RADIUS Protocol

Teldat-Dm 733

Legal Notice

Warranty

This publication is subject to change.

Teldat offers no warranty whatsoever for information contained in this manual.

Teldat is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply or use of this manual.

Table of Contents

I Related Documents

Teldat-Dm 704-I Configuration and Monitoring

Teldat-Dm 710-I PPP Interface

Teldat-Dm 724-I FTP Protocol

Chapter 1 Introduction

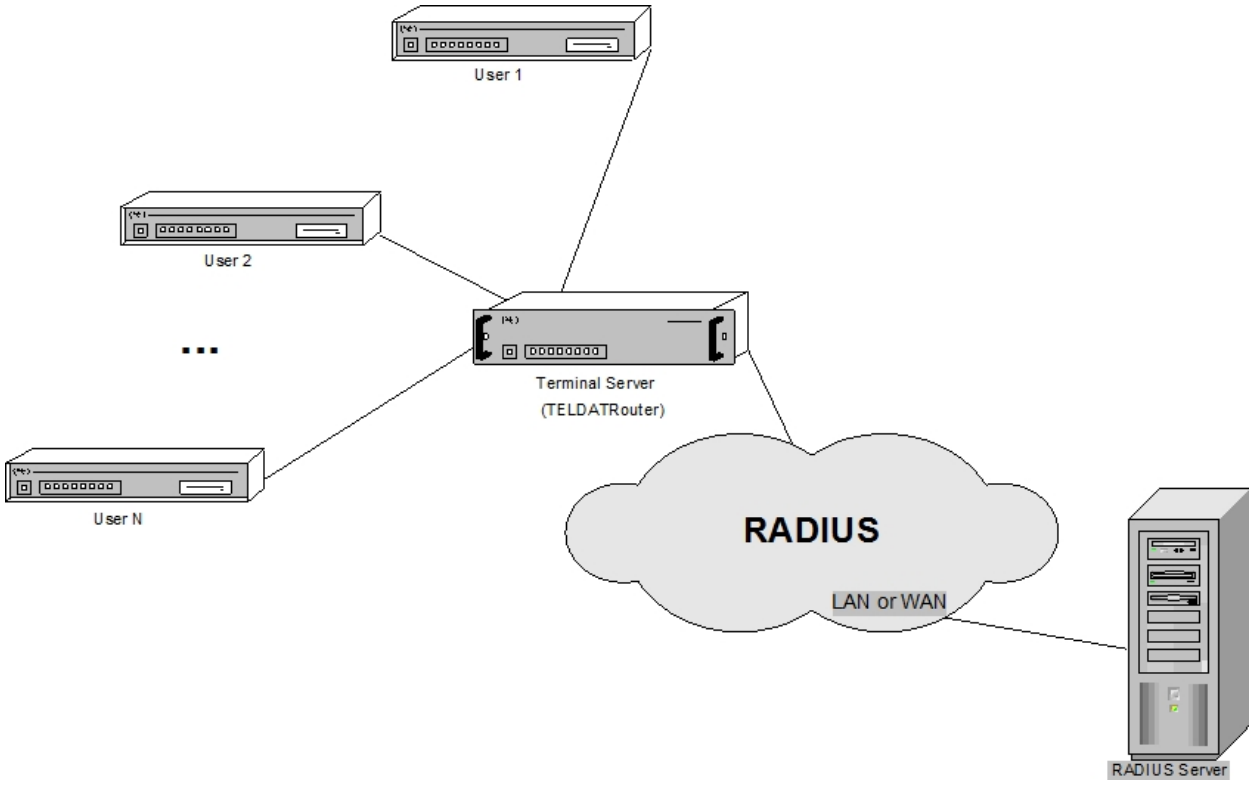
1.1 Introduction to Radius Protocol

At present, Network Managers have very few tools to protect the security of their networks against undesired events (e.g. break-ins). State-of-the-art security systems generally require specific hardware or are only compatible with a limited number of products. This problem is further aggravated in large networks due to the high number of access points. RADIUS (Remote Authentication Dial In User Service) can help solve problems associated with security requirements in accesses, or linked to authentication and authorization, by allowing you to send configuration information from a RADIUS Authentication Server.

The following section refers to the main environments that can use the RADIUS protocol.

1.1.1 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.

