settings and their spelling. Ports are logical devices which manage data. The port types are:

- ta- this port manages V.120, V.110, and X.25 calls
- syn- this port manages PPP and MLPP calls
- asy- this port manages asynchronous voice calls associated with digital modems.

FIGURE 6. Overview of the Monitor structure



A typical command would be “show port all”. This command will show all the port settings.

Annex commands deal with generic system items such as:

- IP addresses
- CLI and VCLI parameters
- Name Servers
- Security
- Event Logging
- Routing
- SNMP Maintenance

Wan of course deals with the two T1 based WAN’s. In the WAN section the T1 characteristics are set up along with B channel parameters.

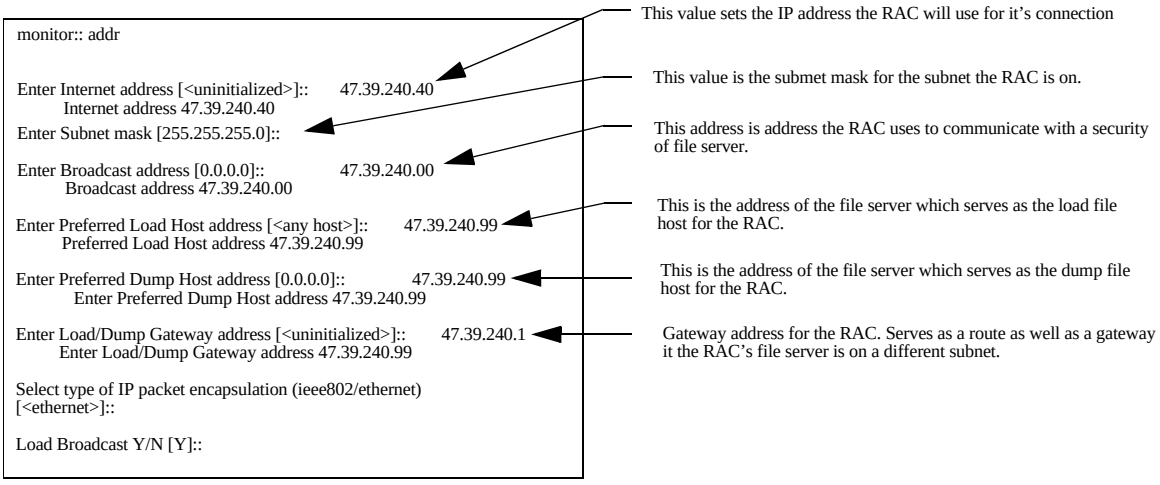
Following any changes it is necessary to reset the device or in some cases boot the RAC to make the parameter change take effect.

5.5.2 Setting the Initial Parameters.

The initial parameters are set using the Console monitor in the ROM monitor portion or the RAC. This information is covered in the publication “Installing the Model 8000 Remote Access Concentrator”. This document covers setting the RAC into its initial setup mode, it also covers the requirements for the IP addresses and supplementary information.

Figure 7 gives a view of the parameters and their significance.

FIGURE 7. Initial Address Setup



Setting up the initial addresses in the ROM monitor

If the RAC is being re-deployed and was previously used somewhere else, it is a good practice to erase the EEPROM and start over. By erasing the EEPROM you insure that everything is cleared and the default settings are in place.

Once the IP addresses information has been entered, the config information should be viewed. It is important to look at the WAN downloads that are resident in the unit. A typical view is shown in figure 8

FIGURE 8. ROM Monitor monitor: prompt type "config"

```
                REVISION/CONFIGURATION INFORMATIONROM

Software Rev: 1124                          Board ID: 64 Board Type: 8000
CPU Type: 486DX2                            Ethernet Address: 00-80-2d-xx-xx-xx
Memory size: 8 Meg                          EEPROM size: 65504
Flash size: 4 Meg Flash ID:0089
Available Interfaces (* = selected): ThickNet *Twisted Pair

WAN 1:  PRI T1 USA CSU                      Revision: VERSION A MGR=1.234b
WAN 2:  CAS T1 CSU                          Revision: VERSION CAS-E1T1 1.40
 General Purpose Sync Port Interface: No Cable
 Compression Card Rev: 0
SLC 1
      SLC SRAM Size: 128 K          Modem Count: 31          Modem Rev: 0
SLC 2
       SLC SRAM Size: 128 K         Modem Count: 31          Modem Rev: 0
```

The current personality load in the WANs needs to be noted if you do not plan on providing a external load server for the RAC. If there is not a planned external load server (Windows NT or UNIX) there is no way to change the WAN personalities. This is because new code will need to be loaded into the WAN modules to reconfigure them.

Once it is determined if a external load server is required the boot sequence will need to be set in the ROM Monitor. The choices are "net" or "self". Self should be the first choice if you expect to use the RAC in a stand alone mode.

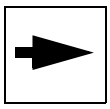
Once the IP addresses are setup and the boot sequence has been set for your application it is a good idea to test the network connection by pinging a known address on your IP network both on and off the subnet. If the ping succeeds it's time to move on to booting the RAC. If the ping fails the IP address settings need to be verified also the LAN connection should be inspected. If the device you are pinging is on another subnet try a device that is local.

Once the LAN is functional, boot the RAC. This will take several minutes. Log messages will be displayed on the console monitor indicating the state of processes as they come up.Theses messages are important, they provide a log of the processes starting up.

5.5.3 Setting up the WAN

There are two WANs associated with the RAC they can be configured as either ISDN PRI or T1 A/B bit signaling trunk interface. The settings are made from the Admin prompt of CLI.

Figure 9 shows a overview of the settings associated with a PRI configured WAN. The correct syntax to addressing the WANs is to use “show wan=1 all”. The “wan=X”selects which WAN is being addressed, where x= 1, 2 or all. Figure 9 shows a graphic of the settings for a PRI configured WAN. Figure 10 shows a similar graphic of a WAN configuration using a standard TI trunk interface.



