RADTAC 2000 SERVER

Radius and Tacacs Server For Windows 32bit.

(Windows 2000 - NT - 98/95)

User Manual

Media Online Italia s.r.l.

INDEX

Chapter 1

INTRODUCTION

Media Online Italia has achieved the first Radius Tacacs Server perfectly integrated with Windows 2000, 2003 or NT 4.0, which can also be used with Windows 98/95. Radius and Tacacs are authentication protocols supported by various Router producers. Ascend and Cisco produce and commercialize NAS (Network Access Server) with Tacacs and Radius authentication protocol. The features of RadTac 2000 Server are unique. The speed of validation and the security of the user's internet database are guaranteed directly by the operating system. RadTac 2000 Server validates the user using the same user database managed by Windows 2000, Active Directory, or S.A.M. for Windows NT. RadTac 2000 Server utilizes the user's Global Group settings in Windows 2000/3/NT to manage the various types of access to the network

Minimum Hardware Requirements

- Intel Pentium 3 or superior Intel processor
- 64 Mega Ram (RadTac 2000 Server uses 32 Mega Byte).
- Windows 2000, Windows 2003, Windows XP Professional, Windows 95, Windows 98, Windows NT Workstation, Windows NT Server 4.0.
- Hard Disk with 50 Mega free.
- Microsoft IIS 4,5 or 6 for Remote administration..
- Access Server with Radius or Tacacs protocol.

MAIN CHARACTERISTICS

PROTOCOL RADIUS AND TACACS BACKING

RadTac 2000 Server uses Radius and Tacacs protocols. Tacacs is very a easy authentication protocol. Individual protocol personalization is not possible. This is so it more compatible with NAS brands not supported but does not send to RadTac all the information that Radius is able to send and enhances Access Management. **Xtacacs Protocol is not provided**.

USE OF THE INTERNAL USER DATABASE OF WINDOWS NT.

RadTac 2000 Server operates through the Windows 2000, 2003 or NT Server user base. The Domain Controller is suitable ways to duplicate user information. By correctly and adequately setting up the Net resources and the number of Servers in the net, used to duplicate information, it guarantees directly the operating speed of RadTac. A large ISP, managing authentication through the Internal User Database S.A.M of Window NT or Active Directory in Windows 2000, at the adding of users will ensure a more rapid response if an adequate number of Backup Domain Controller are distinguished in the net. At the same time abovementioned BDCs constantly process the duplication of basic user data.

USE OF INTERNAL DATABASE GROUP OF WINDOWS NT.

A RadTac 2000 Server User Group has remote pre-setup access privileges. For example, User Group “Full Time” unifies all the internet users that have this particular setting. The User having a definition in Windows NT which regards also his belonging to the “Full Time” Group, has to also belong to a Windows NT Global Group with the name “Full Time”. RadTac is able to read and apply the setup not only in the Windows NT users but also in the group belonging to the same users.

USE OF ACTIVE DIRECTORY IN WINDOWS 2000 OR WINDOWS 2003.

RadTac 2000 Server permit use of active directory users database. You can generate a global group of windows 2000 for storage remote access user. RadTac control the permission of “Logon locally” for authorize the user to be access. RadTac need only that you create a Group in RadTac with the same name of the glocal group in active directory. RadTac during the logon in remote access control the login and password in Active directory, read the name of the global group and if find it authorize the access. During the logoff of the user, RadTac create the user in internal access radtac database for manage progressive log and other information. If you use RadTac in Active Directory modality, please not use RadTac administrator for add new user. You can use only Active Directory Usrr and Computer Tools, in Windows 2000 Administrative program.

USE AND CONFIGURATION DATABASE RADTAC.MDB

RadTac 2000 Server uses a standard Microsoft Access (C) database to store remote access users and carry out configurations. The internal database contains all the RadTac 2000 Server setups, work groups, users and passwords. This information when running in "Windows NT" can not be used to control access, but are nevertheless stored, so as, at any time can be used by the "Internal Database". If RadTac 2000 Server is configured in "Internal Database" mode it will no longer operate through the defined users in Windows NT Primary Domain Controller but uses the users stored on the internal database, enabling new loading via the administration interface "RadTac Administrator" or via Web with remote administration interface. The internal database radtac.mdb can also be managed independently, through personalization, by the administrator.

PROGRESSIVE DATABASE USER RADTACLOG.MDB.

RadTac 2000 Server uses a standard Microsoft Access © database, radtaclog.mdb, to store records relating to the remote access user connections. The database allows, at any time, consultation by the administrator, of a particular user's access by hour or to correct eventual errors of utilization sums so as new totals can be calculated.

USER CONNECTION DATABASE RADTACTMP.LOG

RadTac Manager Server uses the standard Microsoft Access © database, radtactmp.log, to record moment by moment user connection to the net. The Database can be visualized using remote administration or the "RadTac Display User" program.

REMOTE ADMINISTRATION THROUGH WEB PAGE.

RadTac Manager Server contains a set of ASP applications that can be used for configuration maintenance and for loading remote access users. The remote access users loaded with remote administration interface are valid both in "Windows NT" mode and in "Internal Database" mode. All the same, the applications via WEB, which are not able to add users to the database of Windows NT, in this operative mode, generates a "Temporary" remote access user, that is, perfectly operative but considered temporary because of their real existence only inside the access database. The temporary user should be transferred, by the administrator, as soon as possible, to the Windows NT user archives.

ACCESS MANAGEMENT BY HOUR, MONTH OR YEAR.

RadTac Manager Server permits management access with a maximum number of hours of access (by Month or Year).

ANNUAL ACCESS MANAGEMENT.

The access expiry date can be automatically fixed at one year from activation or a personalized expiry date can be set, either by the Windows NT expiry date or by the internal database expiry date field.

HOUR BAND ACCESS MANAGEMENT.

Users that have access exclusively at certain hours of the day, can be configured with a setup using a different access hour for every day of the week.

RECHARGE ACCESS MANAGEMENT.

"Recharge" access, is access by hour, that once used up can be automatically regenerated, using a recharge "Password" with and equal or superior number of hours. ISPs that use this type of access sell separately the recharge "Password" that can be used only once, instead of its own usual access password. The value in hours will be transferred immediately, to the user, when the "Password" is used to enter the Net

ACCESS MANAGEMENT WITH USE OF KBYTE.

Radius protocol at the end of an access session sends to Radtac 2000 Server the exact number of tcp-ip packets and k byte passed to and from the user. RadTac allows setting up and manages access with a maximum number of K byte (input+output). Once reached a maximum number of Kbyte, RadTac will block user access.

ACCESS MANAGEMENT WITH MINUTES FOR DAY.

RadTac 2000 Server permit to be management user with a max number of minutes of access in day. The user that is configured with this profile can be connect until the number of minutes is minor of the preconfigured value. After he can connect only the next day, until the number of minutes for day is used.

CONTEMPORARY ACCESS MANAGEMENT..

RadTac 2000 Server is able to manage a maximum of contemporary access by a concurrent user. The number of accesses allowed, are set by the administrator.

OPERATATING IN WINDOWS NT SERVICE Or 2000 MODE

RadTac 2000 Server has a program "RadTacSv.Exe" that allows to operate in WindowS 2000 or NT "Service". In Service mode, RadTac is able to validate the user, even if there are no users logged on Server NT. The application operates in Background (like all the other functions of the net).
RadTac 2000 Server, in Windows 98/95 mode, has another application, "RadTacS.Exe", that has the same validation function and can be reduced to an icon, during it's running, into icon tray.

TYPE OF ACCESS MANAGEMENT.

A Router frequently is able to support Analogical or ISDN connection on the same connection port. RadTac 2000 Server, allows differentiated connection management of the user on the same router port, based on the type of access used.

PORT ACCESS MANAGEMENT.

It can manage a single Router port or groups together single router ports into one type of access, assigning explicit rights of access to a group of users. In this way it can manage with the same router, various telephone line fluctuations to different PBX.

IP SOURCE CONTROL.

RadTac 2000 Server can be configured so as to run a precautionary control on the IP source of the Router that requests access. If the "IP Check" control is active, Radtac allows access only if the user comes from predefined IP Routers and also applies the setup for that incoming Router.

USER QUERY UTILITY.

The Web RadTac 2000 Server interface has a ASP (Active Server Page) for Microsoft© IIS 4,5 or 6 that allows the user to visualize in real time, with the browser, a complete list of all access to the net, the hours of connection used and in case of subscription by hour, the number of hours existing.

INCOMING TELEPHONE NUMBER CONTROL.

When using Radium protocol, RadTac Manager Server is able to manage Home subscription only from a telephone number, declared by the User when specifying their contract. RadTac Manager Server at access request, permits access only after controlling if the telephone number, of who is trying to access, corresponds with the one declared by the client. To be able use this feature you need to have a Router with a integrated Digital Modem connected directly to the primary ISDN access. As a matter of fact the incoming Telephone Number is returned from the Router to RadTac only if the telephone company is enabled for this feature.

OUTGOING TELEPHONE NUMBERCONTROL.

RadTac Manager Server allows Group User Management on the number used access the net. (OUTGOING Number is an aspect of Radius protocol provided exclusively by some preset Network Access Servers (example: Ascend Max 4000-6000 o Cisco 3600). This type of control can be very useful if on the same "Primary ISDN" there is more than one number and there is a need to distinguish the incoming calls.

TRAFFIC CONTROL (FREE AND PAID USE).

One of the most appreciated features of RadTac Manager Server is the IP Pool management in relation to the type of access that the user is classified under. With an appropriate entry which controls the band, the administrator can set band priority or assurances on the IP Pools managed by RadTac.

SENDING EMAIL TO ADMINISTRATOR.

RadTac Manager Server can also be configured to send warning email to all the net administrators. The situations in which emails are sent are: reporting of inaccessibility to the Internal work Database; serious program malfunctions; warning of remote connection time length that could have been left hanging

because of error in the user connection list and access attempts to the net by users that exceed the limit set on the concurrent user.

SENDING EMAIL TO THE REMOTE ACCESS USER.

RadTac Manager Server can be configured so as to send email to the remote access user. The emails can be sent in close proximity to the expiry date of access and with wishes of "Happy Birthday" in the vicinity of date of birth of the access holder.

PAP & CHAP MODE SUPPORT.

RadTac 2000 Server has both PAP and CHAP Async Mode. The use of CHAP is allowed exclusively if the application operates in "Internal Database". In "Windows NT" Authentication mode CHAP can't be used because the password saved by Windows NT are in crypt and because CHAP also works in crypt mode. In the last case RadTac 2000 Server is unable to run a control of the password because both sides, NAS (Network Access Server) and Windows NT use a strong authentication algorithm on only one path.

PAP can be used in either "Internal Database" and Windows NT Authentication.

AUTOMATIC HISTORICIZZATION MONTHLY.

RadTac 2000 Server do a automatic historicizzation of the database progressive log for remote access user. This operation are recursive and create a single month database in directory c:\radtac\data\history. The administrator with repair and compact procedure do a compact database of work.

Trial Release & Full Licensed.

RadTac 2000 Server is released on our Web Site in Shareware http://www.radtac.com. RadTacXXX.exe, it is the only file that needs to be downloaded, it included four (4) executions. In the Trial Release there are six (6) executions. The definite release can be downloaded directly from the site after payment of the User licence.

Limitations of the Trial Release

After installation the trial release has a maximum operating period of 30 days. This Trial Release should be configured and tested with your own Access Server. At the end of the 30 day trial period the application will shutdown without prior notice. Once the trial period has expired the application will not start up again, however when passing to the Full Release reinstallation is not necessary. If you decide not to purchase the application removal is possible without any consequences to the host Server.

All functions except the execution from Windows NT “Service” is possible. The application that will authenticate users, during the trail period, should be used on the Window’s Desktop.

Purchase of RadTac 2000 Server Full Licensed.

RadTac 2000 Server is distributed by Media Online Italia s.r.l. and other distributors in all the world. To find your nearest distributor, please consult our web site: http://www.radtac.com.

For further information, regarding the purchase of this product, talk directly to the distributor of the Trial Release.

Chapter 2

INSTALLATION

RadTac 2000 Server includes:

- N.1 "RadTacXXX.exe" , containing the software;
- N. 1 operations guide.

To install the program onto your hard disc follow these proceedings:

A) Turn on computer and wait for loading of Windows 2000/3/NT, Windows XP Professional or Windows 98/95/ME.

B) Run Windows Explorer and find the RadTacXXX.exe fine, XXX indicates the release number.

C) Double click on the file to start.

D) Follow the instructions as they appear on the screen. This procedure will automatically transfer the programs from the CDROM to the Server's Hard Disk.

Chapter 3

PLANIFICATION

At the end of the installation there is no need to restart the system. However, the first thing you must do is start the “RadTac Administrator” Program.

RadTac Administrator.

RadTac Administrator is the procedure that configures all the RadTac 2000 Server functions.

RadTac Schedule.

RadTac Schedule is the procedure that records all the control functions of the IP Pool that have been set on the Router. It also, sends email to the administrator and to remote access users. The program has been created to operate both in Desktop, automatically started by RadTac Service, and in Windows 2000/3/NT Service.

RadTac Display User.

RadTac Display User is the procedure that displays, moment by moment, the user that is connected to the net. This program is useful for supervising.

RadTac Display Status.

RadTac Display Status is the procedure that displays the dialog between the Router and Radtac 2000 Server. This function works, exclusively when RadTac 2000 Server is operating in Windows 2000/3/NT “Service” mode. RadTac Service executed from the Desktop has the same functions as “RadTac Display Status”.

RadTac Service.

RadTac Service is the “Desktop” procedure that manages the dialog with NAS, it and the Radius Tacacs Server. Radtac Service validates remote access user, applying all the configurations set by RadTad Administrator. The application operates on Windows Desktop and can’t be used as “Windows NT Service”. To authenticate a user he must always be active on the Desktop.

If the product is not a Trial Release, it is advisable not to use the program in “Windows NT” domain, but to use “RadTac 2000 Service”. “RadTac 2000 Service” has the same functions as “RadTac Service”, without the need to run the program on the Desktop.

RadTac Start-Stop.

RadTac Start-Stop is the RadTac 2000 Server procedure that installs, starts and stops the Windows NT Services that involves RadTac.

RadTac Emergency.

RadTac Emergency is a utility application. Not being available in the trail release, in emergency conditions, it has the functions of Radius Tacacs Server, that is when there isn’t an internal database. RadTac Emergency is useful especially when there is a need to reorganize and compact the RadTac Manager internal database.

Preliminary Setup

OPERATIONS MODE

Firstly, you must select a operation mode for RadTac 2000 Server. RadTac 2000 Server can operate in 3 ways, "Internal Database", "Windows NT User Database" or "Windows 2000 Active Directory".

INTERNAL DATABASE.

"Internal Database" mode is the best operations mode when using the Windows 98/95/ME operating system. It is, all the same, frequently also used in Windows 2000/NT domain. When using this mode RadTac 2000 uses, as its only resource, its internal database. The remote access user has to be defined directly by RadTac Administrator in the RadTac MDB database.

The RadTac.MDB Database, in c:\radtac\data directory, contains ALL operations data concerning both the remote access user and the configuration setup.

By using "Internal Database", you can use remote connection either in CHAP or in PAP, a drawback to this type of connection is that it is subject to slowing down, especially if there are more then 10.000 active users. This database can reach a considerable size and authentication as a result can showdown a little.

WINDOWS NT USER DATABASE.

"Windows NT User Database" operations mode is used only in Windows NT domain. It allows, through Windows "User Manager" the authentication of definite users.

Windows NT, Domino users, managed by PDC (Primary Domain Controller) and by BDC (Backup Domain Controller) are themselves remote access users managed by RadTac Manager Server. The advantage of this mode is in the grated of this solution. It is sufficient to stick to the Microsoft specifications, in regards to the number of BDC Server and the number of users to improve RadTac performance. In this mode RadTac Manager Server operates with two difference filters. The first, regard the setup made on the Serve NT; expiry date, weekly hour groups, user type. The second, regards the setup made in RadTac Manager Administrator; number of hours, allowed nets etc. etc. RadTac Service first executes a "LogOn Locally" of the remote access users, controlling the Login and the Password set in Windows NT, immediately after, it controls on its internal database successive procedures to then, if in accordance, allow entry of the user. It is sufficient that one of the specifications is not correct that RadTac refuses access to the user.

WINDOWS 2000 ACTIVE DIRECTORY MODALITY.

"Windows 2000 Active Directory" operations mode is used only in Windows 2000 and 2003 active directory domain. It allow, though Windows Active Directory the authentication of definite users.

Server Windows NT Configuration

If RadTac Manager Server is to be installed in Windows NT mode, through the "User Database" of Microsoft Environment , some configurations of the operating system have to carried out. The program can be installed on the Serve NT, even in "Internal Database" mode. In this case, the configurations changes detailed in this section need not be made.

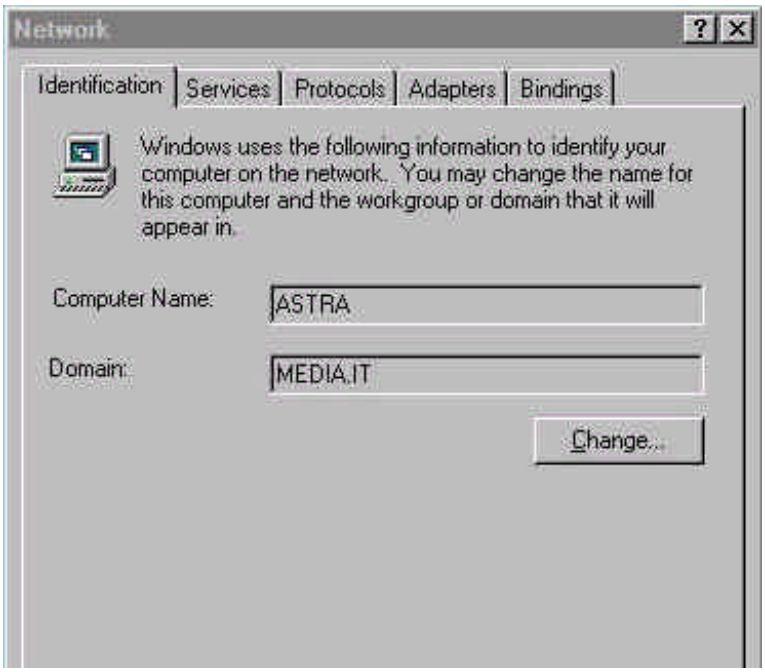
PRIMARY DOMAIN CONTROLLER, BACKUP DOMAIN CONTROLLER.

RadTac Manager Server can be installed on any NT server that is part of the Microsoft Domain, whether it is a PDC or a BDC or on any Standalone Server, just as long as it is part of the Microsoft Domain.
RadTac Manager Server, during the authentication of a user, executes a common Domain Logon. The Logon can be done on any Server. It is for this reason that the Net Administrator can install the product on the desired Server, either Windows NT Server or Windows NT Workstation. The product has been also tested, with success, in Window2000 Enterprice and Professional.

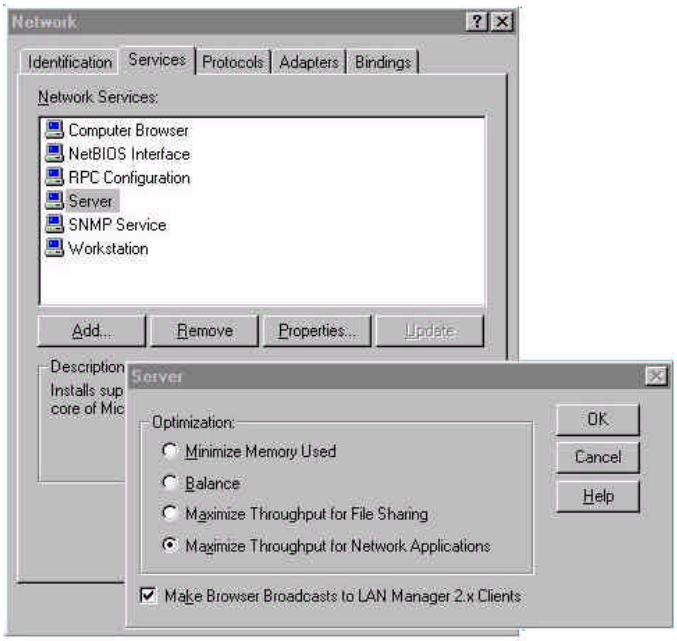
WINDOWS NT NETWORK SETUP.

Open Control Panel and execute Network Setup.

At end of RadTac Manager Server configuration it is important to that you know the net Names of the PDC and BDC Server, and the Microsoft Domain Name. This information can be acquired by executing the following operation on all the PDC and BDC Server present in the Domain.

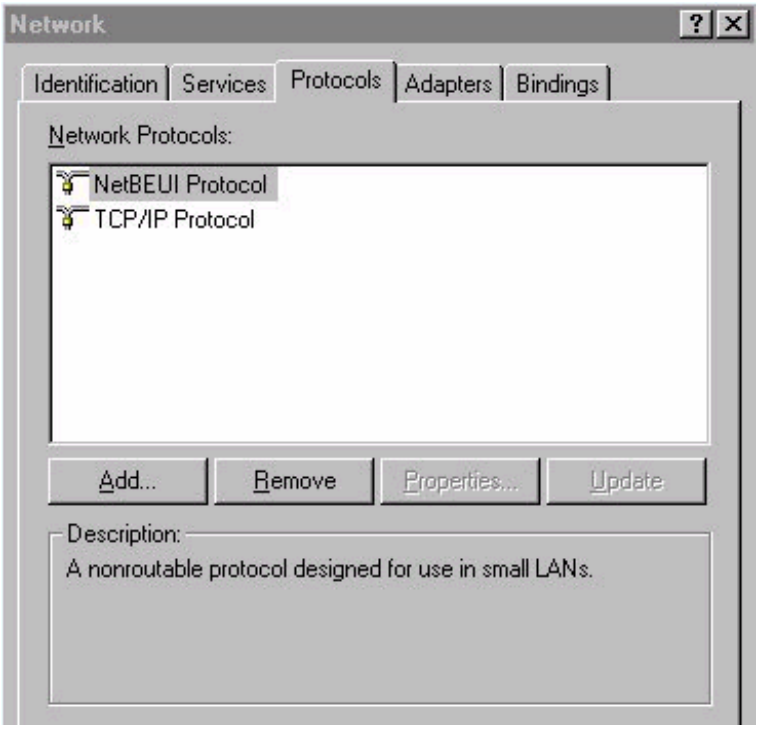


The information is in the "Identification Folder". Example: Computer: ASTRA Domain: MEDIA.IT. Move onto the 'Services' folder and click twice on 'Server'. Once open, select in Optimization: 'Maximize Throughput for Network Application' and the check box 'Make Browser Broadcasts to LAN Manager 2.x Clients'.

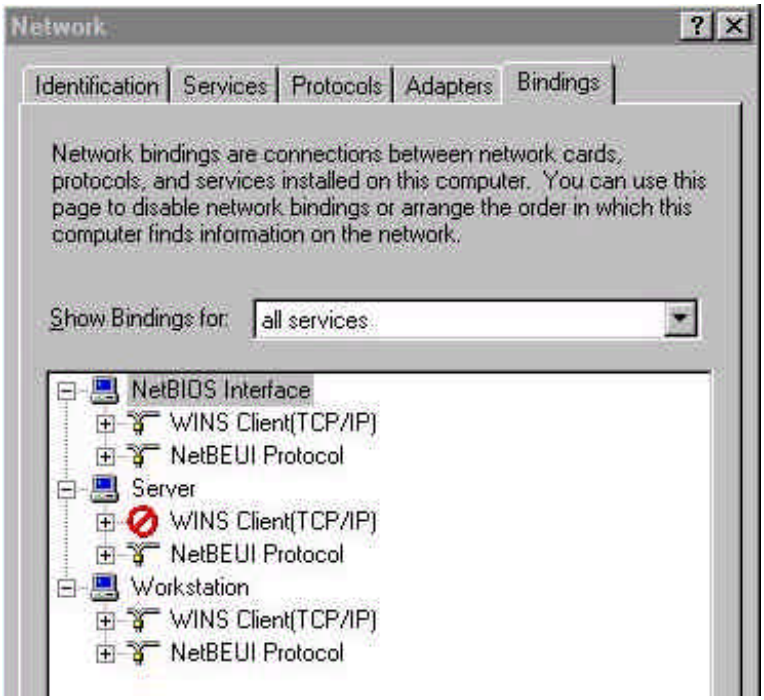


Now move onto "Protocols". The two installed protocols are TCP/IP and the NetBeui. The NetBeui protocol is recommended because RadTac Manager Server needs to use NetBios on NetBeui. Tcp/IP, and can be used exclusively, leaving the

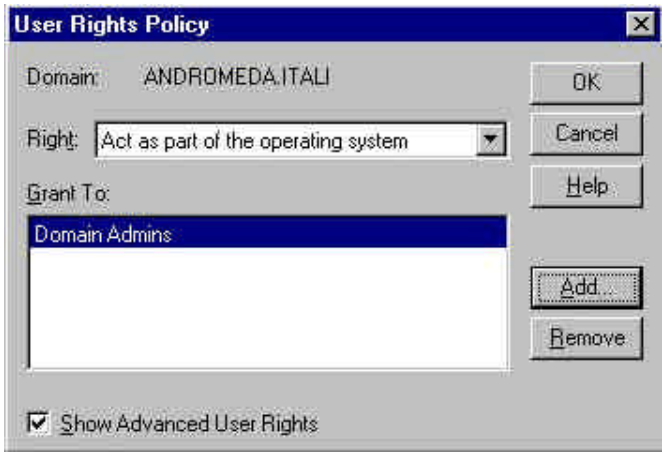
NetBios on TCP/IP. This, however is not recommended for security reasons. NetBios on TCP/IP allows the possibility of sharing on the internet net.



Move onto the 'Bindings' folder and compare what has been installed on your computer with the illustration below. The WINS protocol is STOPED only in the Windows NT SERVER. The NetBIOS protocol standard and also the Workstation is active. This same configuration is recommended on all the NT Server existing on the net. Configuring in this way ensures major security on your Server and at the same time you have correctly configured RadTac Manager Server.



