Teldat Router

RADIUS Protocol

Doc. *DM733-I* Rev. *10.10*
June, 2003

INDEX

Chapter 1
Introduction

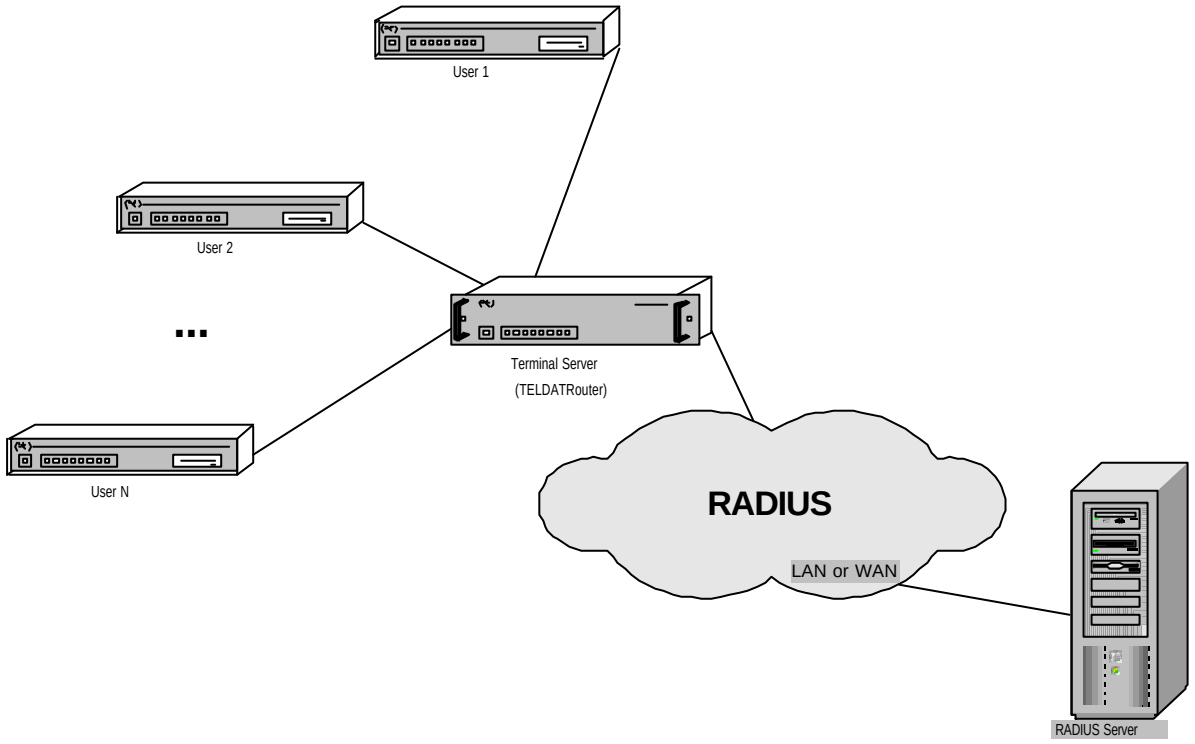
1. Introduction to Radius Protocol

At present, Network Managers have very few tools in order to protect the security of their networks against undesired events i.e. break-ins. State of the art security systems generally require specific hardware or are only compatable with a limited number of products. This problem is further aggrevated in large networks due to the high number of access points. From this point of view, RADIUS (Remote Authentication Dial In User Service) constitutes a solution for those problems associated with security requirements in accesses and in addition to authentication and authorization, permiting you to send configuration information from a RADIUS Authentication Server.

The main environments that can use the RADIUS protocol are explained below.

1.1. Authentication and configuration for PPP connections

This scenario corresponds to a Terminal Server providing a network access service to users though PPP connections via a serial line, modem or ISDN.



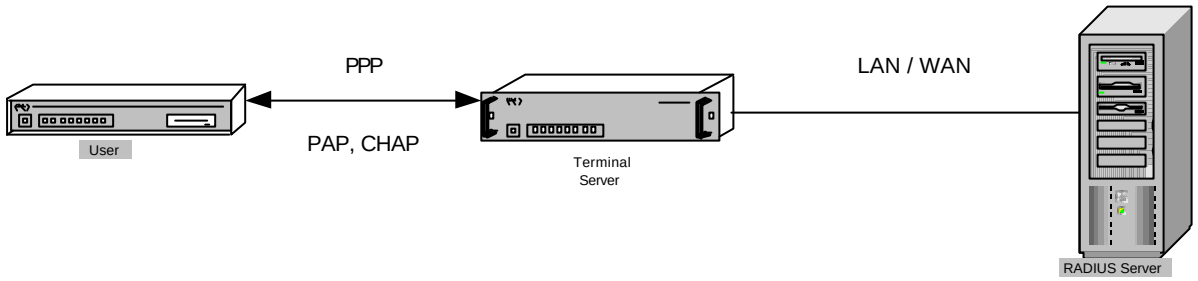
Within this context and so a user can connect to the network through the Terminal Server, access must be authorized. In order for this to happen, the user transmits unique information on his identity to the Terminal Server who decides whether to authorize this connection or not by comparing data received related to authorized users. In this case, the Terminal Server must also provide the results of the authentication, negociating in a positive case the IP address through which the user may connect.