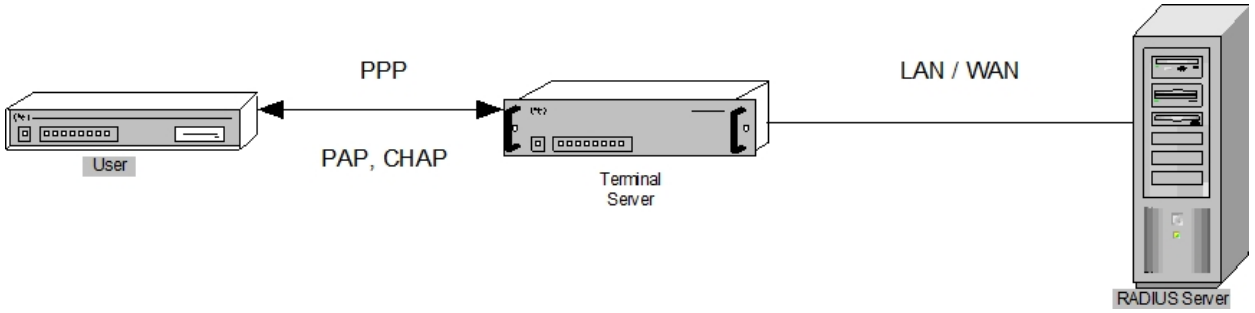


In this context, for a user to connect to the network through the Terminal Server, access must be authorized by that server. To do this, users send information about their identity to the Terminal Server using the links. If the RADIUS protocol is not used, the Terminal Server is responsible for deciding whether to authorize the connection or not (by comparing the received data with its list of approved users). In cases like this, the Terminal Server should also report the results of the authentication and negotiate the IP address with which the user can connect.

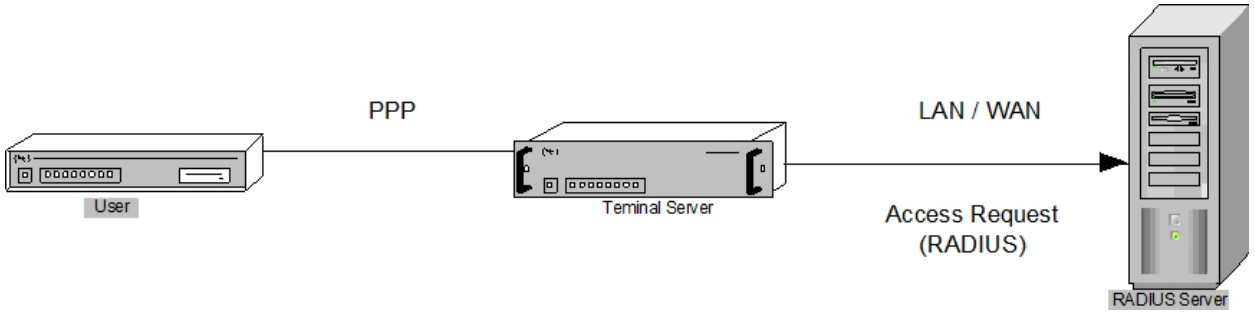
However, if the RADIUS protocol is used, information from the different users captured by the Terminal Server is sent to the RADIUS Server. Based on its database, the latter is then responsible for granting or denying access to the network requested by the user. The decision taken by the RADIUS Server is transmitted to the Terminal Server, which then notifies the user. In this case, the IP address with which an authorized user can connect is obtained from the RADIUS Server's database (**Framed-IP-Address**) and sent to the recipient through the Terminal Server. The RADIUS Server also sends the address mask (**Framed-IP-Netmask**) to determine the range of addresses requested by the user, the routes that must be configured in the Terminal Server to access networks connected to the user (**Framed-Route**), and information on whether the user is about to listen and/or send packets with routing announcements (**Framed-Routing**). In the latter case, the local end of the Terminal Server should automatically configure an address belonging to the same subnet as the remote end user to perform the exchange of such packets.

In this mode of operation, and since it transfers user connection requests to the RADIUS Server for validation, it is said that the Terminal Server acts as a RADIUS client.

Users can submit the necessary information for validation purposes to the Terminal Server following different authentication mechanisms. For PPP connections, however, the alternatives are PAP and CHAP authentication protocols.



The RADIUS authentication process is carried out as follows. The Terminal Server uses the information it has obtained on the identity of users to create an access request (**Access Request**) that is sent to the RADIUS Server through the network. When a password is present in the request, it is hidden in order to ensure confidentiality. If the RADIUS Server does not respond to the request for some time, the Terminal Server resends it. This may be repeated a number of times.

