Router Teldat

Protocolo RADIUS

Doc. *DM733* Rev. *10.10*
Junio, 2003

ÍNDICE

Capítulo 1
Introducción

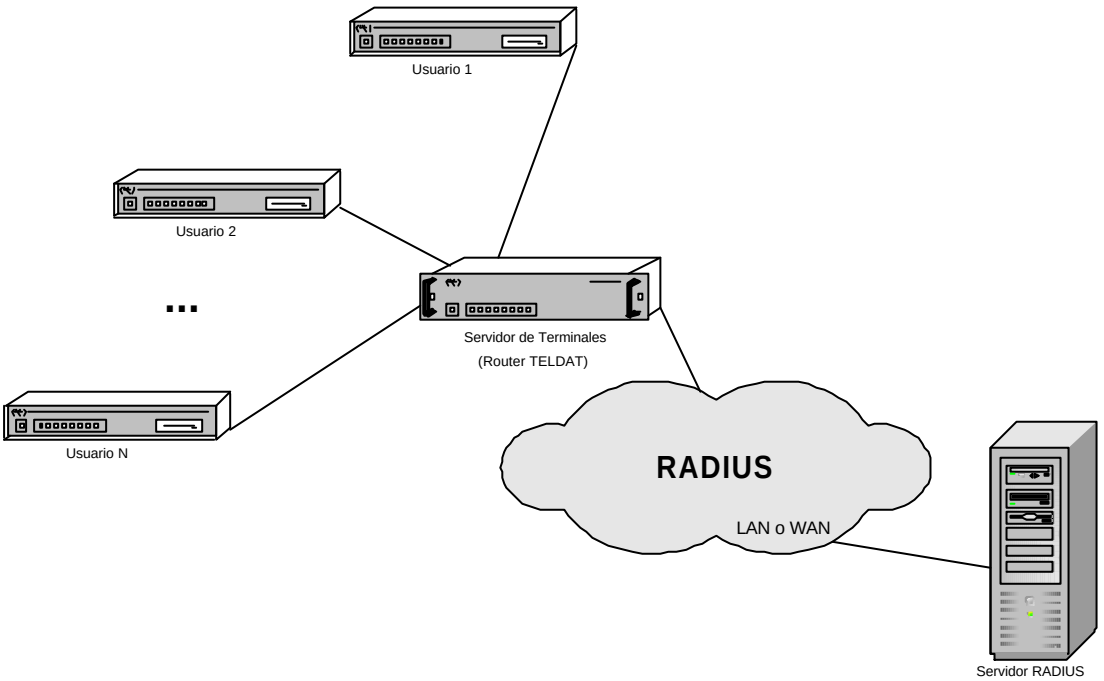
1. Introducción al Protocolo Radius

En la actualidad, los Administradores de Red disponen de pocas herramientas para preservar la seguridad de sus redes frente a incursiones no deseadas. Los sistemas de seguridad requieren generalmente un hardware específico o son únicamente compatibles con una cantidad limitada de productos. Este problema se agrava en redes de gran tamaño debido al elevado número de puntos de acceso. En este sentido, RADIUS (Remote Authentication Dial In User Service) constituye una solución a los problemas asociados con los requerimientos de seguridad de los accesos, que además de autenticación y autorización, posibilita el envío de información de configuración desde un Servidor de Autenticación RADIUS.

A continuación se detallan los entornos principales de utilización del protocolo RADIUS.

1.1. Autentificación y configuración de conexiones PPP

Este escenario es el correspondiente a un Servidor de Terminales que da servicio de acceso a una red a usuarios mediante conexiones PPP a través de línea serie, módem o RDSI.



En este contexto, para que un usuario pueda conectarse a la red a través del Servidor de Terminales es necesario que éste autorice dicho acceso. Para ello, los usuarios transmiten información unívoca sobre su identidad al Servidor de Terminales utilizando sus enlaces. Si no se utilizase el protocolo RADIUS, sería el Servidor de Terminales el encargado de decidir si autoriza o no la conexión, cotejando los datos recibidos con su relación de usuarios autorizados. En este caso, el Servidor de Terminales también debería informar del resultado de la autenticación, negociando en caso positivo la dirección IP con la que el usuario puede conectarse.