On the other hand, if you use the RADIUS protocol, information proceeding from the various users collected by the Terminal Server, is in turn sent to the RADIUS Server who takes over the role of deciding whether network access when requested by a user, is authorized or denied depending on the

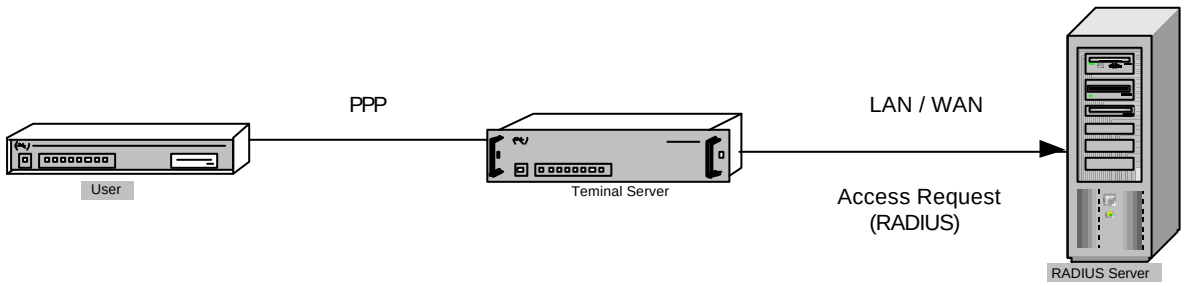
database. The decision taken by the RADIUS Server is then communicated to the Terminal Server who in turn transmits this to the user. In this case, the IP address through which an authorized user can connect, is taken from the RADIUS Server's database (**Framed-IP-Address**) and sent to the destination thorugh the Terminal Server. The RADIUS Server also sends the mask for the said address (**Framed-IP-Netmask**) in order to determine the range of addresses requested by the user, the routes must be configured in the Terminal Server in order to access to the networks connected to the user (**Framed-Route**), and information on whether the user is available to listen and/or send packets containing routing advertising (**Framed-Routing**). In this latter case, the Terminal Server's local end must autoconfigure an address pertaining to the same subnet as the remote end for the user in order to be able to carry out the exchange of the said packets.

In this operation mode, it is said that the Terminal Server acts as a RADIUS client as it transfers the users connection petitions to the RADIUS Server so the latter can validate these.

The users can provide the necessary information for validation purposes to the Terminal Server following the various authentication mechanisms. However for PPP connections, the possible alternatives are PAP and CHAP authentication protocols.



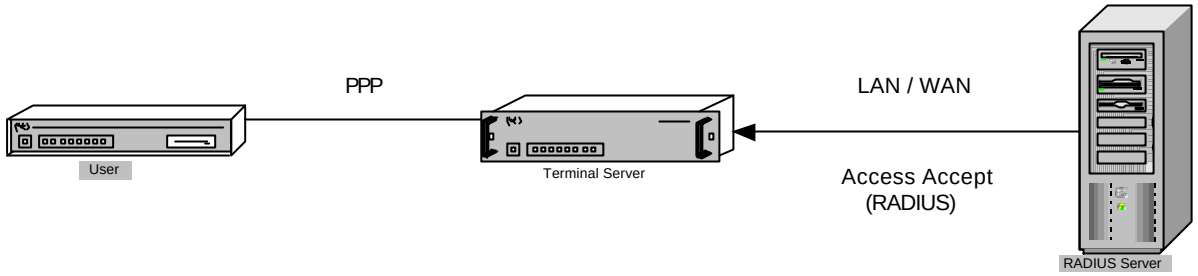
The RADIUS authentication procedure unfolds in the following way. When the Terminal Server receives the information concerning the users identification, it creates an access petition (**Access Request**) and then sends this to the RADIUS Server through the network. When a password is present in the petition, it is hidden in order to ensure confidentiality. If the RADIUS Server does not respond to the petition within a certain period of time, the Terminal Server resends it and can repeat this process a determined number of times.



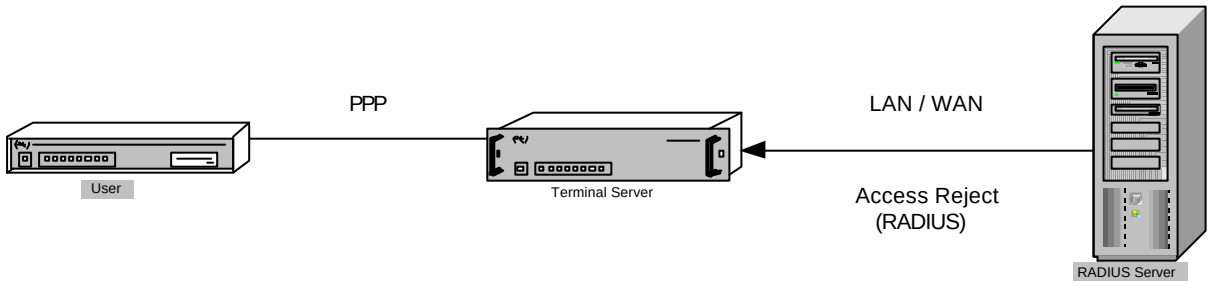
Once the RADIUS Server receives the petition, it first authenticates the Terminal Server sending it. To achieve this, the RADIUS Server uses information contained in the petition and a secret configured in both devices. This secret is a password shared among the Servers and is never transmitted through the network so providing greater security If the Terminal Server is not valid, the petition is discarded; otherwise, the RADIUS Server consults its database to check that the user mentioned in the petition is permitted access.

In cases where the Terminal Server has been validated, the RADIUS Server can respond to an access request in one of three ways.