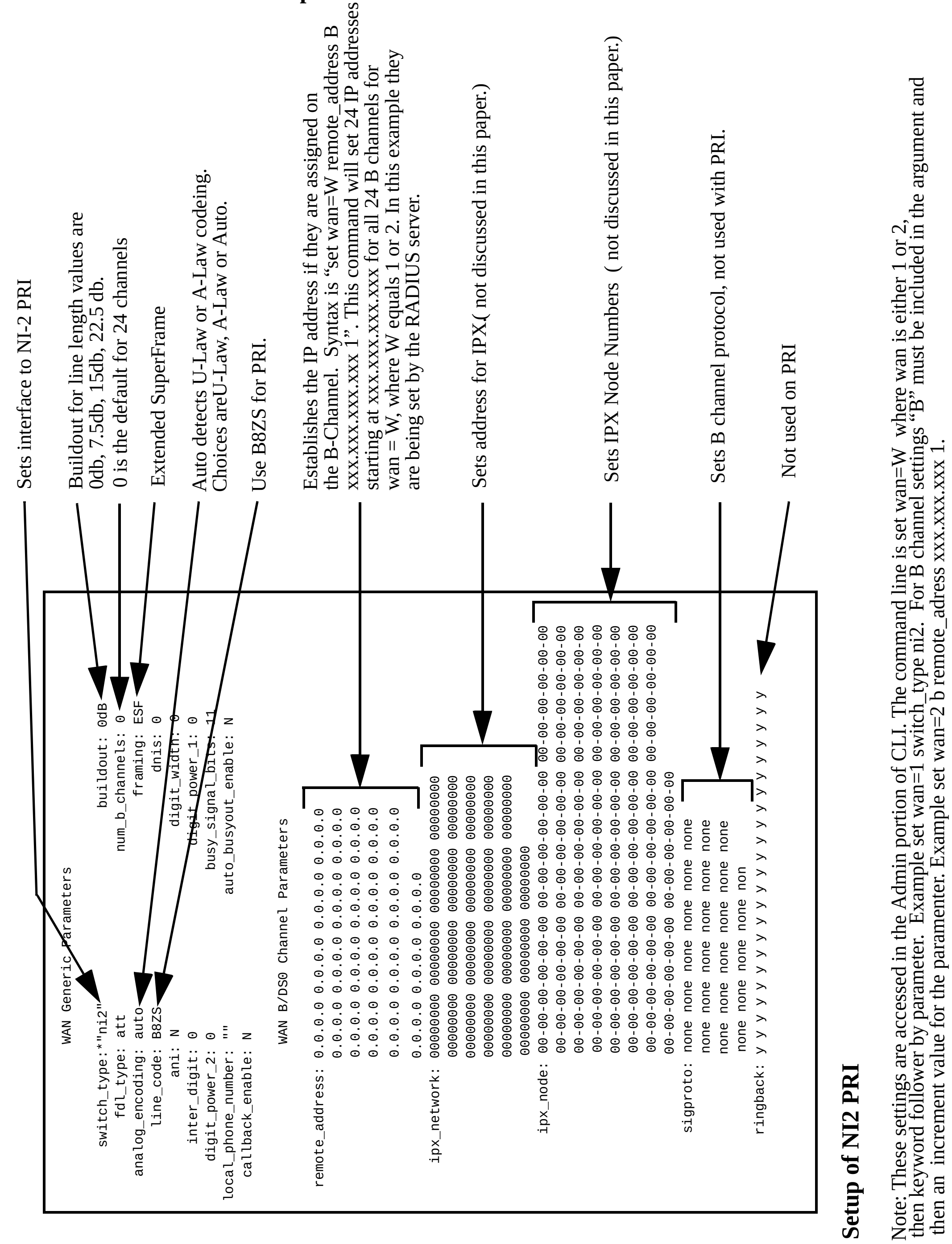
Note: When a value has been changed from the default a “*” will appear ned to the parameter.

The figures should be self explanatory in their setup. The following parameters will need to be setup:

- switch_type - sets ust1 for a trunk interface or ni2 for PRI.
- line_code - set to AMI for ust1 or B8ZS for ni2.
- build_out - sets the build_out for the distance between the DMS-10 and the RAC.
- framing- set to D4 for ust1 or ESF for ni2.
- remote_address - this parameter sets a unique IP address for each B channel. It is not required if the RADIUS server or DHCP will be setting the IP addresses.
- sigproto - this parameter is only valid for ust1. It sets the supervision for answering the call.

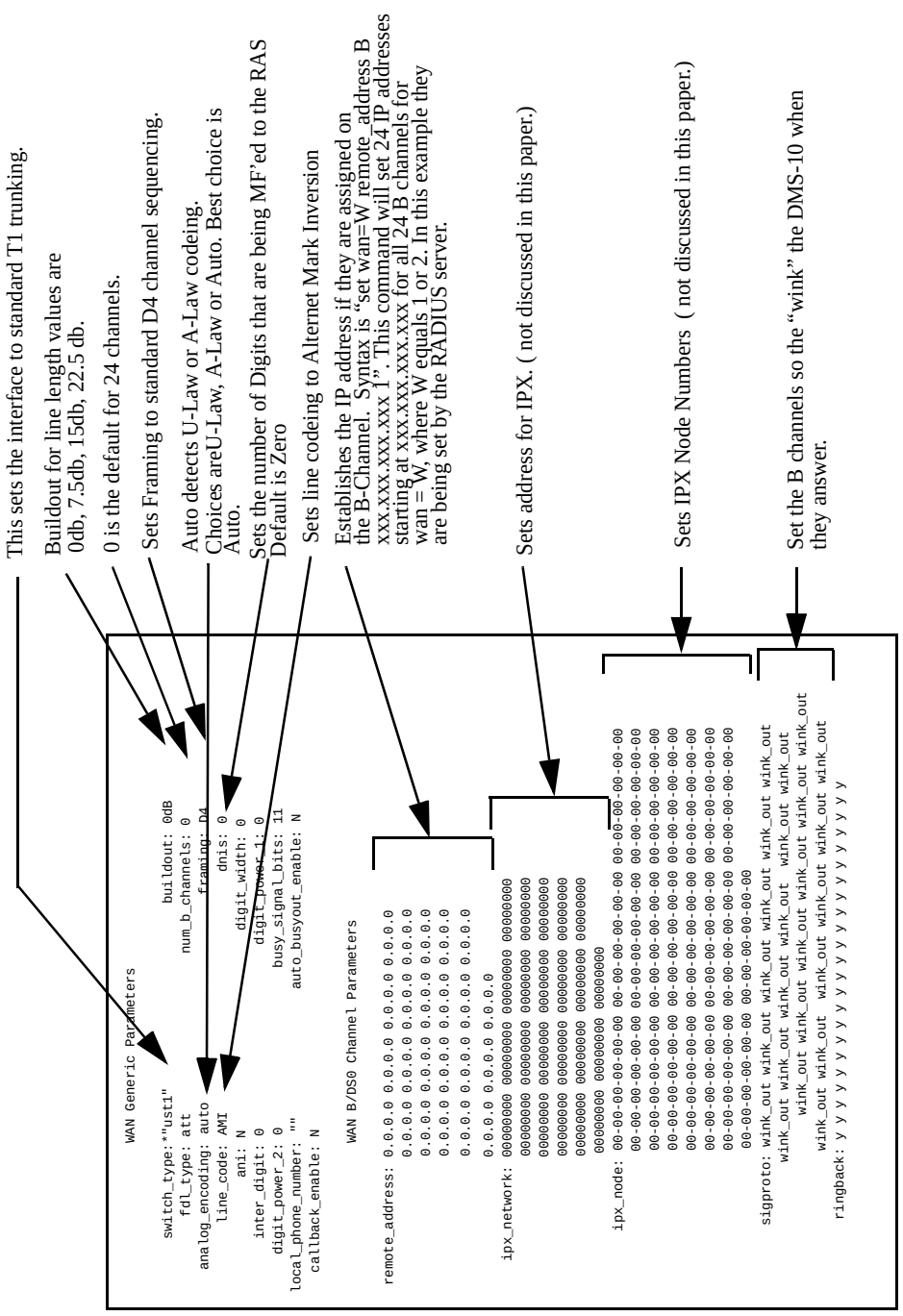
The commands to set these parameters will be similar to the command to the “`show`” command. With the exception of “`remote_address`” and “`sigproto`”. These commands control B channel conditions so the command is structured as “`set wan=1 b remote_address 207.45.240.40 1`” will set the first B channel of WAN 1 to IP address 207.45.240.40 the next B channel to 207.45.240.41 till the last channel (23 channels for PRI or 24 channels for ust1).

