B

Appendix B RADIUS Server

Managing dispersed serial lines and modem pools for large numbers of users can create the need for significant administrative support. Since modem pools are a link to the outside world, they require careful attention to security, authorization, and accounting. This can best be achieved by managing a single "database" of users, allowing for authentication (verifying user name and password) as well as configuring information which details the type of service to deliver to the user (for example: SLIP, PPP, telnet, rlogin). Moxa CN2500 Async Server supports RADIUS protocol, which requires only one database for remote user management.

What is RADIUS?

Definition

Remote Authentication Dial-In User Service, or RADIUS, is the standard for centralizing the authentication, authorization, and accounting of remote access users.

Here is a brief description of how RADIUS works: When a user dials in to a remote access device, that device communicates with the central RADIUS server to determine if the user is authorized to connect to the LAN. The RADIUS server performs the authentication and responds with the result – either accept or reject. If the user is accepted, the remote access server routes the user onto the network; if not, the RAS will terminate the user's connection. The RADIUS server also provides accounting services if supported by the remote access server.

With RADIUS, a network manager or ISP only needs to maintain a single, central database against which all remote user authentication takes place. This greatly eases the management burden associated with administering large numbers of dial-in users.

Client/Server Architecture

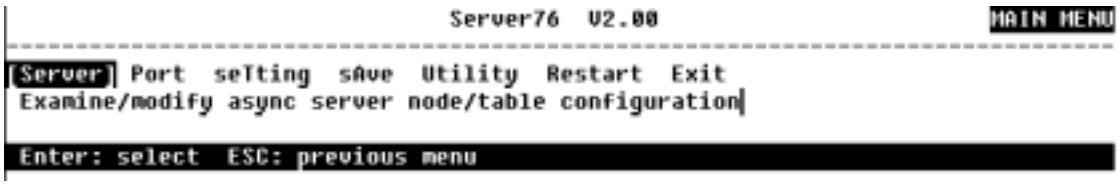
RADIUS is a type of client-server software. Communication servers, such as CN2500, play an active role, whereas a RADIUS server is passive.

1. When a remote host is connected to CN2500, it is prompted to enter its user ID and password.
2. After receiving the user ID and password, CN2500 sends the information to a defined RADIUS server. Up to this point, the remote user is still unable to access the network.
3. The RADIUS server compares the user ID and password with its internal database, and then uses the internet to respond, either accepting or rejecting.
4. If CN2500 receives the "accept" message from the RADIUS server, the remote user is allowed to enter the network. Otherwise, CN2500 will wait for another try, or terminate the connection when a specified time limit has been reached.

Setting up CN2500

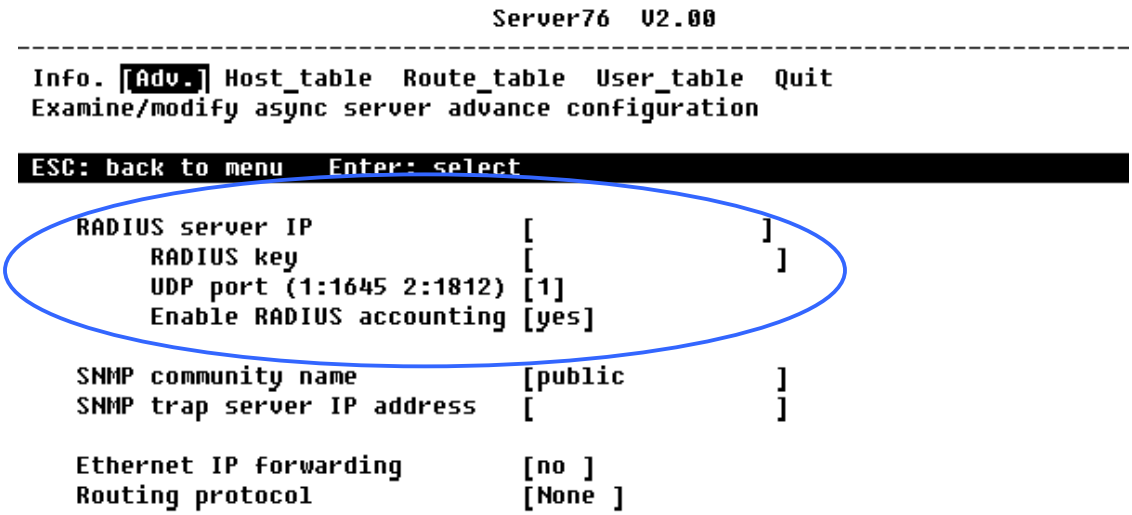
I. Setting up the RADIUS server IP address

1. In **MAIN MENU** select **Server**.



2. In **SERVER MENU**, select **Adv.**

3. RADIUS settings.



RADIUS server IP: [RADIUS server IP address]

RADIUS key: [RADIUS password] (must be the same in the RADIUS server)

UDP port: [1/2]

Mode 1: An earlier but rather common setting is 1645. If you choose 1645, the authentication has to be set as 1645, and accounting as 1646 in the RADIUS Server.
Mode 2: The latest setting is 1812. If you choose 1812, the authentication must be set as 1812, and accounting as 1813 in the RADIUS Server.