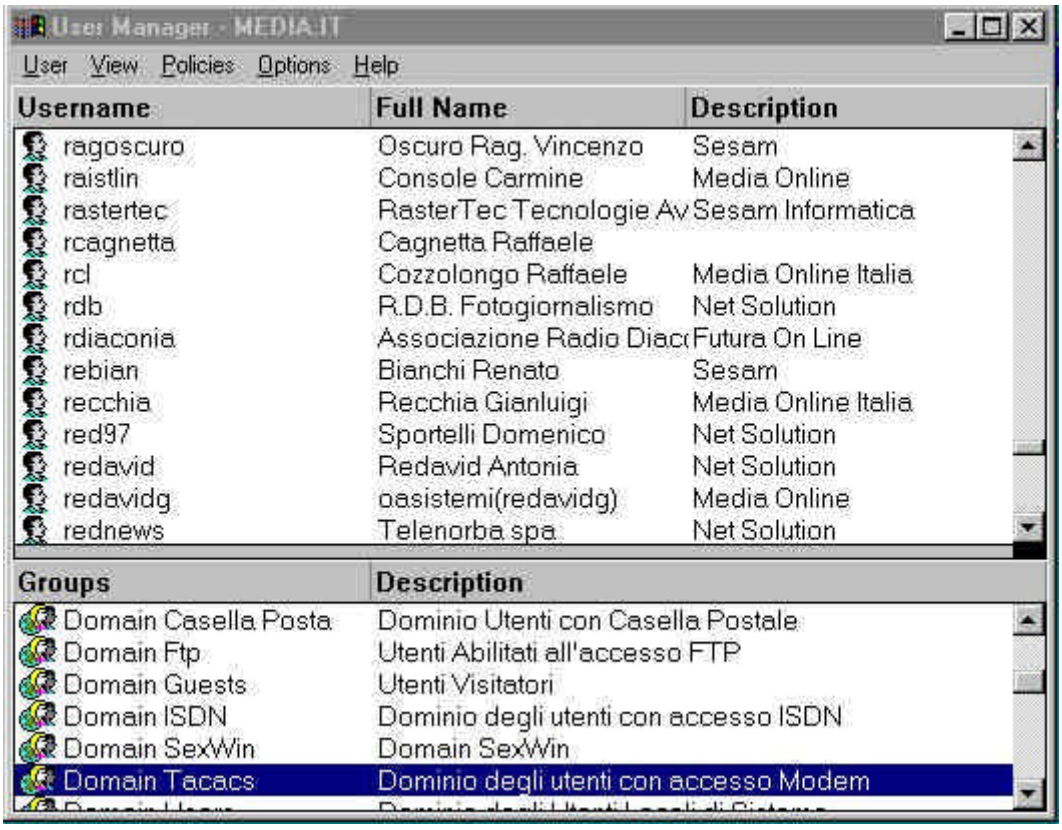
A final control of Windows NT has to be made. Open User Manager in Windows NT and select 'User Rights Policy'. Control, as shown below in the illustration, that in 'Rights', 'Act as part of the operating system', has been inserted in 'Domain Admins' and/or the user that will execute on the desktop 'RadTac Service', (administrator logged).



Execute a Startup of the System.

Windows NT User Manager

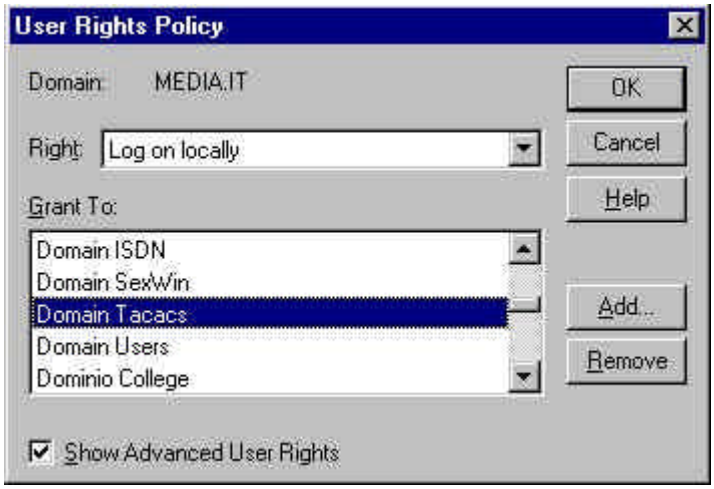
If "Windows NT" operating mode is to be used the remote access user has to be inserted with User Manager for Windows NT Server Domain. The user that has to be authenticated has to belong to one specific Global Group.



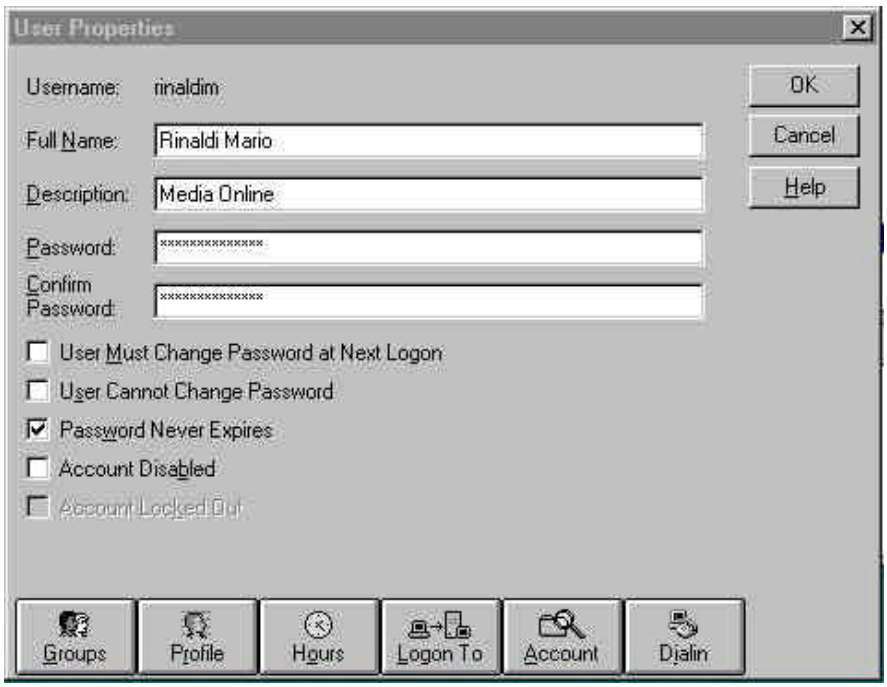
RadTac Manager Server uses the relationship of a user to a Global Group to manager him with major detail in his database. The RadTac Manager Database is not essential for the running of the program. It is preferable that a base configuration is setup and examined thoroughly, and at a later date apply the same procedure so as to manage various and more complex types of users.

1. Generate A Global Group of Windows NT example “Domain Tacacs”.
2. Select from the “Policies” Menu “User Rights”

Look for in the List-Box Right “Access this computer from network” and click on “ADD”. Select “Domain Tacacs” as soon as it is created and confirmed.



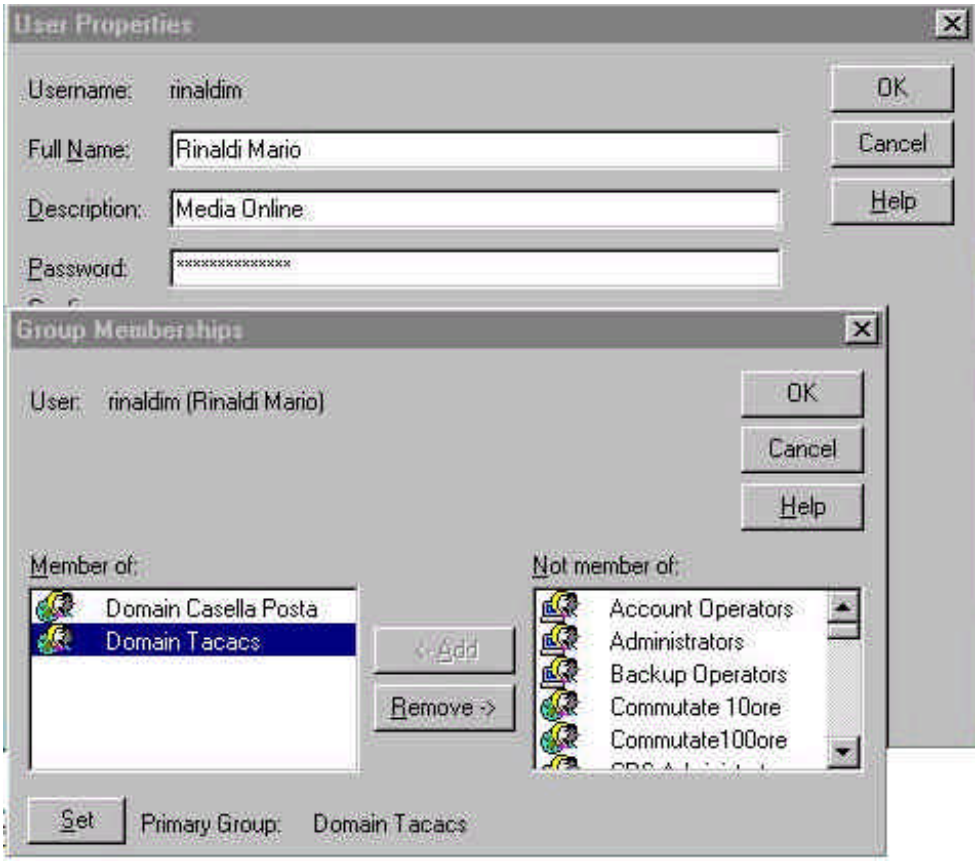
Look for in List-Box, Right “Log on locally” and click on “ADD”. Select again “Domain Tacacs” as soon as it as been created and confirmed. Click on “OK” to end the setup of User Rights policy.



1. To add a new remote access Windows NT-RadTAC Manager Server user Select “User” from First Curtain Menu, the option “New User”.

2. The “Username” is the same at the Login of Remote Access. The Password is used during remote access connection. Control with attention the Check Box keeping the same setting as illustrated above.

3. Click on “Groups” to select the related user Group. Select “Domain Tacacs”. It is with Related Group, that RadTac Manager Server connects the Windows NT server to the remote access user. A User can’t belong to more that one Group defined in RadTac Manager Server. More that one Windows NT Group can be assigned to the single user, but only one of the groups can be defined in RadTac.



4. In the above illustration you can note how the user belongs to TWO Groups, one Group related to RadTac Manager Server, and the other to the electronic mail program.

Windows 2000/3 SERVER.

RadTac 2000 Server can be operate in Windows 2000 o 2003 Server modality, using active directory as base data of the remote access users.. To be use this modality you will be prepare the operating system.

PROMOTE SERVER 2000 TO DOMAIN CONTROLLER.

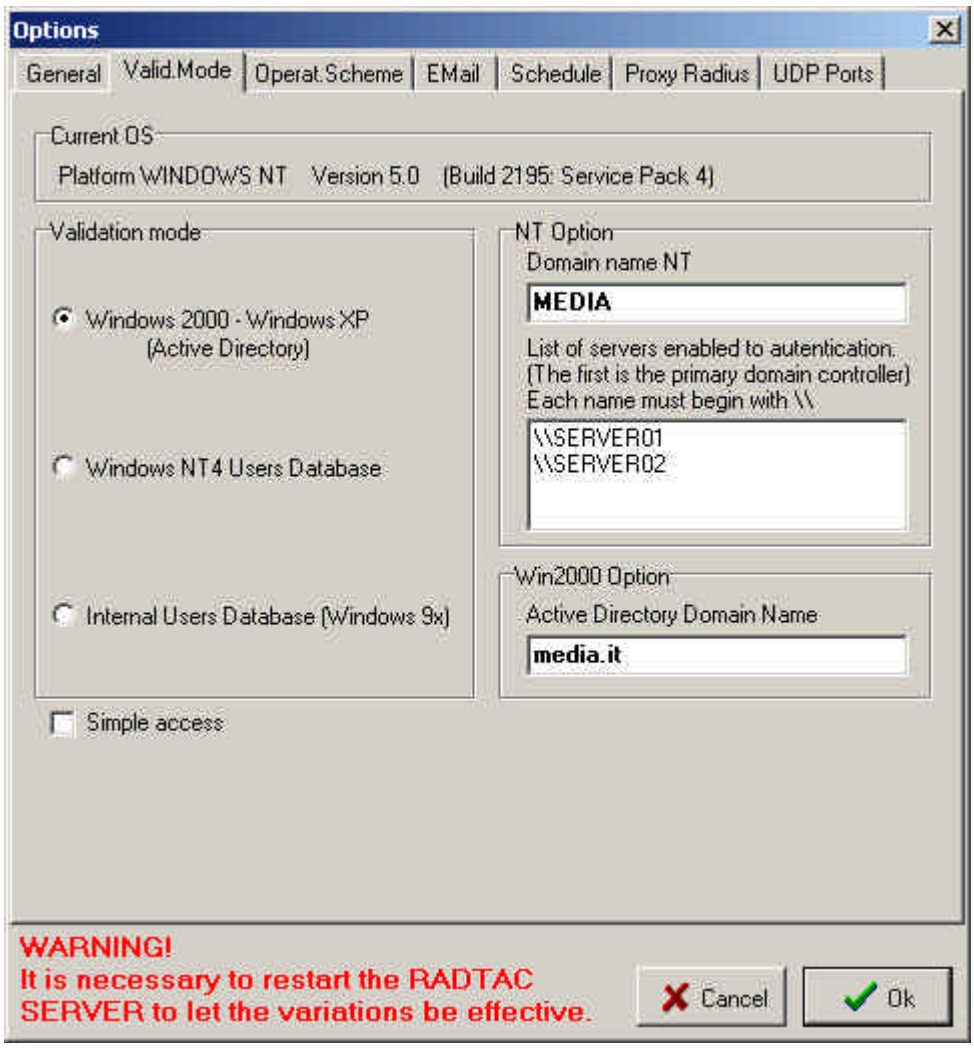
The Windows 2000 basic install procedure not promote the server to domain controller. Active directory is not operational after the first installation. RadTac 2000 Server use the Active Directory user database. Are required this step:

1. Click on Start.
2. Select RUN.
3. Type “dcpromo” and press carriage return.

Now the server display a wizard step procedure for implement active directory. Is important the name that you type for NETBIOS Name and Active Directory Domain Name. This parameters are required in option of RadTac Administrator.

SETTING OF RADTAC IN MODALITY WINDOWS 2000.

Run program “RadTac Administrator” and select “Option” and “Validation Mode”. You can look the next print figure:

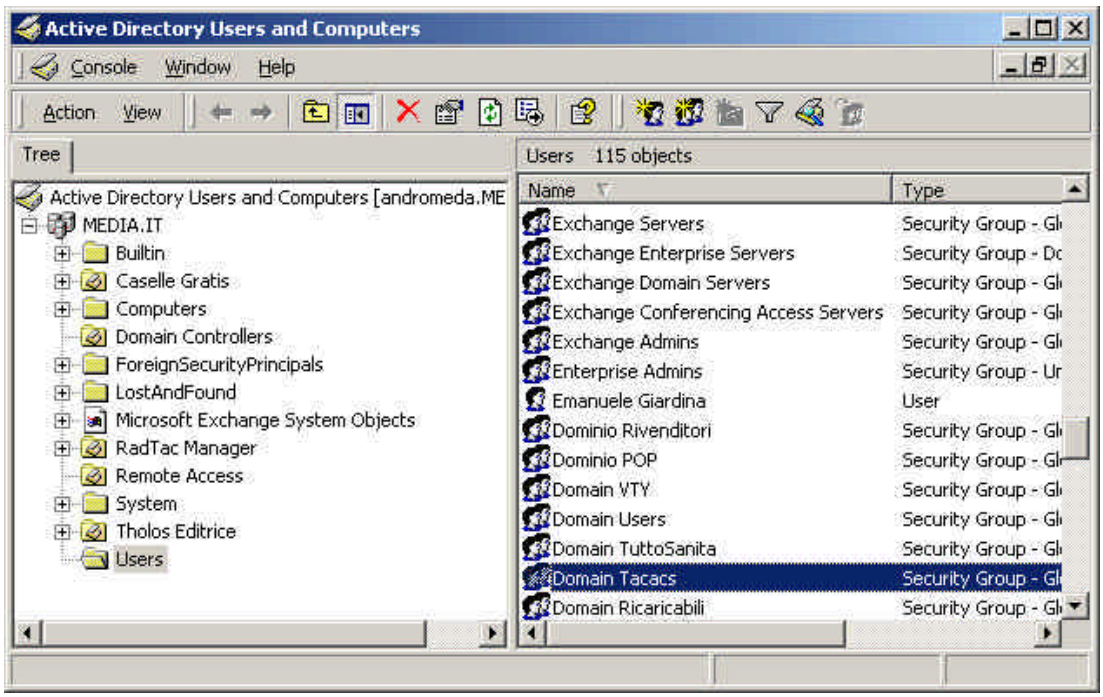


Select the Windows 2000 Active Directory modality and type the value required.

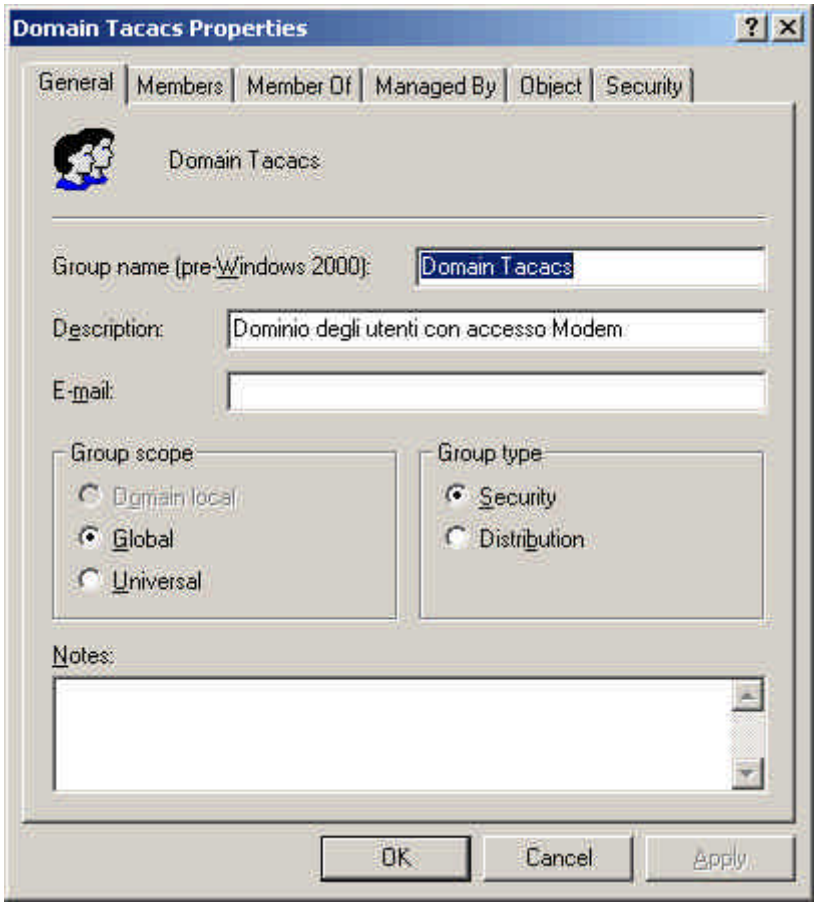
a) Domain Name NT is the name NETBIOS of the Domain Active Directory generated.
b) Type the name of the server Domain Controller of the network. If you have more Domain controller type the name with return carriage, as you look in the up figure.
c) The name of Active Directory is required, it can be different to the netbios name.

ADD A NEW GLOBAL GROUP IN ACTIVE DIRECTORY.

After that you select the modality “Active Directory” is required the you create a new global group with the Windows 2000 administrative tools. In the folder “Administrative Tools” you can run the tools “Active Directory User and Computer”. This tools permit to management the group of Windows 2000 and permit to add a new user, valid also for RadTac Server.



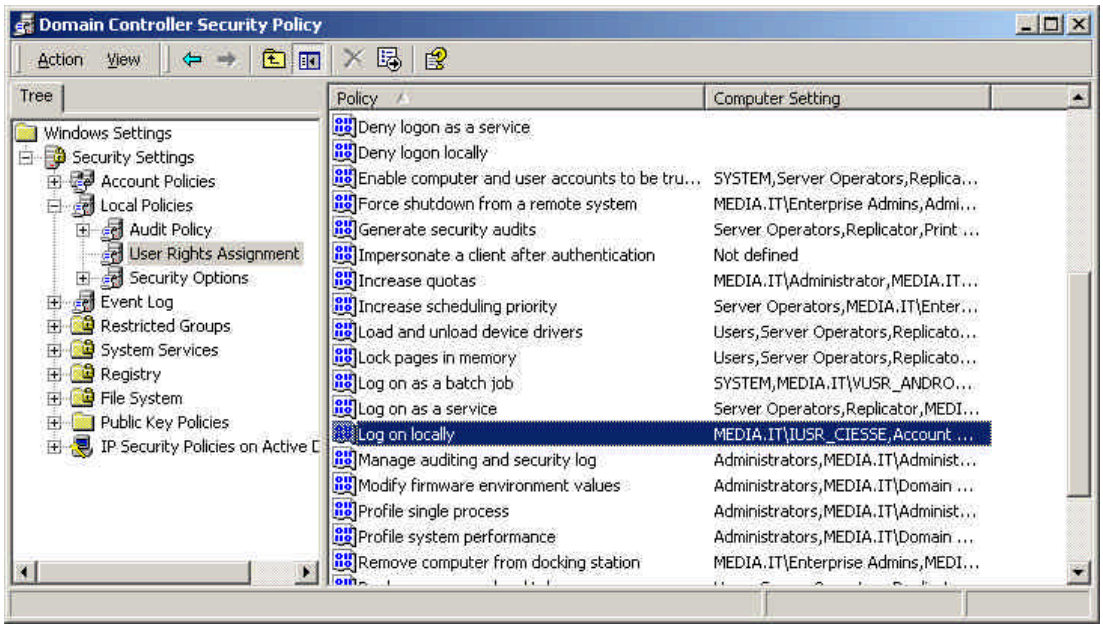
Now you can create a New Global Group (sample Domain Tacacs) .



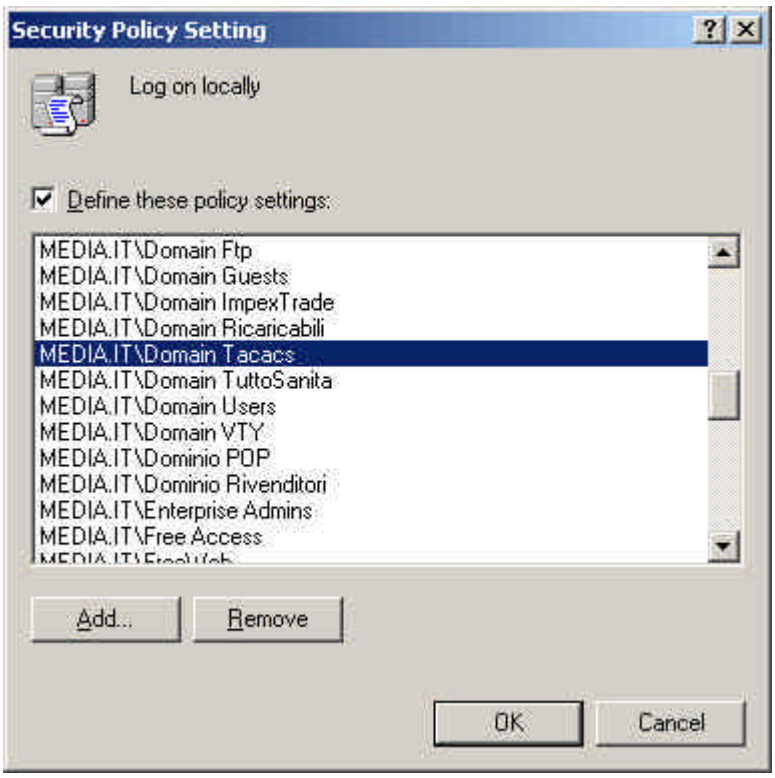
The name of the Group is important. RadTac use the twister name of the group, RadTac group and Active Directory Group for match the user in the group and apply the setting.

POLICY.

Now open the program “Domain Secuty Policy” in Administrative Tools of Windows 2000 or if RadTac is installed on Domain controller server “Domain Controller Security Policy”.



Select now the policy “Log on Locally” and add new value to this policy. You will be add the new Global Group created. For permit the remote access is important this policy because when radtac try a login use this policy.



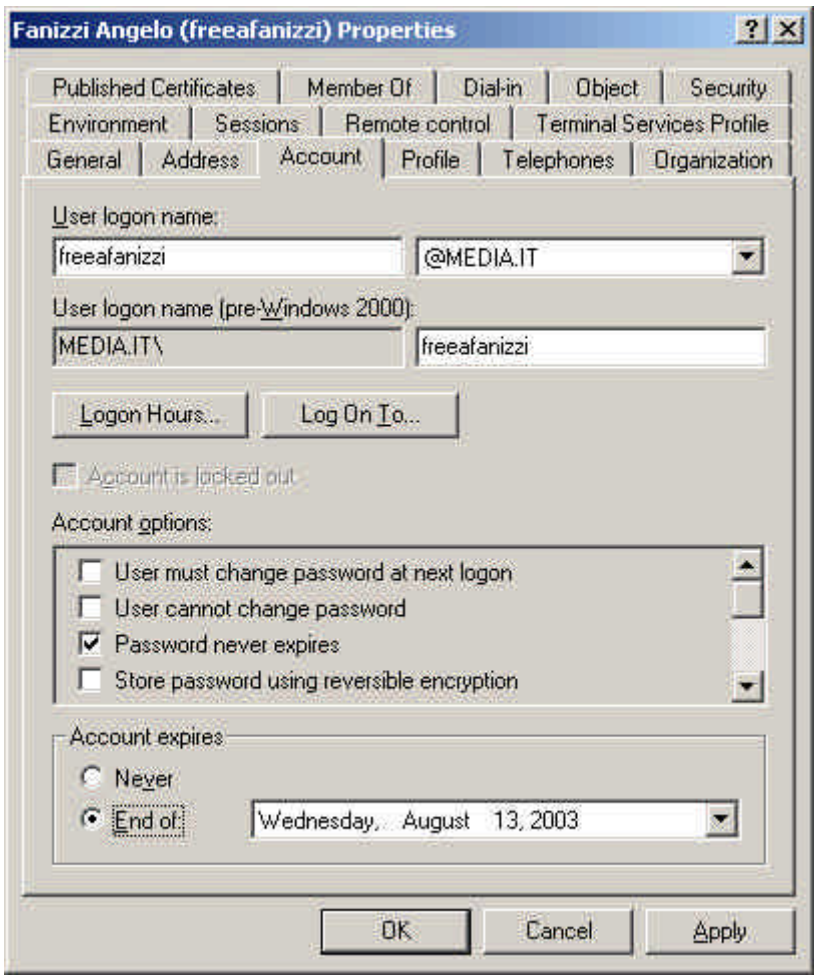
As you can look in the image display up, to the policy “log on locally” is be add all the Global Group that required remote access permission. This setting tell to the operating system that the user of this group can logon in Windows Domain. It is necessary for RadTac.

When you add a new user in Active Directory do more attentino to deactive Termina Server check box. The login and password that you create have logon locally permission and if also Terminal Server permission is enabled the user can be try logon via terminal server.

USERS OF WINDOWS 2000.