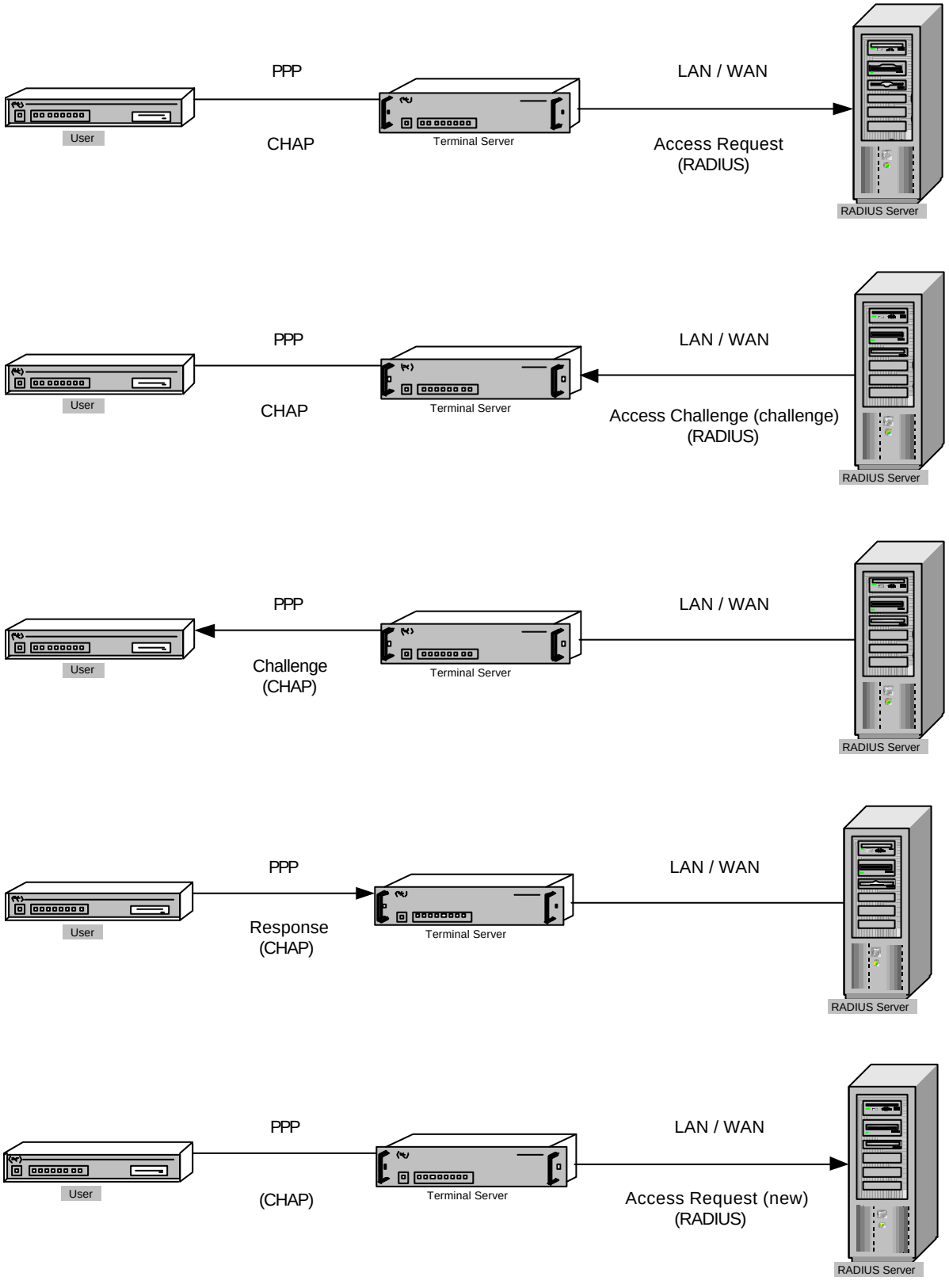
If the RADIUS Server checks that the user making the connection request is on the list of authorized users, it transmits an access acceptance (**Access Accept**) to the Terminal Server, where the user configuration values figure as for example the user connection IP address.

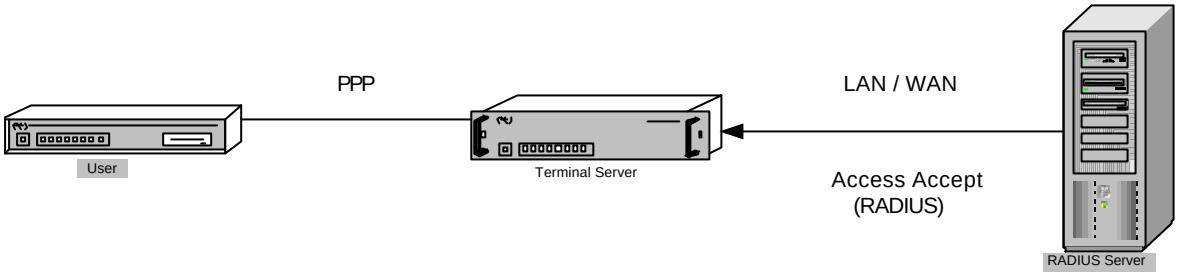


Otherwise, if the user wishes to connect to a network that is not contained in the RADIUS Server's database, the RADIUS Server denies the petition and sends a reject response (**Access Reject**) to the Terminal Server. This rejection in turn to sent to the user informing him that the connection has not been conceded.