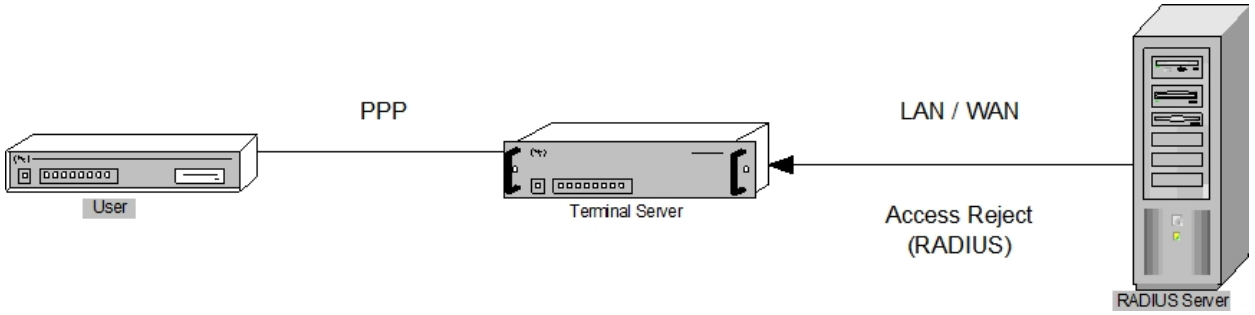


Once the RADIUS Server receives the request, it first authenticates the Terminal Server that sent it. For this, the RADIUS Server uses information contained in the request and a "secret" configured on both devices. This "secret" is a password shared among the Servers and is never sent over the network (to provide greater security). If the Terminal Server is not valid, the request is discarded. If it is valid, the RADIUS Server consults its database to see if the user contained in the petition is allowed access.

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

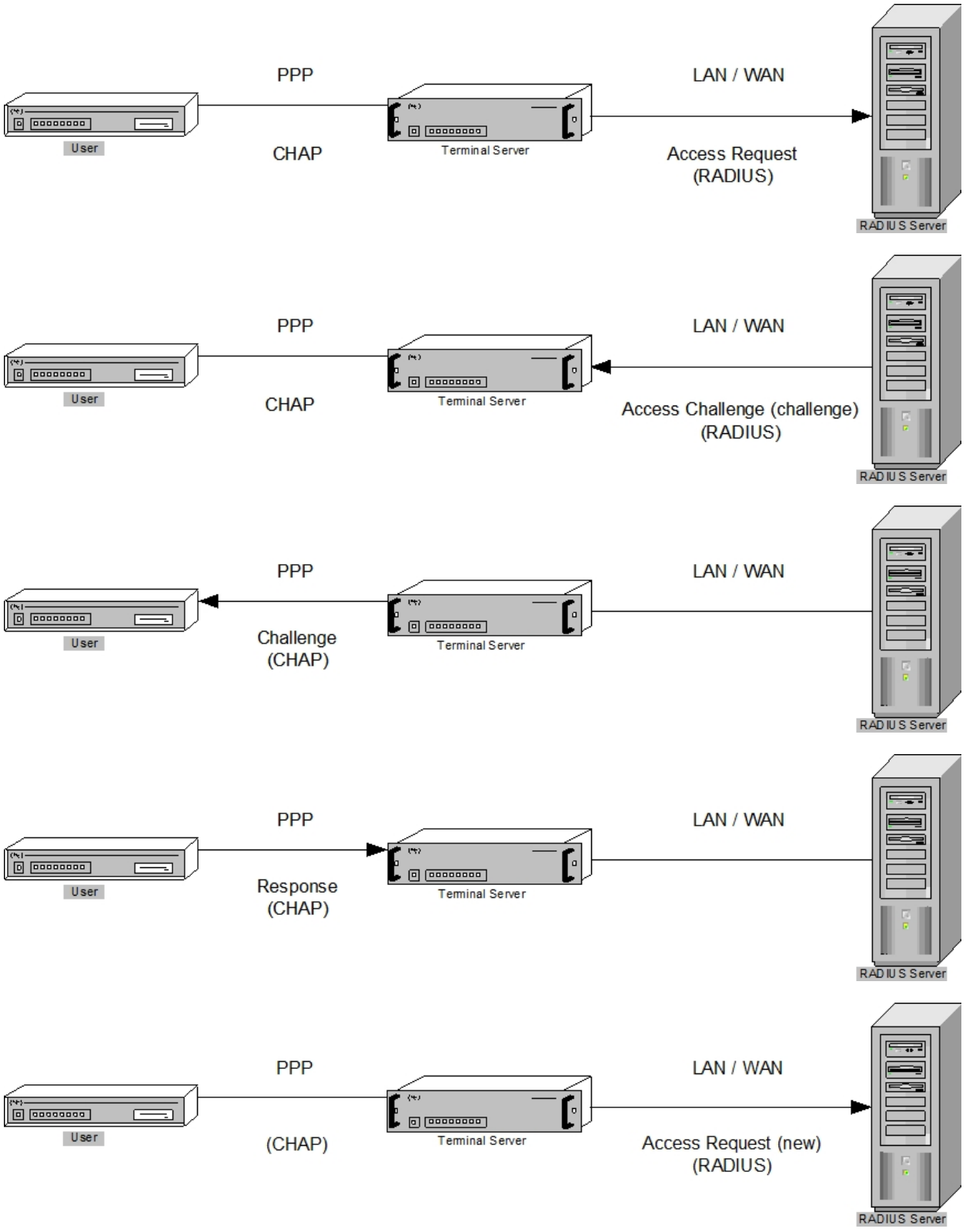
If the RADIUS Server verifies that the user who requested the connection is on the list of authorized users, it sends an access acceptance (**Access Accept**) to the Terminal Server, which lists the configuration values for the user (such as the user connection IP address).