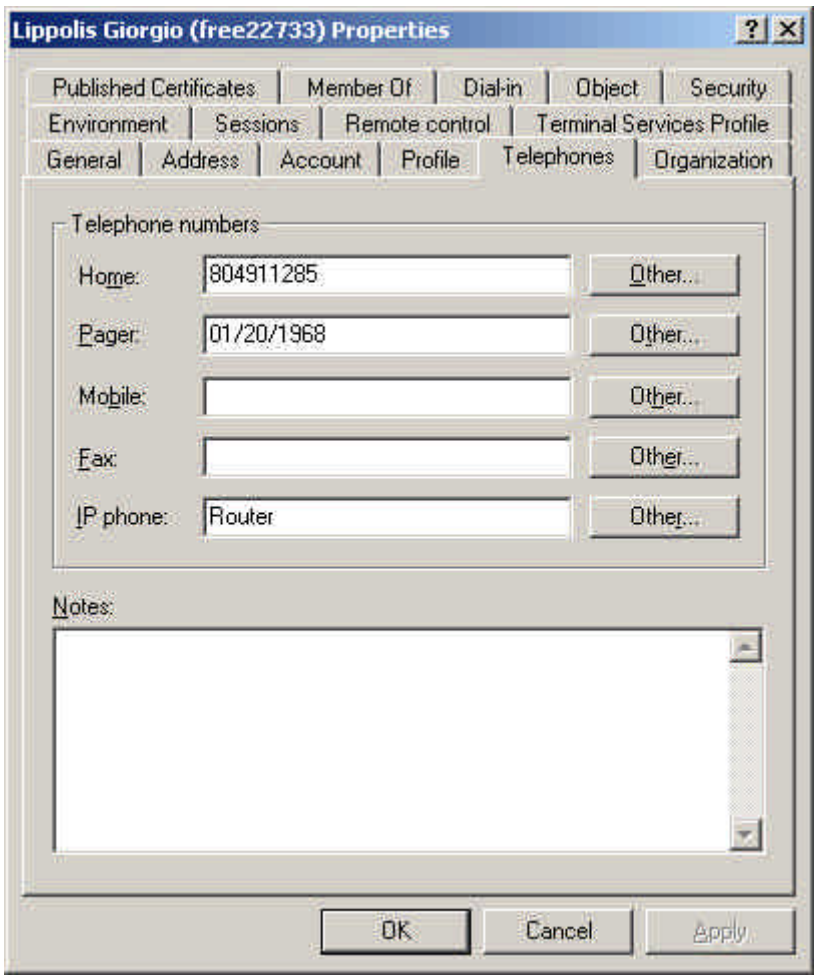
Always with Windows 2000 Administrative Tools, “Active Directory User and Computer” you can add a new user. The new user after the first attempt of Radius Logon will be copied in RadTac Database automatically.

The fields managed from RadTac are:



1) “User logon name” and “User logon name (pre-windows 2000)” are two fields with value twisted and contain the remote access login.

2) Account Expires. This is the expired date of the remote access. After this date RadTac reject login.

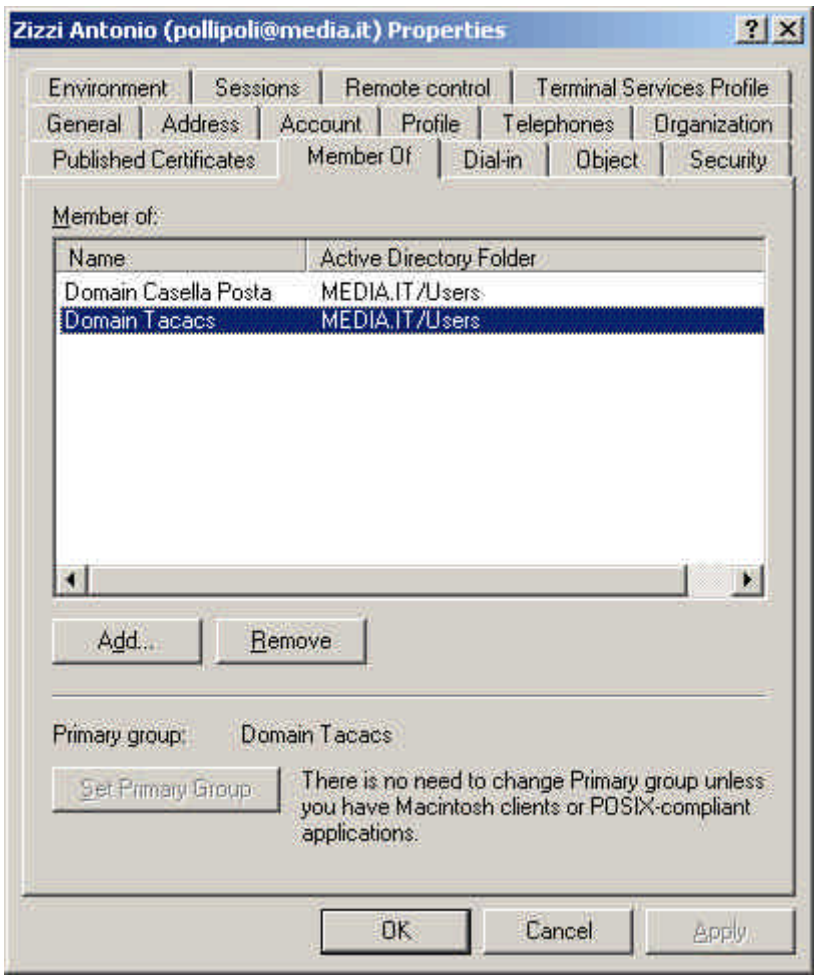


In the section “Telephones”, in the user form is possibile to be define the next specified value.

Home – In this field you can put the Telephone Number from witch the user can be access. This is the user telephone number.

Pager – In this field you can put the date of burn of the user. If you put this date RadTac can send birthday email message.

IP Phone – In this field you can put the static ip address for remote access or the value “Router”. In case you put IP Address, RadTac send it at the request of access. The user can be access only with this value. In case you put the value “router” as in sample, RadTac not assign any ip address and demande to the NAS this operation.



In the section “Member of” you can select the group assigned to the user. This operation is import because RadTac match the Name of the Active Directory Group Name with RadTac Group Name. Is important that the name of the Goup is identical to the RadTac Group Name. If you not have the same Group Name create a new group in RadTac with the twisted name.

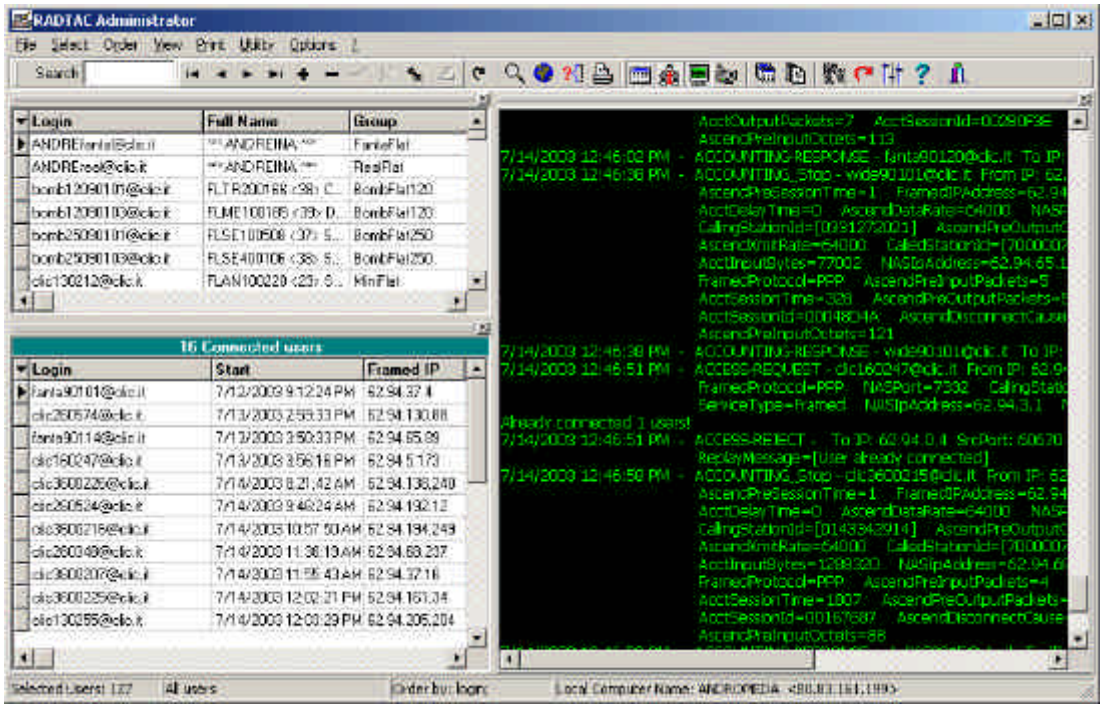
RadTac when receive a new request of remote access from the router do a query in Active Directory with login and password. If match look the Group in Active Directory and search in RadTac database this group. Now applied the RadTac feauture configured in group and if all is ok authorize the remote access. This procedure is simple and full of message help, in RadTac Log.

Chapter 4

CONFIGURATION

Only after having setup the configurations of RadTac Mananager Server it is now possible to proceed. If RadTac Manager Server is used in “Internal Database” mode it is possible to configure the application from this point on, consulting the guide.

- Execute “RadTac Administrator”.

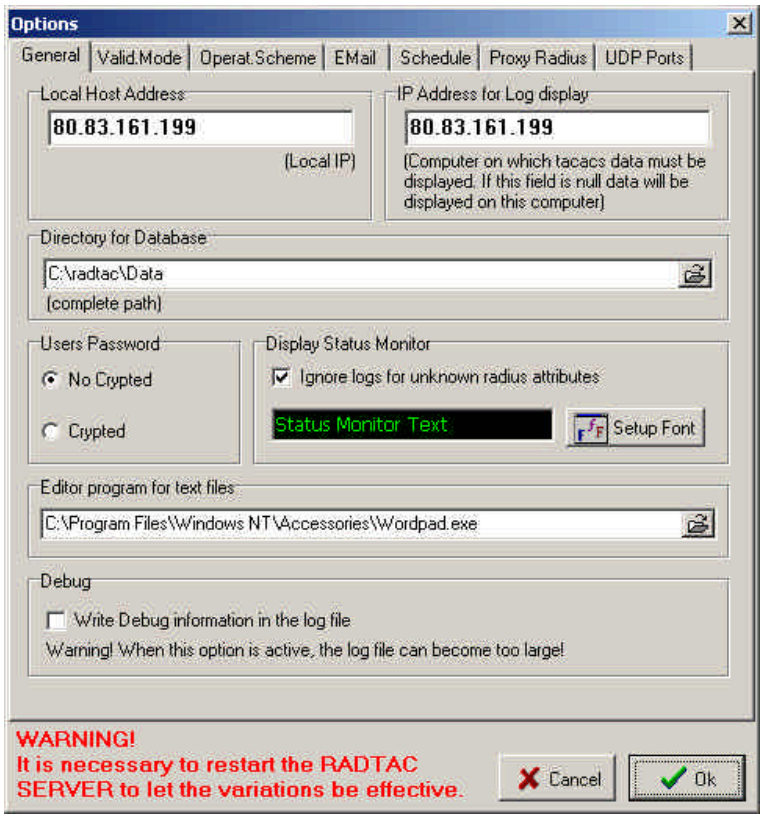


- Click on “Options” and select “General Option”

OPTIONS

General

- LocalHost Address is the IP address of Server Windows on which RadTad Manager Server has to be run. It is possible to automatically buy the IP address with the “Default IP” key. This is allowed with this release of the software licence. It is advisable to keep an IP Address in your own net and to assign it each time to the RadTac Manager Server. In this way the Licence can be moved from one Server to another.
- Ip Address for Log Display is the IP address of Windows Sever and has to be redirect the output of monitoring of the athentication system.
- Database Name contained the complete path of the Internal Database used by RadTac Manager Server to memorize the register “by hour” and the configurations.
- Users Password allows to select the way the password is memorized in the internal database; if in crypto or in clear. If the internal database already contains users, selecting the check box it is not sufficient to change the selection from one to the other. After having changed the type of password it is necessary, using the appropriate entry in RadTac Manager Administator, to convert the password.



- Ignore logs for unknown radium attributes inhibits the visualization in the logs of the Radium attachments non managed by the application. This selections is useful when, during NAS → Radius Server dialog, irritating warning messages are visualized about NAS attribute properties. In Defualt this check box is selected.
- "Write Debug Information in the log file" permit to enable the RadTac Debug. This option will be enabled only in rare case because it increase the log traffic and storage file. It is necessary in case RadTac not work fine and you need find the error. Debug information is storage in c:\radtac\data directory in RadTac??????.log file, with all the login log procedure. It archive all subroutines begin and exit.

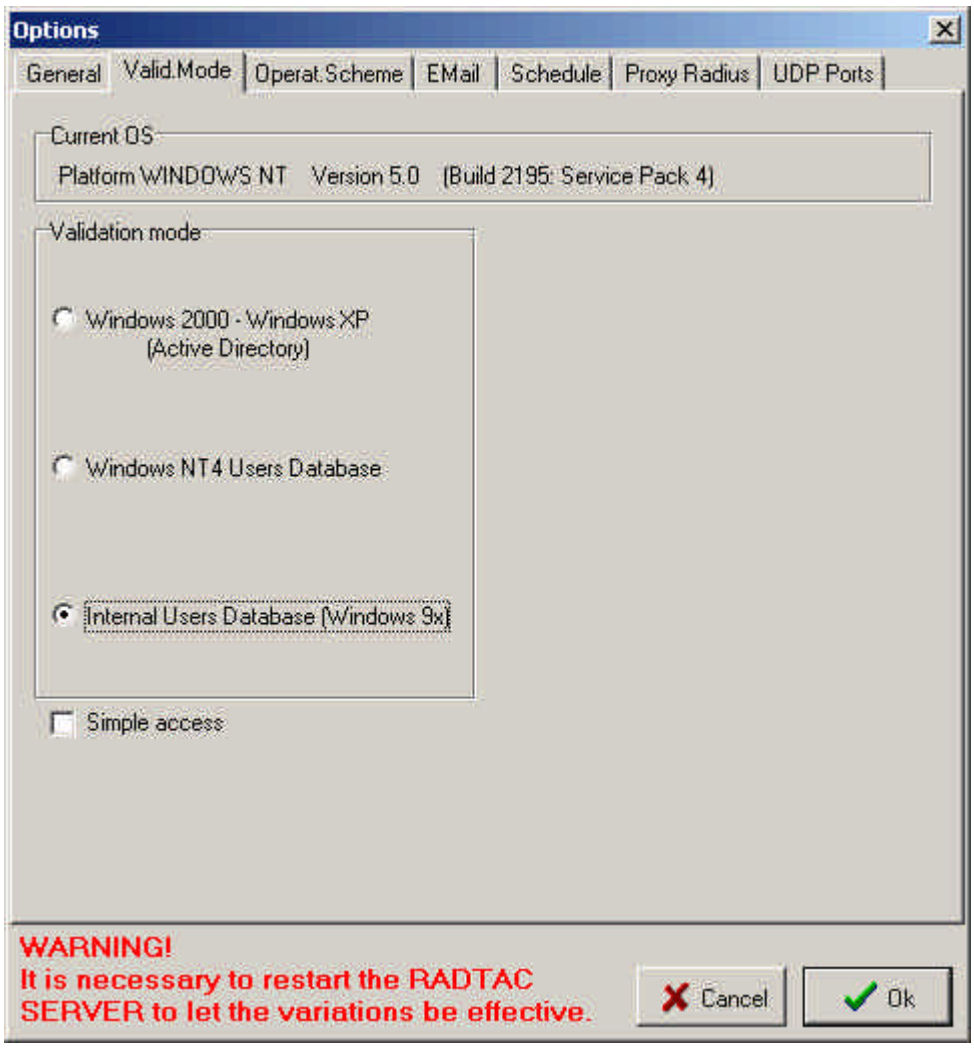
Validation Mode

WINDOWS NT USER DATABASE.

Selecting this operations mode, RadTac Manager Server authenticates the remote access user checking access through the Primary Domain Controller of the net and the Backup Domain Controller. Refer to the section "Pianification" of this manual for the effects of this mode.

- Domain Name NT.
  In this field the name of the Microsoft Domain © to which the RadTac Server belongs to has to be defined. We have noticed that frequently system administrators mistake the NT Domain with the Internet Domain of their own company. The Microsoft Domain © and the NetBIOS Domain of the Net and not the DNS domain of TCP/IP.

- List of Servers Enabled to Authentication.
  In this field Memo need to indicate all the NetBIOS names of the Microsoft Server © PDC and BDC of the net. Server Standalone can't be described. All names must begin with "\\".



INTERNAL USERS DATABASE (WIN95/98).

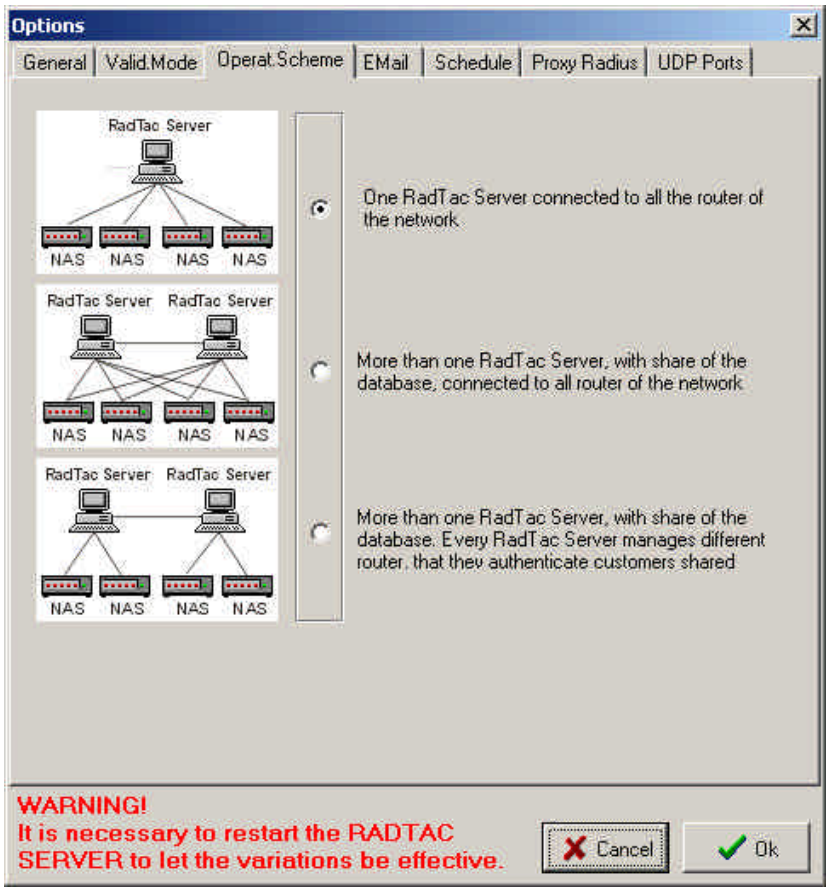
This mode is decisively easier to configure, even in Window NT domain. It is the only operations mode needed if the product is installed in Microsoft Window Windows 98 © or Microsoft Windows 95©. Refer to the entry “Planification” of this manual for further details.

WINDOWS 2000.

In this mode RadTac use the Active Directory of Windows 2000 or 2003 to store and autheticate the remote access users. The user create in Active Directory will be copied in local database of RadTac after the first successful attempt of access. Please read this manual in module of Planning.

Operational Scheme.

In this form you can select the type of installation of RadTac.



In **First option** you can define the “Single Installation”. You can select it if your have only one RadTac Installation.

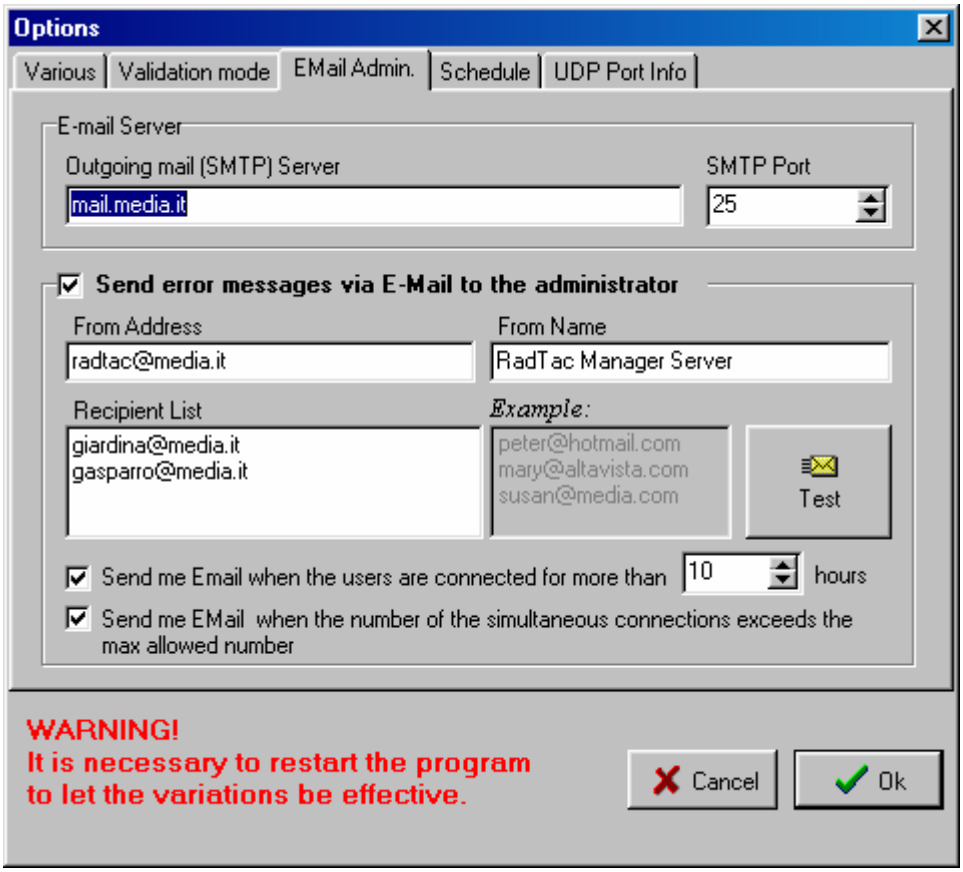
In **Second option** you can define multiple RadTac installation “All to All”, All Router to All RadTac. This installation is choised when you want a backup radius configuration. In all Router you put first and second ip radius, the same ip. All to All.

With the **last modality** you have many router and many RadTac, but the radius traffic are distribute on it. This modality is used from all the ISP, Internet Service Provider, that want distribute the radius traffic, if authentication’s traffic is high.

Email Admin.

Selecting the check box “Send error messages via E-Mail to the administrator” RadTac Manager Server will send informative email to the net administrators.

- Outgoing mail (SMTP) Server.
  Filling in this field with the DNS name of the out-mail Server, will enable RadTac Server to send email to the net administrators.
- SMTP Port.
  Number of the electronic mail Server tcp/ip ports. The default value is 25.



- Recipient List.
  Fill in the net administrator’s email addresses, so as he can receive information messages.
- Send me Email when the user are connected for more than ??? hours. By selecting this check box RadTac, Manager Server will send email messages recording all users that are connected for more than ??? hours. This selection is useful to the administrator because it highlights all users that are connected for more than a certain number of hours. These users could be, in fact, disconnected by the net, but results connected because of eventual lose of dialog data between NAS → Radius Server. When using maximum number of users connected, the user could have problems connecting. The administrator once having received the message should control the users really connected on the NAS and eventually manually remove the user trapped inside the user connected list.

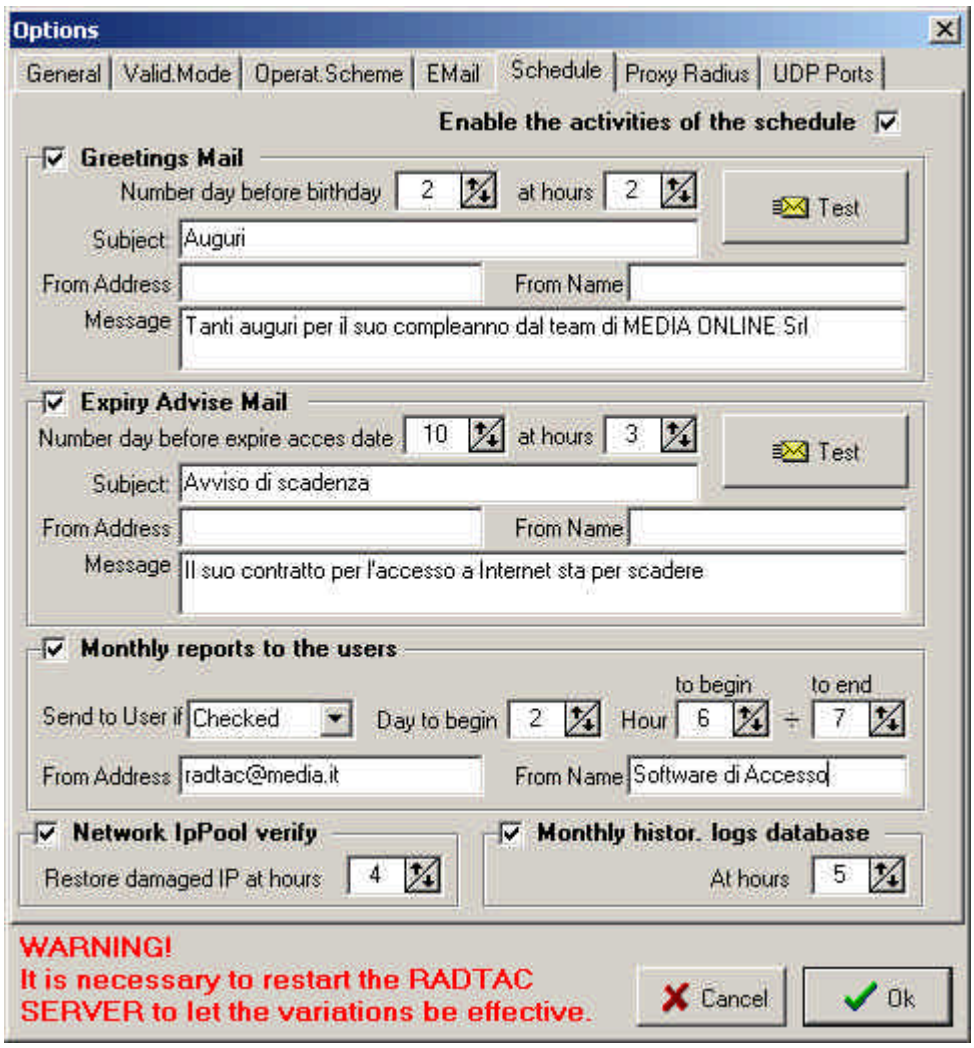
- Send me email when the number of the simultaneous connections exceeds the max allowed number.
  By selecting this check box RadTac Manager Server will send email in the case a user tries to access the net but has exceeded the maximum number of contemporary access allowed.

Schedule and Email Users

Activating the appropriate check box RadTac Manager Server is able to automatically send email to the remote access users. The input data regarding the electronic mail Server name is closely related to the users that are set inside the User Groups.

GREETINGS MAIL AND EXPIRY ADVISE EMAIL.

- Number of days before birthday.
  Through this numeric value it is possible to set the number of days before a users birthday so as RadTac can send email birthday wishes
- At Hours.
  With this numeric value is it possible to set the hour of the day in which RadTac runs a control of all the remote access users to which birthday wishes are to be sent. It is recommended that this elaborating is run during the night when RadTacc has a low access load on the net.
- From Address
  Senders Email Address. The user will receive a email message to which he can also reply using this electronic mail address.
- From Name.
- The Name visualized to the user who received Email message.
  This field has to contain the message to be sent to the user.



MONTHLY REPORT TO THE USER.

Through this functionality it is possible to monthly send to the customers report of all accesses carries out you to the net. It is necessary to indicate the Day of the Month in which carrying out the operation and the hour of beginning. RadTac Schedule, as an example, day two of the month, from the 6 to the 7 of the morning will carry out the generation of the report and it will send to all the users to it checked (selected). The selection comes made customer for customer or if we select “no checked” the report it will be sended to all the customers does not select to you.

NETWORK IPPOOL VERIFY.