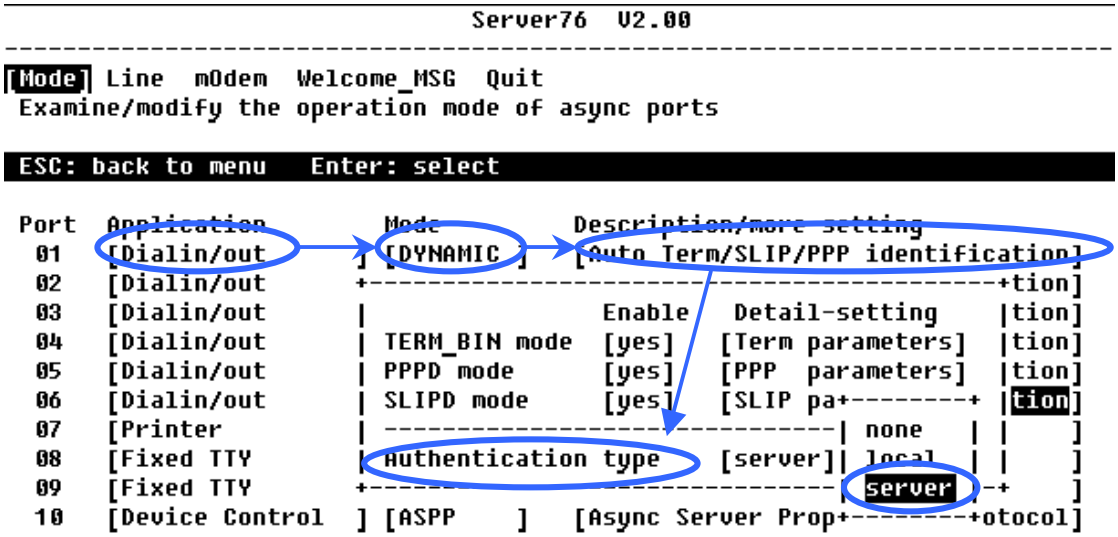
Enable RADIUS accounting: [yes/no]

4. Save, and then restart CN2500.

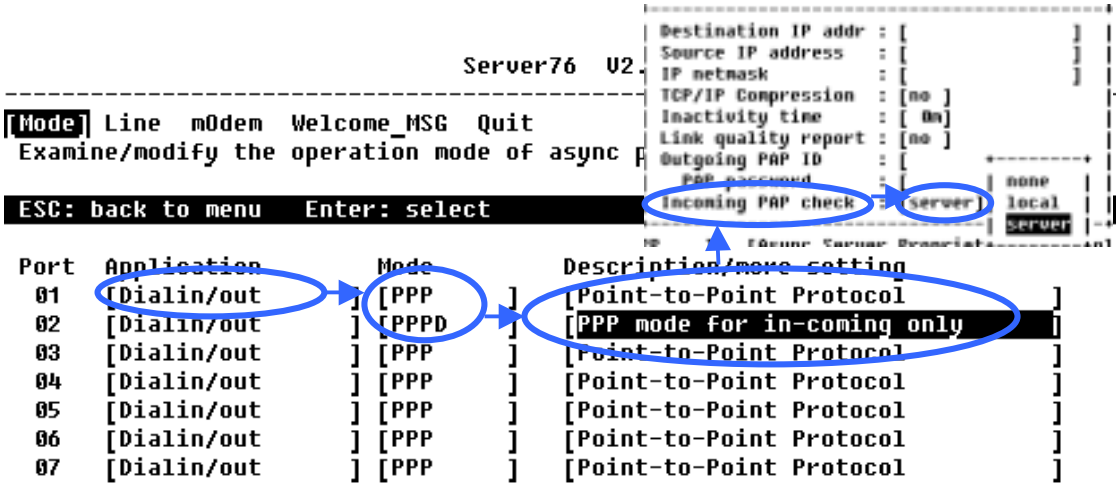
II. Setting up port configuration

RADIUS is effective for dial-in services. Therefore, select **server** for **Authentication type** in **DYNAMIC**, and **PPP, PPPD, TERM_BIN, and TERM_ASC** modes in **PORT MENU**.