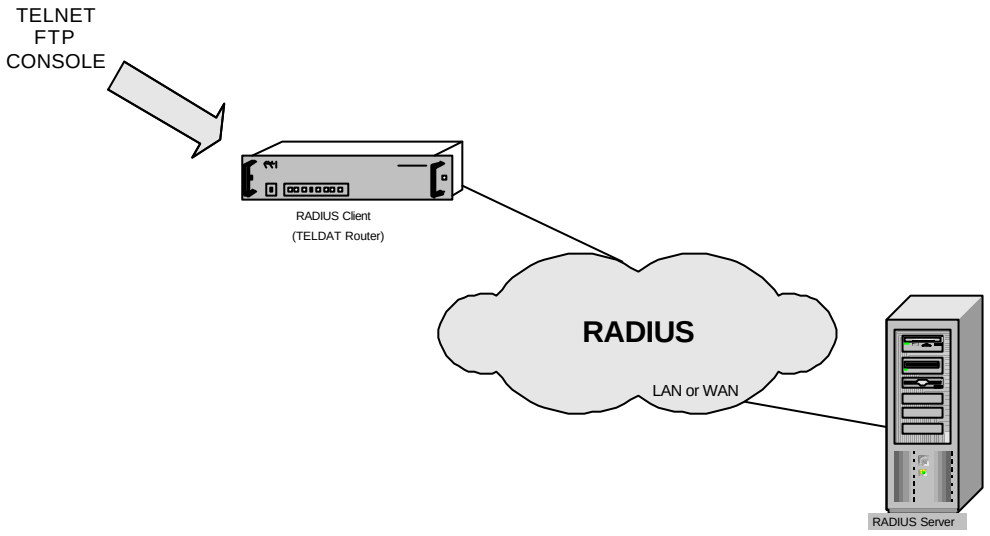
If the authentication protocol is CHAP, there exists the possibility that the RADIUS Server will not transmit the expected Access Accept packet for a user connection petition that has been authorized, and instead "challenges" the said user to authenticate again. To do this, the RADIUS Server sends an **Access Challenge** packet to the Terminal Server where it includes a unique and unpredictable numerical value in one of its attributes known as **challenge**. The Terminal Server communicates the challenge to the user and the latter with this value effects a new access request to the network (**response**). The user also sends this new petition to the Terminal Server who in turn transmits this to the RADIUS Server through a new Access Request packet. Finally the RADIUS Server compares the data received in this packet with those it expected to receive and acts in consequence. I.e. if the information contained in the packet is what the RADIUS Server expected, an Access Accept packet containing the connection IP address is sent to the Terminal Server. Contrariwise, if the information is not the expected, an Access Reject packet rejecting the access request is sent. Finally, the RADIUS Server can challenge the user again for authentication purposes by transmitting another Access Challenge packet.


PPP
CHAP
User
Terminal Server
LAN / WAN
Access Request
(RADIUS)
RADIUS Server
PPP
CHAP
User
Terminal Server
LAN / WAN
Access Challenge (challenge)
(RADIUS)
RADIUS Server
PPP
Challenge
(CHAP)
User
Terminal Server
LAN / WAN
RADIUS Server
PPP
Response
(CHAP)
User
Terminal Server
LAN / WAN
RADIUS Server
PPP
(CHAP)
User
Terminal Server
LAN / WAN
Access Request (new)
(RADIUS)
RADIUS Server



1.2. Authentication and configuration for the Telnet FTP and console connections

In this case, it is the TELNET, FTP and console connections over a device that needs authentication and configuration through the RADIUS protocol.



In order for a user to access the router through these connections, authorization for the said access is required. For this, the users transmit unique information on their identity to the device when this requests it. If the RADIUS protocol is not being used, it is the router itself that decides whether to authorize the connection or not, matching the received data with that configured in the same.

On the other hand, if the RADIUS protocol is used, the information proceeding from the various users collected by the router is in turn sent to the RADIUS Server. It is the RADIUS Server in this case that determines whether the connection requested by the user is authorized or not depending on its internal database and subsequently transmits the results to the router. The RADIUS packets exchange process is identical to that explained above for PPP connections.

In cases of authentication over the **Teldat Router**, you have permission when accessing the different processes and executing some restricted commands depending on the user you have authenticated through.

The Teldat routers change all the user name characters to uppercase even if they are introduced in lowercase therefore in the RADIUS servers configurations you must include these with this characteristic.

So that the user can be authenticated in the system, you must introduce the user and the corresponding password unless there is a device access key locally defined through the **SET PASSWORD** command and there are no users locally defined. In this case, in the TELNET and console connections over the Teldat routers, the user name is not requested and only the key or password will be requested. Due to the fact that the RADIUS Servers need a user name, the router sends "TELNET" when there is a TELNET connection and "CONSOLE" with a console connection, this being hidden from the user, but should be taken into account when configuring the RADIUS Server.

The following example shows how to define a user with his/her coresponding password and the Config access level:

```
vcm Auth-Type = Local, Password = "LaMia"
         Service-Type = Login-User,
         Login-Service = Config
```

The following access levels are defined for the **Service-Type** attribute in order to access FTP, telnet or console:

Administrative: Permits access through FTP, Telnet and console. Access through FTP is carried out as ROOT. The access level for Telnet and console is determined by the Login-Service attribute.

NAS Prompt: Permits access through FTP, Telnet and console. Access through FTP is carried out as ANONYMOUS. The access level for Telnet and console is determined by the Login-Service attribute.

Login: Access is only permitted through Telnet and console. The access level for Telnet and console is determined by the Login-Service attribute.

The Service-Type attribute must always be present in the user attribute definition.

Five different access levels have been defined for the **Login-Service** attribute:

None: You are not permitted to access the system.

Events: Permits you to access the Console Management (P1), Events Viewing (P2) and you are not permitted to execute the Ping, Telnet, Restart nor Load commands.

Monitor: Permits you to access the Console Management (P1), Events Viewing (P2) and the Monitoring process (P3). You can also execute the Ping and Telnet commands however you cannot execute the Restart or Load commands.

Config: You have access to all the processes and the standard commands.

Root: In addition to having access to all the standard commands, you can also access the user management own commands. These are explained further on in the manual.

Due to the fact that these access levels are not standard, you need to define them in the Radius server dictionary as indicated below:

```
VALUE     Login-Service          None            800
VALUE     Login-Service          Event           801
VALUE     Login-Service          Monitor         802
VALUE     Login-Service          Config          803
VALUE     Login-Service          Root            804
```

On registering the authorized users in the Radius server, you need to indicate the corresponding access level. If you omit the Login-Service attribute value, then the access level is considered as Root.

Further information on local device authentication can be found in Chapter 1 "The Teldat Router Console" in manual Dm 704-I "Configuration and Monitoring".

If you activate authentication through Radius, this takes preference over any other type of local device authentication.