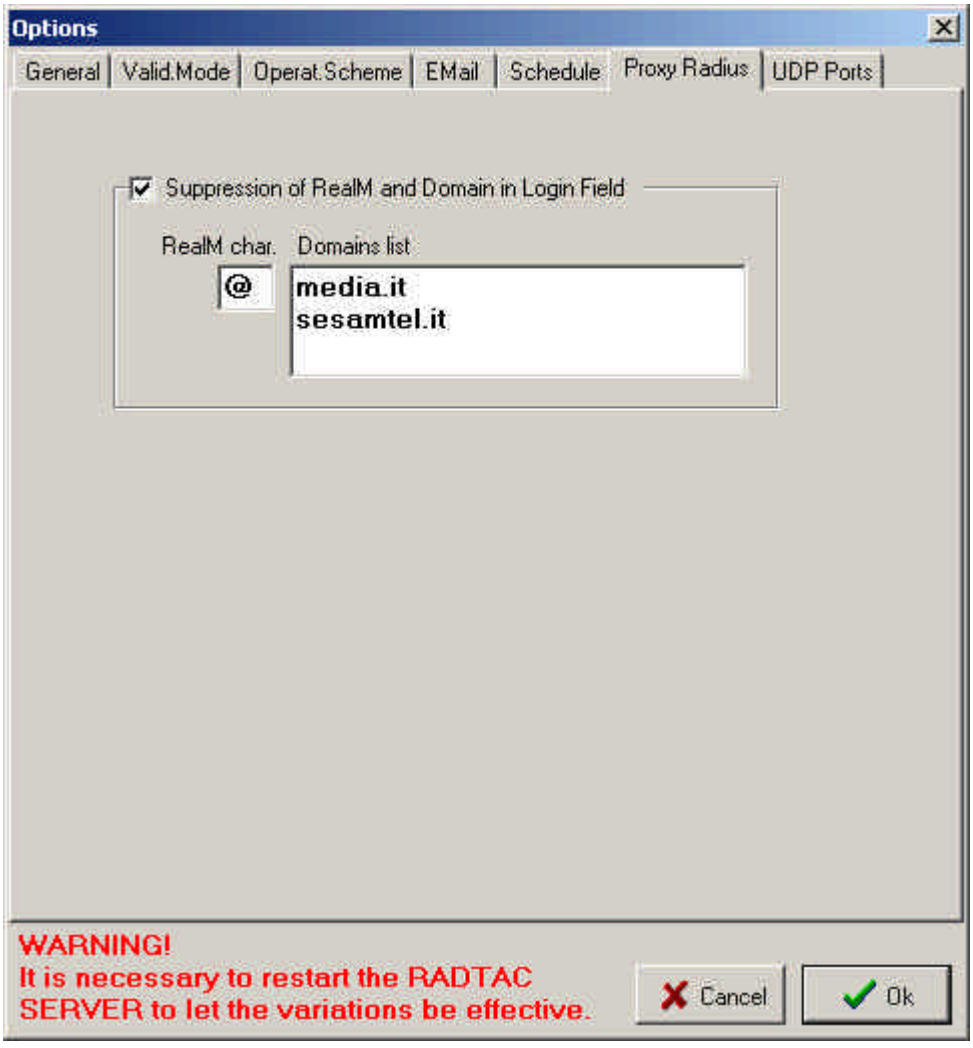
RadTac Manager Server do a control of the network ip pool release to the remote access user. This control permit to verify if an user is really connected or the nas port is free because the user is disconnect without sent radius information to RadTac. In Fields “At Hours” you will be define the time of clock in witch RadTac Schedule execute this control.

MONTHLY HISTORICIZZATION LOGS DATABASE.

RadTac Manager Server do a monthly recursive historicizzation of log database. In “At Hours” field you will be define the hour when radtac manager server execute the monthly clear up of primary database and create the little month database in directory c:\radtac\data\history.

Proxy Radius

Through this folder of options it is possible to indicate the behavior that RadTac in case of coming from authentication from an other Radius Operator. RadTac is not a proxy radius but operativity of authentication under proxy works fine. A Proxy Radius often sends back to RadTac the demands for authentication sending the login with all the real of access, as an example: giardina@libero.it RadTac can manage these users or with all the real, or widthout realm. As an example:

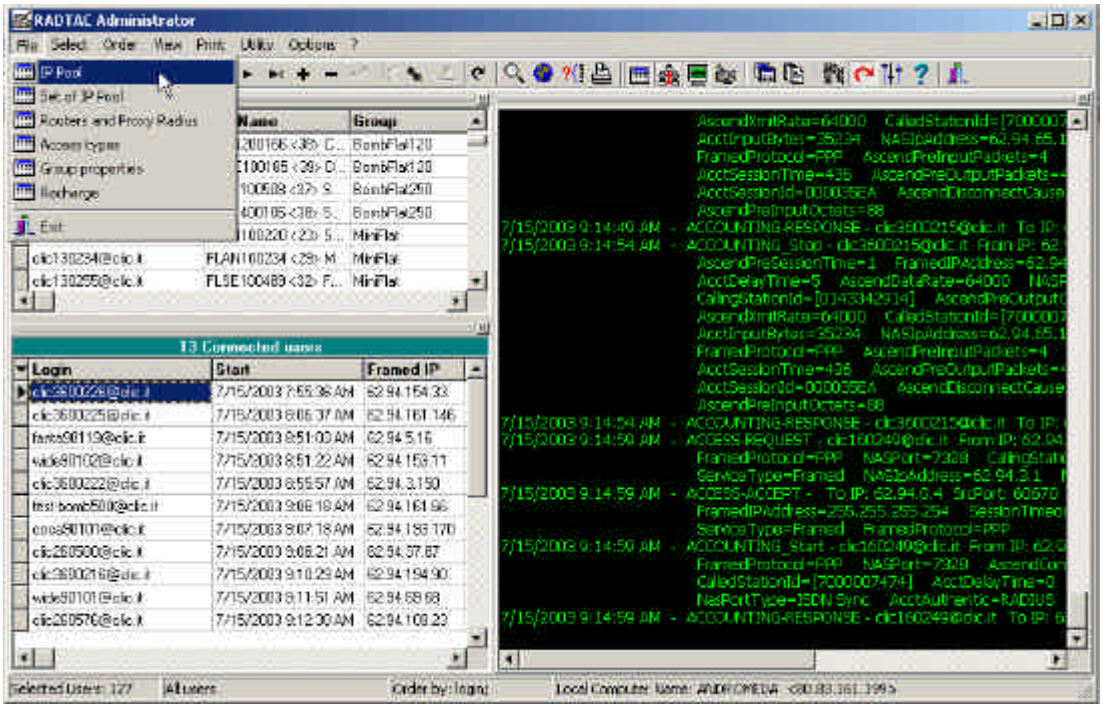


With this configuration when radtac receive a request from giardina@media.it match it in database with only “giardina” login, widthout @libero.it. This option is used only if you store login in database widthout @docomdomain. If you want authenticate different dotcom domain with same login do not use this option and deselect it.

IP POOL TABLE

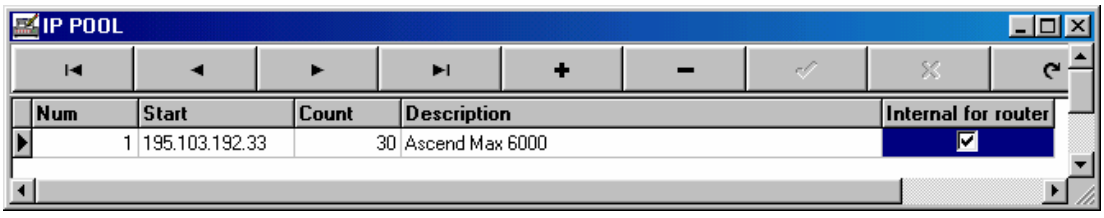
Ip Pool - Internal and External.

The first thing that the administrator has to do is plan the Pool assignments of the IP Internet Addresses necessary for the Router to connect the remote access user. RadTac Manager Serve is able to manage two different types of IP Pool.



Internal IP Pool.

A Internal IP Pool is a Pool of IP addresses used by RadTac Manager Server to automatically configure Router Ascend Max. These Access Server have a Set of Property Radius Attributes that is able to configure automatically the NAS by a Radius Server. RadTac Manager Server is able to take advantage of this capability. If you have an Access Server Max Ascend it is adequate that you define a Internal IP Pool and then assign in the Router Table said IP to the NAS Ascend. Then it is possible to cancel from the configuration of MAX the Pool of IP Addresses destined to the Modem and/or Digital Port. RadTac Manager Server will send the configurations every time the Max executes a Start.

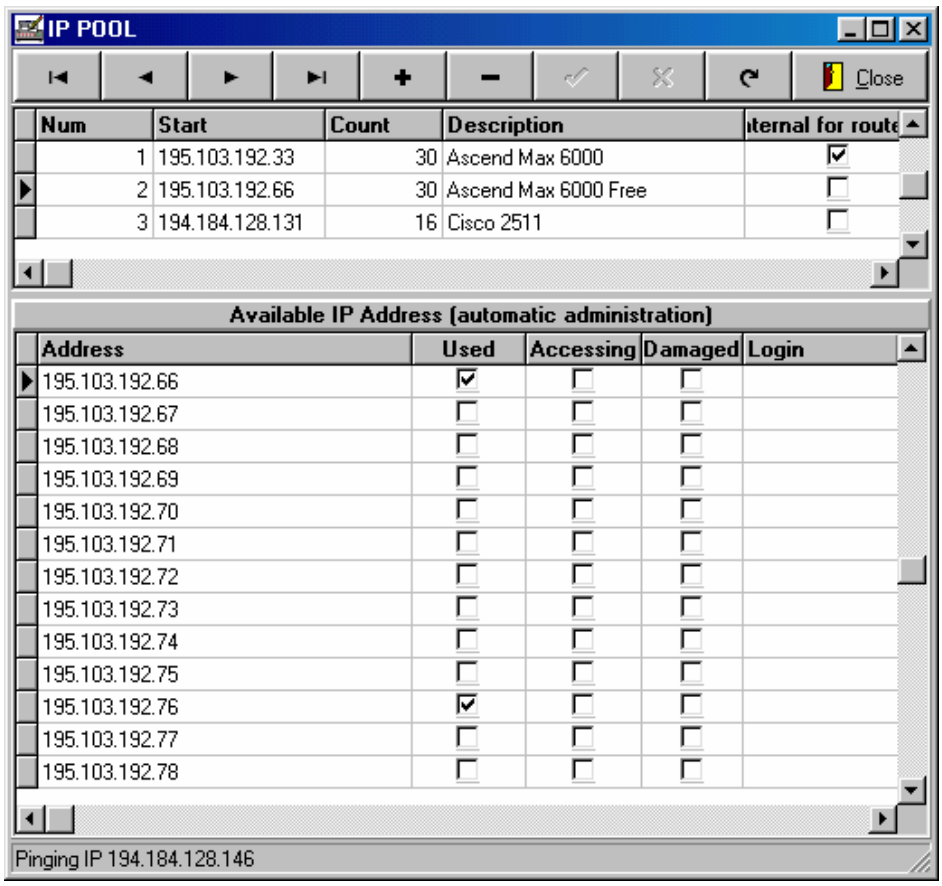


IP Pool (external).

An Ip Pool (not internal) is managed totally by RadTac Manager Server and does not require any type of property Radius Attribute. In fact, if this check box is not selected RadTac Manager Server will manager the new IP Address Pool through the standard Radius. An IP Pool which has been defined in this way, has to be, subsequently, assigned to a Router, using the Router Table of RadTac Manager Server.
By assigning an Ip Pool to a Access Server, through a router table, it informs RadTac of which Ip Address it can send to the user that is requesting access from that Access Server.

In fact RadTac Manager Server manages the assignment of the Ips exclusively so as to allow the administrator to plan access to his own net by type of user.

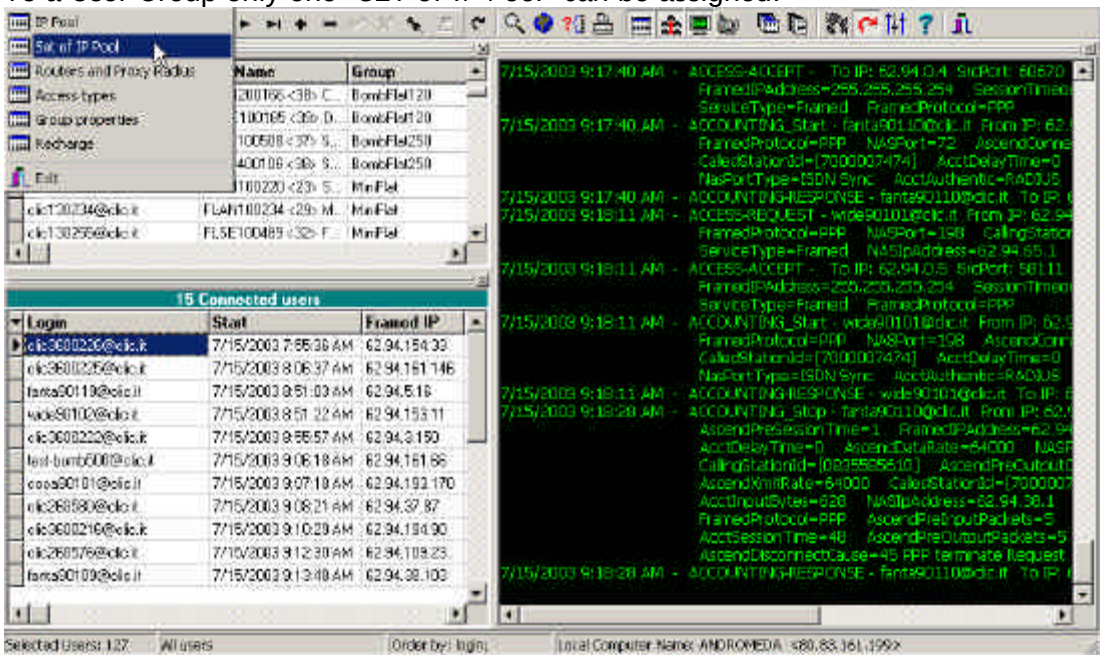
If the administrator wants to manage two Different Access Types. Example: Paying Users and Free of charge Users. He could have the need to differentiate the use of the band according to who is requesting access – a paying User or a Free of charge User. In this context RadTac Manager Server allows the assignment of different IP Address according to if he is a Paying User or Free of Charge User. After this, with Hardware or Software that is able to control bands, the administrator will be able establish to the IP Pool Different Priority and/or Secure Band. In the context it is necessary that TWO IP POOL are defined for every Router. After this, with the Router Table we will tie together the IP Pools to the same Router and with the "Set of IP POOL" table we will divide the two pools into two different categories of use, one paying and one free of charge.


IP POOL
Close
Num
Start
Count
Description
ıternal for route
1
195.103.192.33
30
Ascend Max 6000
2
195.103.192.66
30
Ascend Max 6000 Free
3
194.184.128.131
16
Cisco 2511
Available IP Address (automatic administration)
Address
Used
Accessing
Damaged
Login
195.103.192.66
195.103.192.67
195.103.192.68
195.103.192.69
195.103.192.70
195.103.192.71
195.103.192.72
195.103.192.73
195.103.192.74
195.103.192.75
195.103.192.76
195.103.192.77
195.103.192.78
Pinging IP 194.184.128.146

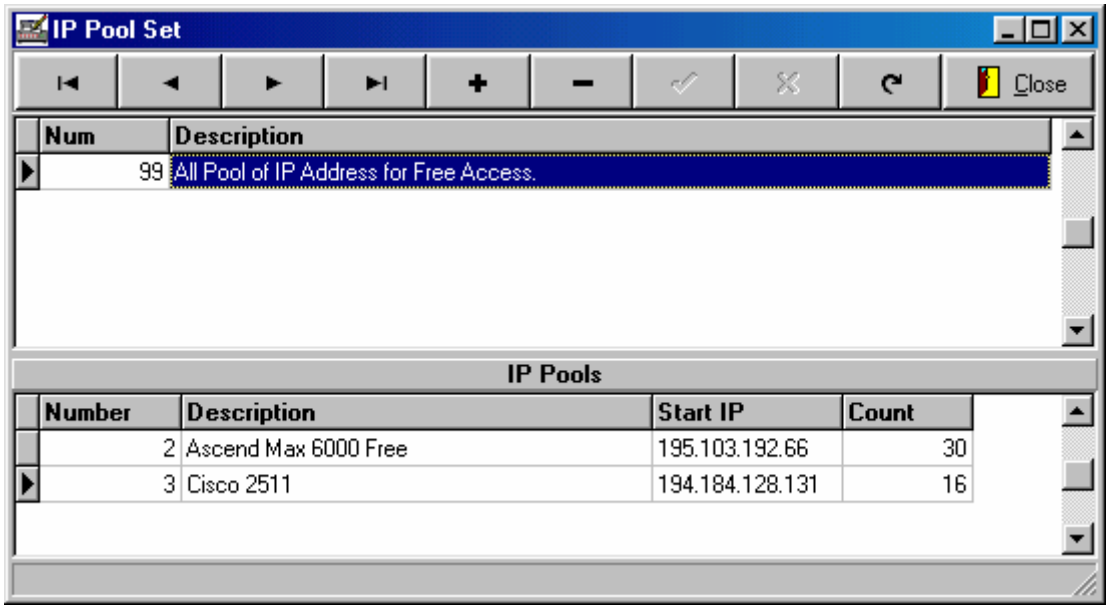
SET OF IP POOL TABLE.

SET of Ip Pool Management

Through the SET of Ip Pool table the administrator defines the Ip Pool Groups. The IP Pool Groups collect all the IP Pools that have to be used by the NAS so as to allow net access to selected User Groups.
To a User Group only one “SET of IP Pool” can be assigned.



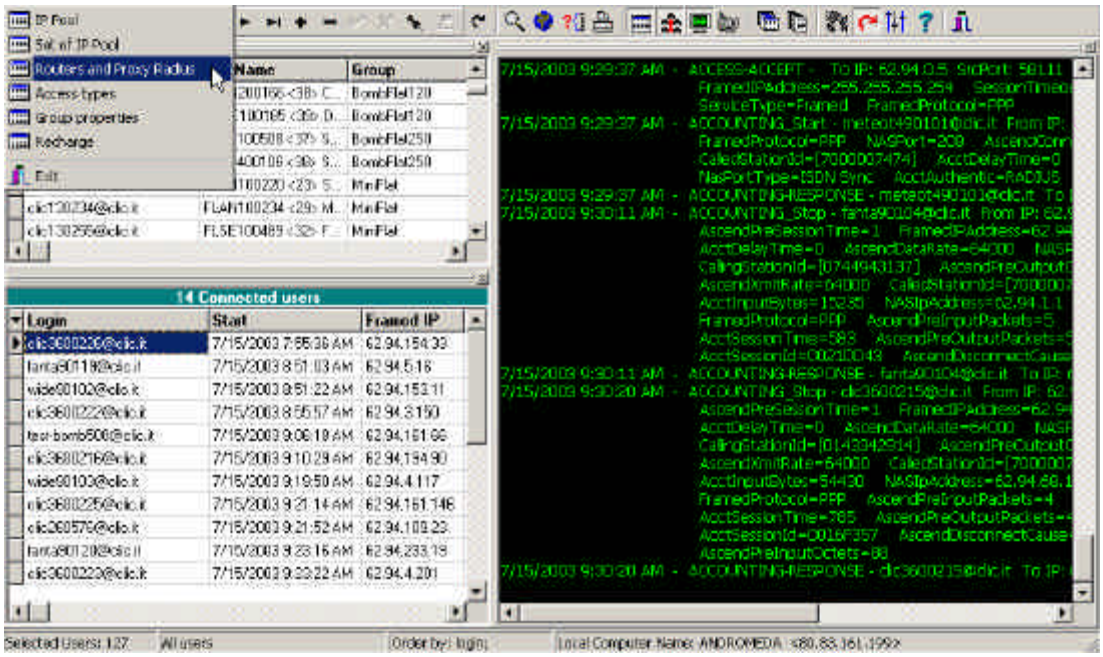
For example in the illustration below it is possible to observe that a Set of Ip Pool has been defined for Free of Charge Access. The Paying User, referring again to the example, will be managed from the Internal IP Pool.



ROUTER TABLE – N.A.S.

Router and Attributes.

In this table, it is necessary, that all Routers are defined, that are part of the same net and have to authenticate remote access users. Also, it is necessary that for every single Router all the Radius attributes and supported Ip Pools are defined.



IP ADDRESS.

Fill in this field with the Primary IP Addresses of the Router.

SHARED SECRET.

By Clicking on the border of the field the share password can be inputted onto the Router (which have been previously set). This field is optional. Only input the value if the share password is configured on the Router.

DESCRIPTION

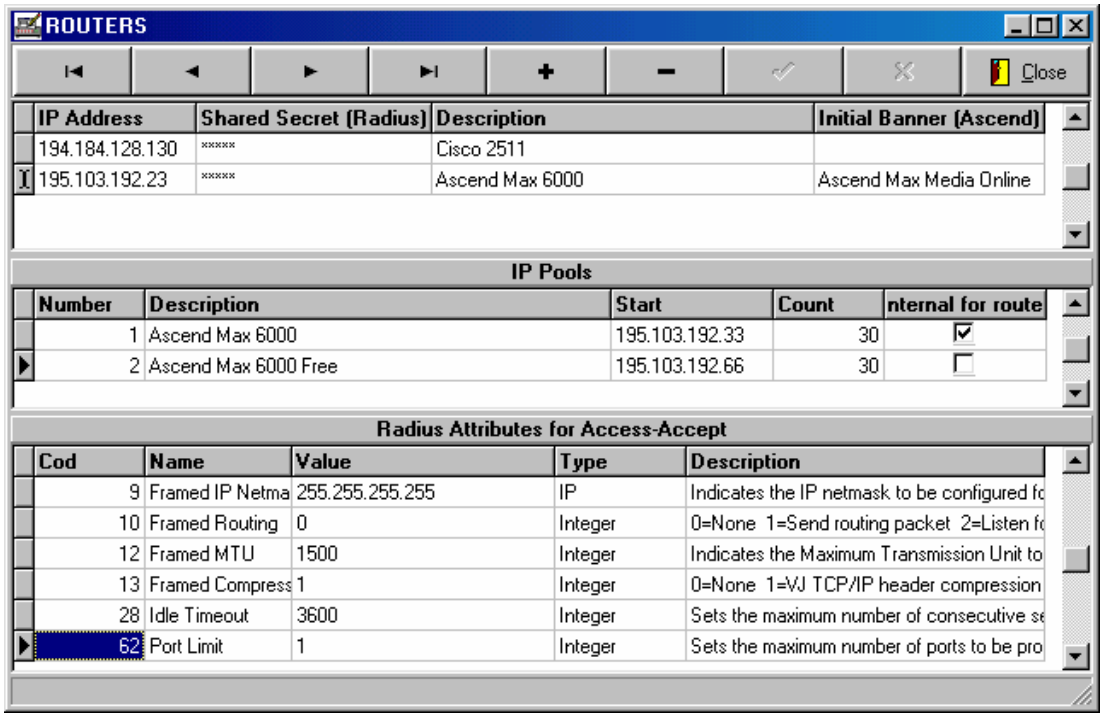
This is a reference field. Fill in the DNS Name of the Router or the make and model of the Access Server.

INITIAL BANNER.

This field can be defined only in the presence of a NAS Ascend. The value set will be sent to the Max Ascend at the start, during the outbound phase.

RADIUS ATTRIBUTES

In the below table, fill in, selecting among the existing ones, the attributes for every single access server. Firstly, click on any part of the attribute table and then click on the + key, this will add on an attribute. Proceed with the same procedure until all the attributes managed by the Router are inserted. The upper keys have different functions depending on the part of the table selected.

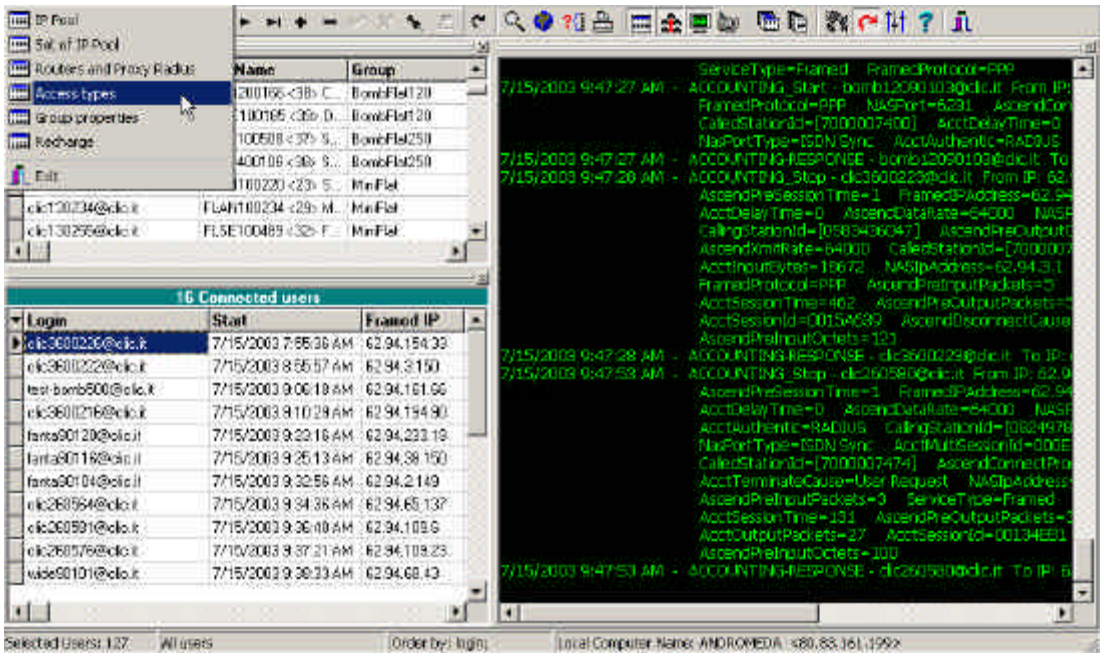


IP POOLS.

Inside the central section of the Router Table the IP Pool supported by the Router have to be defined. For example, the Router Ascend Max 600, illustrated above, supports an "Internal" Address Pool used in default by the generic users or paying users and a Address Pool "Ascend Max 6000 Free" managed by RadTac. Later on we will illustrate free of charge access

ACCESS TYPE

With the settings in the “Access Type” you can define the various net access strategies. These Access strategies will be evoked during the definition of the Users Groups. The “Access Type” table defines the type of access; ISDN, Ana logic, consented Network etc. etc. What is defined in a type of access represents the resources allowed to one user group.