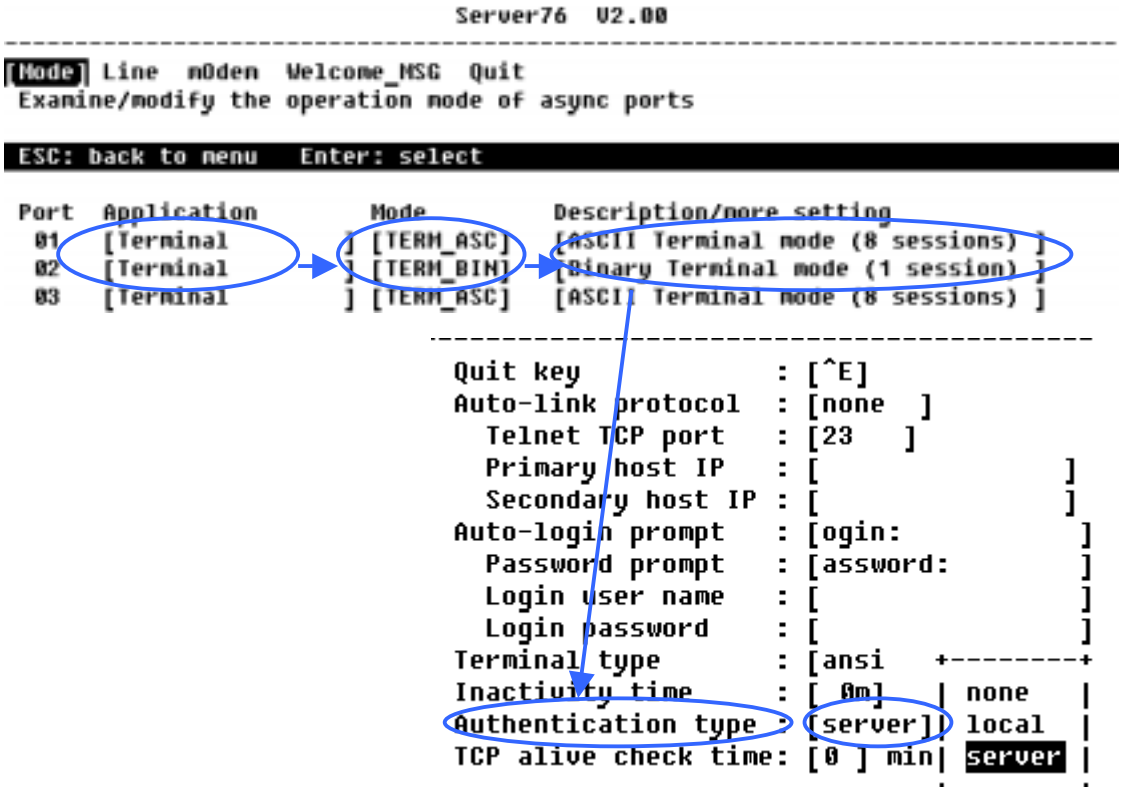
Dial-in/out- Dynamic mode



Dial-in/out- PPP/PPPD modes



Terminal- TERM_BIN/TERM_ASC modes



Setting up UNIX hosts

You can use your own RADIUS software to do this. Moxa, however, provides a RADIUS program for UNIX. To use Moxa RADIUS Server, extract `radius.2.2.tar` from the CN2500 CD. All files are extracted to the `/radius2.2` directory.

I. Installing the RADIUS execution file.

a. Login to the UNIX host and create a directory.

#mkdir /radius

#cd radius

b. Mount CD-ROM volume

OS	Command
SCO OpenServer	***#mount-f ISO9660, filemode=444 <device>*** Example: #mount-f ISO9660, filemode=444 /dev/cd1/mnt
Solaris x86	In the volume manager mounts the CD-ROM on mount point /cdrom/cdrom0
Linux	#mount /dev/cdrom or #mount-t iso9660-ro mode=0555<device> Example: #mount-t iso9660-ro mode=0555/dev/hdb/mnt

c. Copy file to host

#cp /mnt/cdrom/radius.2.2.tar

d. Extract the .tar to files.(radiu.2.2 subdirectory)

#tar xvf radius.2.2.tar

After extracting, there are subdirectories, as follows:

/src: source code

/conf: configuration

/log: log record

/temp: temporary files

/bin: excution files

e. Compile and link

#cd /src

#sh mk_radius

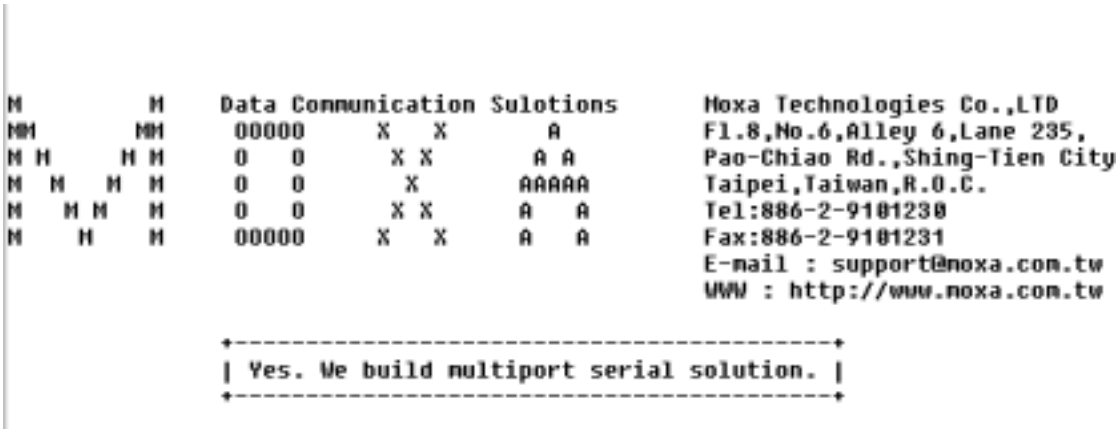
II. RADIUS Server configuration

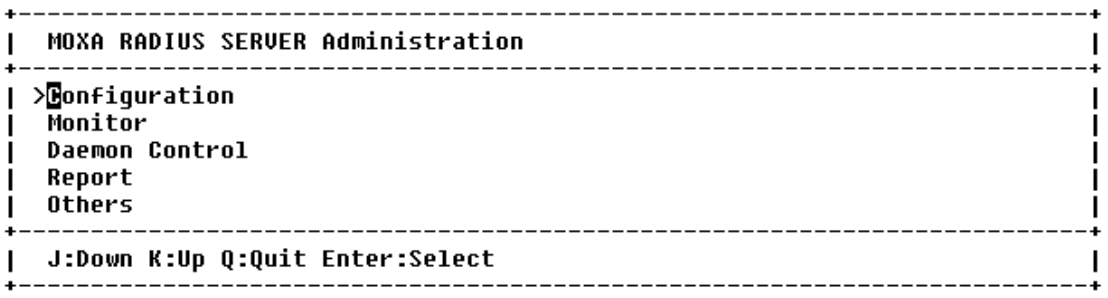
1. Enter RADIUS administration

   #cd radius.2.2/bin

   #./radiusadm

2. You will see a welcome message, and then enter RADIUS SERVER administration.





3. Specify password file

"Configuration"→"Basic Configuration"→Password File

(/etc/passwd for LINUX)

(/etc/shadow for SCO UNIX and SOLARIS)

(/etc/master.passwd fot FREEBSD and BSDI)

```
+------------------------------------------------------------------------------+
|  Basic Configuration                                                         |
+------------------------------------------------------------------------------+
| >Password File : /etc/passwd                                                 |
|  Async Server Administration                                                 |
|  Save & Exit                                                                 |
+------------------------------------------------------------------------------+
```

4. Specify CN2500 IP.

"Configuration"→"Basic Configuration"→" Async Server Administration"→"Add Async Server"

```
+------------------------------------------------------------------------------+
|  Basic Configuration                                                         |
+------------------------------------------------------------------------------+
|  Password File : /etc/passwd                                                 |
| >Async Server Administration                                                 |
|  Save & Exit                                                                 |
+------------------------------------------------------------------------------+
+------------------------------------------------------------------------------+
|  Async Server Administration                                                 |
+------------------------------------------------------------------------------+
| >Add Async Server                                                            |
|  Modify Async Server                                                         |
|  Delete Async Server                                                         |
+------------------------------------------------------------------------------+
|  J:Down K:Up Q:Quit Enter:Select                                             |
+------------------------------------------------------------------------------+
|  Add Async Server                                                            |
+------------------------------------------------------------------------------+
| >IP Address       :                                                          |
|  Name             :                                                          |
|  Console Password :                                                          |
|  Ok                                                                          |
+------------------------------------------------------------------------------+
|  J:Down K:Up Q:Quit Enter:Select                                             |
+------------------------------------------------------------------------------+
```

IP address : [ ]→ CN2500 IP

Name: : [ ]→CN2500 server name

Console Password:[ ]→CN2500 console password

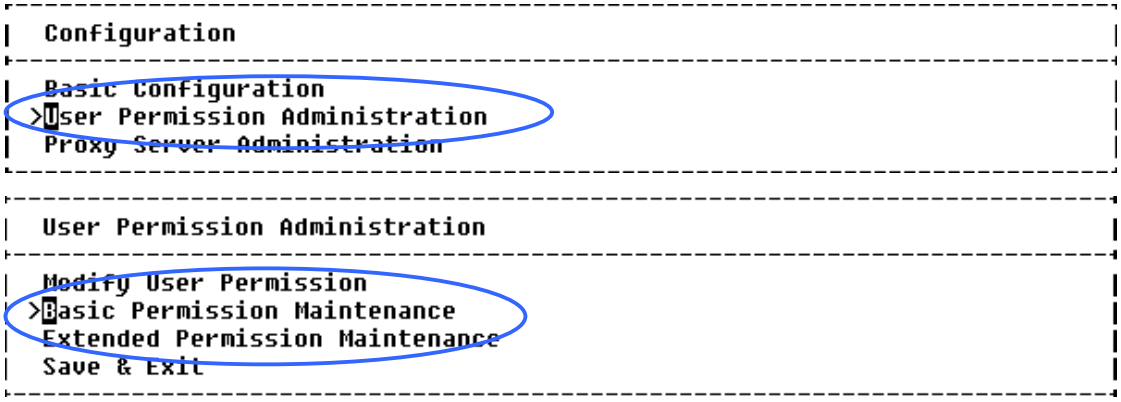
5. Save and exit.