As you can see, the RADIUS authentication process simplifies the security process by separating the user authentication and authorizing tasks from the communications processes themselves. However, the existence of a RADIUS Server drawing the information from different users together, provides greater security than locating this data in various servers scattered around the network. In the same way, the RADIUS Server is capable of supporting hundreds of Terminal Servers who in turn can provide service for up to tens of thousand of users in a safe simple way.

Given the advantages offered by the use of a RADIUS server in this environment, TELDAT has implemented this protocol in its routers complying with the **RFC 2138** standard. In these devices, the RADIUS authetication process operates in the same way as described above except that the router currently does not support challenge/response function. This means that if a TELDAT router, acting as a Terminal Server, receives Access Challenge packets from the RADIUS Server, it treates them in the same way as if they were Acess Reject packets.

The RADIUS protocol can be enabled in any interface that has a PPP connection established through a serial line or ISDN with the user requiring authentication. For this, you must globally enable the primary RADIUS in the RADIUS configuration menu and subsequently enable RADIUS validation in the required PPP interface. In the same way, you need to globally enable the RADIUS in the device and then in the TELNET, FTP and console connections in order to authecate these through the protocol. RADIUS authentication cannot be enabled if the IP address for the RADIUS Server where the connection petitions are sent has not been configured, as well as the "secret" shared between the router and this RADIUS Server.

At this point you can also configure the IP address and "secret" for an alternative RADIUS Server which intervines if the primary Server does not respond, the UDP ports, the Terminal Server's ID, the number of times it is possible to resend a peitition should no reponse be received from the RADIUS Servers and the time between resends. The value for these parameters can be independently

established or established as a group with the rest making consultation between them possible with the obvious exception of the "secrets".

> ***In cases of TELNET connections and console with authentication through RADIUS, if you do not receive any type of response from the RADIUS servers, local authentication of the device will be carried out.***

In the protocol monitoring on the other hand, you can list the statistics for the exchanged packets in the different authentication processes that have been executed since the device was last restarted. These are defined in the **RFC 2618** standard. Lastly, an events system has been defined for this protocol that "marks" the key points during the user validation process through the RADIUS Servers.

You will find the configuration and monitoring for this protocol been fully explained in the next two chapters.

Chapter 2
Configuration

1. Accessing the Radius Protocol configuration

The commands required to configure the device as client Terminal Server for a RADIUS Server are described. In the first place you need to access the configuration environment ("RADIUS config>" prompt); for this you need to enter the following commands:

```
*P 4

Config>FEATURE RADIUS

-- RADIUS User Configuration --
RADIUS config>
```

2. Configuration Commands

Once situated in the configuration environment, you can configure the parameters. For this you have the following commands summarized in the below table:

Command	Function
? (HELP)	Displays all the available commands and their options.
ALTERNATE-ADDRESS	Configures the alternate Radius server IP address.
ALTERNATE-PORT	Configures the connection port to the alternate Radius server.
ALTERNATE-SECRET	Configures the access password for the alternate Radius server.
ATTEMPTS	Configures the number of Radius petition transmisión attempts.
CONSOLE	Enables or disables Radius authentication for console access to the device.
DELAY	Configures the time between authentication petition resends to the Radius server.
DISABLE	Disables the Radius protocol.
ENABLE	Enables the Radius protocol.
FTP	Enables or disables Radius authentication for access via FTP to the device.
IDENTIFIER	Configures the identifier for the device.
LIST	Displays the values of the configured parameters.
NO	Configures the distinct parameters to their default value.
PRIMARY-ADDRESS	Configures the primary Radius server IP address.
PRIMARY-PORT	Configures the connection port for the primary Radius server.
PRIMARY-SECRET	Configures the access password for the primary Radius server.
SOURCE-INTERFACE	Configures the RADIUS packets source interface.
TELNET	Enables or disables Radius authentication for access via TELNET to the device.
EXIT	Returns to the previous prompt.

Each of the commands have been explained in more detail below.

2.1. ? (HELP)

This command can be used in two ways. Firstly, it permits you to obtain a list of all the available commands in the RADIUS configuration environment by entering **?** at the "RADIUS config>" prompt.

Syntax:

```
RADIUS config>?
```

Example:

```
RADIUS config>?
  alternate-address
  alternate-port
  alternate-secret
  attempts
```

```
  console
  delay
  disable
  enable
  ftp
  identifier
  list
  no
  primary-address
  primary-port
  primary-secret
  source-interface
  telnet
  exit
RADIUS conf>
```

This command can also be used to view the available options for a specfic command in the configuration menu. In this case, you can view the options for a specific command by entering the command name followed by a questions mark **?**. In the case of **CONSOLE**:

Example:

```
RADIUS config>CONSOLE ?
DISABLED
ENABLED
RADIUS config>
```

2.2. ALTERNATE-ADDRESS

This command is used to configured the IP address for the alternative RADIUS Server that the device will send RADIUS authentication requests to should the primary RADIUS Server not respond. This address is configured in the following way:

Example:

```
RADIUS config>SET ALTERNATE-ADDRESS
Alternate RADIUS server IP address [192.6.1.227]? 192.6.1.112
RADIUS config>
```

The address appearing in the message between brackets corresponds to the IP address value previously configured, or if this has not been configured, the IP address of the primary Server.

Should an invalid IP address be entered, the following error message appears.

```
Bad address, try again
```

And a new IP address requested.

2.3. ALTERNATE-PORT

Through this command you can configure the alternate RADIUS Server UDP port that the device sends its authentication petitions to if the primary Server does not respond, and the UDP port receiving the responses to these possible requests. The port is configured in the following way:

Example:

```
RADIUS config>ALTERNATE-PORT
Alternate RADIUS server port (1645|1812)[1812]? 1645
RADIUS config>
```

The value appearing between the brackets for the two ports is the one officially assigned for the RADIUS protocol although you can configure a value of 1645 for extended use in the RADIUS community. If you change the port value, the currently configured value is shown between brackets.