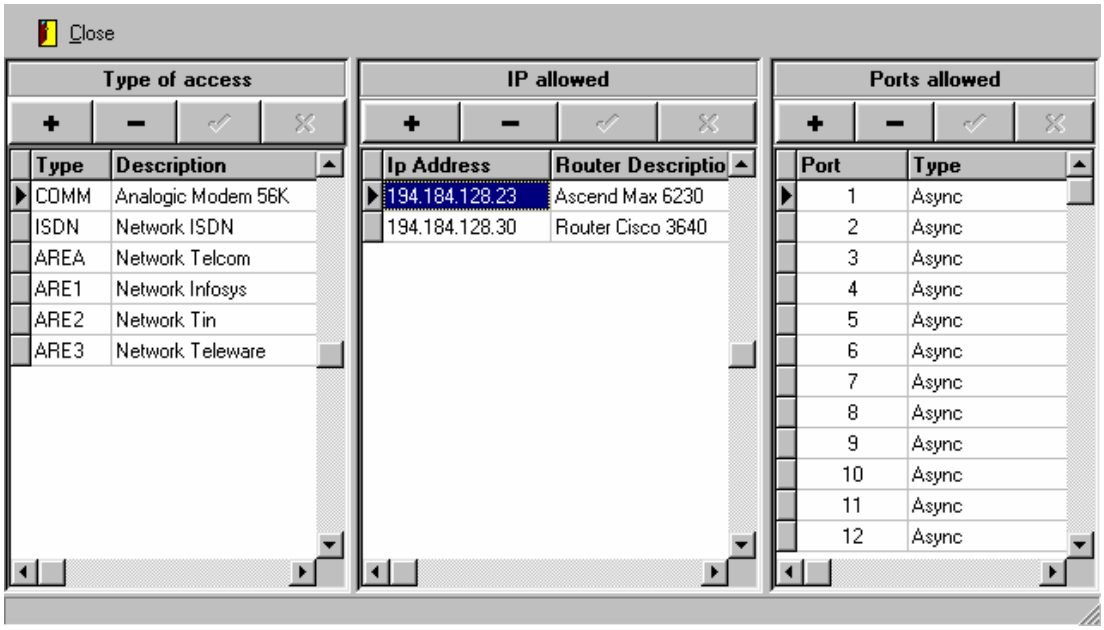
CREATING A NEW ACCESS TYPE.

With the first column you can create new profiles of access. Every access profile can be grouped on one or more, previously defined, Router. For every Router one or more access ports can be defined. The same Router can be exist on more than one access profile, that has different access ports or with the same ports. For example, you can define different access profiles for ana logic or isdn user types. Define different profiles for different connection of the same Access Server.

HIERARCHIC STRUTTURE.

The three columns have a creating structure and manages independent or hierarchic types. The third column illustrates the data relating to the factor selected in the second column. The second column illustrates the IP Access Server relating to the Access type selected in the first column. It is for these reasons that inserting data must be from left to right and after every entry a save of the column is to be made before moving onto the next column, on the right, which is independent from the one just entered.

Example: In the below illustrations, we see all the access data regarding the COMM, IP Address 194.184.128.23, and the ports defined for this IP Router from 1 to 12.



IP ALLOWED.

This field contains a value that can only be selected. Clicking on the "IP Address" field a bar menu appears that allows to select a value that has been previously exposed and acquired by the Router Table. "Router Description" is a descriptive field which is automatically filled by selecting the router.

ROUTER DESCRIPTION.

This field is only for reference. It is automatically filled in by selecting the Router. This value can be modified by intervening directly on the Router Table.

PORTS ALLOWED.

Depending on the Router selected, in the field, you can define all the access ports allowed to the remote access user. Special care has to be made when defining the access ports. Also, every Access Server supplied with ports that seem easy to define, example from 1 to 30, in fact, are ports to be numbered in a different way – from 20030 to 20060 for analogic and maybe from 20130 to 20160 for isdn digital. To define correctly the value to be inserted in this field, it is recommended that initially 1 to 30 is used, then monitor the access LOG and correct it. In this case, look in the log for the Radius attribute "Nas IP Port".

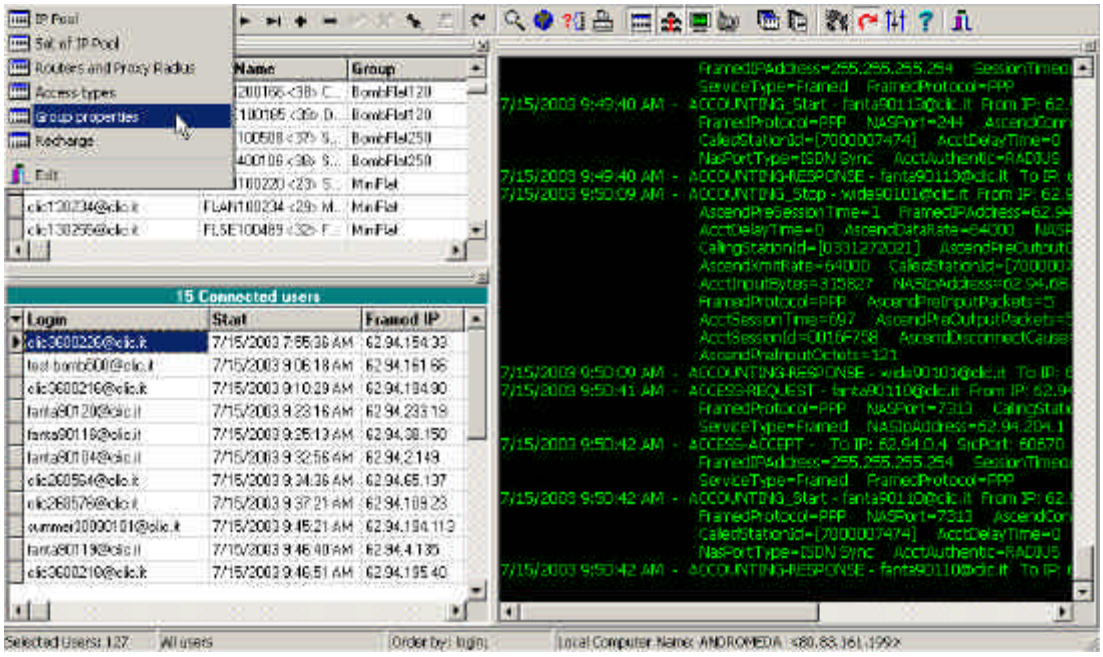
PORT TYPE.

This is a List-Box field and one of the preset values can be selected by clicking on the lower part of the field. For a correct compilation of this field it is recommended that the "Async" Type is selected, after the first test, and then it is improved by an analysis of the access log. During the log consultation look at the Radius attribute "Nas Port Type".

GROUP PROPERTIES

User Group Planning

A remote access User can belong only to one group. The group is a collection of remote access users that use the same access type. More than one access type can form part of the same Group. The remote access user that belongs to a group, automatically take advantage of all rights of access defined for the access type, connect to that group.

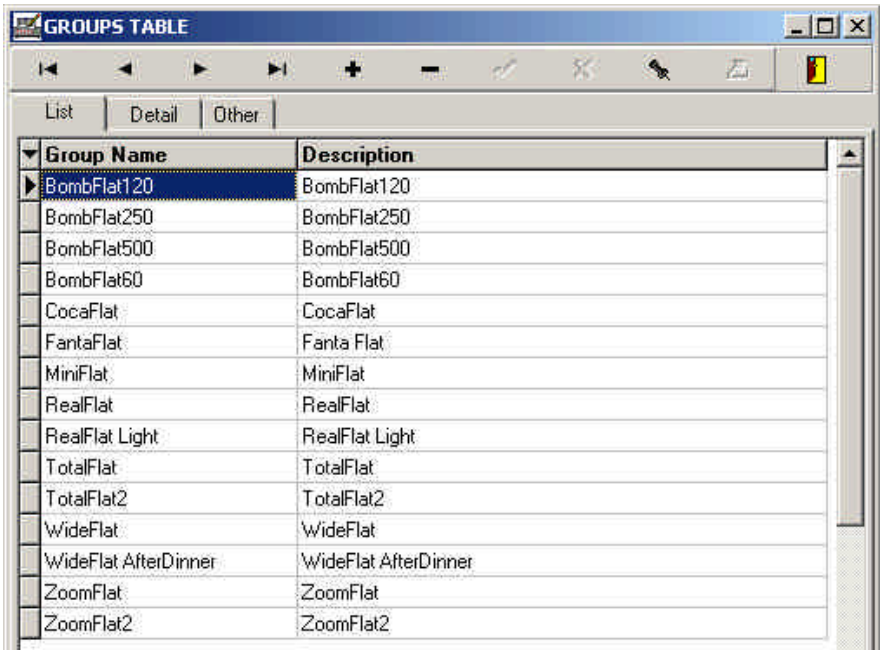


Radtac Groups in Windows 2000 2003 and NT.

The interconnection between the Windows 2000 or NT users and the RadTac 2000 Server users occurs through the Groups. The **RadTac 2000 Server Group Name** has to be **identical** to **Windows 2000 or NT Server Global Group Name.** In fact, it is with this same named group that RadTac Server can understand which RadTac user Group belongs a Windows 2000 or NT user.

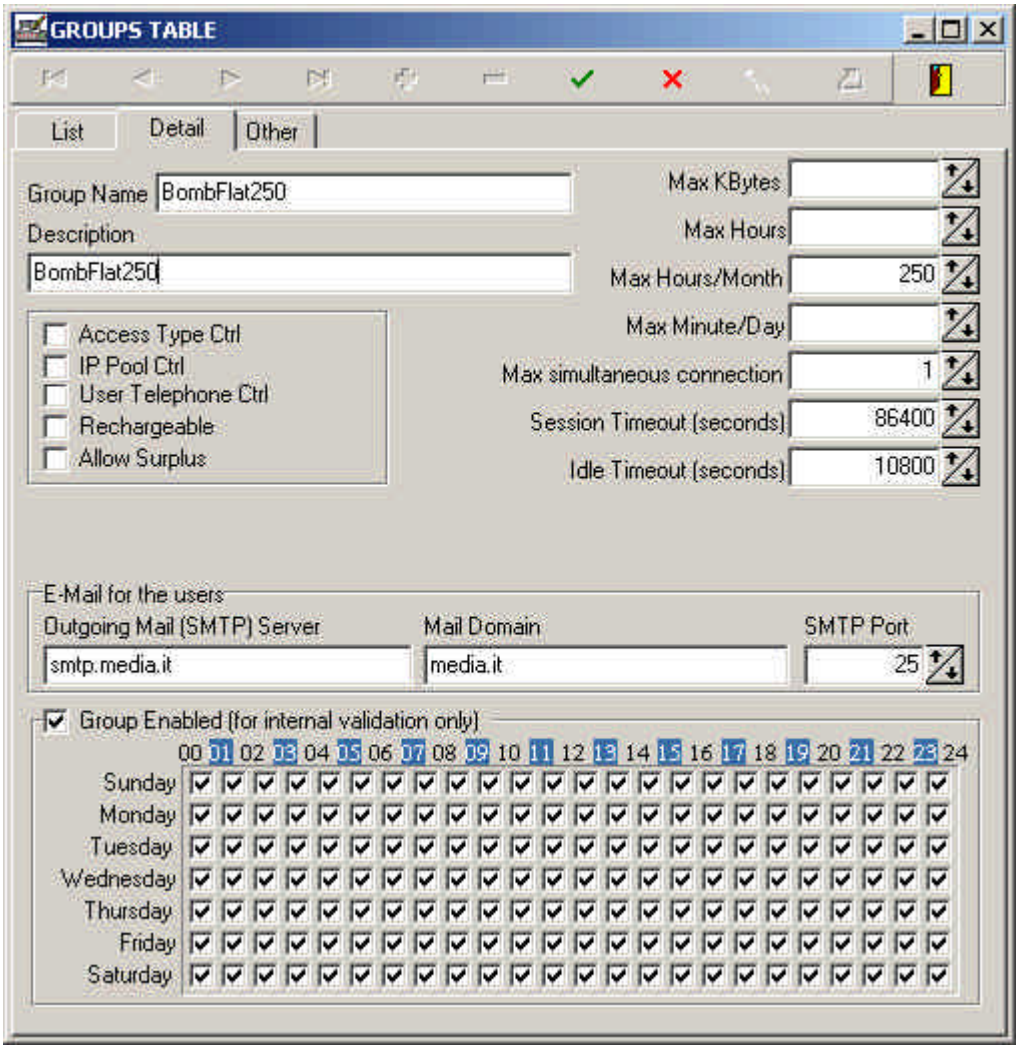
CREATING A NEW USER GROUP.

Open RadTac Administrator and select “Files” and then “Group Properties”. The configuration options, could in part, not be activated. This will depend on the operation mode selected. When using Windows NT, some functions, like allowed hour bands, are managed directly by the operating system.



GROUP NAME.

The “Group Name” field contains the RadTac Group names. It is with this field that Windows NT connects the global groups of Windows NT with the local RadTac group. When operating in “Internal Database – Windows 95/98” this is only a reference field.



MAX HOURS AND SURPLUS CTRL.

If the Max Hours field contains a value different than 0 (Zero), RadTac Service will regard the access as "use by hour", denying access to the users belonging to this group who have exceeded the maximum number of hours set in the field. In fact, the access block will occur only if the Check Box "Surplus Check" has been selected. If this check box is not selected, RadTac Service once reached the maximum number of hours, will not stop access but will continue to add the excess hours.

MAX HOURS MONTH.

If the Max Hours Month field contains a value different than 0 (Zero), RadTac Manager Server will treat access as use of hours per month. The remote access user can access the net until he reaches the value set in this field for the current month. Once reached this set value, if the check box "Surplus Check" as been selected, RadTac will automatically deny access until the next month.

MAX MINUTE FOR DAY.

If the Max Minute for day contains a value different than 0 (Zero), RadTac will treat access as minutes consumption in one day. the customer will be able to

access the network until to attainment of the value in minute for the day. The successive day the progressive will be annulled.

MAX KBYTES.

If the Max Kbytes field contains a value different than 0 (Zero), RadTac Manager Server will treat access as use in Kbytes. The remote access user can access the net until he reached the maximum number of input Kbytes + output Kbytes. **This control can only be used with Radius protocol; the Kbytes calculations in input and output are not supplied by the Tacacs protocol.**

MAX SIMUL CONNECT.

This field can contain one numeric value. It represents the maximum number of simultaneous connected allowed by the remote access user that belongs to the group.

SESSION TIMEOUT (IN SECONDI).

If the field contain one numeric value different to 0 (zero) RadTac apply to the user in this group a max duration connection. In any case the time of the remote access connection not can to exceed.

IDLE TIMEOUT (IN SECOND).

If the field contain one numeric value different to 0 (zero) RadTac apply to the group a maximum idle timeout in second. If the user do not generate internet traffic for the second value set in this field will be disconnected.

OUTGOING SMTP MAIL SERVER.

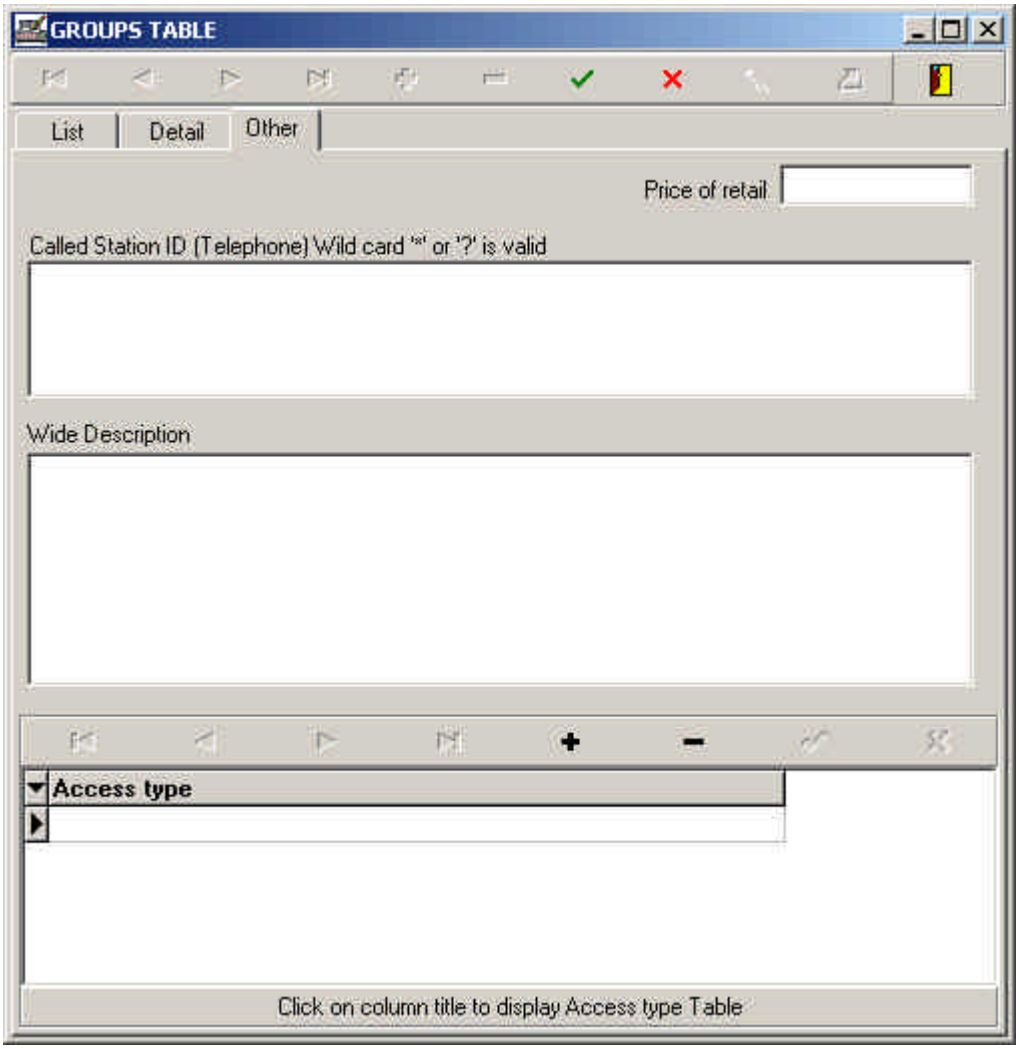
In this field will be inserted the name of the smtp server used for send email warning to this group of user. RadTac send to this user email message with mountly report of connection and greating email of birthday or expire message advice.

MAIL DOMAIN.

In this field you can insert the @dotcom domain for the user of this group. This value is used with login of the user, sample login: rossi + mail domain: @domain.com = rossi@domain.com. In this case the email is send to rossi@domain.com

SMTP PORT.

In this field you can set the tcp port used to send email message to smtp senver previously configured. The standard port is 25.



CALLED STATION ID.

In this field you can set the list of the telephone number called from the user. The user of this RadTac Group can be call only this telephone number for access to the network, if the call from telephone number is not include in this list the remote access user is rejected. You can use also wildchar dos syntax as 0804089* or ???4089????.

WIDE DESCRIPTION.

In this field you can describe the group created. This is only text field. Not have any feauture in RadTac operational's work. This description can be display from the user in online web report. http://www.domain.com/radtacadminsecure/...

ACCESS TYPE CONTROLL.

If the "Access Type Ctrl" check box is active, RadTac Manager Server runs a IP NAS, Nas Port and Nas Port Type source control, previously defined in the "Access Type" and assigned to the current Group.
If the "Access Type Ctrl" check box is not activated, RadTac Manager Server will only control access characteristics in relation to password, hour bands and maximum number of hours allowed, permitting access from any net.

ACCESS TYPE.

In the "Access Type" window the Access Types have to be selected to which the remote access user, who is part of the Group, can access.

USER TELEPHONE CTRL.

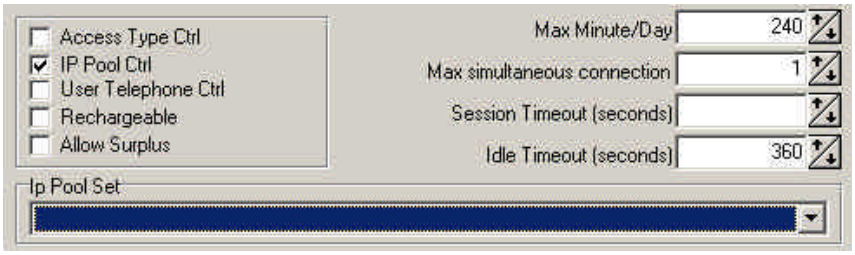
If the "User Telephone Ctrl" check box is active, RadTac Manager Server runs a control on the incoming user telephone numbers. This setting is made when inputting the user to a Group. During the input phase of the user to this Group it is important that the correct telephone number is inserted, so as to allow access.

CALLED STATION TELEPHONE.

Using the "Called Station Telephone" field, RadTac Manager Server runs a control on outgoing telephone numbers. This field can contain the net access telephone number. This type of control is used in case to one same group of telephone lines correspond more than one string of numbers with the same beginning. By indicating in the "Called Station Telephone" group, only the users belonging to this Group, they will be able to access calling the "Called Station Telephone".

IP POOL CTRL.

By activating the "IP Pool Ctrl" check box it will be possible to assign to a User Group an IP Pool Net from which they can access. The Users belonging to the group will access the net using one of the IP Pool Address on which they are requesting access, supported by the Router.



RECHARGEABLE.

If the "Rechargeable" check box is activated, RadTac Manager Server will consider the access as Rechargeable. A rechargeable access is to a large extent an access to the net by use in hours. Hours can be incremented by blocks of extra hours, inserted with a recharge password. For supplementary information, go to the "Recharge" section.

The Group defined in the above illustration is an initial 40 hour "Rechargeable". The recharges can be printed directly by the Administrator program, in various hour sizes.

E-MAIL FOR THE USERS.

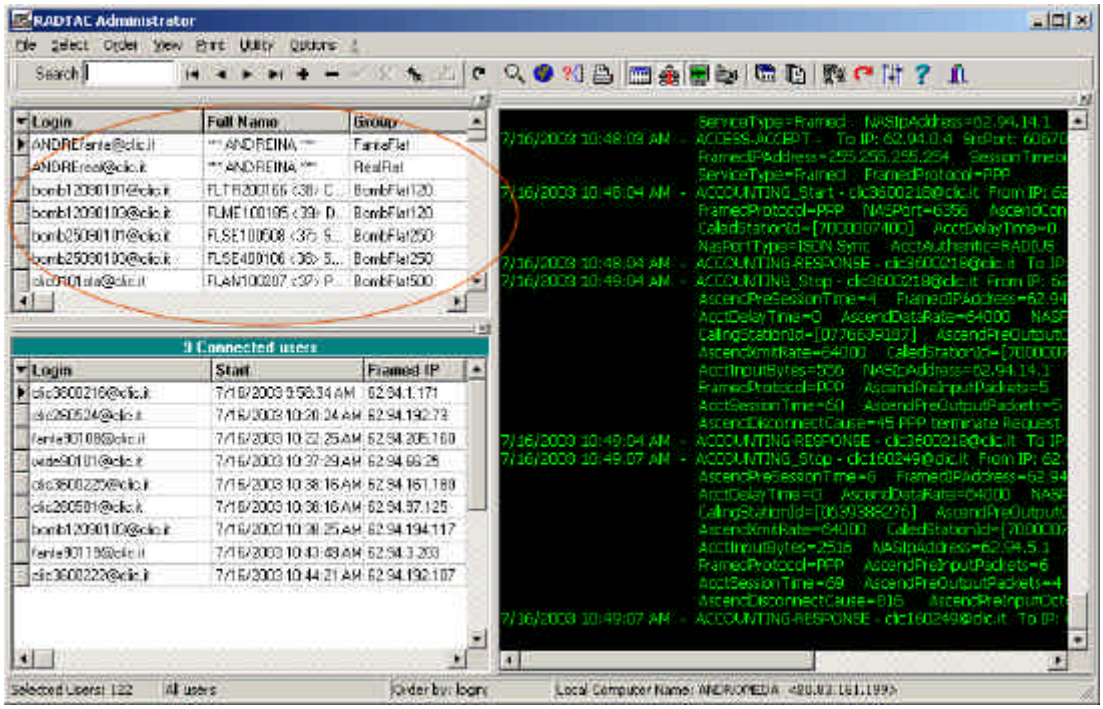
For every single User Group a different electronic mail server and a different internet domain can be defined. For example, in the above illustration the User Group “Access Recharge 40” has a outgoing mail server named “mail.media.it” and a mail domain name “mail.media.it”. E-mail messages send automatically to the “Recharge 40” will be address to an email composed by an access login + a mail domain “LOGIN@MAIL.MEDIA.IT” and will be sent by the server of electronic mail - MAIL.MEDIA.IT.
Therefore you can correctly and automatically send expiry date messages and “Happy Birthday” wishes to different user nets, subnets and Web service suppliers

ACCESS TYPE.

In the “Access Type” field you can call up, predefined, access types. To an access group, more than one “Access Type” can be set. An “Access Type” will group together more than one Network Access Server, hence representing a net. The result of selecting one or more access types in the group is an operation that defines what nets a User Group can access. With the “Access Type” you can differentiate type of access, ISDN or Ana logic. In fact, you can create two different “Access Types” that use the same Router but with different port types (Sync, Async, ISDN, ISDN Sync, etc. etc.).

USERS MANAGEMENT

When you execute RadTac Administrator the list of RadTac users is visibile immediatelly in the grid up to left, as you can look in next image. After the first installation this grid is empty. You can use bottom for add, edit or remove remote access user.



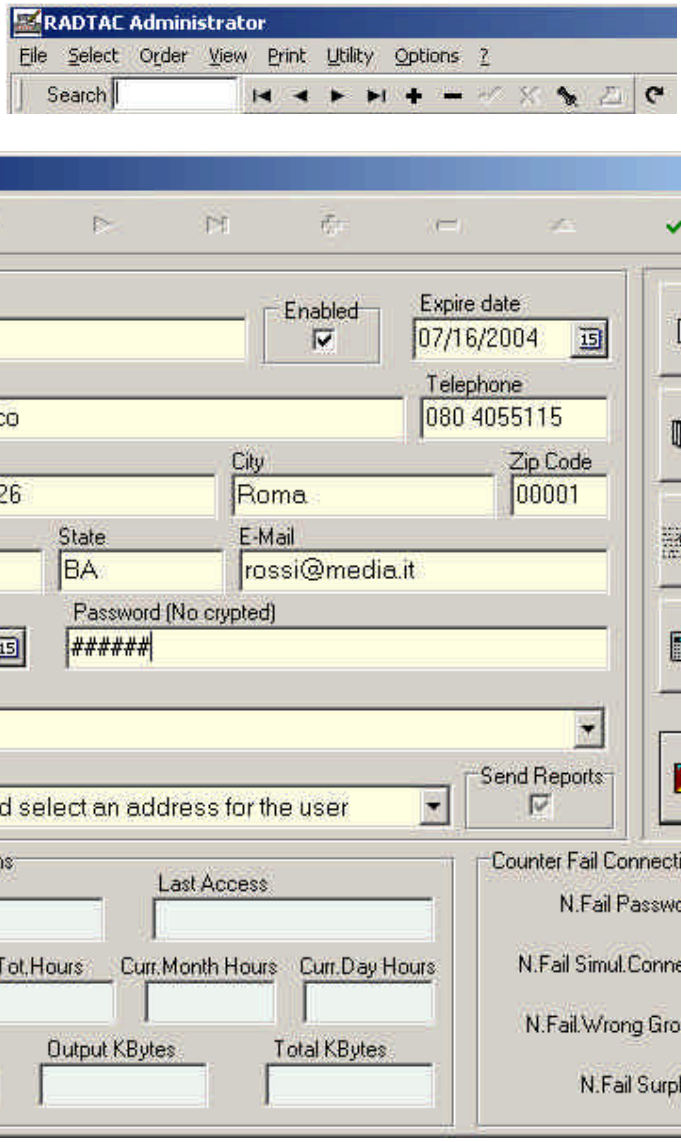
If you use modality Windows 2000 Active Directory or Windows NT Sam Database the new user will be inserted from the operating system tools. You can use RadTac Administrator for add new user only if the application is configured for work with internal database.