FIGURE 9. PRI WAN Example



Once the WANs are setup it is necessary to re-boot the RAC in order for the changes to take effect. If the WAN switch_type has been changed the RAC will need to load a new driver for the WAN port. This can take 5 to 10 minutes for the load to be completed. If the RAC is set for self boot and the switch_type has been changed it will not take affect since there is no download host.

FIGURE 10. Setup for a DCM or Trunk DSI



Initially when you bring up the RAC there is no security set. It is a good idea to first test the unit with all security off. This allows verification of the interfaces and allows you to become familiar with the operation of the RAC. The following test should be tried:

- Telnet - first telnet to the RAC and make sure you can log into it. This can be done using a PC, which is on the network, and at the “START” prompt type telnet

"xxx.xxx.xxx.xxx" where xxx.xxx.xxx.xxx is the IP address you assigned to the RAC. When you type a carriage return in the telnet window there should be a message:

```
 "Rotaries Defined:
    cli
Enter Annex port name or number:"
```

type "`cli`" and you should be in the monitor as in figure 6.

- Using the DMS-10 in DED verify that the trunks are in service. This can also be verified in the RAC monitor by typing "`wan`" at the super user "`annex#`" prompt. See Figure 11.
- The next thing to try is to dial into the RAC using a analog pots phone. You should get modem tones, when the call terminates on the RAC.

FIGURE 11. WAN status display

```
annex# wan
General WAN Statistics             Interface #1          Interface #2
-------------------------------------------------------------------------------
WAN Firmware Vers:                 A MGR=1.234b          CAS-E1T1 1.40
WAN Type:                          T1 CSU                CAS T1 CSU
WAN FDL Type:                      ATT                   ATT
Switch Type:                       NI2                   UST1
Analog Encoding:                   mu_law                mu_law
WAN Interface Errors:              0                     0
Accepted Incoming Calls:           0                     15
Rejected Incoming Calls:           0                     0
Accepted Outgoing Calls:           0                     0
Rejected Outgoing Calls:           0                     0
Normal Call Disconnects:           0                     15
Abnormal Call Disconnects:         0                     0
B Channels Currently Allocated:    0                     15
Number Times WAN Fully Allocated:  0                     0

WAN Interface #1 Information:
Frame errors    = 0
Code violations = 0
CRC errors      = 0
Errored blocks  = 0

WAN Interface #2 Information:
Frame errors    = 0
Code violations = 0
CRC errors      = 0
Errored blocks  = 0
annex#
```

This insures that the basic interface between the DMS-10 and the RAC is working and the RAC is on the IP network.

5.5.4 RAC Security

Security is one of the more complex aspects. The RAC has very limited security built into its operating system. Its internal security is limited to simple password protection on its ports. It is recommended to implement RADIUS security as described in this White Paper. Another option is to use the security from the Windows NT workstation. The Windows NT security works in conjunction with the Bay Access Control Protocol (ACP) daemons that are installed along with the Bay boot software. ACP is also available for UNIX as well. While ACP will work, RADIUS security provides industry standard approach which is a much better overall integrated security for dial in access. Only RADIUS security will be discussed in detail in this document. BaySecure RADIUS software for Windows NT will be assumed to be the RADIUS choice. BaySecure can utilize NT domains, names and passwords in addition to the normal RADIUS database.

The security on the RAC ports is built around using RADIUS security, with the RADIUS security taking precedence over the local security. The RADIUS server has a database of all the valid users and their passwords and attributes. These attributes supply information to the RAC regarding the connection. Included in the attribute can be the type of framed protocol i.e. PPP, a IP address for the connection, and port-limits for MLPP connections. The RADIUS server also serves the accounting function of tracking user access and usage. In addition the RAC uses RADIUS security to control logins and restrict access to the CLI ports as well as PPP ports.

5.5.5 ANNEX Security

In a typical network there are two RADIUS servers declared for redundancy. Each of these servers have two parts, an authentication server and an accounting server. The authentication server deals with validating the user names and passwords, while the accounting server records the call and the time for accounting and billing. Key to RADIUS security is a “secret” or encryption key which both the RAC and the RADIUS server know, but never send. This secret is used to encode all transmissions between the RAC and the RADIUS server, therefore the passwords are never sent in the “clear”.

Setting up the RADIUS server is a reasonably simple matter of filling the information shown in figure 12. The syntax for showing RADIUS security parameters is at the “`admin:`” prompt type

```
“show annex security”.
```

This command will display the information is figure 12. In order to set the parameters the command structure