III. Basic/Extended Permission Group Setting

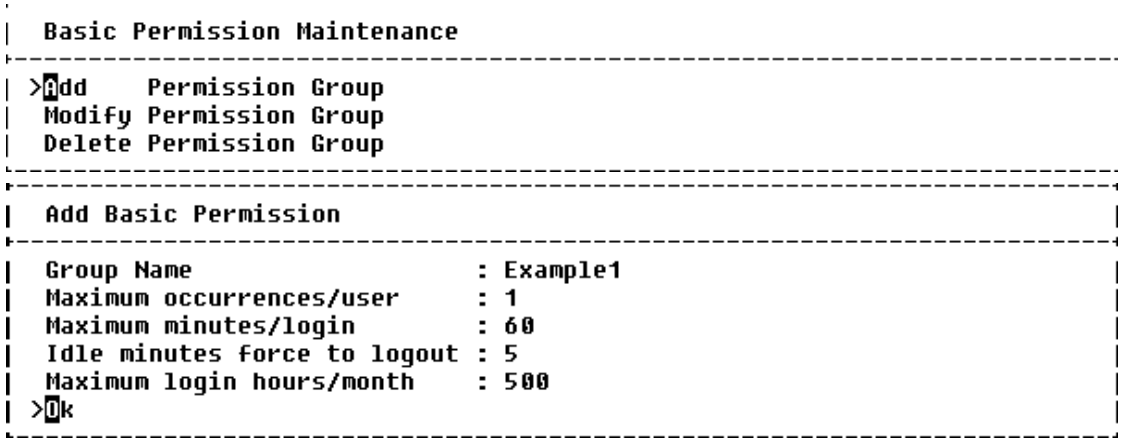
Basic and extended permission group defines regulations for users.

1. Add/Modify permission group

"Configuration"→"User Permission Administration"→"Basic Permission Maintenance" or "Extended Permission Maintenance".



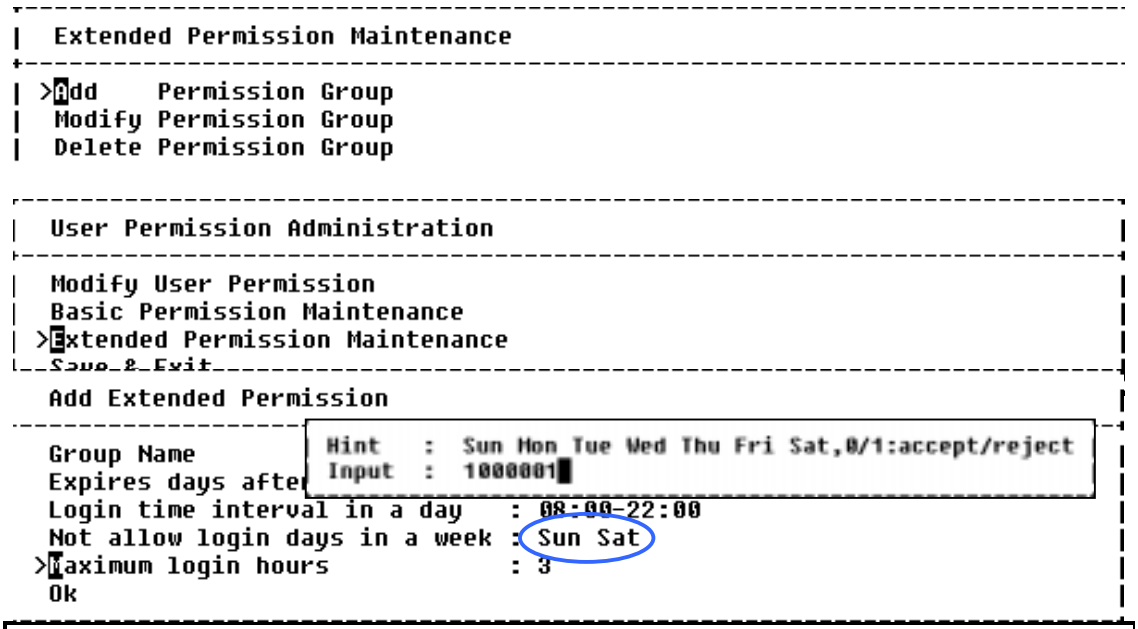
2. Basic Permission Maintenance



Basic Permission Group	Example	Description
Group Name	Example1	Name of this permission setting
Maximum occurrences/user	1	The user can only login once at the same time. "0" for simultaneous unlimited login sessions
Maximum minutes/login	60	The user has only 60 minutes in each login session "0" for unlimited time
Idle minutes force to logout	5	If the user idles for 5 minutes, the session will be terminated "0" for no kick-out
Maximum login hours/month	500	The user has max. 500 hours per month. "0" means unlimited access

Select "OK" to save.