Conversely, if the user who wants to connect to the network is not in the RADIUS Server database, his/her request is denied and a rejection response (**Access Reject**) is sent to the Terminal Server. The user is then notified that the connection has not been granted.



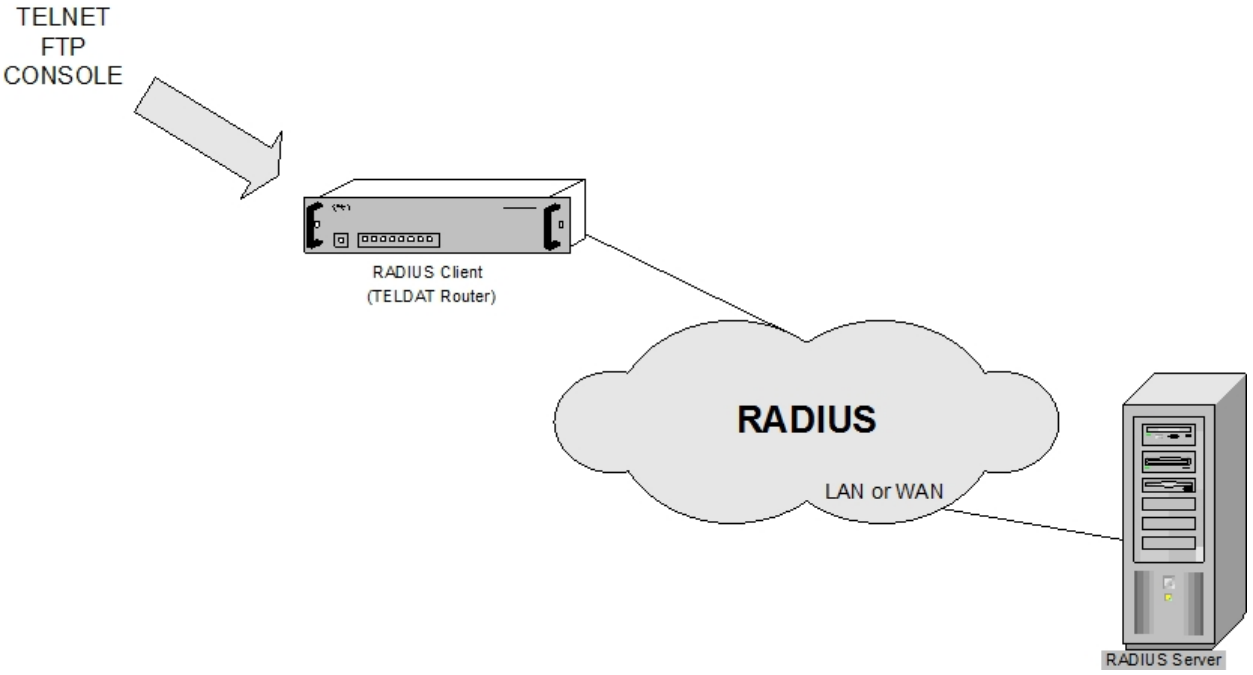
If the authentication protocol is CHAP, there is a possibility that the RADIUS Server will not transmit the Access Accept packet for a user connection request that has been authorized, but decides to “challenge” the user to attempt authentication again. To do this, the RADIUS Server sends an **Access Challenge** packet to the Terminal Server that, in one of its attributes, includes a unique and unpredictable numerical value called **challenge**. The Terminal Server communicates the challenge to the user who uses this value to submit a new access request to the network (**response**). The user also sends this new petition to the Terminal Server, which, in turn, transfers it to the RADIUS

Server through a new Access Request packet. Finally the RADIUS Server compares the data received in this packet with the data it expected to receive and acts accordingly. That is, if the information contained in the received packet is what the RADIUS Server was expecting, the RADIUS Server sends an Access Accept packet containing the connection IP address to the Terminal Server. However, if such information is not as expected, an Access Reject packet denying the access request is sent. Finally, the RADIUS Server can also challenge the user to authenticate once again by transmitting another Access Challenge packet.



1.1.2 Authentication and configuration for the Telnet, FTP, console and SSH connections

On this occasion, it is the TELNET, FTP, console and SSH connections on a device that you want to authenticate and configure via the RADIUS protocol.



For a user to access the router through these connections, it is necessary to authorize such access. To do this, users transmit unique information on their identity to the device when the device requests it. If the RADIUS protocol is not used, the router will be responsible for deciding whether to authorize the connection or not (by comparing the received data with the data configured in the device).