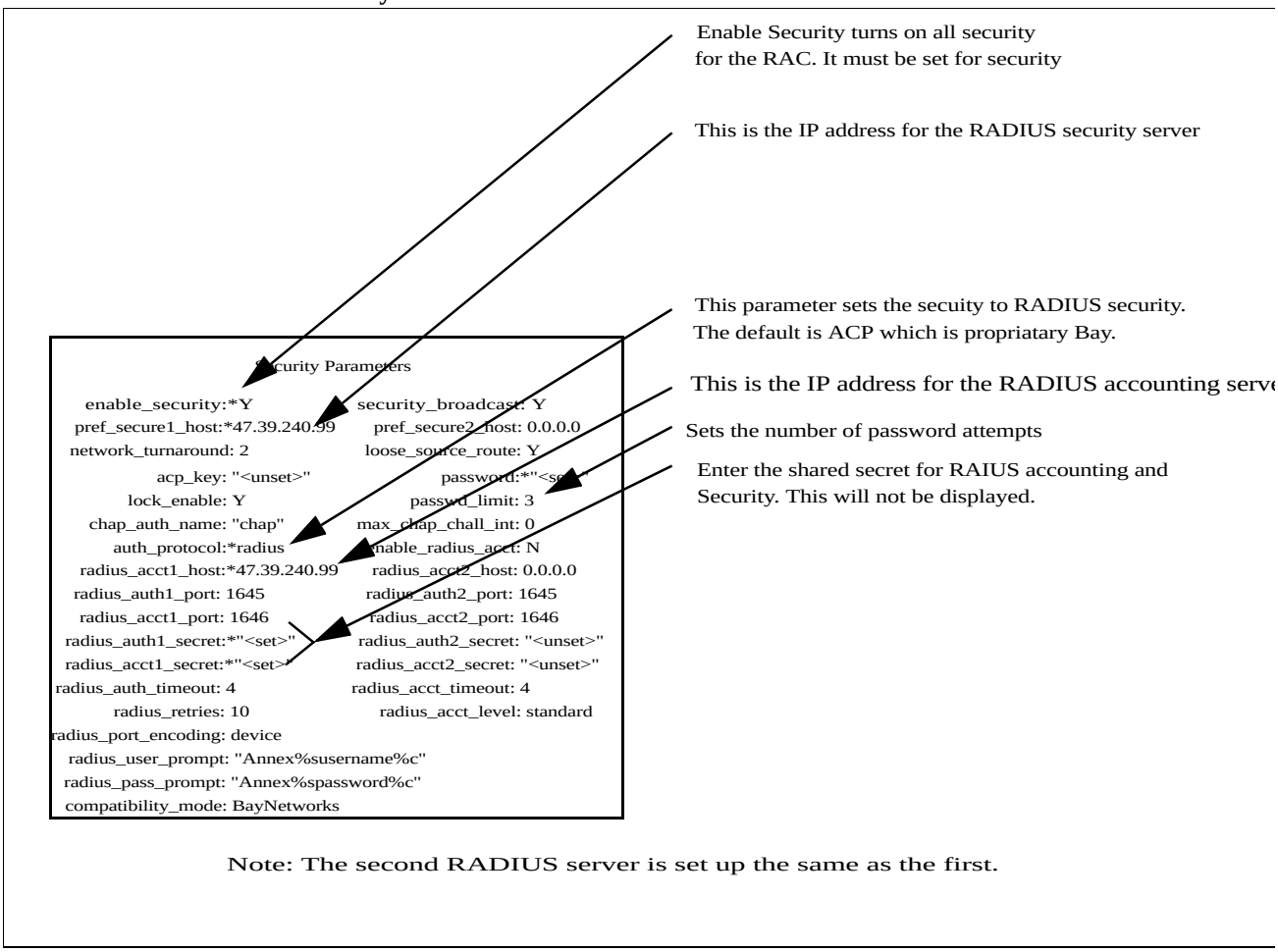
```
“set annex enable_security y”
```

format is used.

Make sure that the secret is inputted exactly as it is in the RADIUS server and note that it is case sensitive.

Note: RADIUS security will not take affect till the RAC has been rebooted.

FIGURE 12. RADIUS Security Parameters



Once the RADIUS server is set up the other services will need to have their security services turned on. The other services that can be controlled with RADIUS security are:

- PPP and MP authentication
- VCLI authentication
- CLI authentication

Before setting up any services that use security, the RADIUS server should be setup with accounts for the services that are being tested. It is best to first get RADIUS services

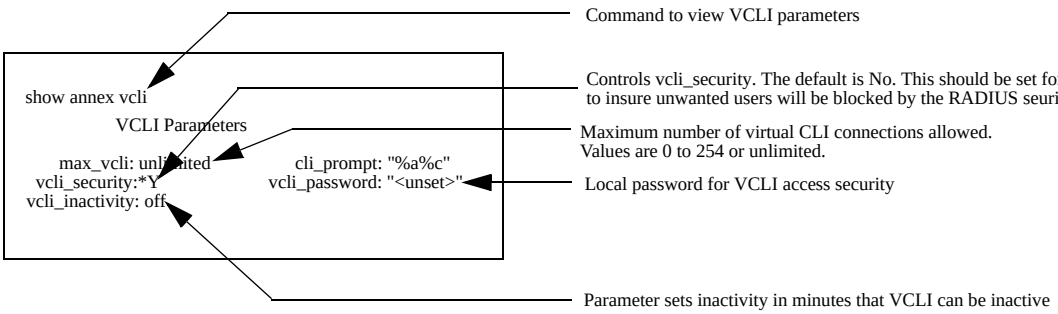
working with a simple security function such as VCLI. Using VCLI allows you to still have console CLI access while you work out any bugs. See below.

Note: The interface will need to be reset inorder for the changes to take affect.

5.5.6 VCLI Security

VCLI security deals with telnet (and rlogin) access to the CLI. Figure 13 shows a overview of the parameters associated with VCLI security.

FIGURE 13. VCLI Security Setup



Virtual Command Line Interface security.

Note: Commands are executed in the admin portion of CLI. Example to set the vcli_security parameters the command is “set annex vcli_security y”

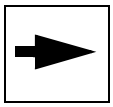
From the figure above you can see that there are two levels of security. There is a annex based password, vcli_password, for access to VCLI and also RADIUS capability which is enabled through vcli_security. Table 1 shows the precedence between the two security schemes.

TABLE 1. Precedence of VCLI Security

vcli_security	vcli_password	Host Security status*	Action
no	unset	don’t care	No security (no password)
yes	set	up	Will use host based security
yes	set	down	Use local vcli password
no	set	don’t care	Use local vcli password

vcli_security	vcli_password	Host Security status*	Action
yes	unset	up	Will use host based security
yes	unset	down	Can’t login to vcli

* RADIUS security



Note: The interface will need to be reset inorder for the changes to take affect.

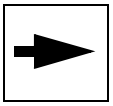
5.5.7 CLI Security

CLI local security is based on the port password which is also associated with PPP security which will be described later. Since CLI security is associated with the physical console port security. It is recommended but, it may not be as necessary since physical access to the RAC will be required.