Por el contrario, si se emplea el protocolo RADIUS, la información procedente de los diferentes usuarios recogida por el Servidor de Terminales, es a su vez enviada al Servidor RADIUS, que es ahora el que determina si se autoriza o se deniega el acceso a la red solicitado por un usuario en

función de su base de datos. La decisión tomada por el Servidor RADIUS es comunicada al Servidor de Terminales que finalmente la transmite al usuario. En este caso, la dirección IP con la que un usuario autorizado puede conectarse se obtiene de la base de datos del Servidor RADIUS (**Framed-IP-Address**) y es enviada a su destinatario mediante el Servidor de Terminales. El Servidor RADIUS también envía la máscara de dicha dirección (**Framed-IP-Netmask**) para determinar el rango de direcciones solicitado por el usuario, las rutas que se deben configurar en el Servidor de Terminales para tener acceso a las redes conectadas al usuario (**Framed-Route**), e información de si el usuario se dispone a escuchar y/o a enviar paquetes con anuncios de rutas (**Framed-Routing**). En este último caso, el extremo local del Servidor de Terminales debe autoconfigurarse una dirección perteneciente a la misma subred que el extremo remoto en el usuario para poder realizar el intercambio de dichos paquetes.

En este modo de operación, se dice que el Servidor de Terminales actúa como cliente RADIUS ya que traslada las peticiones de conexión de los usuarios al Servidor RADIUS para que éste las valide.

Los usuarios pueden presentar al Servidor de Terminales la información necesaria para validarse siguiendo diferentes mecanismos de autenticación, pero para conexiones PPP, las alternativas posibles son los protocolos de autenticación PAP y CHAP.

El proceso de autenticación RADIUS se desarrolla de la siguiente manera. Cuando el Servidor de Terminales ha obtenido la información concerniente a la identidad de los usuarios, éste crea con ella una petición de acceso (**Access Request**) que envía al Servidor RADIUS a través de la red. Cuando una clave está presente en dicha petición, se oculta de tal forma que se asegure su confidencialidad. Si el Servidor RADIUS no responde a la petición durante un cierto periodo de tiempo, el Servidor de Terminales la reenvía de nuevo, pudiendo repetirse este hecho un determinado número de veces.

Una vez que el Servidor RADIUS recibe la petición, autentica en primer lugar al Servidor de Terminales que la ha enviado. Para ello utiliza información contenida en dicha petición y un secreto configurado en ambos equipos. Este secreto es una clave compartida entre los Servidores, que nunca es enviada a través de la red para proporcionar mayor seguridad. Si el Servidor de Terminales no es válido, la petición es descartada; en caso contrario, el Servidor RADIUS consulta su base de datos para comprobar si al usuario que figura en la petición, se le permite el acceso.

En el caso de que el Servidor de Terminales haya sido validado, el Servidor RADIUS puede responder de tres formas diferentes ante una petición de acceso.

Si el Servidor RADIUS comprueba que el usuario que ha solicitado la conexión se encuentra en la lista de usuarios autorizados, transmite al Servidor de Terminales una aceptación de acceso (**Access Accept**), donde figuran los valores de configuración para el usuario, como por ejemplo su dirección IP de conexión.

Por el contrario, si el usuario que desea conectarse a la red no figura en la base de datos del Servidor RADIUS, deniega su petición transmitiendo al Servidor de Terminales una respuesta de rechazo al acceso (**Access Reject**). Ésta es a su vez enviada al usuario para informarle de que no le concede la conexión

Si el protocolo de autenticación es CHAP, existe la posibilidad de que el Servidor RADIUS no transmita el paquete Access Accept esperado, ante la petición de conexión de un usuario que ha comprobado que está autorizado, sino que decida "desafiar" a dicho usuario a que se intente autenticar nuevamente. Para ello, manda al Servidor de Terminales un paquete **Access Challenge** en el que incluye en uno de sus atributos un valor numérico único e impredecible denominado **challenge.** El Servidor de Terminales comunica el challenge al usuario y éste efectúa con dicho valor una nueva solicitud de acceso a la red (**response**). El usuario dirige también esa nueva petición al Servidor de Terminales, que la traslada a su vez al Servidor RADIUS mediante un nuevo paquete Access Request. Finalmente, el Servidor RADIUS compara los datos recibidos en dicho paquete con los que esperaba recibir y actúa en consecuencia. Es decir, si la información contenida en el paquete recibido es la que el Servidor RADIUS esperaba, éste transmite al Servidor de Terminales un paquete Access Accept donde figura la dirección IP para la conexión. Por el contrario, si dicha información no es la esperada, envía el paquete Access Reject rechazando la solicitud de acceso. Por último, el Servidor RADIUS también puede "retar" nuevamente al usuario para que se autentique transmitiendo otro paquete Access Challenge.