However, if the RADIUS protocol is used, information from the different users captured by the router is sent to the RADIUS Server. Based on its database, the latter is then responsible for granting or denying access to the network requested by the user. It communicates its decision to the router at a later time. The RADIUS packets exchange process is identical to the one explained in the previous section for PPP connections.

In cases of authentication over our router, the access you may have to different processes and the right to execute some restricted commands depends on the user you have authenticated.

Note

By default, our routers change the user name characters to uppercase (even if they are entered in lowercase) in cases where Radius authentication is used for the console, Telnet, FTP or SSH. This behavior can be changed through the SET LOGIN CASE-SENSITIVE command. For further information, please see manual *Teldat-Dm 704-I* "*Configuration and Monitoring*" .

In order to authenticate in the system, you can locally define users or define a password for the device through the **SET PASSWORD** command.

In cases regarding SSH, it is essential that users are locally defined and that you enter the appropriate user and password.

Both cases can be used for the rest of the protocols. In cases with a password for the device, in Telnet connection and console over the routers, the user name is not requested, you are only asked for the password. Given the fact that the RADIUS Servers need a user name, the router sends “TELNET” when in a Telnet connection, and

“CONSOLE” when in console. This attribute is 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 corresponding password at the Config access level:

```
vcm Auth-Type = Local, Password = "LaMia"

              Service-Type = Login-User,

              Access-Level = Config
```

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

Administrative:	Allows 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 VSA Access-Level attribute.
NAS Prompt:	Allows 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 VSA Access-Level attribute.
Login:	Access is only permitted through Telnet and console. The access level for Telnet and console is determined by the VSA Access-Level attribute.

Note

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

A VSA is a Vendor Specific Attribute. This refers to attributes that do not form part of the standard and have been defined by a manufacturer. To allow users to benefit from the various access levels for Telnet and the console, a VSA attribute, known as Access-Level, is used.

The 5 basic access levels (there are more) granted through the Access-Level attribute are:

None:	You are not allowed to access the system.
Events:	Allows you to access the Console Management (P1) and Events Viewing (P2). However, you are not permitted to execute the Ping, Telnet, Restart nor Load commands.
Monitor:	Allows you to access the Console Management (P1), Events Viewing (P2) and the Monitoring process (P3). You can also execute the Ping and Telnet commands but cannot execute the Restart or Load commands.
Config:	You have access to all processes and standard commands.
Root:	In addition to having access to all standard commands, you can also access the user management commands.

Given that this attribute is non-standard, you need to define it in the RADIUS Server Dictionary (together with the values it can take). For further information, please see section 3 under chapter 2 ("The Dictionary").

On registering the authorized users in the RADIUS Server, you need to indicate the corresponding access level through the VSA Access-Level attribute. If you omit the value for said attribute, the RADIUS client starts to check if the access levels are contained in the Login-Service attribute. In cases where neither of these two attributes has been received from the RADIUS Server, the value configured through the default-access-level command is used.

For more information on local device authentication, please see Chapter 1 “The Router Console” in manual *Teldat-Dm 704-I “Configuration and Monitoring”*.

Note

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, having a RADIUS Server draw information from different users simultaneously 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 thousands of users in a safe and simple way.

Given the advantages offered by the use of a RADIUS server, we have implemented this protocol in the routers that comply with the **RFC 2138** standard. In these devices, the RADIUS authentication process operates as described above (but without the challenge/response function). This means that if our router, acting as a Terminal Server, receives Access Challenge packets from the RADIUS Server, it treats them in the same way as if they were Access 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 then enable RADIUS validation in the required PPP interface. In the same way, you need to globally enable RADIUS in the device and then in the TELNET, FTP, console and SSH connections (to authenticate them through the protocol). RADIUS authentication cannot be enabled if the IP address for the RADIUS Server where the connection petitions are sent, as well as the “secret” shared between the router and this RADIUS Server, have not been configured.

At this point you can also configure: the IP address and “secret” for a backup RADIUS Server; the UDP ports; the Terminal Server’s ID; the number of times it is possible to resend a petition should no response be received from the RADIUS Servers; and the time between resends. The value for these parameters can be set independently or as a group (which makes consultation between them possible, except for “secrets”).

Note

In cases of TELNET, console and SSH connections 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 a full explanation on the protocol's configuration and monitoring in the next two chapters.

Chapter 2 Configuration

2.1 Accessing the Radius Protocol configuration

This section describes the commands required to configure the device as client Terminal Server for a RADIUS Server. First, you need to access the configuration environment ("RADIUS config>" prompt). To do this, enter the following commands:

```
*P 4
Config>FEATURE RADIUS
-- RADIUS User Configuration --
RADIUS config>
```

2.2 Configuration Commands

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 transmission attempts.
ATTRIBUTE	Configures certain attributes involved in the authentication process.
CONSOLE	Enables or disables Radius authentication for console access to the device.
DEFAULT-ACCESS-LEVEL	Configures the access level by default to assign to the user if the Radius server does not specify this.
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.
SSH	Enables or disables Radius authentication for accessing the device through SSH.
EXIT	Returns to the previous prompt.