TABLE 2. Precedence of CLI Security

cli_security	port_password	Host Security Status*	Action
no	unset	don’t care	No security (no password)
yes	unset	up	Will use host based security password
yes	unset	down	Cli will be blocked
yes	set	up	Will use host based security password
yes	set	down	Will use port_password

* RADIUS security

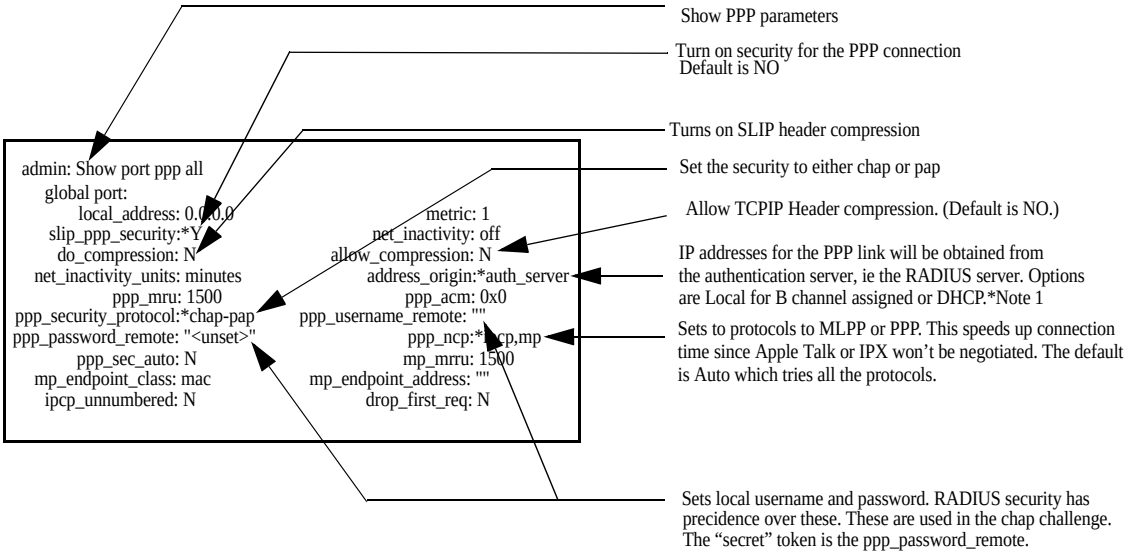


Note: The interface will need to be reset inorder for the changes to take affect.

5.5.8 PPP Port Security

PPP security deals with the security associated with dial in access. Both PPP and MLPP use the same services since MLPP is a subset of PPP. PPP security up as in figure 14.

FIGURE 14. Port PPP security Setup



*Note 1: With address_origin set to "RADIUS", the Framed-IP-Address from the RADIUS server, if provided, will have precidence over any IP address assignments made on the B-Channels.

Figure 14 details all the important parameters that will need to be set for host based security to take affect. It is optional to provide a local username and password, since dial in access should probably be denied when the redundant security servers are unavailable.

If address_origin is set to "auth_server" the RAC will use the Framed-IP-Addresses from the RADIUS server over any assigned on a per B-Channel basis. This allows only users with the Framed-IP-Address attribiute set to get a unique IP address. If you are using a B-Channel dedicated IP addresses.

TABLE 3. Port Security Precedence

port_security	port_password	Host Security status	action
yes	set	up	Will use host based security password
yes	unset	down	Will use port_password
no	set	don't care	Will use port_password
no	unset	don't care	No security (no password)
yes	unset	down	Can't login

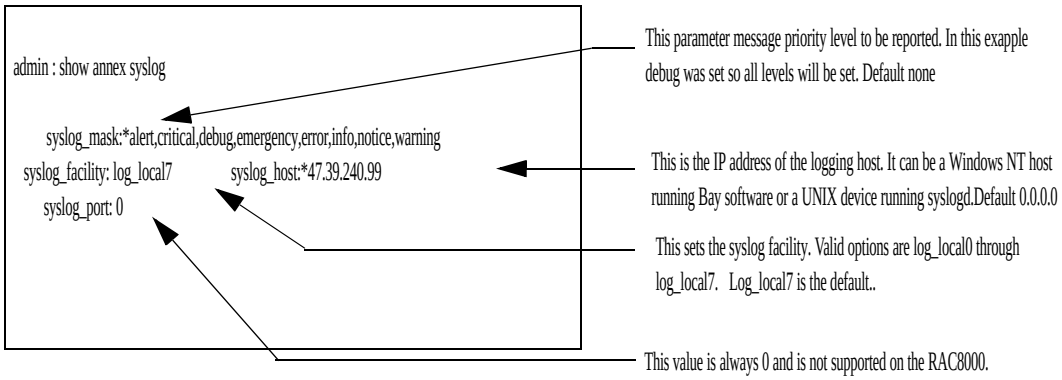
5.5.9 System Logging

The RAC can provide extensive logging of its events during a call setup. This information is extremely valuable when troubleshooting connection problems. These logs are normally (default) sent to the console port unless a syslog device has been defined.

In order to monitor the syslog messages on the console terminal the user will need to be logged out of CLI and the RAC must be in the default state for “annex syslog”. See figure 15 for the view of the syslog parameters.

Note: If you are in the console monitor in CLI and you want to view syslog messages, type “ha” (hangup). This will allow console messages to be outputted to the console, if no syslog host has been set.

FIGURE 15. Syslog Event Logging



If you choose logs can be sent to a external logging device. The event logs can be sent to a Unix 4.3 BSD syslog daemon or the can be sent to a Windows NT server running the Bay “Annex syslogd” services. Either syslog daemon are set up the same on the RAC.

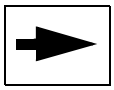
Setup is simple, the parameters which control the syslog are in the annex syslog menu. Figure 15 gives an overview of the parameters. The syslog_host IP address must be set to the device doing the recording. The syslog_facility can likely be left to the default. syslog_mask should be set to the minimum level of your requirements. Initially debug might be your choice, but with the quantity of messages that are generated the buffers in the syslogd device can easily be overflowed.

Table 4 shows the priority levels “high “emergency to low “debug”. When a priority has been chosen that level plus all higher levels will be reported to the syslogd host.

TABLE 4. Priority Levels for the syslog_mask Parameter

Level	Name	Description
High	emergency	Hardware failures.
	alert	All RAC reboots.

Level	Name	Description
	critical	Configuration and initialization problems, such as format errors in the gateway section of the configuration file or lack of memory.
	error	All line initialization errors, including CLI.
	warning	Indications of minor problems.
	notice	Time server queries and information about responses.
	info	Starting and ending of CLIs and of RAC jobs created by the rlogin and telnet commands and the ping and tap superuser CLI commands.
Low	debug	Activation and exit of all RAC processes.



Note: The RAC will need to be re-booted for logging changes to take effect.

Turning on “debug” will cause the log file to become filled up rapidly and the buffer might be overrun quickly. Therefore, “debug” should only be used for short periods of time while troubleshooting. Another option, is to turn sys logging off and have the messages displayed on the serial console port.

5.5.10 Useful Commands for the RAC

The RAC provides a number of useful commands to observe connections as well as troubleshoot problem. Unfortunately there are so many commands and options the author would like to highlight some that have proven to be very useful. These commands are covered in Bay Publication “Managing Remote Access Concentrators Using Command Line Interface” section 16.

5.5.11 WAN

This command provides information on the status of the DS-1 links and B-Channels or trunks. The Wan command is a super user command so you will have to log in as SU and enter the password (either the IP address of one you assigned in passwd prompt).