If you enter a port number other than these values, the following error message appears:

```
Invalid port (1645|1812)
```

2.4. ALTERNATE-SECRET

Through this command you can configure the device "secret". This must coincide with one in the established alternate RADIUS Server. This is configured in the following way.

Example:

```
RADIUS config>ALTERNATE-SECRET
Alternate RADIUS server secret?*******
Secret again?*******
RADIUS config>
```

As you can see, the user must enter the secret twice in order to check it has been correctly introduced. If these values do not coincide, the following message appears

```
Different secrets
```

And subsequently has to be configured again.

When you request secret configuration and no value is introduced, the following error message appears

```
Null secret
```

This parameter can contain up to 32 characters with the exception of tabs and blank spaces.

NOTE: If the IP address and secret values have not been configured in either of the two RADIUS Servers and you try to enable RADIUS, an error message appears with this information.

2.5. ATTEMPTS

This command is used to set the number of attempts it is possible to send a RADIUS authentication request, should the RADIUS Servers not respond in the established time.

Initially, the user can send up to three consecutive authentication petitions to the primary Server subsequently beginning to alternate between the primary Server and the alternative Server until a response is received from one of them or until the configured time period has lapsed since the last petition was sent. In this latter case, the user corresponding to the petitions is rejected.

When you begin to send authentication petitions, if the device interfaces connecting to the RADIUS Servers are not up, further transmission attempts are made every two seconds until a successful petition transmission has occured or a total time of ten seconds has lapsed. In this latter case, the user will also be rejected.

Once you have begun resending petitions, if one of the interfaces is not up or has dropped, when you need to retransmit the packet to the reachable RADIUS Server through this particular interface the packet will be sent to another Server whose interface is up. On the other hand, if both interfaces are

down, a wait cycle is entered equal to that configured between petitions until a further attempt to retransmit is made. These to all effects are considered as retransmissions even though no packet has been sent as yet.

This parameter is configured in the following way:

Example:

```
RADIUS config>SET ATTEMPTS
Number of attempts (1-100)[5]?
RADIUS config>
```

The number appearing in the message between brackets corresponds to the previous value.

The default value for this parameter is **5**.

The permitted range of values for the number of attempts is (1-100). If the number entered here is outside the permitted range, the following message appears

```
Number of attempts out of range (1-100)
```

2.6. CONSOLE

This command enables or disables authentication for console access to the device through the RADIUS protocol.

Syntax:

```
RADIUS config>CONSOLE ?
ENABLED
DISABLED
```

a) CONSOLE ENABLED

This command enables authentication for console access to the device through the RADIUS protocol.

Example:

```
RADIUS config>CONSOLE ENABLED
RADIUS config>
```

b) CONSOLE DISABLED

This command disables authentication for console access to the device through the RADIUS protocol.

Example:

```
RADIUS config>CONSOLE DISABLED
RADIUS config>
```

2.7. DELAY

This command is used to configure the time between resending RADIUS authentication petitions. It is configured in the following way:

Example:

```
RADIUS config>DELAY
Time between attempts (ms) (1-30 sc)[1000]?
RADIUS config>
```

The number appearing in the message between brackets corresponds to the previous value.

The default value for this parameter is **1000 ms.**

The permitted range of values for the number of attempts is (1- 30 secs). If the value entered here is outside the permitted range, the following message appears

```
Time between attempts out of range (1-30 sc)
```

2.8. DISABLE

Through this command you can globally disable the RADIUS protocol in the device.

Syntax:

```
RADIUS config>DISABLE RADIUS
```

Example:

```
RADIUS config>DISABLE RADIUS
RADIUS disabled
RADIUS config>
```

Although the RADIUS facility is enabled in the device's PPP interfaces as well as in the FTP, TELNET and console connections, this command prevent authentications from these applications being carried out through a RADIUS Server.

2.9. ENABLE

This command permits you to globally enable the RADIUS protocol in the device.

Syntax:

```
RADIUS config>ENABLE RADIUS
```

Example:

```
RADIUS config>ENABLE RADIUS
RADIUS enabled
RADIUS config>
```

In cases where parameters SECRET and ADDRESS for one of the RADIUS Servers have not been configured, you cannot enable the RADIUS protocol and information to that effect is provided through the following message.

```
Some parameters are not set
```

As well as using this command to enable the RADIUS authentication in the device's PPP interfaces (manual Dm 710-I), FTP connections (manual Dm 724-I), TELNET and console (manual Dm 704-I), you need to enable the RADIUS facility in each of these applications, using the corresponding commands in their configuration environments. For FTP, TELNET and console connections, the RADIUS facility can also be enabled from the RADIUS configuration menu using the commands described in this manual (CONSOLE, FTP and TELNET commands).

2.10. FTP

This command enables or disables access authentication for FTP connection to the device through the RADIUS protocol.

Syntax:

```
RADIUS Cconfig>FTP ?
ENABLED
DISABLED
```

a) FTP ENABLED

This command enables access authentication for FTP connection to the device through the RADIUS protocol.

Example:

```
RADIUS config>FTP ENABLED
RADIUS config>
```

b) FTP DISABLED

This command disables access authentication for FTP connection to the device through the RADIUS protocol.

Example:

```
RADIUS config>FTP DISABLED
RADIUS config>
```

2.11. IDENTIFIER

Through this command you can configure an identifier for the device of up to 128 characters in length, without tabs or blank spaces. This is configured in the following way:

Example:

```
RADIUS config>IDENTIFIER
Identifier [TeldatRadiusClient]?
RADIUS config>
```

The identifier appearing between the brackets corresponds to the previously configured identifier. The default value is **TeldatRadiusClient**.