If you use Windows 2000 or NT user database look Windows 2000 or NT section manual for more information about the management of user with RadTac.

If you want use Internal Database continue to read this manual section.

ADDING A NEW USER.

By clicking on the [+] key, in RadTac Explorer you can add a new user.



LOGIN.

The login field contains Net Access ID. A definite user when assessing the net will use this login.

ENABLED.

With this check box you can activate or dis-activate a definite user.

EXPIRE DATE.

In the expiry date field the access expiry date has to be inputted. If operating in Windows NT this field must not be filled in. The Windows NT expiry date overrides this field.

FULL NAME.

"Full Name" field can contain the user's Name and Surname. It is a reference field and does not have any function.

TELEPHONE

With this field you input the User's Telephone Number. This is NOT a reference Field. Making this user part of a Group that controls the source of incoming numbers, RadTac Manager Server RadTac Manager Server will be able to precondition access to the net so as the incoming number and the definite number of this field are the same.

ADDRESS.

With this field you input the address of the user.

CITY.

With this field you input the city of the user.

ZIP CODE.

With this field you input the Zip Code for this user.

COUNTRY.

With this field you input the Country of the user.

STATE.

With this field you input the State or Province.

E-MAIL ADDRESS.

With this field you input the E-mail address of the user. If not inserted RadTac create it automatically from settino of the group, (login + Mail domain) configured in group properties.

GROUP.

Here you can select the Group to which this user will belong. The group to which this user belongs to is fundamental to Radtac Manager Server so as to establish which characteristics have to be used. The GROUP filed is FUNDAMENTAL in Windows NT mode. In fact the GROUP NAME has to be defined identically to the one set in Windows NT.

BIRTH DATE.

The "Birth Date" field contain the user's birth date. By filling in this field and activating the "Email To User" function, RadTac Manager Server will be able to send birthday wishes to a definite user.

PASSWORD.

In this field the net access password that will be used by the user during connection, has to be inputted.

ROUTING MODE.

The different possible selections in this field are:

THE NAS SHOULD SELECT AN ADDRESS FOR THE USER.

Selecting this mode, Network Access Server will emit, to the user, an IP address belonging to the range of addresses specified in the configuration of the NAS.

THE NAS SHOULD ALLOW THE USER TO SELECT AN ADDRESS.

Selecting this mode, RadTac Manager Server will allow the user to access the net with the IP address revealed to him. If the user's Remote Access Client does not indicate the IP Address with which he wants net access the same user will be disconnected.

THE NAS SHOULD USE THIS IP ADDRESS (STATIC IP).

As soon as this mode is selected, RadTac Manager Server, will assign to the user an IP address with a definite status in the "STATIC IP" field, that appears as emission data.

CHECK BOX – SEND REPORT.

This check-box select or deselect the report send procedure to the user. This check box work with the setting in radtac option. In RadTac option menu you can configure if RadTac will be send report to select or NO Select user. If you set radtac to send report to the checked user, when you select this check box RadTac send report.

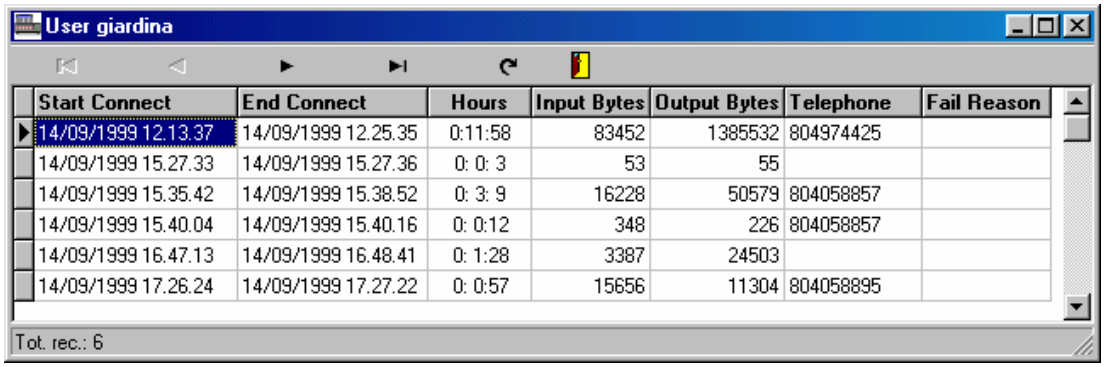
COUNTERS CONNECTIONS.

The values visualized in "Counters Connections" can not be changed. They are automatically updated by RadTac Service during access authentication. You can check the following operations: first access date; last access date; the total number of connection to the net; the total number of access hours regarding the current month; and input and output Kbyte Totals regarding the user.

COUNTER FAIL CONNECTIONS.

The values visualized in "Counter Fail Connections" can not be changed. They are automatically updated by RadTac Service during access authentication. You can check the number of failed connections because of wrong passwords, for simultaneous net access, failed access because the user doesn't correspond with the characteristics of the Group ore for surplus of hours

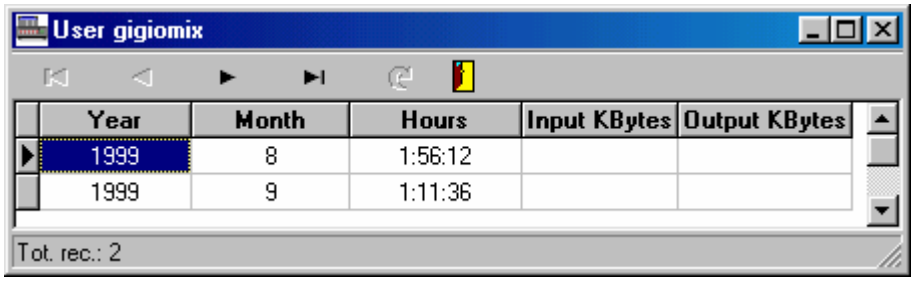
CURRENT MONTH LOG BUTTON.



By selecting the "Current Month Log" you can consult the current monthly user access log. Above is illustrated a user's connection table that visualizes date and hour of connection start, connection end, duration in hours, input and output bytes, incoming telephone number and in case of failure the reason why.

MONTHLY LOG.

By selecting the "Month Log" you can consult a reference table giving user access for the month. The data of this table are constantly used by RadTac Manager Server to control the user that has hours per month access.

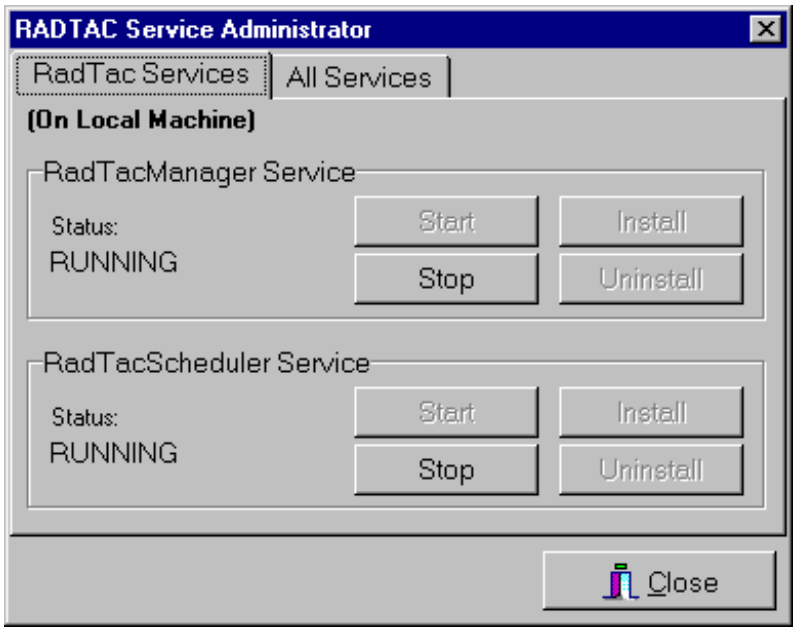


RESET LOG.

By selecting "RESET Log" you can cancel user progressive fields in account record . This button do not cancel any log record in the month log.

WINDOWS 2000/3/NT RADTAC SERVICE.

RadTac 2000 Server can be installed as a Windows 2000- 2003- XP PRO or NT Service. This feature can be used only by installing the licenced package. The trial release does not contain this software. Installation in Windows NT Services is done with the “RadTac Start-Stop” program.



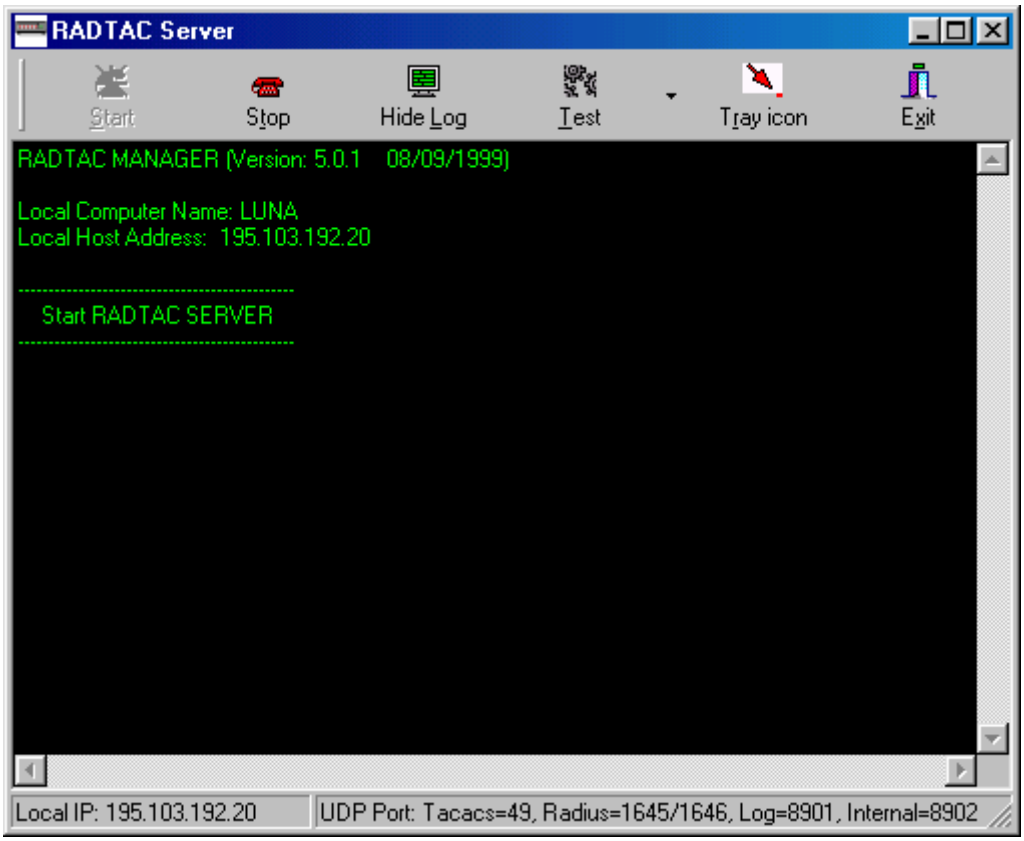
Chapter 5

USE

In this chapter we will describe how RadTac Manager Server authenticates the remote access user and which are the useable software instruments.

RadTac Service.

RadTac Service authenticates the user. Respecting all the condition set, it continually monitors the Tacacs UDP and Radius ports waiting to receive authentication requests. As soon as it receives a request it runs a check on the conditions set and then responds to the NAS that has sent the request.



Windows ME-98-95 Mode.

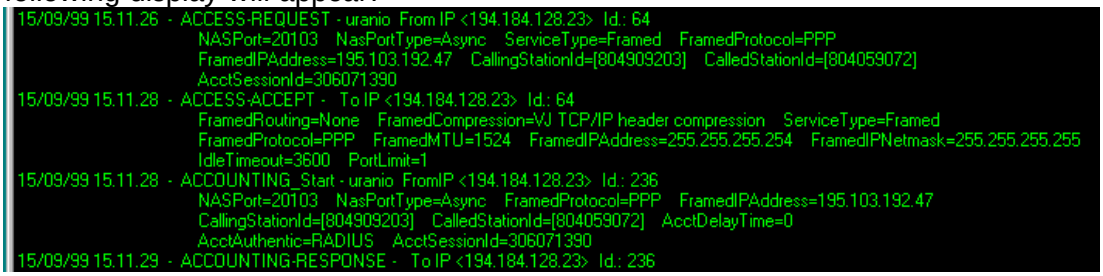
In Windows 98-95, RadTac Service has to be constantly running. In the Log window it continually shows the dialog between NAS and Radius Server. Nevertheless, you can reduce the software into the Windows' ICON TRAY, instead of having it always on the desktop. Once reduced in the Windows' TRAY ICON, RadTac Service will continue to operate as though it is open on the Desktop. If you click with the right mouse key on the RadTac Service icon, when it is in the Tray Icon, you can close the applications, that in future, will be started directly from the Tray Icon. Therefore, create an automatic RadTac Service link in the Start up folder. Doing so, RadTac Service will automatically execute at the system startup.

Windows 2000-2003-XP PRO-NT Mode.

By using Windows NT, RadTac Service can be run either on the desktop or as a Windows NT Service. The Windows NT Service is only part of the licenced user package (those who have purchased the product). After having run the first installation it is advisable to run "RadTac Service" temporally on the Desktop so as to immediately analysis any problems. Windows NT Service mode operates in total silence and is therefore difficult to pickup eventual installation errors. After having tested if everything runs to specification you can close "RadTac Service on the Desktop and then run it in NT. It is therefore clear, that both the applications can not be run simultaneously because they use the same UDP port.

Radius Authentication.

As soon as RadTac Service receives an authentication request on its UDP port the following display will appear:

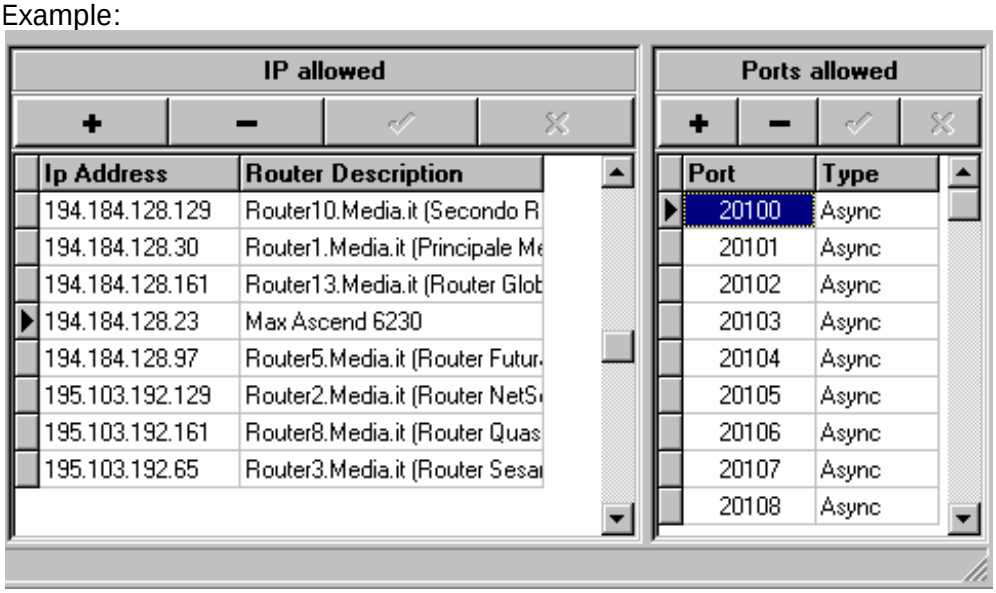


ACCESS-REQUEST
Analysis two fundamental elements so as to fine tune the access type configuration.

- NASPort (example 20103)
- NASPortType (example Async)

NasPort represents the number of NAS ports on which the user is accessing. The number of ports is not a Hardware value but changes according to the Type of Port. On a NAS Ascend Max 6000 the Async ports are numbered from 20100 to 20160, whereas the ISDN ports are numbered from 10100 to 10160.

The numbering of the NAS ports has to be correctly put in the access type table. For Example:



NASPortType represents the Connection Type, Asyn or Sync (if ISDN): The port type defined in the Type of Access and assigned to the user has to have the same value as the one given during the authentication phase

RadTac Service controls if the user comes from a defined source, if from a port and with a consented connection type. It also controls, if defined, if the access by hour settings are respected. Once run all controls, it will reply to the NAS with

ACCESS-ACCEPT

And quickly after the access attributes that the NAS has to apply to the incoming connection. Even if only one setting does not correspond RadTac rejects connection, replying to the NAS with ACCESS-REJECT. In this case, the cause is visualized on the Display.

AUTENTICAZIONE TACACS

Tacacs authentications is very easy and does not involving the setting made in RadTac Administrator

```
14/09/99 0.00.06  -  LOGIN - davide  <195.103.192.129>  Port 16
14/09/99 0.00.07  -  LOGOUT - davide  <195.103.192.129>  Port 16
14/09/99 0.00.07  -  SLIPON - davide  <195.103.192.129>  Port 16
```

The request for access arrives through a LOGIN – username IP ADDRESS NAS and Port.
The Connection Type is not supported by the procedure and for this reason the TYPE field in the Access Type table does not have to be defined.

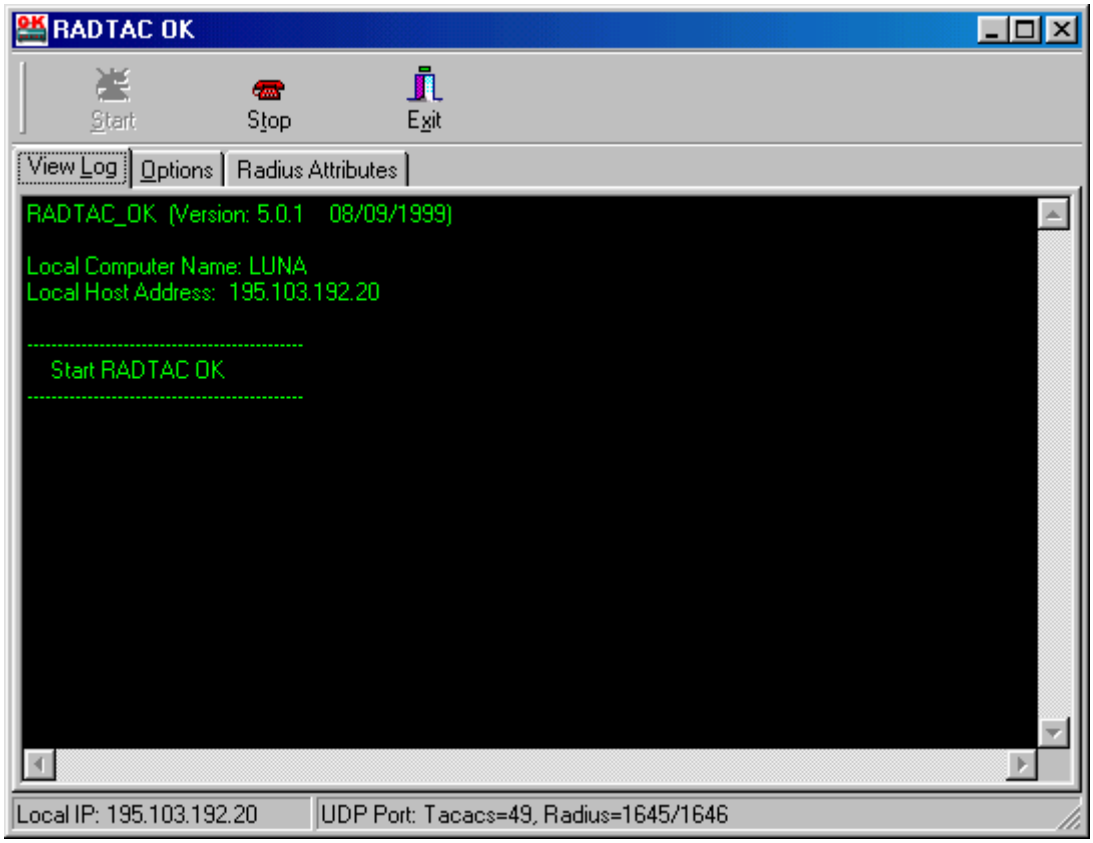
Chapter 6

MAINTENANCE TOOLS

RadTac Server features two different software that effect the usual maintenance operations. Radius Server maintenance is essential. A fast user authentication is strictly related to the Radius Server situation and to the Server NT or Windows 98/98 where the software is installed.

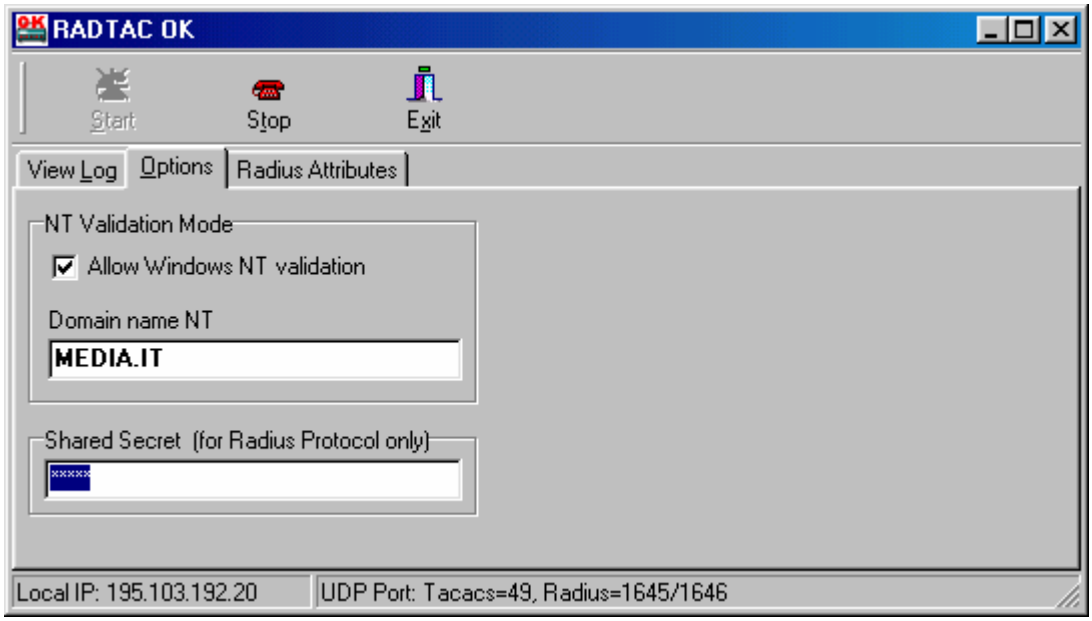
RadTac Emergency.

RadTac Emergency, also called RadTac OK, is a utility software included only in the licenced user package. It buffers a brief period of inactiveness of the “RadTac Service” authentication software. Authentication Software inactiveness is requested during the access log maintenance phase. They are contained in the internal database on the server in the c:\radtac\data directory. RadTac Emergency does not operate using the abovementioned database, at the same time all the authentication operations are active. This program has to be run every time that a maintenance of the database is required.



RADTAC EMERGENCY OPTION.

The only configurations possible for RadTac Emergency are available in the options menu.



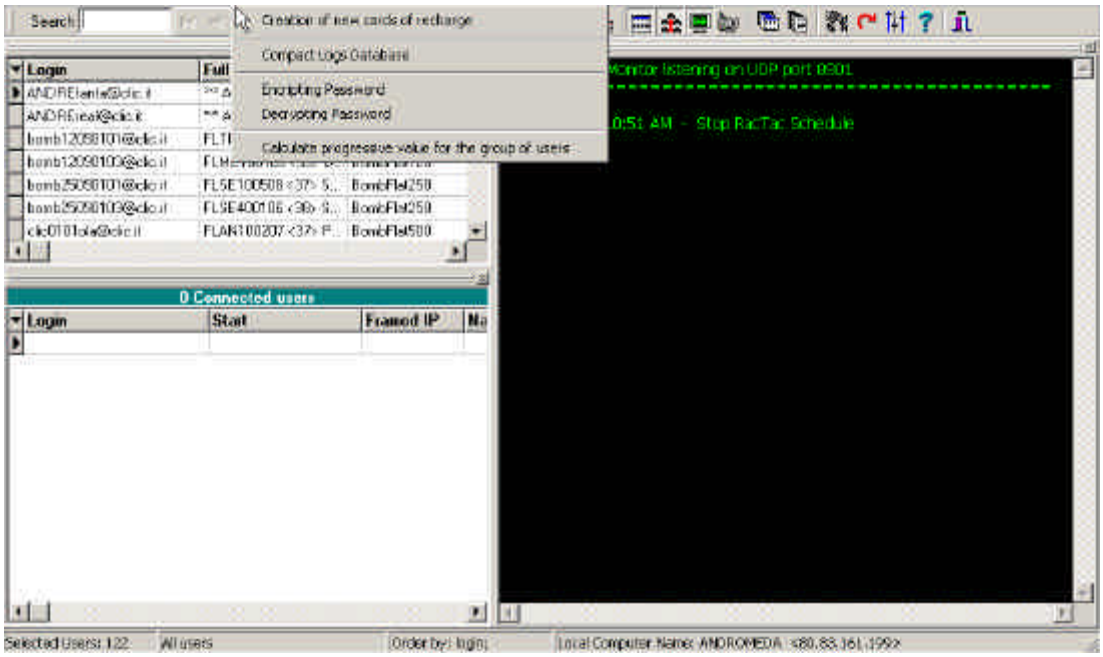
The software will operate in Windows NT mode, by selecting the "Allow Windows NT Validation Mode" check box, after this, indicate the Microsoft Domain name (NOT INTERNET). If the software is to operate in Windows 98/95 mode don't select the abovementioned check box. In this last case all users requesting access will enter the net without any checks. Having selected the Windows NT mode, RadTac Manager Server will run access controls in accordance with the settings made for the user in Windows NT; controlling password login, expiry date and hour bands.

MAINTENANCE PREARATION.

There are two different log types. One is in the c:\radtac\data, directory as a text file called RadTacGGMMAAAA.log , and the other is in the internal database c:\radtac\data\radtac.mdb Microsoft Access ©. The text type logs (.log) are generally saved so as to printout records of connections, for legal reasons. The access transactions contained in the RadTac Manager Server operations database are used by the applications to manager user by hour. The radtac.mdb Database can not be cancelled from the command line but has to be cleared by a suitable selections. To do this stop, Windows NT Service "RadTac Manager Service" in the services list or in Windows 98/95, and close the RadTac Service software. Then start RadTac OK, this will avoid time out reject access from net NASs. Then start RadTac Administrator to run the maintenance requests.

RADTAC Administrator TOOLS.

With RadTac Administrator you can run a maintenance on c:\radtac\data\radtaclog.mdb database. All operations allowed are under the Tools heading. It is a good habit to periodically run a “Compact Log Database”.