PPP
CHAP
LAN / WAN
Access Request
(RADIUS)
Usuario
Servidor de Terminales
Servidor RADIUS


PPP
CHAP
LAN / WAN
Access Challenge (challenge)
(RADIUS)
Usuario
Servidor de Terminales
Servidor RADIUS


PPP
Challenge
(CHAP)
LAN / WAN
Usuario
Servidor de Terminales
Servidor RADIUS

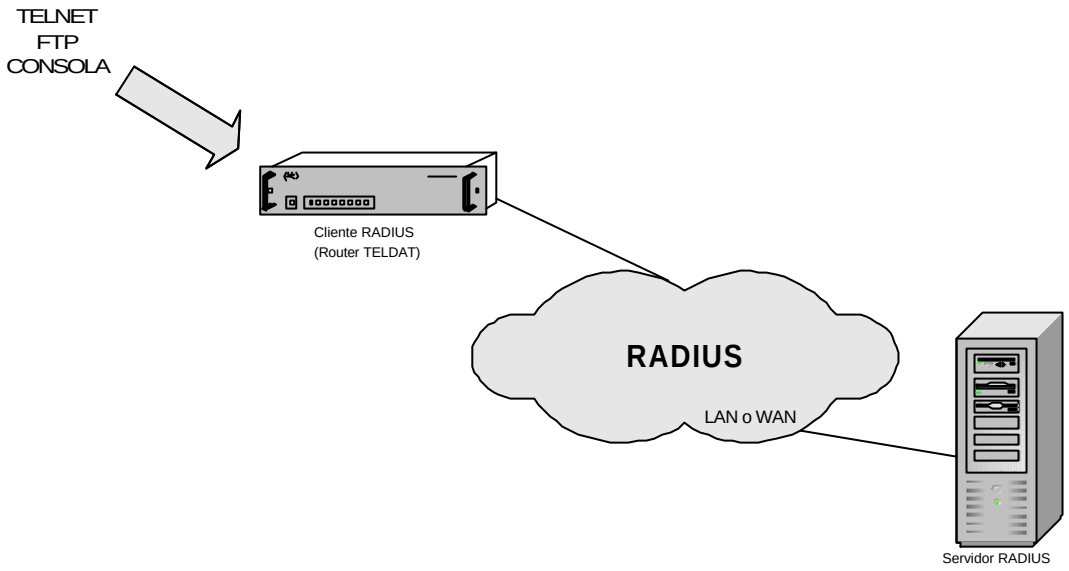

PPP
Response
(CHAP)
LAN / WAN
Usuario
Servidor de Terminales
Servidor RADIUS


PPP
(CHAP)
LAN / WAN
Access Request (nuevo)
(RADIUS)
Usuario
Servidor de Terminales
Servidor RADIUS


PPP
LAN / WAN
Access Accept
(RADIUS)
Usuario
Servidor de Terminales
Servidor RADIUS

1.2. Autentificación y configuración de las conexiones Telnet FTP y consola

En esta ocasión, son las conexiones TELNET, FTP y consola sobre un equipo las que se desean autenticar y configurar a través del protocolo RADIUS.



Para que un usuario pueda acceder al router a través de estas conexiones, es necesario que éste autorice dicho acceso. Para ello, los usuarios transmiten información unívoca sobre su identidad al equipo cuando éste la demanda. Si no se utilizase el protocolo RADIUS, sería el router el encargado de decidir si autoriza o no la conexión, cotejando los datos recibidos con los configurados en el mismo.

Por el contrario, si se emplea el protocolo RADIUS, la información procedente de los diferentes usuarios recogida por el router es a su vez enviada al Servidor RADIUS, siendo éste último el que determina si se autoriza o se deniega la conexión solicitada por un usuario en función de su base de datos interna, comunicándole con posterioridad el resultado al router. El proceso de intercambio de paquetes RADIUS es idéntico al relatado en el apartado anterior para las conexiones PPP, por lo que ahora no se detalla.

En el caso de la autenticación sobre los **Router Teldat**, dependiendo del usuario con el que nos hayamos autenticado, tendremos permiso a la hora de acceder a los diferentes procesos y ejecutar algunos comandos restringidos.