Each of the commands is explained in more detail below.

2.2.1 ? (HELP)

This command can be used in two ways. Firstly, it allows 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     Configure the alternate Radius server IP address
  alternate-port        Configure the alternate Radius server port
```

```
  alternate-secret      Configure the alternate Radius server password
  attempts              Configure the number of authentication attempts
  attribute             Configure radius attributes
  console               Configure the authentication for console access
  default-access-level  Configure the default user access-level if not specified by Radius server
  delay                 Configure the time between authentication petitions
  disable               Globally disable the RADIUS protocol
  enable                Globally enable the RADIUS protocol
  ftp                   Configure the authentication for FTP access
  identifier            Configure an identifier for the device
  list                  List configuration
  no                    Negates a command or sets its defaults
  primary-address       Configure the primary Radius server IP address
  primary-port          Configure the primary Radius server port
  primary-secret        Configure the primary Radius server password
  source-interface      Configure the source interface
  ssh                   Configure the authentication for SSH access
  telnet                Configure the authentication for TELNET access
  exit
RADIUS conf>
```

This command can also be used to view the available options for a specific 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>
```

2.2.2 ALTERNATE-ADDRESS

This command is used to configure the IP address for the backup RADIUS Server the device will send RADIUS authentication requests to (in case the primary RADIUS Server stops working). This address is configured in the following way:

Syntax:

```
RADIUS config>alternate-address <ip address>
```

Example:

```
RADIUS config>SET ALTERNATE-ADDRESS 192.6.6.112
RADIUS config>
```

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

```
CLI Error: Unrecognized command or invalid value
```

2.2.3 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:

Syntax:

```
RADIUS config>alternate-port <1..65535>
```

Example:

```
RADIUS config>ALTERNATE-PORT 1645
RADIUS config>
```

Command history:

Release	Modification
11.0.3	This command has been introduced.

2.2.4 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.

Syntax:

```
RADIUS config>alternate-secret <text>
```

Example:

```
RADIUS config>ALTERNATE-SECRET whatever
RADIUS config>
```

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

```
CLI Error: Incomplete command
```

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

2.2.5 ATTEMPTS

This command is used to set the number of attempts a RADIUS authentication request may be sent when RADIUS Servers do not respond within the time set.

Initially, the user can send up to three consecutive authentication petitions to the primary Server. It can then alternate between the primary Server and the backup Server until a response is received from either of them (or until the configured time period has lapsed since the last petition was sent). In this latter case, the user linked to the petitions is rejected.

If the device interfaces connecting to the RADIUS Servers are not up when you start sending authentication petitions, further transmission attempts are made every two seconds until a petition is successfully transmitted or ten seconds pass. In this latter case, the user will also be rejected.

Once you begin resending petitions, if one of the interfaces is not up or has dropped, the packet you need to retransmit to the reachable RADIUS Server 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. To all effects, these are considered as retransmissions despite no packet being sent.

This parameter is configured in the following way:

Syntax:

```
RADIUS config>attempts <# attempts>
```

Example:

```
RADIUS config>SET ATTEMPTS 5
RADIUS config>
```

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

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

```
CLI Error: Unrecognized command or invalid value
```

2.2.6 ATTRIBUTE

This command configures certain attributes involved in the authentication process.

Syntax:

```
RADIUS config>ATTRIBUTE ?
  calling-station-id    Attribute number 31
```

2.2.6.1 ATTRIBUTE CALLING-STATION-ID

This command enables sending in the Calling-Station-Id attribute in the petition to access the RADIUS Server.

This only takes affect when the authentication process is initiated by a TELNET, SSH or FTP client and provides information on the IP address of said remote client.

Example:

```
RADIUS config>ATTRIBUTE CALLING-STATION-ID
RADIUS config>
```

2.2.7 CONSOLE

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

Syntax:

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

2.2.7.1 CONSOLE ENABLED

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

Example:

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

2.2.7.2 CONSOLE DISABLED

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

Example:

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

2.2.8 DEFAULT-ACCESS-LEVEL

This command allows you to configure the default access level that the device must assign to a user when, in the RADIUS authentication process, the server does not specify said user's access-level.

Syntax:

```
RADIUS config>default-access-level <access-level>
  configuration    Configuration access level
  events           Events access level
  keymanager       Keymanager access level
  monitor          Monitor access level
  none             None access level
  root             Root access level
```

- **< access-level >** specifies the default access level

Example:

```
RADIUS config>default-access-level monitor
RADIUS config>
```

The default value for this parameter is *none*.

2.2.9 DELAY

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

Syntax:

```
RADIUS config>delay <time between attempts>
```

Example:

```
RADIUS config>DELAY 2000
RADIUS config>
```

The <time between attempts> value is introduced in milliseconds.