2.12. LIST

This command permits you to list the configured parameter values with the exception of the secrets whose values cannot be viewed. This is carried out as follows:

Syntax:

```
RADIUS config>LIST
```

Example:

```
RADIUS config>LIST
Primary RADIUS server: 192.6.1.227
Alternate RADIUS server: 192.6.1.112
Primary RADIUS Server Port: 1812
Alternate RADIUS Server Port: 1645
Identifier: TeldatRadiusClient
Number of attempts: 5
Time between attempts (ms): 1000
RADIUS enabled

RADIUS disabled on Console Authentication
RADIUS disabled on Telnet Authentication
RADIUS disabled on FTP Authentication

RADIUS config>
```

As can be seen in the example, the LIST option also provides information on the state of the RADIUS protocol, both globally as well as withreference to authentication through the RADIUS protcol for device access via console, telnet or FTP.

If RADIUS has been globally enabled the following message appears.

```
RADIUS enabled
```

Otherwise the message reads

```
RADIUS disabled
```

2.13. NO

This command is used to set the distinct parameters to their default value.

Syntax:

```
RADIUS config>NO ?
ALTERNATE-ADDRESS
ALTERNATE-PORT
ALTERNATE-SECRET
ATTEMPTS
DELAY
IDENTIFIER
PRIMARY-ADDRESS
PRIMARY-PORT
PRIMARY-SECRET
SOURCE-INTERFACE
RADIUS config>
```

The default values are as follows:

Command	Default value
ALTERNATE-ADDRESS	0.0.0.0
ALTERNATE-PORT	1812
ALTERNATE-SECRET	empty (without secret)
ATTEMPTS	5
DELAY	1000 ms
IDENTIFIER	TeldatRadiusClient
PRIMARY-ADDRESS	0.0.0.0
PRIMARY-PORT	1812
PRIMARY-SECRET	empty (without secret)
SOURCE-INTERFACE	Associates the RADIUS packets to the outbound interface.

2.14. PRIMARY-ADDRESS

This command is used to configure the primary RADIUS Server IP address that the device is going to send the RADIUS authentication requests to. The address is configured in the following way:

Example:

```
RADIUS config>PRIMARY-ADDRESS
Primary RADIUS server IP address [0.0.0.0]? 192.6.1.227
RADIUS config>
```

The address appearing in the message between brackets corresponds to the IP address value previously configured, or if this has not been configured, the IP address of the alternative Server.

Should an invalid IP address be entered, the following error message appears.

```
Bad address, try again
```

And a new IP address is requested.

2.15. PRIMARY-PORT

Through this command you can configure the primary RADIUS Server UDP port that the device sends its authentication requests to and the UDP port where the responses to these requests are received. This port is configured in the following way:

Example:

```
RADIUS config>PRIMARY-PORT
Primary RADIUS server port (1645|1812)[1812]?
RADIUS config>
```

The value appearing between the brackets is the one officially assigned for the RADIUS protocol although you can configure a value of 1645 for extended use in the RADIUS community. Should you change the port value, the current configured value is shown between brackets.

If you enter a port number other than these values, the following error message appears:

```
Invalid port (1645|1812)
```

2.16. PRIMARY-SECRET

Through this command you can configure the device "secret". This must coincide with one in the established primary RADIUS Server. This is configured in the following way.

Example:

```
RADIUS config>PRIMARY-SECRET
Primary RADIUS server secret?*******
Secret again?*******
RADIUS config>
```

As you can see, the user must enter the secret twice in order to check it has been correctly introduced. If these values do not coincide, the following message appears

```
Different secrets
```

And subsequently has to be configured again.

When you request secret configuration and no value is introduced, the following error message appears

```
Null secret
```

This parameter can contain up to 32 characters with the exception of tabs and blank spaces.

2.17. SOURCE-INTERFACE

A source interface is associated to the RADIUS packets through this command. The source IP address for these will be that associated to this interface. If this interface does not have an IP configured, the default configuration will be used (IP associated to the output interface.)

If the associated interface has more than one IP configured, then the last one configured is used.

If the interface is deleted, the default configuration will be used.

Example:

```
RADIUS config>source-interface ?
  <interface>    Interface name
RADIUS config>
```

2.18. TELNET

This command enables or disables access authentication via the TELNET remote terminal to the device through the RADIUS protocol.

Syntax:

```
RADIUS Cconfig>TELNET ?
ENABLED
DISABLED
```

a) TELNET ENABLED

This command enables access authentic ation via the TELNET remote terminal to the device through the RADIUS protocol.

Example:

```
RADIUS config>TELNET ENABLED
RADIUS config>
```

b) TELNET DISABLED

This command disables access authentication via the TELNET remote terminal to the device through the RADIUS protocol.

Example:

```
RADIUS config>TELNET DISABLED
RADIUS config>
```

2.19. EXIT

This command is used to exit the RADIUS configuration environment and to return to the previous prompt, User configuration. This is executed in the following way:

Syntax:

```
RADIUS conf>EXIT
```

Example:

```
RADIUS conf>EXIT
Config>
```

Chapter 3
Monitoring

1. Accessing the Radius Protocol monitoring

The RADIUS protocol monitoring commands are described in this chapter. In order to access these command, you need to enter the RADIUS Monitoring environment (RADIUS> prompt) and enter the following commands:

```
*P 3

+FEATURE RADIUS

-- RADIUS User Console --
RADIUS>
```

2. Monitoring commands

Once in the correct monitoring environment, you can execute any of the following commands:

Command	Function
? (HELP)	Displays all the available commands or their options.
LIST	Permits you to view the statistics and values of some parameters.
EXIT	Returns to the previous prompt.

Each of the commands have been explained in more detail below.