3. Extended Permission Maintenance



Extended Permission Group	Example	Description
Group Name	Example2	Name of this permission setting
Days to expire after first login	30	The user account expires after 30 days after first login "0" for no expires
Login time interval in a day	08:00-22:00	The user has only 60 minutes in each login session "0" for unlimited 24 hours usage,
Barred login days	Sun Sat	The user is not allowed to login in on Saturday or Sunday. "0" for accept, "1" for reject.
Maximum login hours	500	The user has max. 500 hours for this account. "0" means unlimited access.

Select "OK" to save.

```
|  User Permission Administration                                              |
|------------------------------------------------------------------------------|
| >Modify User Permission                                                      |
|  Basic Permission Maintenance                                                |
|  Extended Permission Maintenance                                             |
|  Save & Exit                                                                 |
|------------------------------------------------------------------------------|
```

"User List" lists all UNIX/LINUX users.

```
|  User List                                                                   |
|------------------------------------------------------------------------------|
| >adm                                                                         |
|  bin                                                                         |
|  daemon                                                                      |
|  ftp                                                                         |
|  games                                                                       |
|  gdm                                                                         |
|  george                                                                      |
|  gopher                                                                      |
|  halt                                                                        |
|  lp                                                                          |
|------------------------------------------------------------------------------|
|  J:Down K:Up Ctrl-F:PgDn Ctrl-B:PgUp Q:Quit G:GoTo Enter:Select              |
|------------------------------------------------------------------------------|
```

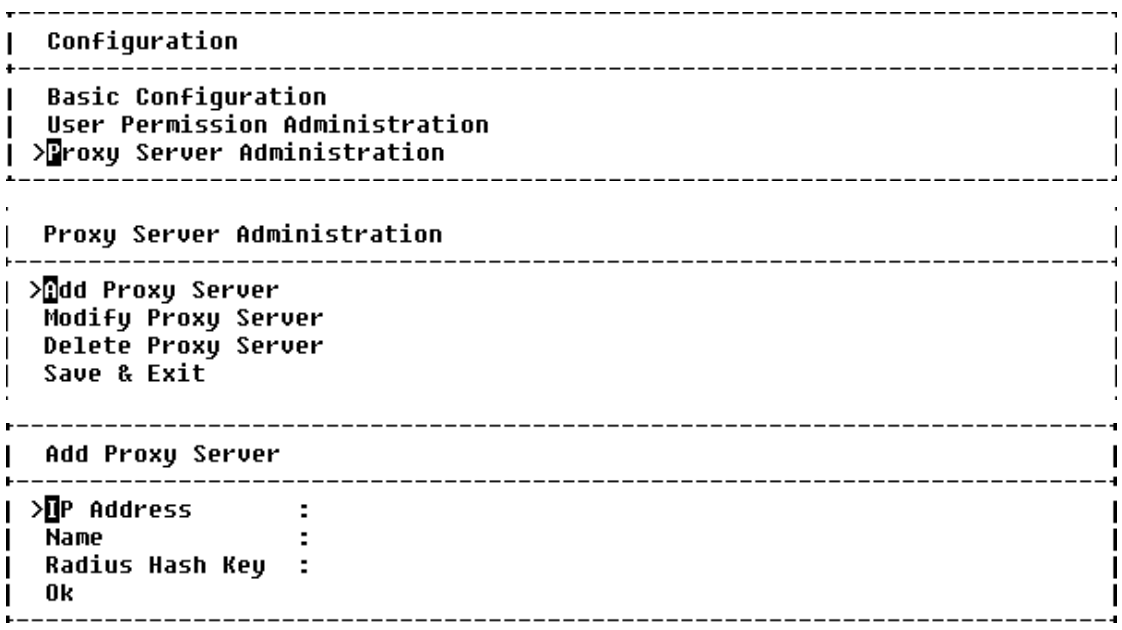
1. Select the user "george" and press [Enter] to modify setting. Press [Ctrl-F] for page down, [Ctrl-B] for page up.
2. Specify basic permission group and extended group for the user "george".

```
|  User Name = george                                                          |
|------------------------------------------------------------------------------|
|  Basic Permission Group    : Example 1                                       |
| >Extended Permission Group : Example 2                                       |
|  Ok                                                                          |
|------------------------------------------------------------------------------|
```

3. Select "OK" to save.

V. RADIUS proxy

"Configuration"→"Proxy Server Administration"→"Add Proxy Server"