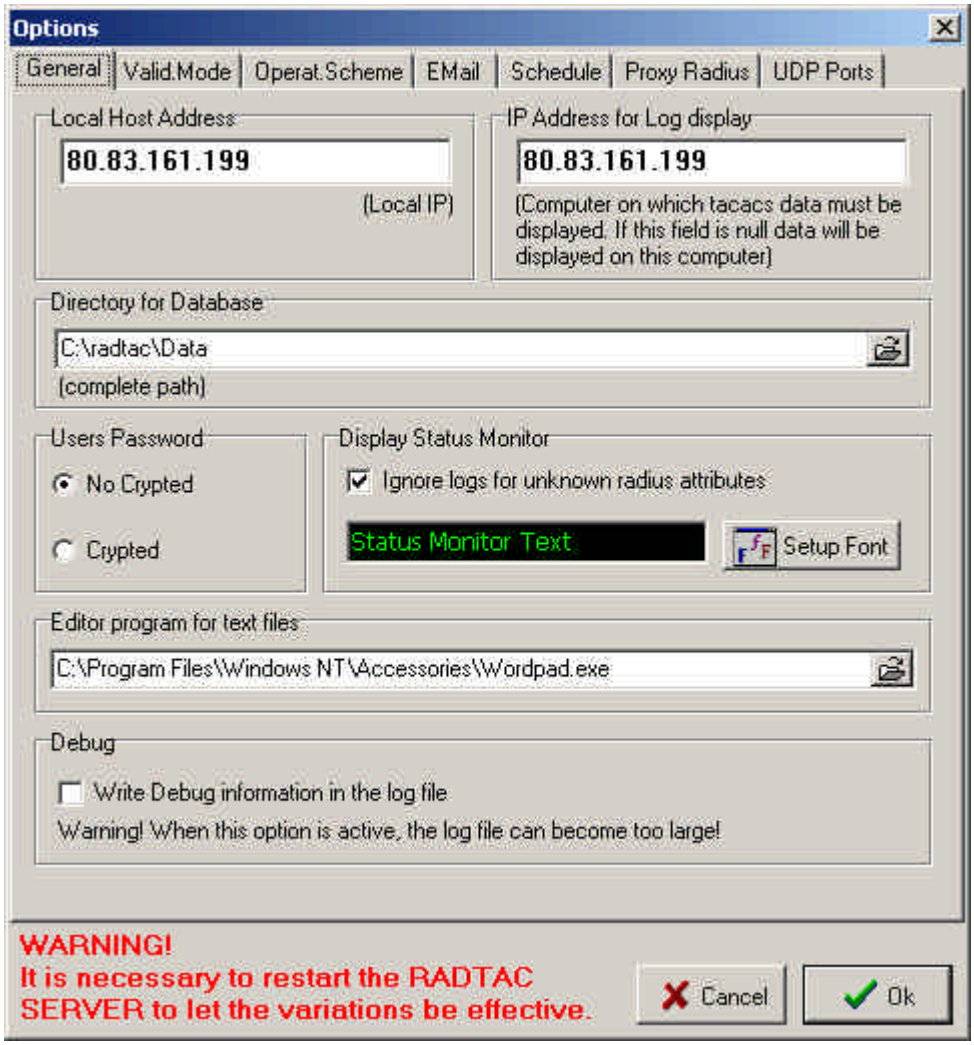


Compact database.

Compact database is one of the most important maintenance functions. It really cancels from the database all records cancelled logically with the Clear Log Function and then runs a structural repair of the tables. The Repair is also advisable after an unexpected shutdown of the Server NT. At restart, the user table could be damaged. RadTac Administrator uses repair to repair the structure of the database closing all un-computed records

ENCRYPT and DECRYPT Password.

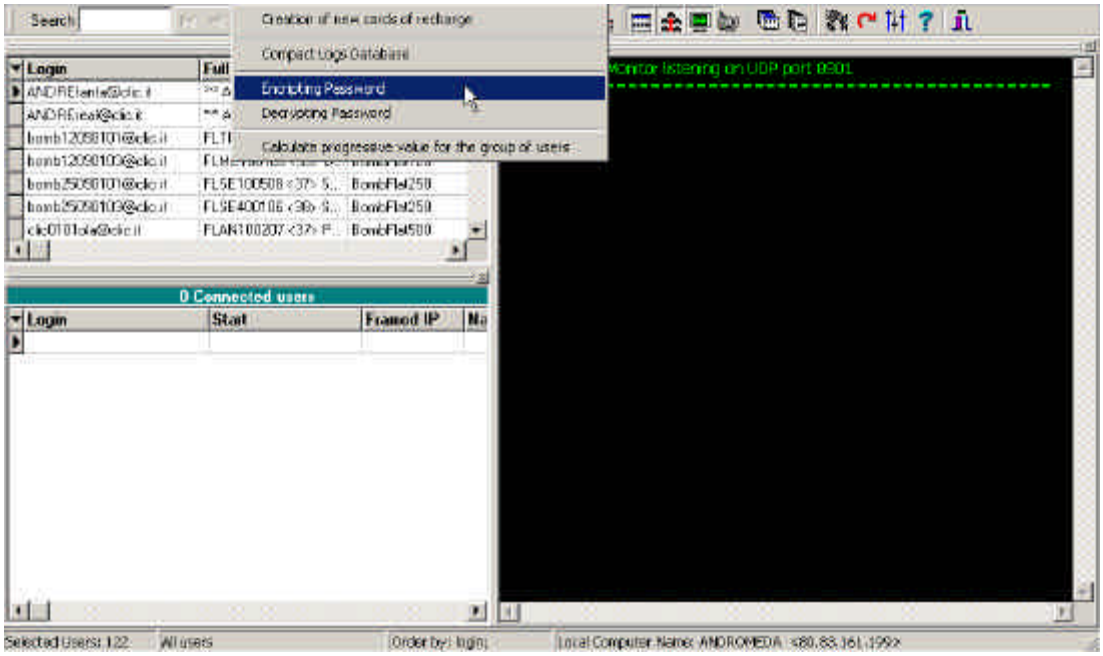
RadTac Manager Server manages the remote access user password in crypt or in clear. Selecting the operations mode is done from the RadTac Administrator



It is necessary to restart the program for variations to be effective.

All the same, if you need to modify the selection, changing the check box, from crypt to clear or vice versa, is not sufficient. You need to convert all the passwords present in the file from one mode to the other. The user password is memorized into the database during the inserting phase.

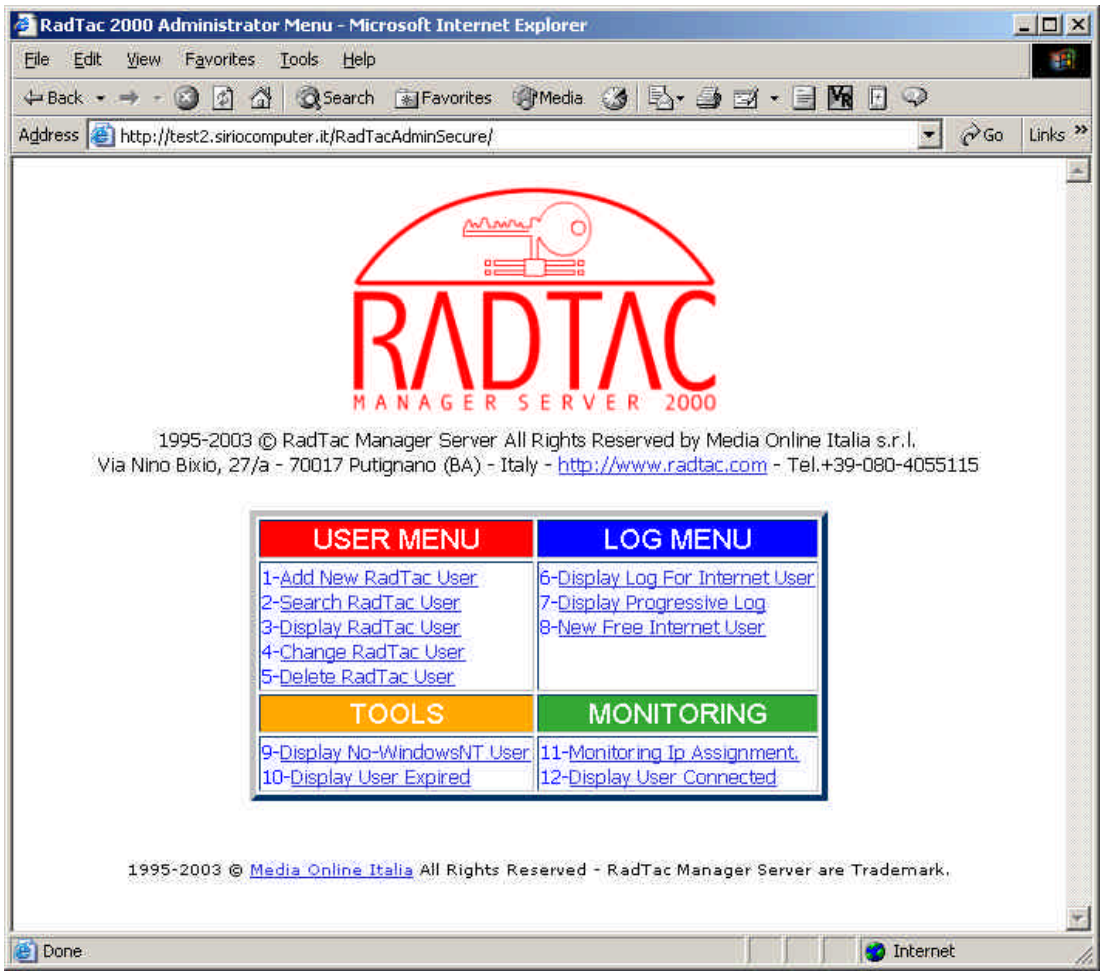
If you are operating in “NO CRYPTED” (clear), when inserting a new user the administrator will submit to the database the password in clear. During an access request the password in the database is compared with the value given by the NAS. By modifying the option from “No Crypted” to “Crypted” RadTac when authenticating thinks it has to compare a crypted password and thus runs a decrypt of the password (set in the database as clear), going into error. It is thus obligatory, if you want to change the operating mode, to convert the user password in the correct way.



Chapter 7

REMOTE ADMINISTRATION

RadTac 2000 Server has a configuration interface via Web, that allows to manage remote access users and the connections logs of these users. The applications operates through the Microsoft IIS 4.0 (or superior) ASP interpreter and the ODBC component data access.



WEB SERVICE

There are two different remote administration releases; one for Windows NT and another for Windows 98/95. They are on the hard disk, in RadTac Manager Server installation directory. The Windows NT release is in the c:\radtac\TacNTWeb directory. The Windows 98/95 is in the c:\radtac\Tac95Web. So as to use the remote administrations component, Microsoft IIS © has to be configured appropriately.

REMOTE ADMINISTRATOR VIA NT- 2000 O 2003 AUTHENTICATION.

This modality can be used if RadTac is configured in operational mode "active directory" or in "S.A.M. of Windows NT". During the step installation RadTac have generated in IIS a web folder alredy ready for use the web service remote access administrator.

To be access to this procedure is required the reset of the operating system, after the installation. After the reset you can digit the next url to be access:

http://Name_Of_The_Server.com/RadTacAdminSecure

Will be required a administrative login and password a after the confirmation will be displayed the webpage print in up page.

REMOTE ADMINISTRATOR VIA INTERNAL DATABASE AUTHENTICATION.

This modality can be used if you have configured RadTac for work with internal Microsoft Access database. The authentication is do with login and password stored in MSaccess database, for display progressive log access to the remote access user. The administrative access security is null if you use Windows 95-98. If you use internal database on Windows 2000 or NT you can set file permission on ASP web page for prevent the piracy attach.

To be access to this procedure is required the reset of the operating system, after the installation. After the reset you can digit the next url to be access:

http://nomedidominio.com/RadTacAdmin98

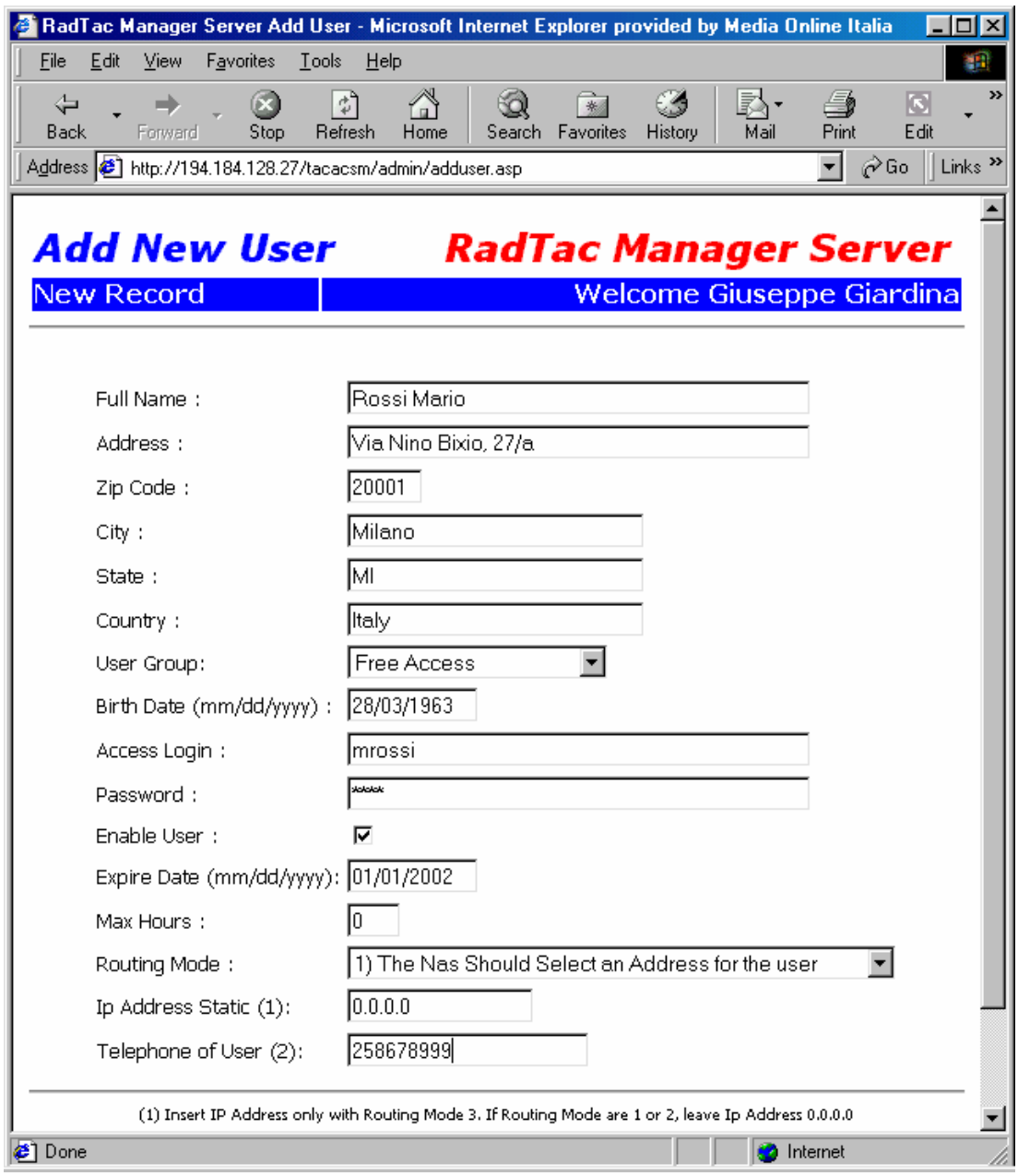
Will be displayed the menu web for remote administrator.

ACCESS RESTRICTIONS

In Windows 95/98 environment you can not restrict access to remote administers. In Windows NT environment you need only configure appropriately the access rights of the directory (example. c:\radtac\TacNTWeb). The web pages are located in this directory and "Domain Admin" should only access them. The (example c:\radtac\TacNTWeb\userlog) directory has to be appropriately configure, with restrictions on the file only to the Windows NT Group. For example "Domain Tacacs" so as the access remote user can visualize his access logs.

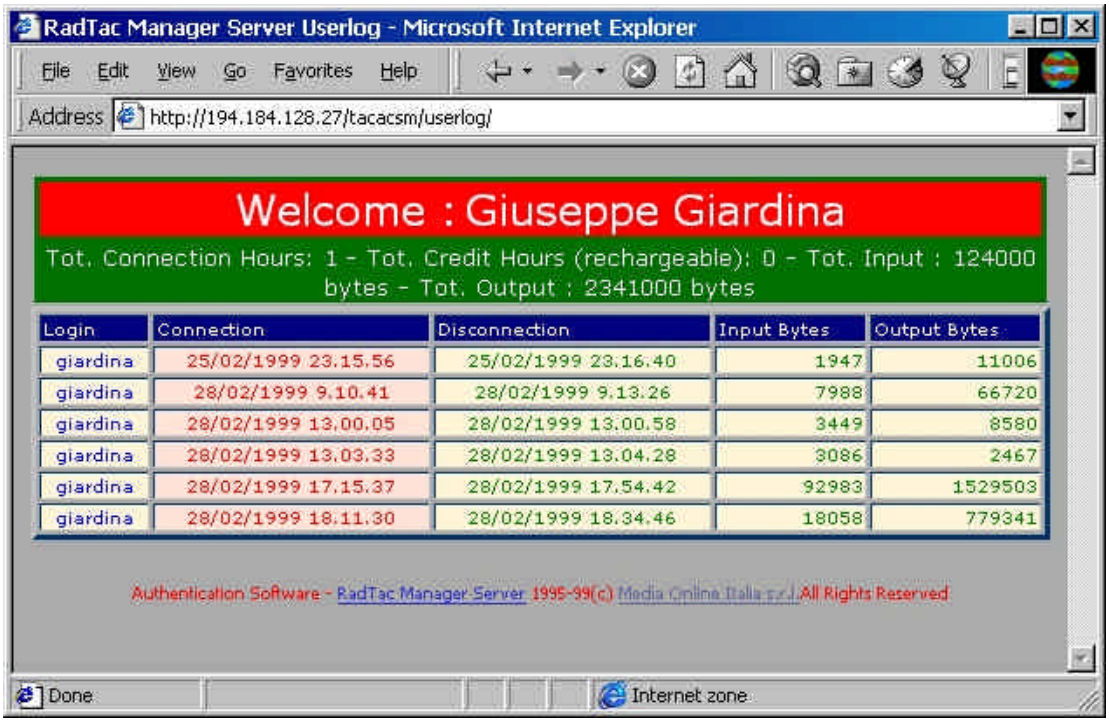
USER VIA WEB MANAGEMENT.

This procedure allows to add a new remote access user. The user is inserted by the administrations interface which is active both in Windows NT and Windows 98/95 mode. When RadTac Manager operated in Windows NT the user should not be inserted with the remote administrations interface but directly in the Windows NT Database. Notwithstanding this, you can all the same, load a user remotely, but for security reasons, is preferable that these users are copied into the Windows NT Database, as soon as possible. In fact, the Windosw NT users are automatically copied from the PDC (Primary Domain Controller) onto the BDC (Backup Domain Controller).



VIA WEB USERS EFFECTED CONNECTIONS DISPLAY.

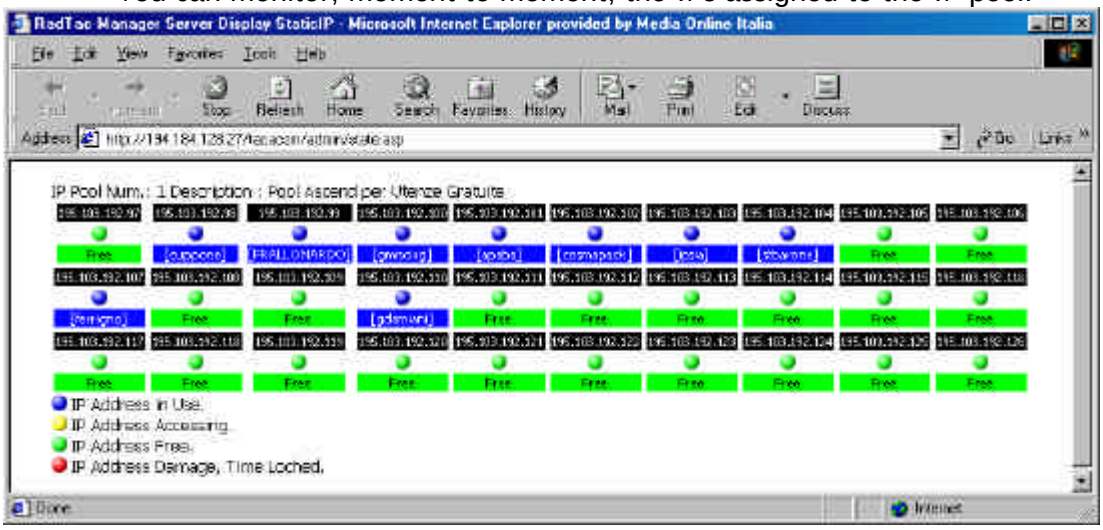
This Web function can be shown in the Service Provider's services. It has been connected in the administration menu only as to document its presence. Access to this page is protected by login and password.



To allow assess to the page by the log owner (example Giuseppe Giardina), in Windows NT environment, you need to restrict access to the userlog directory by Windows NT “Full Time” group where the ASP page is allocated. In this way the internet user the belongs to “Full Time” (of remote access) after have been validated can look at his access log. This function is useful for an “hour” user to keep track of his used hours, and his remaining hours.

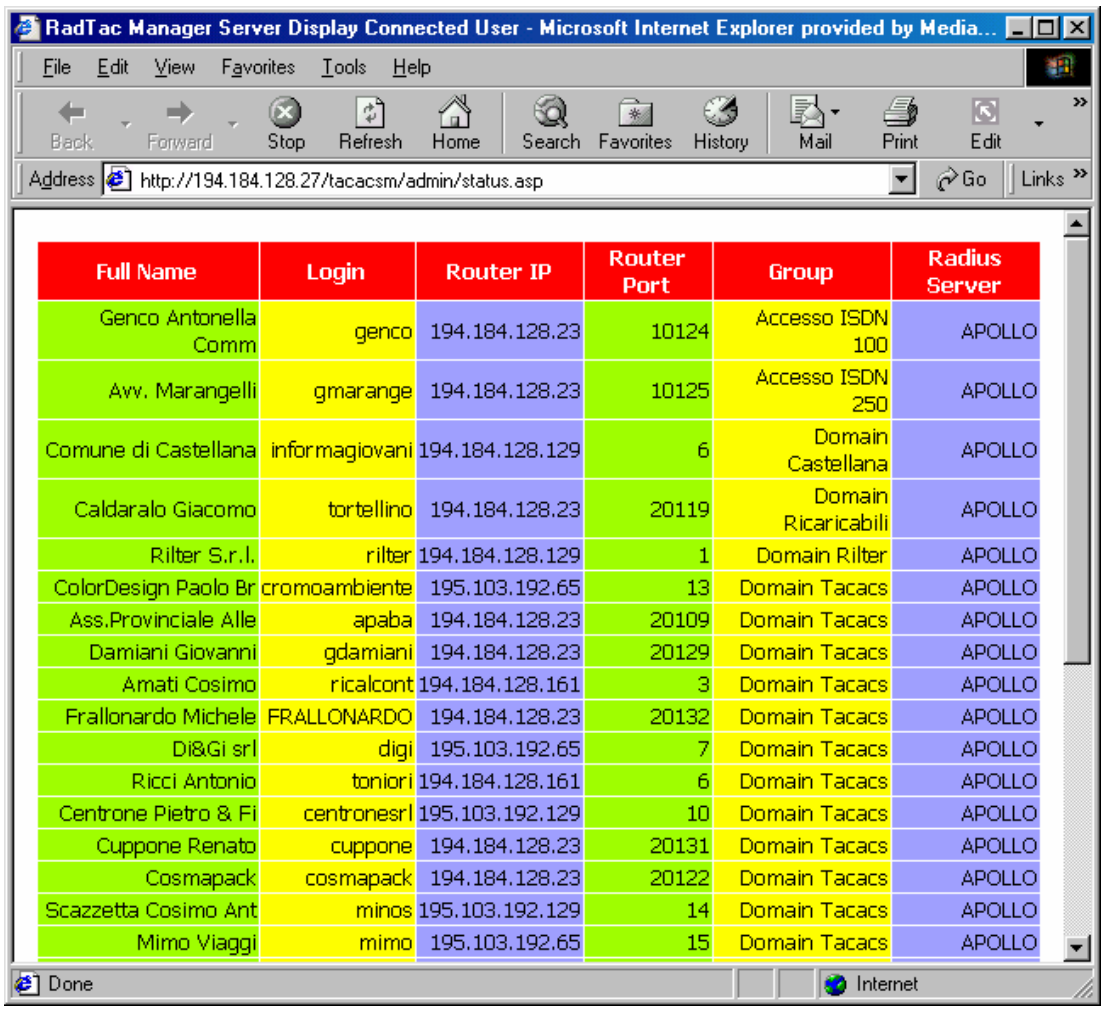
MONITORING THE IP POOL.

You can monitor, moment to moment, the IPs assigned to the IP pool.



MONITORING USERS CONNECTED.

You can monitor, moment to moment, users connected to the net.



Full Name	Login	Router IP	Router Port	Group	Radius Server
Genco Antonella Comm	genco	194.184.128.23	10124	Accesso ISDN 100	APOLLO
Avv. Marangelli	gmarange	194.184.128.23	10125	Accesso ISDN 250	APOLLO
Comune di Castellana	informagiovani	194.184.128.129	6	Domain Castellana	APOLLO
Caldaralo Giacomo	tortellino	194.184.128.23	20119	Domain Ricaricabili	APOLLO
Rilter S.r.l.	rilter	194.184.128.129	1	Domain Rilter	APOLLO
ColorDesign Paolo Br	cromoambiente	195.103.192.65	13	Domain Tacacs	APOLLO
Ass.Provinciale Alle	apaba	194.184.128.23	20109	Domain Tacacs	APOLLO
Damiani Giovanni	gdamiani	194.184.128.23	20129	Domain Tacacs	APOLLO
Amati Cosimo	ricalcont	194.184.128.161	3	Domain Tacacs	APOLLO
Frallonardo Michele	FRALLONARDO	194.184.128.23	20132	Domain Tacacs	APOLLO
Di&Gi srl	digi	195.103.192.65	7	Domain Tacacs	APOLLO
Ricci Antonio	toniori	194.184.128.161	6	Domain Tacacs	APOLLO
Centrone Pietro & Fi	centronesrl	195.103.192.129	10	Domain Tacacs	APOLLO
Cuppone Renato	cuppone	194.184.128.23	20131	Domain Tacacs	APOLLO
Cosmapack	cosmapack	194.184.128.23	20122	Domain Tacacs	APOLLO
Scazzetta Cosimo Ant	minos	195.103.192.129	14	Domain Tacacs	APOLLO
Mimo Viaggi	mimo	195.103.192.65	15	Domain Tacacs	APOLLO

Chapter 8

N.A.S. CONFIGURATION

Illustrated are some configurations regarding an Access Server Cisco, 2511, Cisco 3640 and an Ascend Max 6000. RadTac Manager Server supports Radius and Tacacs standards and thus compatible with any Access Server that repects these standards.

ALL THE SAME, IT IS ADVISABLE TO INSTALL THE SHAREWARE PRODUCT AND TEST ITS FUNCTIONS BEFORE BUYING IT. THE OFFICIAL SUPPORTED ROUTERS ARE CISCO AND ASCENT. YOU WILL NOT BE ABLE TO ASK, MEDIA ONLING ITALIA, FOR SUPPORT TO CONFIUGRE YOUR OWN ACCESS SERVER.