Los routers Teldat trasladan todos los caracteres del nombre de usuario a mayúsculas aunque se introduzcan en minúsculas, por lo que en la configuración de los Servidores RADIUS se deben incluir estos con esta característica.

Para poder autenticarnos en el sistema, tendremos que introducir el usuario y la password correspondiente, a no ser que se haya definido localmente una clave de acceso al equipo mediante el

comando **SET PASSWORD** y no se hayan definido usuarios localmente. En este caso, en las conexiones TELNET y consola sobre los routers Teldat, no se pide el nombre de usuario, sino que únicamente se pregunta por la clave o password. Debido a que los Servidores RADIUS necesitan que se les facilite un nombre de usuario, el router envía "TELNET" en la situación de una conexión TELNET, y "CONSOLE" en la de consola, estando esta propiedad oculta para el usuario, pero debiendose tener en cuenta a la hora de configurar el Servidor RADIUS.

El siguiente ejemplo muestra como se realiza la definición de un usuario con su password correspondiente y el nivel de acceso Config:

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

Se definen los siguientes niveles de acceso para el atributo **Service-Type** para acceder a FTP, telnet o consola:

Administrative: Se permite el acceso mediante FTP, Telnet y consola. El acceso a través de FTP se hace como ROOT. El nivel de acceso para Telnet y consola viene determinado por el atributo Login-Service.

NAS Prompt: Se permite el acceso mediante FTP, Telnet y consola. El acceso a través de FTP se hace como ANONYMOUS. El nivel de acceso para Telnet y consola viene determinado por el atributo Login-Service.

Login: Se permite el acceso solo mediante Telnet y consola. El nivel de acceso para Telnet y consola viene determinado por el atributo Login-Service.

El atributo Service-Type siempre ha de estar presente en la definición de los atributos de los usuarios.

Para el atributo **Login-Service** se han definido 5 niveles de acceso diferentes:

None: No permite acceder al sistema.

Events: Permite acceder a la Gestión de Consola (P1), a la Visualización de Eventos (P 2) y no permite ejecutar los comandos Ping, Telnet, Restart ni Load.

Monitor: Permite acceder a la Gestión de Consola (P1), a la Visualización de Eventos (P 2) y al proceso de Monitorización (P 3). También permite ejecutar los comandos Ping y Telnet, pero no Restart ni Load.

Config: Tiene acceso a todos los procesos y a todos los comandos estándar.

Root: Además de tener acceso a todos los comandos estándar, tiene acceso a los comandos propios de gestión de usuarios, los cuales se explican más adelante.

Debido a que estos niveles de acceso no son estandar, hay que definir en el diccionario del servidor de Radius estos niveles como se indica a continuación:

```
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
```

Al dar de alta en el servidor Radius los usuarios autorizados, tendremos que indicar el nivel de acceso correspondiente. Si omitimos el valor del atributo Login-Service, se considera que el nivel de acceso es Root.

Puede encontrar más información sobre la autenticación local del equipo en el Capitulo 1 "La Consola del Router Teldat"del Manual Configuración y Monitorización Dm 704.

Si se activa la autenticación por Radius, ésta tiene preferencia sobre cualquier otro tipo de autenticación local del equipo.

Como se puede observar, el proceso de autenticación RADIUS simplifica el proceso de seguridad al separar las tareas de autenticación y autorización de los usuarios, del propio proceso de comunicación. Por otro lado, la existencia de un Servidor RADIUS que aglutina la información de los diferentes usuarios, proporciona mayor seguridad que la localización de dichos datos en distintos servidores dispersos en la red. Asimismo, un único Servidor RADIUS es capaz de soportar cientos de Servidores de Terminales, que a su vez pueden dar servicio a decenas de miles de usuarios de forma sencilla y segura.

Dadas las ventajas que ofrece la utilización de un servidor RADIUS es este ámbito, TELDAT ha implementado este protocolo en sus routers siguiendo la **RFC 2138**. En estos equipos, el proceso de autenticación RADIUS opera de la forma descrita anteriormente con la salvedad de que el router, por el momento, no soporta el funcionamiento challenge/response. En efecto, si el router de TELDAT, que actúa como Servidor de Terminales, recibe paquetes Access Challenge del Servidor RADIUS los trata como si fueran paquetes Access Reject.