IP address:[ ] →Proxy Server IP

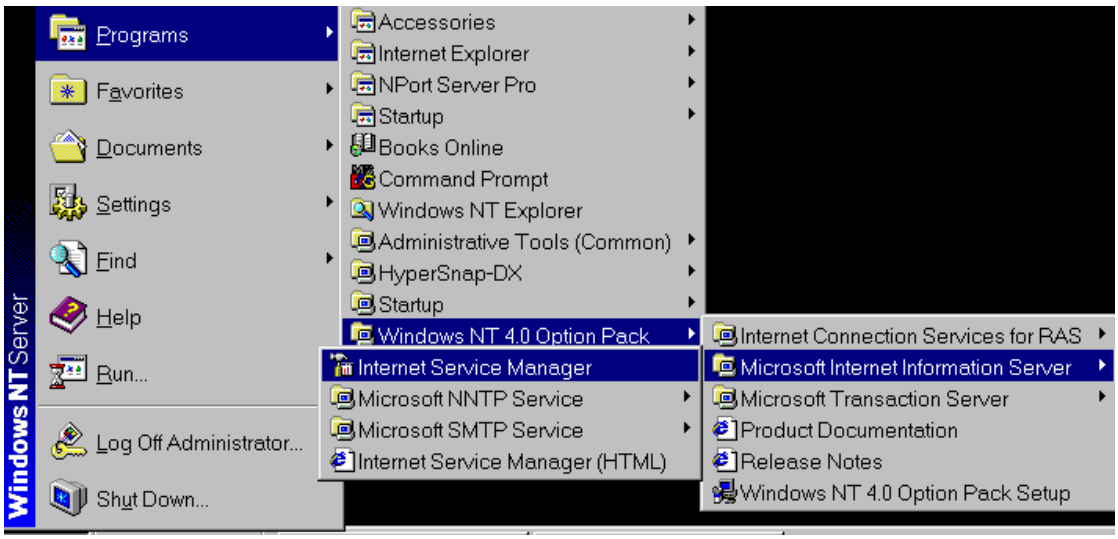
Name: [ ]→ Proxy Server Name

Radius Hash Key:[ ]→ RADIUS encryption key, must be the same key in the proxy server end.

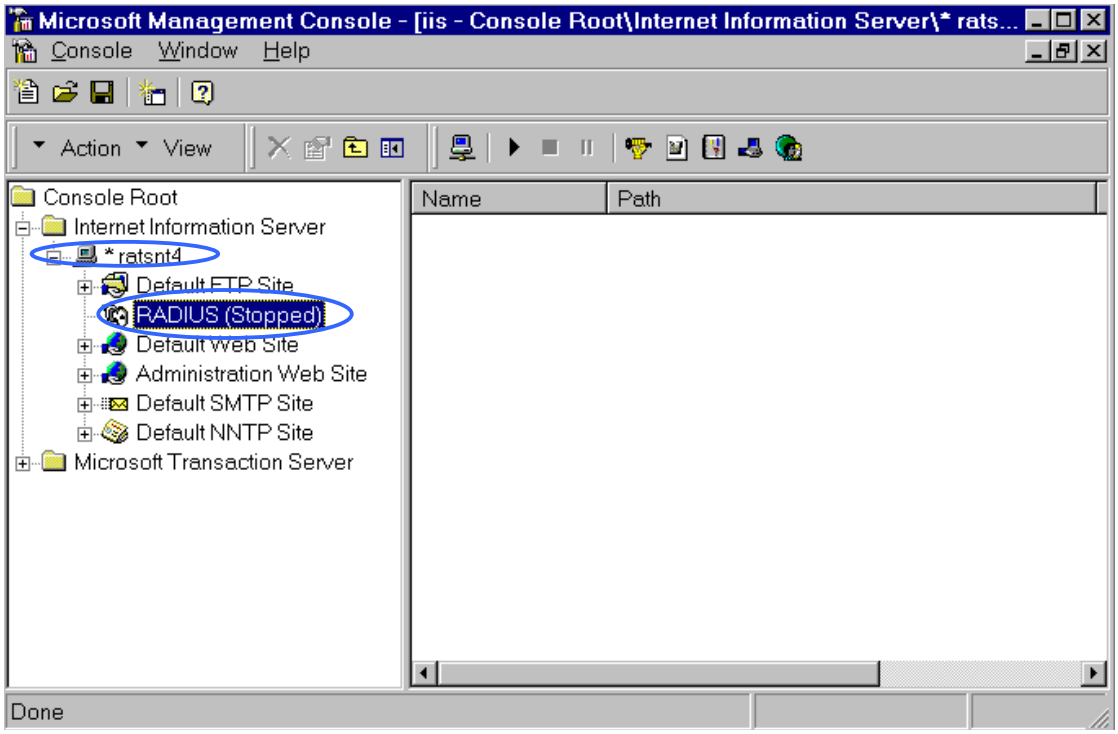
Select "OK" to save.