CISCO 2511 (TACACS).

```
!
interface Async1
ip unnumbered Ethernet0
ip tcp header-compression
encapsulation ppp
async dynamic routing
async mode dedicated
peer default ip address 194.184.128.66
no cdp enable
ppp authentication pap
ppp use-tacacs
!
tacacs-server host 195.103.192.18
tacacs-server attempts 10
tacacs-server last-resort password
tacacs-server timeout 4
tacacs-server extended
tacacs-server authenticate slip
tacacs-server notify connections
tacacs-server notify enable
tacacs-server notify logout
tacacs-server notify slip
!
line 1 14
script dialer cisco-default
login tacacs
modem DialIn
transport input all
stopbits 1
rxspeed 115200
txspeed 115200
flowcontrol hardware
!
```

CISCO 2511 (RADIUS).

```
!
version 11.3
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname router1.media.it
!
boot system flash
aaa new-model
aaa authentication login use-radius radius
aaa authentication ppp ppp-radius radius
aaa authorization network radius if-authenticated
aaa accounting network start-stop radius
aaa accounting system start-stop radius
!
ip subnet-zero
no ip finger
ip domain-name media.it
ip name-server 194.184.128.11
ip name-server 194.184.128.12
async-bootp dns-server 194.184.128.11 194.184.128.12
chat-script cisco-default ABORT ERROR "" "AT Z" OK "ATDT \T" TIMEOUT 30 \c
CONNECT \c
!
!
interface Ethernet0
 ip address 194.184.128.30 255.255.255.224
 no ip redirects
 no ip unreachables
 no ip directed-broadcast
 no ip proxy-arp
 no ip route-cache
 no ip mroute-cache
!
interface Serial0
 ip unnumbered Ethernet0
 no ip redirects
```

```
 no ip unreachables
 no ip directed-broadcast
 no ip proxy-arp
 no ip route-cache
 no ip mroute-cache
 bandwidth 64
 no fair-queue
!
interface Serial1
 ip unnumbered Ethernet0
 no ip redirects
 no ip unreachables
 no ip directed-broadcast
 no ip proxy-arp
 no ip route-cache
 no ip mroute-cache
 bandwidth 64
!
interface Group-Async1
 ip unnumbered Ethernet0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip tcp header-compression
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 bandwidth 56
 async dynamic address
 async dynamic routing
 async mode dedicated
 peer default ip address pool asincrone
 no fair-queue
 no cdp enable
 ppp authentication pap ppp-radius
 group-range 1 12
!
interface Group-Async2
 ip unnumbered Ethernet0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip tcp header-compression
 encapsulation ppp
 no ip mroute-cache
 bandwidth 64
 async dynamic address
 async dynamic routing
 async mode dedicated
 peer default ip address pool isdn
 no fair-queue
 no cdp enable
```

```
 ppp authentication pap ppp-radius
 group-range 13 16
!
ip local pool asincrone 194.184.128.66 194.184.128.77
ip local pool isdn 194.184.128.78 194.184.128.81
ip classless
ip route 0.0.0.0 0.0.0.0 195.103.192.1
ip route 194.184.128.96 255.255.255.224 Serial0
ip route 195.103.192.128 255.255.255.224 Serial1
!
no logging console
radius-server host 194.184.128.27 auth-port 1645 acct-port 1646
radius-server retransmit 1
radius-server timeout 4
!
line con 0
line 1 16
 script dialer cisco-default
 login authentication use-radius
 modem Dialin
 transport input all
 stopbits 1
 speed 115200
 flowcontrol hardware
line aux 0
 transport input all
line vty 0 4
 login authentication use-radius
!
end
```

CISCO 3640 (RADIUS).

```
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname cisco3640
!
aaa new-model
aaa authentication login use-radius radius local
aaa authentication ppp ppp-radius radius
aaa accounting network start-stop radius

modem country mica italy
ip domain-name cisco.com
ip name-server 212.210.246.2
ip name-server 212.210.246.4
isdn switch-type primary-net5
chat-script offhook "" "ATH1" OK
chat-script default ""at&fs0=1 ok
clock timezone MET 2
clock summer-time MET recurring last Sun Mar 2:00 last Sun Sep 2:00
!
controller E1 0/0
framing NO-CRC4
pri-group timeslots 1-31
!
interface Serial0/0:15
ip unnumbered Ethernet1/0
encapsulation ppp
no ip mroute-cache
isdn incoming-voice modem
peer default ip address pool reteLAN
dialer-group 1
no cdp enable
ppp authentication pap ppp-radius
!
interface Ethernet1/0
ip address 212.210.246.30 255.255.255.0
!
interface Group-Async1
```

```
ip unnumbered Ethernet1/0
ip tcp header-compression
encapsulation ppp
async dynamic routing
async mode dedicated
peer default ip address pool reteLAN
no cdp enable
ppp authentication pap ppp-radius
group-range 65 94
!
router igrp 1
network 212.210.246.0
!
ip local pool reteLAN 212.210.246.32 212.210.246.61
ip classless
ip route 0.0.0.0 0.0.0.0 212.210.246.1
dialer-list 1 protocol ip permit
radius-server host 212.210.246.7 auth-port 1645 acct-port 1646
radius-server retransmit 1
radius-server timeout 10
!
line con 0
line 65 94
autoselect during-login
autoselect ppp
script startup default
script reset default
login authentication use-radius
modem Dialin
no history
no editing
transport input all
autohangup
stopbits 1
flowcontrol hardware
line aux 0
line vty 0 4
login authentication use-radius
!
end
```

ASCEND MAX 6000

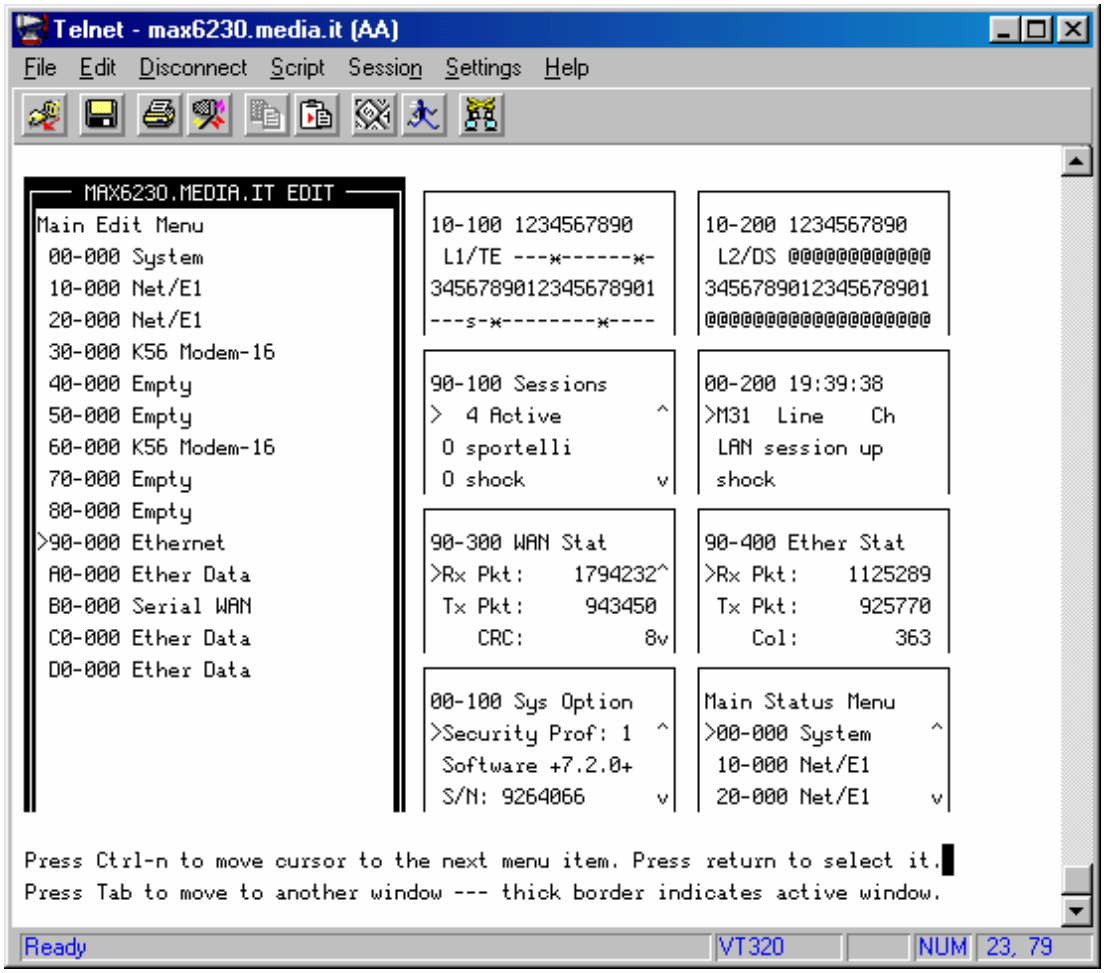
All Access Server Ascend, to function correctly with RadTac Manager Server have to make the following NAS configuration. These setting are in the Menus:

- Ethernet-> ModConfig -> Auth -> Auth src Port -> 1645
- Ethernet-> ModConfig -> Accounting -> Accounting src Port -> 1646

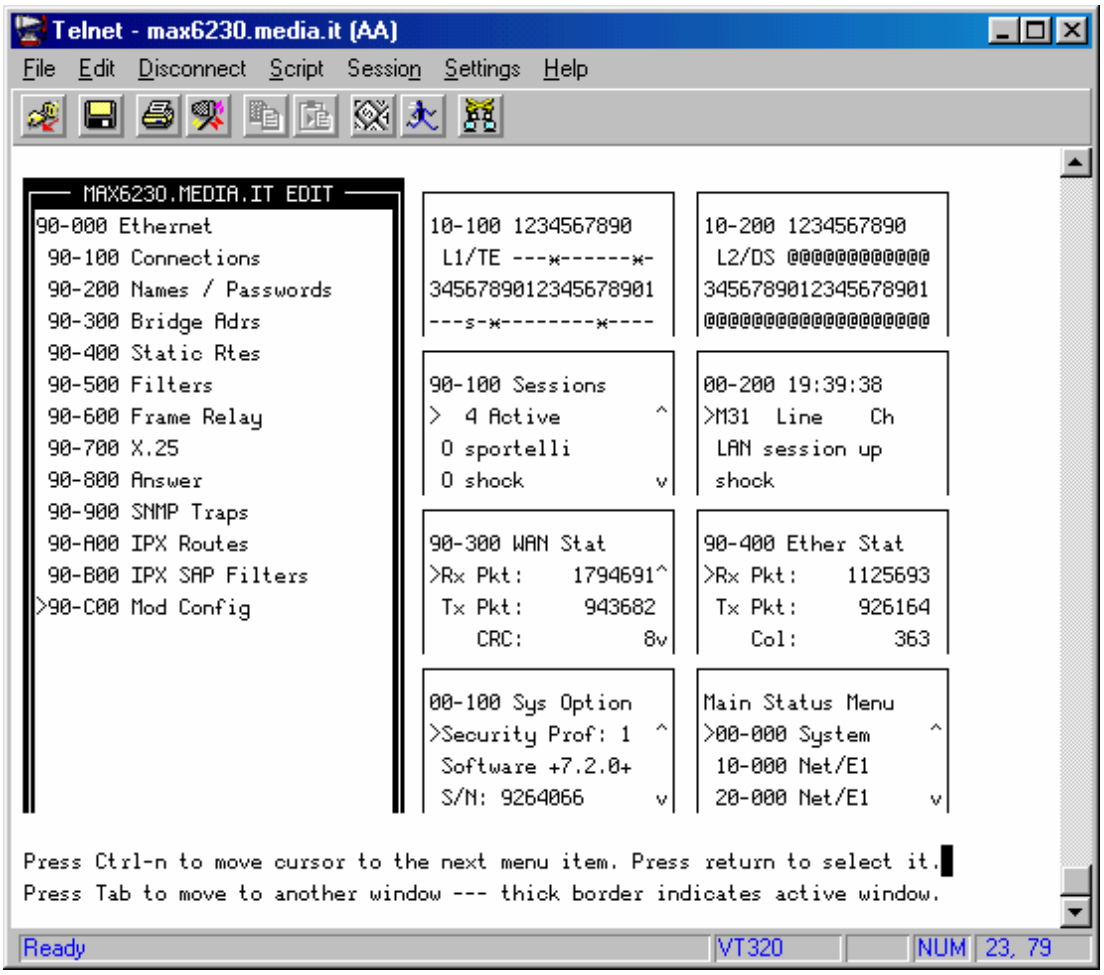
The Default value for both entries 0 (Zero).

For further details about these setting refer to the below illustration.

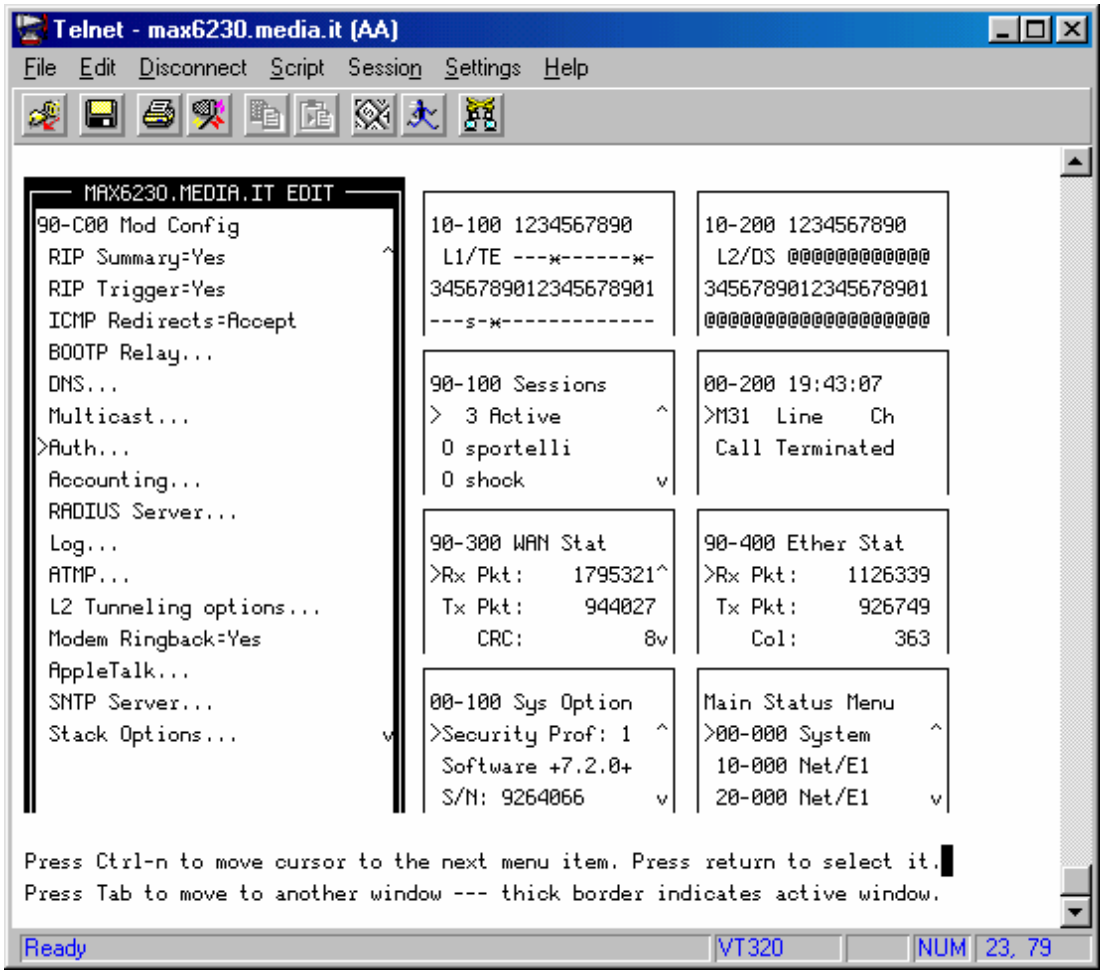
- Selection Ethernet from the Administration Menu via Telnet.



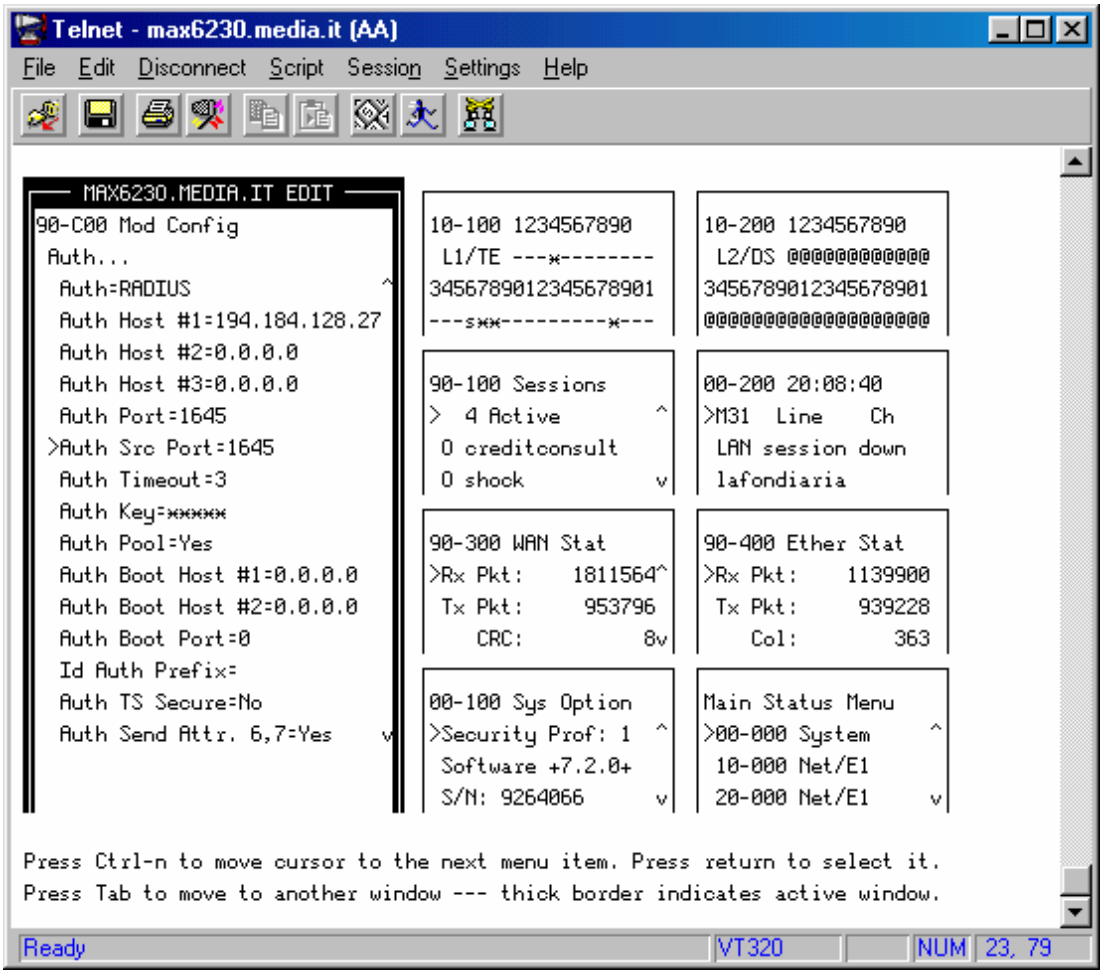
The Ethernet Menu of an Ascent Max has multiple vocice1. Select Mod Config.



The Mod Config Menu also presents multiple voices. Scroll down the items until you reach “Auth” (Authentication). Select the [INVIO] key.

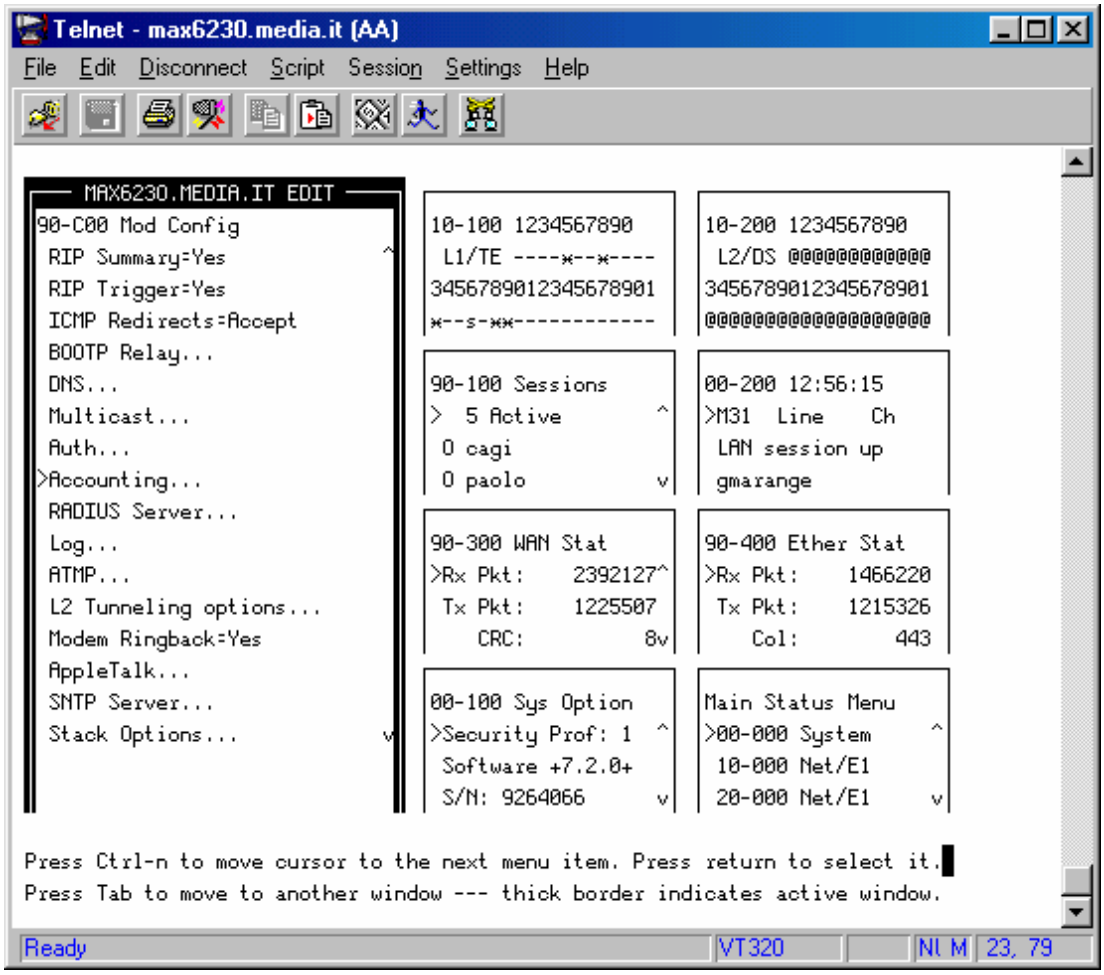


In this item there are all the authentication values regarding the settings. Auth = RADIUS says to Max that the authentication has to be in Radius protocol. Auth Host = IP Address says to Max the Server RadTac Manager IP Addrress. With subsequent Auth Hosts you can define more than one Radius Server. Auth Port = 1645 sets the correct UDP port for RadTac Manager Server. **Take attention to the Auth Src Port = 1645 field,** the defult have is 0 (Zero) and has to be set at 1645 to operate correctly with RadTac Manager Server.

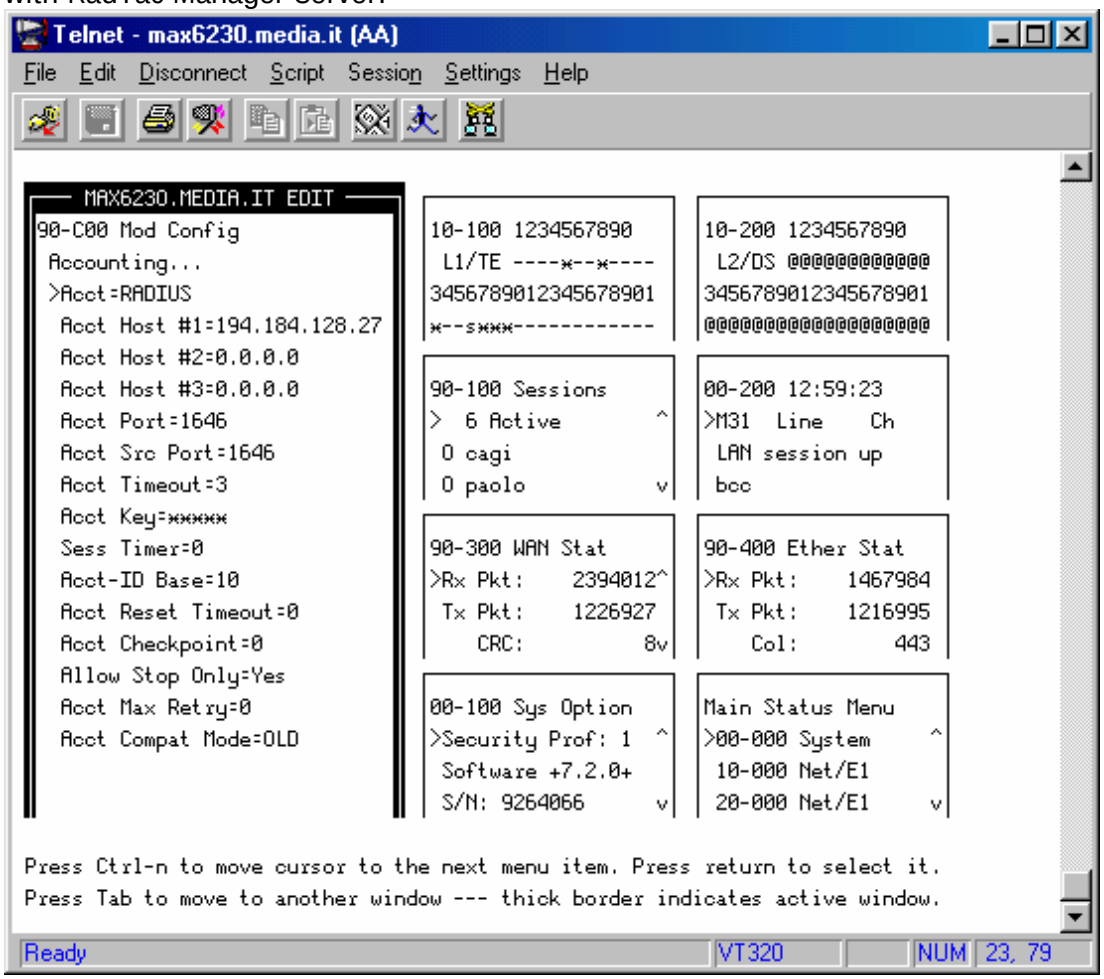


ESC from the Menu and save the settings on NAS FLASH. You now need to set the values that are in the Accounting menu.

The Accounting Menu is in Ethernet setting in Mod Config Menu. Select “edit values”.



All the values regarding Accounting settings are in this entry. Acct = RADIUS says to the Max that accounting has to start Radius protocol. Acct Host = IP Address says to Max the Server RadTac Manager IP Address. With the following Acct Hosts you can define more than one Radius Server. Acct Port = 1646 sets the correct UDP port for RadTac Manager Server. **Take attention to the Acct Src Port = 1646 field,** the default value is 0 (Zero) and has to be set at 1646 to operate correctly with RadTac Manager Server.



NAS Max is now ready to operate with RadTac Manager Server.