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:

```
CLI Error: Unrecognized command or invalid value
```

2.2.10 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 prevents these applications from carrying out authentications through a RADIUS Server.

2.2.11 ENABLE

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

Syntax:

```
RADIUS config>ENABLE RADIUS
```

Example:

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

As well as using this command to enable the RADIUS authentication in the device's PPP interfaces (manual *Teldat-Dm 710-I*), FTP connections (manual *Teldat-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, console and SSH connections, the RADIUS facility can also be enabled from the RADIUS configuration menu using the commands described in this manual (CONSOLE, FTP, SSH and TELNET commands).

2.2.12 FTP

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

Syntax:

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

2.2.12.1 FTP ENABLED

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

Example:

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

2.2.12.2 FTP DISABLED

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

Example:

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

2.2.13 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:

Syntax:

```
RADIUS config>identifier <text>
```

Example:

```
RADIUS config>IDENTIFIER RadiusClient
RADIUS config>
```

2.2.14 LIST

This command allows you to list the configured parameter values (with the exception of "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 disabled on SSH Authentication

Default-access-level: monitor

RADIUS config>
```

As seen in the example, the LIST option also provides information on the state of the RADIUS protocol (both globally and with reference to authentication through the RADIUS protocol for device access via console, Telnet, FTP or SSH).

If RADIUS has been globally enabled, the following message appears:

```
RADIUS enabled
```

If it hasn't, the message reads:

```
RADIUS disabled
```

2.2.15 NO

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

Syntax:

```
RADIUS config>NO ?
  alternate-address       Configure the alternate Radius server IP address
  alternate-port          Configure the alternate Radius server port
  alternate-secret        Configure the alternate Radius server password
```

```
  attempts                Configure the number of authentication attempts
  attribute                Configure radius attributes
  default-access-level    Configure the default user access-level if not
                          specified by Radius server
  delay                   Time between attempts (ms)
  identifier              Configure an identifier for the device
  primary-address         Configure the primary Radius server IP address
  primary-port            Configure the primary Radius server port
  primary-secret          Configure the primary Radius server password
  source-interface        Configure the 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
ATTRIBUTE CALLING-STATION-ID	does not send the attribute
DEFAULT-ACCESS-SERVICE	none
DELAY	1000 ms
IDENTIFIER	empty (without identifier)
PRIMARY-ADDRESS	0.0.0.0
PRIMARY-PORT	1812
PRIMARY-SECRET	empty (without secret)
SOURCE-INTERFACE	associates the RADIUS packets to the outbound interface

2.2.16 PRIMARY-ADDRESS

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

Syntax:

```
RADIUS config>primary-address <ip address>
```

Example:

```
RADIUS config>PRIMARY-ADDRESS 192.6.1.227
RADIUS config>
```

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

```
CLI Error: Unrecognized command or invalid value
```

2.2.17 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:

Syntax:

```
RADIUS config>primary-port <1..65535>
```

Example:

```
RADIUS config>PRIMARY-PORT 1812
RADIUS config>
```

Command History:

Release	Modification
11.0.3	This command has been introduced.

2.2.18 PRIMARY-SECRET

Through this command, you can configure the device “secret” (which must match the one in the established primary RADIUS Server). This is configured in the following way.

Syntax:

```
RADIUS config>primary-secret <text>
```

Example:

```
RADIUS config>PRIMARY-SECRET whatever
RADIUS config>
```

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

```
CLI Error: Incomplete command
```

This parameter can contain up to 64 characters (with the exception of tabs and blank spaces).

2.2.19 SOURCE-INTERFACE

A source interface is associated to the RADIUS packets through this command. The source IP address for these will be the one 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.

Syntax:

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

Example:

```
RADIUS config>source-interface ethernet0/0
RADIUS config>
```

2.2.20 TELNET

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

Syntax:

```
RADIUS config>TELNET ?
ENABLED
DISABLED
```

2.2.20.1 TELNET ENABLED

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

Example:

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

2.2.20.2 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>
```

2.2.21 SSH

This command enables or disables authentication for accessing the device via a remote SSH terminal through the RADIUS protocol.

Syntax:

```
RADIUS config>SSH ?
ENABLED
DISABLED
```

2.2.21.1 SSH ENABLED

This command enables authentication for accessing the device via a remote SSH terminal through the RADIUS protocol.

Example:

```
RADIUS config>SSH ENABLED
RADIUS config>
```

2.2.21.2 SSH DISABLED

This command disables authentication for accessing the device via a remote SSH terminal through the RADIUS protocol.

Example:

```
RADIUS config>SSH DISABLED
RADIUS config>
```

2.2.22 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>
```

2.3 The Dictionary

Below you will see the VSA Access-Level attribute you need to define in the Radius Server (as well as the possible values that this can take) in order to implement access for the access levels:

VENDOR Teldat 2007

ATTRIBUTE	Access-Level 1	integer	Teldat
VALUE	Access-Level	None	800
VALUE	Access-Level	Event	801
VALUE	Access-Level	Monitor	802
VALUE	Access-Level	Config	803
VALUE	Access-Level	Root	804
VALUE	Access-Level	Keymanager	805
VALUE	Access-Level	Level0	900
VALUE	Access-Level	Level1	901
VALUE	Access-Level	Level2	902
VALUE	Access-Level	Level3	903
VALUE	Access-Level	Level4	904
VALUE	Access-Level	Level5	905

VALUE	Access-Level	Level6	906
VALUE	Access-Level	Level7	907
VALUE	Access-Level	Level8	908
VALUE	Access-Level	Level9	909
VALUE	Access-Level	Level10	910
VALUE	Access-Level	Level11	911
VALUE	Access-Level	Level12	912
VALUE	Access-Level	Level13	913
VALUE	Access-Level	Level14	914
VALUE	Access-Level	Level15	915
VALUE	Access-Level	Level0-Strict	916
VALUE	Access-Level	Level1-Strict	917
VALUE	Access-Level	Level2-Strict	918
VALUE	Access-Level	Level3-Strict	919
VALUE	Access-Level	Level4-Strict	920
VALUE	Access-Level	Level5-Strict	921
VALUE	Access-Level	Level6-Strict	922
VALUE	Access-Level	Level7-Strict	923
VALUE	Access-Level	Level8-Strict	924
VALUE	Access-Level	Level9-Strict	925
VALUE	Access-Level	Level10-Strict	926
VALUE	Access-Level	Level11-Strict	927
VALUE	Access-Level	Level12-Strict	928
VALUE	Access-Level	Level13-Strict	929
VALUE	Access-Level	Level14-Strict	930
VALUE	Access-Level	Level15-Strict	931

Chapter 3 Monitoring

3.1 Accessing the Radius Protocol monitoring

This chapter describes the RADIUS protocol monitoring commands. To access these commands, you need to reach the Monitoring environment (+ prompt) and enter the FEATURE RADIUS command.

```
*P 3
+FEATURE RADIUS
-- RADIUS User Console --
RADIUS+
```

3.2 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	Allows you to view the statistics and values of some parameters.
EXIT	Returns to the previous prompt.

Each of the commands is further detailed below.

3.2.1 ? (HELP)

The **?** (HELP) command is used to obtain a list of all commands available in the RADIUS monitoring environment. To run it, enter **?** at the “RADIUS>” prompt:

Syntax:

```
RADIUS+?
```

Example:

```
RADIUS+?
  list    View the statistics and values of some parameters
  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 ?
  all           View the values for all the configured parameters and packet
                statistics
  parameters    View the values for all the configured parameters
  statistics    View the packet statistics
RADIUS+
```

3.2.2 LIST

The **LIST** command displays the values of the configured parameters and the protocol statistics. The command options can be viewed as indicated in the previous example:

Syntax:

```
RADIUS+list?
  all           View the values for all the configured parameters and packet
                statistics
  parameters    View the values for all the configured parameters
  statistics    View the packet statistics
```

3.2.2.1 LIST PARAMETERS

Through the **LIST PARAMETERS** command, you can view the values for all the configured parameters (except 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 disabled on SSH Authentication
Default-access-level: monitor
RADIUS+
```

3.2.2.2 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
Client Account Requests: 0
Client Account Retransmissions: 0
Client Account Responses: 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
Client Account Requests: 0
Client Account Retransmissions: 0
```

```
Client Account Responses: 0
RADIUS+
```

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

If these two Servers have the same "secret" (the same IP address and UDP port configured), only one RADIUS Server is deemed available when sending authentication petitions. 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 (regardless of whether it is the primary or backup Server), said Server shall be considered as primary and only the packets associated to it will be listed.

Finally, if neither Server has a configured address or "secret", the following message appears:

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

3.2.2.3 LIST ALL

This feature displays all parameters and statistics 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
RADIUS disabled on Console Authentication
RADIUS enabled on Telnet Authentication
RADIUS disabled on FTP Authentication
RADIUS disabled on SSH Authentication
Default-access-level: monitor
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
Client Account Requests: 0
Client Account Retransmissions: 0
Client Account Responses: 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
Client Account Requests: 0
Client Account Retransmissions: 0
Client Account Responses: 0
RADIUS+
```

3.2.3 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
+
```

3.3 Radius Protocol Events Viewing

To view the events that have taken place during the RADIUS authentication procedures, you need to activate the events system for this protocol.

You may enable this from the configuration menu as follows:

```
*P 4
Config>EVENT
-- ELS Config --
ELS Config>ENABLE TRACE SUBSYSTEM RAD 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 RAD ALL
ELS>EXIT
+
```