The two most useful Wan commands are “`wan`” and “`wan b`”.

Below is an example of the wan command:

```
annex# wan
```

```
 General WAN Statistics             Interface #1          Interface #2
--------------------------------------------------------------------------------
WAN Firmware Verbs:                 A MGR=1.234b          CAS-E1T1 1.45
WAN Type:                          T1 CSU                CAS T1 CSU
WAN FDL Type:                      ATT                   ATT
Switch Type:                       NI2                   UST1
Analog Encoding:                   mu_law                mu_law
WAN Interface Errors:              0                     0
Accepted Incoming Calls:           2                     18
Rejected Incoming Calls:           0                     0
Accepted Outgoing Calls:           0                     0
Rejected Outgoing Calls:           0                     0
Normal Call Disconnects:           2                     18
Abnormal Call Disconnects:         0                     0
B Channels Currently Allocated:    0                     13
Number Times WAN Fully Allocated:  0                     0

WAN Interface #1 Information:
Frame errors    = 6
Code violations = 2270
CRC errors      = 0
Errored blocks  = 0

WAN Interface #2 Information:
Frame errors    = 0
Code violations = 0
CRC errors      = 0
Errored blocks  = 0
```

Additionally, if there are error conditions on the WANs they will be printed out for each interface.

Another useful command is the “`wan b`” command. This will show the calls currently up and what B-Channel they are asssigned to, see below.

```
annex# wan b
b  called_#             calling_#            br spb_name     time     port
--------------------------------------------------------------------------------
12                                           vo auto_select  00:00:30 asy22
15                                           vo auto_select  01:18:11 asy38
--------------------------------------------------------------------------------
```

5.5.11.1 Actcall

This superuser command displays the calls that are on the RAC. It can be issued specifying a device type or not. Below is an example of a “`actcall”` command with no device specified:

```
annex# actcall
```

```
                          Active Call Summary

 D Device      Called      Calling User           Call start   Duration
               number       number               mm/dd|hh:mm:ss hh:mm:ss
 I asy30                           BJEG          01/06|23:09:33 00:12:37
 I asy46                           agteng        01/06|19:21:51 04:00:19
 I syn11                           didright      01/06|20:35:51 02:46:19
 I syn13                           didright      01/06|20:35:46 02:46:24
 I mp75                            didright      01/06|20:35:46 02:46:24
```

From the display you can see that the devices and available information is displayed. Called and calling number would be displayed if they had been programmed on this interface. The interface above is a “ust1” interface with no digits being forwarded.

Below is a “`actcall`” with a device specified:

```
annex# actcall mp75
Wan:0, channel: 0, User name: didright
Called number: , Calling number:
Called subaddress: , call bearer:
Call date: Tue Jan  6 20:35:46 1970, duration (hh:mm:ss): 02:49:00
Session parameter block:
IP addresses assigned: local:206.74.178.20 remote:206.74.178.140
AppleTalk addresses assigned: local:Apple default remote:Apple default
IPX addresses assigned: local:00000000.000000000000 remote:00000000.000000000000
Port mode: ppp, origin: incoming, application process: PPP
Index of owning MP bundle: 0
Octets Tx: 1255784, octets rx: 360814
Call assigned to device mp75
  bundle index: 1483
```

The above “`actcall`” is of the MP bundle for two associated ISDN calls syn 11 and syn 13. Their connections information can also be retrieved using the “`actcall`” command for syn11 and syn13 as below:

```
annex# actcall syn 11
CLI: Invalid argument.
annex# actcall syn11
Wan:1, channel:14, User name: didright
Called number: , Calling number:
Called subaddress: , call bearer: voice
Call date: Tue Jan  6 20:35:51 1970, duration (hh:mm:ss): 03:01:44
Session parameter block: auto_select
IP addresses assigned: local:0.0.0.0 remote:0.0.0.0
AppleTalk addresses assigned: local:Apple default remote:Apple default
IPX addresses assigned: local:00000000.000000000000
remote:00000000.000000000000
Port mode: ppp, origin: incoming, application process: PPP
Index of owning MP bundle: 1483
```

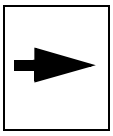
```
Octets Tx: 711462, octets rx: 235036
Call assigned to device syn11
  frames sent:           5754
  frames received:       7906


annex# actcall syn13
Wan:1, channel:12, User name: didright
Called number: , Calling number:
Called subaddress: , call bearer: voice
Call date: Tue Jan  6 20:35:46 1970, duration (hh:mm:ss): 03:02:00
Session parameter block: auto_select
IP addresses assigned: local:0.0.0.0 remote:0.0.0.0
AppleTalk addresses assigned: local:Apple default remote:Apple default
IPX addresses assigned: local:00000000.000000000000
remote:00000000.000000000000
Port mode: ppp, origin: incoming, application process: PPP
Index of owning MP bundle: 1483
Octets Tx: 725793, octets rx: 235817
Call assigned to device syn13
  frames sent:           5776
  frames received:       5340
```

5.5.11.2 Who

The “who” command is used to display the users who are currently logged in. It is accessed from the CLI prompt. It shows all the users connected to the RAC. It shows which port they are connected. When security is turned on, PPP it will also show the user-name under the User column. It shows the time of the connection as well as the IP address assigned to the connection. This is a very useful command to determine which and how many users are connected. Additionally it shows MLPP calls which are indicated with 3 devices. In the example below syn45, syn48 and mp11 are one call which is a ISDN MLPP call. The mp11 device is the composite of syn45 and syn48.

```
annex# who
Port  What User            Location        When         Idle  Address
pts1  CLI  john            Ext456          7:29am        :18  47.39.57.121
syn45 PPP  ---             ---             8:04am             [local]
syn48 PPP  ---             ---             8:04am             [local]
ctl1  CLI  ---             ---             8:04am             [local]
asy32 PPP  ---             ---             ---                47.74.178.169
asy35 PPP  amcacct         ---             ---                47.74.178.143
asy41 PPP  hambulius       ---             ---               47.74.178.134
mp11  PPP  ---             ---             8:04am             47.39.240.44
```

.



Note: User names will not show up, unless you have the appropriate security turned on. For example for PPP names, PPP security must be enabled.