Set up Windows NT host

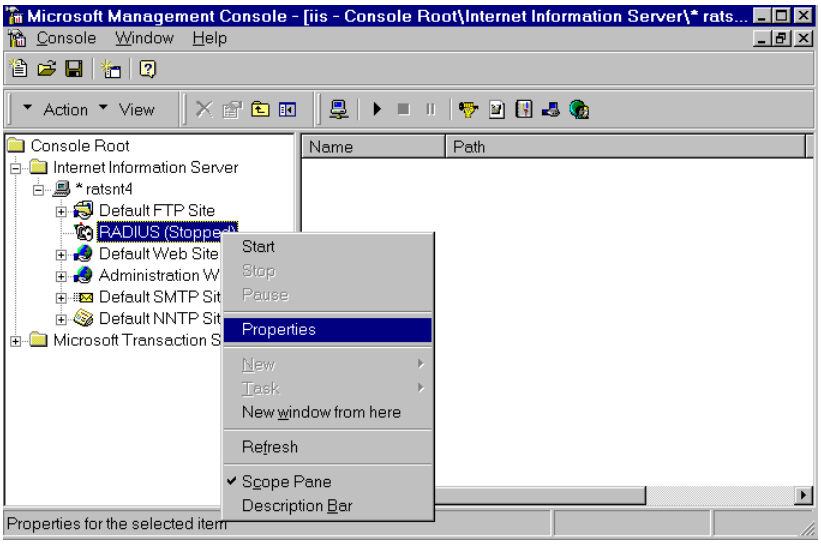
1. Install **Windows NT OPTION PACK 4.0** to Windows NT server.
2. "Start"→"programs"→"Windows NT 4.0 Option Pack"→"Microsoft Internet Information Server"→"Management Console Manger".



3. Click **"Console Root"→"Internet Information Server"** (in the left info window). Your computer's name will be visible.
4. Click **"your computer name"**, after which you will see **"RADIUS"** in the right info window.



5. Right click on **"RADIUS"** in the left info window, and then select "**properties**".



6. Select **"Service"**. Check the **"RADIUS ports".**

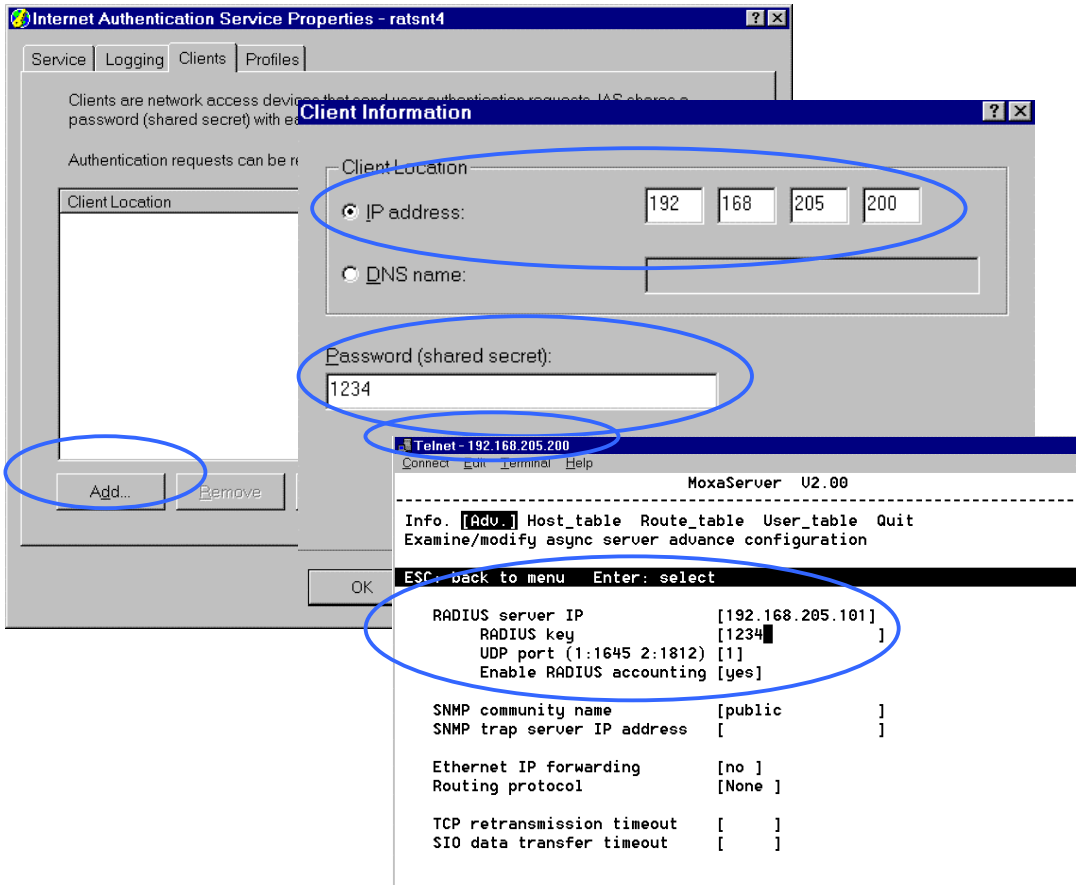
   [Authentication] 1645

   [Accounting] 1646

7. Select **"Client"**. Click **"Add"**

   Enter cn2500 IP address in **"IP address"** field

   Enter cn2500 password in **"password"** field. The password corresponds to the RADIUS key setting in CN2500 Console.



8. Click **"Apply"**.
9. Right click on **"RADIUS"** in the left info window. Select **"Start"**.
10. You will now see that RADIUS is running.