2.1. ? (HELP)

The **?** (HELP) command is used to obtain a list of all those commands available in the RADIUS monitoring environment. For this enter **?** at the "RADIUS>" prompt:

Syntax:

```
RADIUS>?
```

Example:

```
RADIUS>?
LIST
EXIT
RADIUS>
```

This command can also be used to view the options available from the **LIST** command in this menu. In this case, enter **LIST** followed by a question mark **?**.

Example:

```
RADIUS>LIST ?
PARAMETERS
STATISTICS
ALL
RADIUS>
```

2.2. LIST

The **LIST** command is used to view the values of the configured parameters and the statistics for the protocol. The command options can be viewed as indicated in the previous example:

Syntax:

```
RADIUS>LIST ?
PARAMETERS
STATISTICS
ALL
```

a) LIST PARAMETERS

Through the **LIST PARAMETERS** command, you can view the values for all the configured parameters, excepting the secrets, as well as the state of the RADIUS protocol. This is carried out in the following way:

Example:

```
RADIUS>LIST PARAMETERS
Primary RADIUS server: 192.6.1.227
Alternate RADIUS server: 192.6.1.112
Primary RADIUS Server Port: 1812
Alternate RADIUS Server Port: 1645
Identifier: TeldatRadiusClient
Number of attempts: 5
Time between attempts (ms): 1000
RADIUS enabled

RADIUS disabled on Console Authentication
RADIUS disabled on Telnet Authentication
RADIUS disabled on FTP Authentication

RADIUS>
```

b) LIST STATISTICS

By entering this command, you can access the packet statistics corresponding to the different authentication procedures sent since the device was last restarted. This information can be viewed in the following way:

Example:

```
RADIUS>LIST STATISTICS
Client Identifier: TeldatRadiusClient
Client Invalid Server Addresses: 0

Server Index: 1
Server Address: 192.6.1.227
Client Server Port Number: 1812
Client Round Trip Time: 16 ms
Client Access Requests: 33
Client Access Retransmissions: 0
Client Access Accepts: 29
Client Access Rejects: 4
Client Access Challenges: 0
Client Malformed Access Responses: 0
Client Bad Authenticators: 0
Client Pending Requests: 0
Client Timeouts: 0
Client Unknown Types: 0
Client Packets Dropped: 0

Server Index: 2
Server Address: 192.6.1.112
Client Server Port Number: 1645
Client Round Trip Time: 0 ms
Client Access Requests: 0
Client Access Retransmissions: 0
Client Access Accepts: 0
Client Access Rejects: 0
Client Access Challenges: 0
Client Malformed Access Responses: 0
Client Bad Authenticators: 0
Client Pending Requests: 0
Client Timeouts: 0
Client Unknown Types: 0
Client Packets Dropped: 0
RADIUS>
```

As you can see, the device's configured identifier together with the packets received from unknown RADIUS Servers is the first thing to appear. This is followed by a list of statistics for the RADIUS packets that have been exchanged firstly with the primary Server and then with the alternative Server.

If both of these Servers have the same secret, the same IP address and the same UDP port configured, then it is considered that only one RADIUS Server is available when sending authentication peititions. For this reason, only the statistics for packets exchanged with this Server are listed.

If only one of these Servers has the IP address and secret configured and independently of whether it is the primary Server or the alternative, it will be considered as a primary Server and only those packets associated to it are listed.

Finally, if neither of the Servers have the address nor the secret configured, the following message appears:

```
RADIUS Servers have parameters not set
```

after the Terminal Server identifier.

c) LIST ALL

You can view all the parameters and the statistics through this option in the following way:

Example:

```
RADIUS>LIST ALL
Primary RADIUS server: 192.6.1.227
Alternate RADIUS server: 192.6.1.112
Primary RADIUS Server Port: 1812
Alternate RADIUS Server Port: 1645
Identifier: TeldatRadiusClient
Number of attempts: 10
Time between attempts (ms): 1000
RADIUS enabled

Client Identifier: TeldatRadiusClient
Client Invalid Server Addresses: 0

Server Index: 1
Server Address: 192.6.1.227
Client Server Port Number: 1812
Client Round Trip Time: 16 ms
Client Access Requests: 33
Client Access Retransmissions: 0
Client Access Accepts: 29
Client Access Rejects: 4
Client Access Challenges: 0
Client Malformed Access Responses: 0
Client Bad Authenticators: 0
Client Pending Requests: 0
Client Timeouts: 0
Client Unknown Types: 0
Client Packets Dropped: 0

Server Index: 2
Server Address: 192.6.1.112
Client Server Port Number: 1645
Client Round Trip Time: 0 ms
Client Access Requests: 0
Client Access Retransmissions: 0
Client Access Accepts: 0
Client Access Rejects: 0
Client Access Challenges: 0
Client Malformed Access Responses: 0
Client Bad Authenticators: 0
Client Pending Requests: 0
Client Timeouts: 0
Client Unknown Types: 0
Client Packets Dropped: 0
RADIUS>
```

2.3. EXIT

This command is used to exit the RADIUS monitoring environment and to return to the previous prompt, Console Operator. This is executed in the following way:

Syntax:

```
RADIUS>EXIT
```

Example:

```
RADIUS>EXIT
+
```

3. Radius Protocol Events Viewing

In order to view the events that have occurred during the RADIUS authentication procedures, you need to activate the events system for this protocol.

The way to enable this from the configuration menu is as follows:

```
*P 4
Config>EVENT

-- ELS Config --
ELS Config>ENABLE TRACE SUBSYSTEM RADIUS ALL
ELS Config>EXIT
Config>SAVE
Save configuration [n]? y

Saving configuration...OK (configuration saved on Flash)
Config>
```

You can also enable the events from the monitoring menu at any time without needing to save the configuration and restart. The command sequence to be entered is as follows:

```
*P 3
+EVENT

-- ELS Monitor --
ELS>ENABLE TRACE SUBSYSTEM RADIUS ALL
ELS>EXIT
+
```