5.5.11.2.1 Modem

This command is useful for interrogating the quality of connection of a particular user. The modem command is available once you login as superuser. It is best to first use the who command and determine the user you are interested in. The users identification will be the asy number. For example a user amcacct is using asy35 can be queried by typing:

```
annex# modem -s35
asy30 States:  loader 0, protocol 5, link 5, control 10, pump 0xff
      Error correction 5 (V.42), compression 0 (none)
      Drops:  from 0, to 0; HDLC under 0, over 0; event 48
      Rcv:  errs 0, pkts 200; Tx resent 80, pkts 143
      Rrn:  rcvd 0, init 0; train rcvd 0, init 0, disc 0 (unknown)
      V.34 rx precoding 0, non-linear 0, shaping 0, carrier 0, pre-emphasis 0
      X2 status 0x7, RBS 0, PAD 0, speed reduction 0 (0 kb)
      K56flex ver 0 (none), status 0xff, RBS 0, PAD 0, speed reduction 0 kb
      V.90 status 0x14bf, c.i. 0x12345, PAD 0, shaping 1
      V.90 lookahead 0, c.pwr -12 dBm, half duplex RRN rx 0
      Delay 7ms, snr 32dB, qual 0, chan freq 0Hz
      Echo offs 90Hz, lvl -34dBm; osc freq 15PPM; Rcv lvl -22dBm
      Baud rx 4 (3200), tx 6 (8000); speed rx 14 (26400), tx 25 (29333)
      Connect status 3 (connected), modulation 6 (V.90)
```

As you can see the modem command provides extensive information on the characteristics of the modem connection. This information can be very useful in verifying and troubleshooting a customers modem problems.

See Section 1 of the “Remote Access Concentrator Software Reference for more Detail.

5.5.11.2.2 Netstat

Netstat is a very useful command. It can be confusing since it has 30 options. I wish to cover a couple of the more useful commands. Refer to Bay Publication “Managing Remote Access Concentrators Using Command Line Interface” section 16 for a complete list.

5.5.11.2.3 PPP Statistics (netstat -ip)

Netstat -ip displays the connection parameters associated with the PPP session. It can be used for both synchronous connections (ISDN) and asynchronous connections (analog

modem). It displays the status of the PPP link negotiations and can be useful in trouble-shooting PPP establishment problems. Below is an example:

```
Bay_RAC8000# who
Port  What User            Location         When          Idle  Address
pts1  CLI  cli             ---              ---            :20  47.39.57.44
syn22 PPP  nortel          RAC RED LAN      ---                 [local]
syn38 PPP  nortel          RAC RED LAN      ---                 [local]
mp1   PPP  nortel          ---              ---                 47.39.240.50


annex# netstat -ip mp1

                   *** PPP Layering Status ***
State              Current:  NCP Open       Prior:    NCP Opening

                   *** LCP Status ***
State              Current:  Open           Prior:    Ack sent
Options            Local:                   Remote:
MRU                1500                     1500
MRRU               1500                     1500
Short Sequence     On                       Off
Endpoint Disc      3:00-80-2d-05-8f-7e      5:9129213464

                   *** NCP (IPCP) Status ***
State              Current:  Open           Prior:    Ack received
Options            Local:                   Remote:
IP addresses       47.39.240.40   [ANX]     47.39.240.50   [SECSERV]
Compression        None                     None
```

The example above is a MLPP call over ISDN. As you can see it shows up as 3 devices. One for each B-Channel and a MP device representing both B-Channels and the IP address. You can also see that the PPP Link Control Protocol (LCP) is open and therefore working. Similarly the Network Control Protocol (NCP) is open and therefore working.

The next example is a asy or modem connection:

```
annex# who
Port  What User            Location         When          Idle  Address
asy31 PPP  nortel          RAC RED LAN      ---                 47.39.240.52
pts1  CLI  cli             ---              ---            :30  47.39.57.44
pts2  CLI  cli             ---              ---                 47.39.57.121
annex# netstat -ip asy31

                   *** PPP Layering Status ***
State              Current:  NCP Open       Prior:    NCP Opening

                   *** LCP Status ***
State              Current:  Open           Prior:    Ack received
```

```
Options             Local:                  Remote:
MRU                 1500                    1500
Auth type           CHAP                    None
ACFC                On                      On
ACCM                00000000                000a0000
Magic               0x15634a10              0x000c2fe7
PFC                 On                      On
MRRU                1500                    1500
Short Sequence      Off                     Off
Endpoint Disc       0:0                     0:0

                    *** NCP (IPCP) Status ***
State               Current:  Open          Prior:    Ack received
Options             Local:                  Remote:
IP addresses        47.39.240.40   [ANX]    47.39.240.52   [SECSERV]
Compression         None                    None

                    *** Security (CHAP) Status *
State:              Local:    OUT_UP        Remote:   IN_INIT


                    *** NCP (MP) Status ***
State               Current:  Closed        Prior:    Closed
```

The asy printout is similar to the syn printout. If other protocols were declared in the PPP setup (ppp_ncp prompt) they will be displayed. The setup for the RAC being displayed has ppp_ncp set to ipcp and mp. If more protocols were selected the netstat -ip will show their status.

5.5.11.2.4 Routing Tables (netstat -r)

This command will display the routing tables which reside in the RAC. These tables are most likely constructed using RIP and building from information given by other routers. The command serves to verify that routing information is being obtained from neighboring routers. The command is “netstat -r”, this will display the routing tables as below:

```
annex# netstat -r
Routing tables
Destination         NextHop         Flags Usage     UseCount  Mtr Interface
0 - 65534           65292.181       UHF   0         0         0   en0
IP default          47.39.240.1     UR    -9891     916       2   en0
47.39.48.0/20       47.39.240.1     UR    -10405    402       2   en0
47.39.52.55         47.39.240.1     UR    -10807    0         3   en0
47.39.52.56         47.39.240.1     UR    -10807    0         3   en0
47.39.224.0/20      47.39.240.1     UR    -10807    0         2   en0
47.39.240.0/20      *               UI    fixed     3279      1   en0
47.39.240.50        *               UI    fixed     0         1   mp1 (ppp)
```

```
47.45.128.0/20     47.39.240.1     UR    -10807    0         2   en0
47.79.64.0/20      47.39.240.1     UR    -10807    0         2   en0
47.117.128.0/20    47.39.240.1     UR    -10807    0         2   en0
47.194.32.0/20     47.39.240.1     UR    -10805    2         2   en0
127.0.0.0/8        *               UI    fixed     0         1   lo0
137.116.0.0/16     47.39.240.1     UR    -10807    0         6   en0
192.168.0.0/24     47.39.240.1     UR    -10807    0         5   en0
```

5.5.11.3 Statistics

The RAC continually produces statistics about it operation. The basic statistics is available by simply typing “stats” while in CLI either as superuser or not. Below is a typical print-out:

```
annex: stats
S/W: Remote Access X15.1.5          Build #4: Wed Dec 16 11:05:08 EST 1998
H/W: 8000RAC/Turbo, Cmp Crd Rev 0   ROM Rev: 1124, MLB Rev 142.0
QUICC Ver: 130                      Clock Source: Interface 2
Memory: 8MB RAM 64KB EE 128KB SLC1 128KB SLC2 4MB FLSH
Boot from: 47.39.240.99             Date: unknown
Image: oper.64.enet                 Uptime: 4 days 16 hours 40 min.
Inet addr: 47.39.240.40             Subnet mask: 255.255.240.0
Ethernet addr: 00-80-2d-05-8f-7e    Broadcast addr: 47.39.255.255
No name servers                     Domain: <unknown>
IPX Frame Type: 802.3               IPX Network Number: 0
Apple: Node 65292.181  Router 0.0   Zone:
CPU Load: cur 0%, avg 0%
SLC CPU time with no task to execute: slot 1/c 0%, slot 2/c 0%
Procs:    current 36, max 48, limit 1280
Tasking:  rescheds 0/4, switches 54/1328808, activates 45/1328456
Mbufs:    total 8999, free 8787, min free 8393
Memory:   total 8MB, avail 6.0MB, free 2.5MB, min 1.6MB
Ports:    aui&twi 2wan 48mod 64syn/ta 1gsy/No Cable

Port type   Receive  Transmit  R Frames  T Frames  R Errors  T Errors
   asy        9.5KB     8.9KB       219       215         0         0
   syn       929 by     1.1KB        19       113         2         0
   ta          0 by      0 by         0         0         0         0
   ctl      685.2KB   630.7KB         0         0         0         0
   gsy         0 by      0 by         0         0         0         0
```

Based on the printout you can see that the stats command provides useful basic uptime information along with the version of software being executed.

5.5.11.4 Current statistics - WAN

The stats command is useful for monitoring the WAN or T1 performance going into the RAC. The RAC continually monitors and records statistics on a 15 minute interval over a 24 hour period. This command is only available when logged in as superuser (SU).

To display current WAN statistics the command is:

```
stats -T current wan1
```

In this command -T indicates we are requesting “T” carrier statistics, current condition and we want WAN1

Below is a sample printout:

```
annex# stats -T current wan1

WAN Interface 1:
        Alarm History:
                time unknown
                NO SYNC
        Current Alarms:
        Circuit ID:
        T1 info:
        Loopback mode: no loopback

        Current Statistics:
                time unknown
                Number of valid seconds: 22
                Errored Seconds: 0
                Severely Errored Seconds: 0
                Bursty Errored Seconds(ESF only): 0
                Unavailable Seconds: 0
                Controlled Slip Seconds: 0

                CRC6 Error Event(ESF only): 0
                ESF Error Event(ESF only): 50
                Severely Errored Framing Event: 0
                Frame Sync Bit Error Event: 0
                Out of Frame: 0
                Loss of Frame Count: 0
                Line Code Violation Event(BPV): 0
                Controlled Slip Event: 0
                Unavailable Signal State: Clear
```

If you are interested in more that the current 15 minute interval the stats -T all command is useful. This command will display 96 15 minute blocks to the console screen, indicating the WAN status for the last 24 hours. Below is an abbreviated example:

```
WAN Interface 1:
        Alarm History:
                time unknown
                NO SYNC
        Current Alarms:
        Circuit ID:
        T1 info:
        Loopback mode: no loopback

        Current Statistics:
                time unknown
                Number of valid seconds: 249
                Errored Seconds: 0
                Severely Errored Seconds: 0
                Bursty Errored Seconds(ESF only): 0
                Unavailable Seconds: 0
                Controlled Slip Seconds: 0

                CRC6 Error Event(ESF only): 0
                ESF Error Event(ESF only): 50
                Severely Errored Framing Event: 0
                Frame Sync Bit Error Event: 0
                Out of Frame: 0
                Loss of Frame Count: 0
                Line Code Violation Event(BPV): 0
                Controlled Slip Event: 0
                Unavailable Signal State: Clear

        Interval # 0 Statistics:
                time unknown
                Number of valid seconds: 900
                Errored Seconds: 0
                Severely Errored Seconds: 0
                Bursty Errored Seconds(ESF only): 0
                Unavailable Seconds: 0
                Controlled Slip Seconds: 0

                CRC6 Error Event(ESF only): 0
                ESF Error Event(ESF only): 50
                Severely Errored Framing Event: 0
                Frame Sync Bit Error Event: 0
                Out of Frame: 0
                Loss of Frame Count: 0
                Line Code Violation Event(BPV): 0
```

```
                Controlled Slip Event: 0
                Unavailable Signal State: Clear
                      .
 94 other blocks      .
                      .
Interval # 95 Statistics:
                time unknown
                Number of valid seconds: 900
                Errored Seconds: 0
                Severely Errored Seconds: 0
                Bursty Errored Seconds(ESF only): 0
                Unavailable Seconds: 0
                Controlled Slip Seconds: 0

                CRC6 Error Event(ESF only): 0
                ESF Error Event(ESF only): 7
                Severely Errored Framing Event: 0
                Frame Sync Bit Error Event: 0
                Out of Frame: 0
                Loss of Frame Count: 0
                Line Code Violation Event(BPV): 0
                Controlled Slip Event: 0
                Unavailable Signal State: Clear
```

This command is very useful in troubleshooting outages that occurred in the last 24 hours.

5.5.11.5 Clearing Statistics

The clear command is similar to the other commands except the function is clear. The command is in the form of stats -T [clear [history | statistics] | current | total | all] [wan1|wan2]. The Clear command must be followed by either history or statistics and then the associated WAN must be entered. The “history” option clears the 24 hour period while the “statistics” option only clears the current record.

Below is a example of clearing the current interval.

```
annex# stats -T clear statistics wan1
cleared interval statistics on wan1
```

Similarly to clear the history and alarm history:

```
annex#  stats -T clear history wan1
cleared alarm history on wan1
```

6.0 Bibliography

Bay Networks, *Managing Remote Access Concentrator Using Command Line Interface*, Marketing Release 6.0, May 1998.

Bay Networks, *Remote Office Concentrator Software Reference,* Marketing Release 6.0, May 1998.

Bay Networks, *Installing the Model 8000 Remote Office Concentrator*, Marketing Release 5.1, September 1997.

Bay Networks, *Installing and Configuring Remote Office Concentrator Software for Windows and Windows NT* , Marketing Release 6.0, May 1998.

Bay Networks, *Provisioning WAN Lines for Remote Access Concentrators*, Marketing Release 6.0, May 1998.

Bay Networks, *Remote Access Software Version 6.0 Release Notes*, Marketing Release 6.0, May 1998.

Bay Networks, *Remote Annex Administrator's Guide for Unix*, Book A,B and C, Rev A,

Bay Networks, *Release 5.1 Supplement for Remote Annexes*, Marketing Release 5.1, October 1997.

Bay Networks, *BaySecure Access Control Administration Guide*, Release 1.3,October 1997.

Nortel Networks, *NTP 297-3401-311P2.*