El protocolo RADIUS se puede habilitar en cualquier interfaz del equipo que tenga establecida una conexión PPP mediante línea serie o RDSI con el usuario que se desea autenticar. Para ello, se habilita primero RADIUS globalmente en el menú de configuración de RADIUS y a continuación se habilita la validación por RADIUS en el interfaz PPP que se desee. De la misma forma, se necesita habilitar RADIUS de manera global en el equipo y después en las conexiones TELNET, FTP y consola para autenticarlas mediante este protocolo. No es posible habilitar la autenticación por RADIUS si previamente no se ha configurado la dirección IP de un Servidor RADIUS al que se trasladen las peticiones de conexión, además del "secreto" compartido entre el router y este Servidor RADIUS.

Aparte de ello, también se pueden configurar la dirección IP y el "secreto" de un Servidor RADIUS alternativo con el que interactuar si el Servidor primario no responde, los puertos UDP a utilizar, el identificador del Servidor de Terminales, el número de veces que es posible reenviar una petición si no se recibe respuesta de los Servidores RADIUS y el tiempo entre reenvíos. El valor de estos parámetros se puede establecer de forma independiente o de forma conjunta con los demás, siendo posible la consulta de todos ellos, a excepción de los "secretos".

En el caso de conexiones TELNET y consola con autenticación por RADIUS, si no se obtiene ningún tipo de respuesta de los servidores RADIUS se pasa a la autenticación local del equipo.

Por otro lado, en la monitorización de este protocolo se permiten listar los estadísticos de los paquetes intercambiados en los diferentes procesos de autenticación que se han lanzado desde la última vez que se reinició el equipo, y que se encuentran definidos en la **RFC 2618**. Por último, se ha definido un sistema de eventos para este protocolo, que "marcan" los puntos claves durante el proceso de validación de un usuario mediante los Servidores RADIUS.

A continuación, se explican de forma detallada la configuración y monitorización de este protocolo en los dos capítulos siguientes.

Capítulo 2
Configuración

1. Acceso a la configuración del Protocolo Radius

En este apartado se describen los comandos necesarios para configurar el equipo como Servidor de Terminales cliente de un Servidor RADIUS. En primer lugar, se debe acceder a su entorno de configuración (prompt "RADIUS config>"); para ello, se deben introducir los siguientes comandos:

```
*P 4

Config>FEATURE RADIUS

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

2. Comandos de Configuración

Una vez situados en el ámbito de configuración, se puede pasar a configurar los parámetros. Para ello, se dispone de los comandos resumidos en la siguiente tabla:

Comando	Función
? (AYUDA)	Muestra todos los comandos u opciones disponibles.
ALTERNATE-ADDRESS	Configura la dirección IP del servidor Radius alterno.
ALTERNATE-PORT	Configura el puerto de conexión al servidor Radius alterno.
ALTERNATE-SECRET	Configura la clave de acceso al servidor Radius alterno.
ATTEMPTS	Configura número de intentos de envío de petición Radius.
CONSOLE	Habilita o deshabilita la autenticación Radius para accesos por consola al equipo.
DELAY	Configura tiempo entre reenvíos de peticiones de autenticación al servidor Radius.
DISABLE	Deshabilita el protocolo Radius.
ENABLE	Habilita el protocolo Radius.
FTP	Habilita o deshabilita la autenticación Radius para accesos por FTP al equipo.
IDENTIFIER	Configura el identificador para el equipo.
LIST	Permite visualizar los valores de los parámetros configurados.
NO	Configura los difentes parámetros a su valor por defecto.
PRIMARY-ADDRESS	Configura la dirección IP del servidor Radius primario.
PRIMARY-PORT	Configura el puerto de conexión al servidor Radius primario.
PRIMARY-SECRET	Configura la clave de acceso al servidor Radius primario.
SOURCE-INTERFACE	Configura el interfaz origen de los paquetes RADIUS.
TELNET	Habilita o deshabilita la autenticación Radius para accesos por TELNET al equipo.
EXIT	Retorna al prompt anterior.

Se explica a continuación, cada uno de los comandos mencionados de forma más detallada.

2.1. ? (AYUDA)

Este comando se puede utilizar de dos modos diferentes. Por un lado, permite obtener un listado de todos los comandos disponibles en el entorno de configuración RADIUS, para lo que se teclea el comando **?** en el prompt "RADIUS config>".

Sintaxis:

```
RADIUS config>?
```

Ejemplo:

```
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 config>
```

Este comando también se puede utilizar para visualizar las opciones disponibles de un comando específico del menú de configuración. En este caso se escribe el nombre del comando del que queremos conocer sus opciones seguido del signo de interrogación **?**. En el caso de **CONSOLE**:

Ejemplo:

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

2.2. ALTERNATE-ADDRESS

Este comando se utiliza para fijar la dirección IP del Servidor RADIUS alternativo al que el equipo va a enviar las peticiones de autenticación RADIUS, si el Servidor RADIUS primario no responde. Esta dirección se configura de la siguiente forma:

Ejemplo:

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

La dirección que aparece en el mensaje entre corchetes corresponde al valor de la dirección IP configurado anteriormente, o si no se ha configurado el de la dirección IP del Servidor primario.

En el caso de introducir una dirección IP no válida aparece el mensaje de error

```
Bad address, try again
```

y se solicita una nueva dirección IP.

2.3. ALTERNATE-PORT

Con este comando se configura el puerto UDP del Servidor RADIUS alterno al que el equipo envía sus peticiones de autenticación si el Servidor primario no responde, y el puerto UDP donde recibe las respuestas a esas posibles peticiones. La forma de configurar este puerto es la siguiente:

Ejemplo:

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

El valor que aparece entre corchetes para los dos puertos es el oficialmente asignado para el protocolo RADIUS, aún así, se puede configurar el valor de 1645 por estar su uso extendido en la comunidad RADIUS. Si se cambia el valor del puerto, entre corchetes se muestra el valor actualmente configurado.

Si se introduce un número de puerto diferente a estos valores, aparece el mensaje de error

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

2.4. ALTERNATE-SECRET

Mediante este comando se configura el "secreto" del equipo, que debe coincidir con el del Servidor RADIUS alterno establecido. Se configura de la siguiente forma.

Ejemplo:

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

Como se puede observar en el ejemplo, el secreto debe ser tecleado dos veces por el usuario para garantizar que se ha introducido correctamente. Si ambos valores no coinciden aparece el mensaje

```
Different secrets
```

por lo que se debe configurar nuevamente.

En el caso de solicitar configurar secreto y no introducir ningún valor se genera el mensaje de error

```
Null secret
```

Este parámetro puede contener hasta 32 caracteres, todos ellos distintos de tabulaciones y espacios en blanco.

NOTA: Si no se han configurado los valores de dirección IP y secreto en ninguno de los dos Servidores RADIUS y se intenta habilitar RADIUS, aparece un mensaje de error que informa de este hecho.

2.5. ATTEMPTS

Este comando se utiliza para fijar el número de veces que es posible enviar una petición de autenticación RADIUS, si no se recibe respuesta de los Servidores RADIUS en el tiempo establecido.

En un principio, se enviarán hasta tres peticiones seguidas de autenticación de un usuario al Servidor primario, y luego se empezará a alternar entre el Servidor alternativo y éste hasta que se reciba respuesta de alguno de ellos o concluya el intervalo de espera de la última petición. En este último caso, el usuario al que correspondan las peticiones será rechazado.

Si en el instante de empezar a enviar las peticiones de autenticación de un usuario, no se encuentran levantados los interfaces del equipo que lo conectan con los Servidores RADIUS, se realizan intentos de transmisión cada dos segundos hasta que, o bien se consigue transmitir la petición, o transcurre un tiempo total igual a diez segundos. En esta última situación, el usuario también será rechazado.

Si una vez comenzado el reenvío de peticiones, uno de los interfaces no se encuentra levantado o se cae, cuando se necesite retransmitir el paquete al Servidor RADIUS alcanzable a través de ese interfaz, el paquete se enviará al otro Servidor cuyo interfaz sí esté levantado. En cambio, si los dos interfaces

se encuentran caídos, se esperará un tiempo igual al configurado entre peticiones hasta volver a intentar la retransmisión, contando a todos los efectos como reenvíos aunque no se haya mandado ningún paquete.

Este parámetro se configura de la siguiente forma:

Ejemplo:

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

El número que aparece en el mensaje entre corchetes corresponde al valor anterior .

El valor por defecto para este parámetro es el **5**.

El rango de valores permitidos para el número de intentos es (1-100), si el valor introducido se encuentra fuera de este rango aparece el mensaje

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

2.6. CONSOLE

Este comando habilita o deshabilita la autenticación del acceso por consola al equipo mediante el protocolo RADIUS.

Sintaxis:

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

a) CONSOLE ENABLED

Este comando habilita la autenticación del acceso por consola al equipo mediante el protocolo RADIUS.

Ejemplo:

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

b) CONSOLE DISABLED

Este comando deshabilita la autenticación del acceso por consola al equipo mediante el protocolo RADIUS.

Ejemplo:

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

2.7. DELAY

Este comando se utiliza para configurar el tiempo entre reenvíos de peticiones de autenticación RADIUS. Se configura de la siguiente forma:

Ejemplo:

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

El número que aparece en el mensaje entre corchetes corresponde al valor anterior.

El valor por defecto para este parámetro es el **1000 ms.**

El rango de valores permitidos para el intervalo es (1-30 sg), si el valor introducido se encuentra fuera de este rango aparece el mensaje

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

2.8. DISABLE

Mediante este comando se deshabilita el protocolo RADIUS de forma global en el equipo.

Sintaxis:

```
RADIUS config>DISABLE RADIUS
```

Ejemplo:

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

Aunque la facilidad RADIUS se encuentre habilitada en los interfaces PPP del equipo, así como para las conexiones FTP, TELNET y consola que se realicen sobre el mismo, este comando evita que las autenticaciones de estas aplicaciones se realicen a través de un Servidor RADIUS.

2.9. ENABLE

Este comando permite habilitar el protocolo RADIUS de forma global en el equipo.

Sintaxis:

```
RADIUS config>ENABLE RADIUS
```

Ejemplo:

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

En el caso de que no hayan sido configurados los parámetros SECRETO y DIRECCION de uno de los Servidores RADIUS, no es posible habilitar el protocolo RADIUS y se informa de esta situación mediante el mensaje

```
Some parameters are not set
```

Además de utilizar este comando, para habilitar la autenticación RADIUS en los interfaces PPP del equipo (manual Dm 710), así como en las conexiones FTP (manual Dm 724), TELNET y consola (manual Dm704) que se realicen sobre el mismo, es necesario habilitar la facilidad RADIUS en cada una de estas aplicaciones, empleando los comandos correspondientes de sus entornos de configuración. Para las conexiones FTP, TELNET y consola, la facilidad RADIUS puede habilitarse también desde el menú de configuración del RADIUS, usando los comandos que se describen en este manual (comandos CONSOLE, FTP y TELNET).

2.10. FTP

Este comando habilita o deshabilita la autenticación del acceso por conexión FTP al equipo mediante el protocolo RADIUS.

Sintaxis:

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

a) FTP ENABLED

Este comando habilita la autenticación del acceso por conexión FTP al equipo mediante el protocolo RADIUS.

Ejemplo:

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

b) FTP DISABLED

Este comando deshabilita la autenticación del acceso por conexión FTP al equipo mediante el protocolo RADIUS.

Ejemplo:

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

2.11. IDENTIFIER

Con este comando se configura un identificador para el equipo de hasta 128 caracteres de longitud, sin tabulaciones ni espacios en blanco en su contenido. La forma de configurarlo es la siguiente:

Ejemplo:

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

El identificador que aparece entre corchetes se corresponde con el identificador configurado anteriormente. Su valor por defecto es **TeldatRadiusClient**.

2.12. LIST

Este comando permite consultar los valores de los parámetros configurados a excepción de los secretos cuyos valores no pueden visualizarse. Se procede de la siguiente forma:

Sintaxis:

```
RADIUS config>LIST
```

Ejemplo:

```
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>
```

Como se puede observar en el ejemplo, la opción LIST, informa además sobre el estado en que se encuentra el protocolo RADIUS, tanto globalmente como en lo que se refiere a la autenticación a través del protocolo RADIUS del acceso al equipo por consola, telnet o FTP.

Si RADIUS ha sido habilitado globalmente aparece el mensaje

```
RADIUS enabled
```

En caso contrario, el mensaje es

```
RADIUS disabled
```

2.13. NO

Este comando se utiliza para configurar los difentes parámetros a su valor por defecto.

Sintaxis:

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

Los valores por defecto son los siguientes:

Comando	Valor por defecto
ALTERNATE-ADDRESS	0.0.0.0
ALTERNATE-PORT	1812
ALTERNATE-SECRET	vacío (sin secreto)
ATTEMPTS	5
DELAY	1000 ms
IDENTIFIER	TeldatRadiusClient
PRIMARY-ADDRESS	0.0.0.0
PRIMARY-PORT	1812
PRIMARY-SECRET	vacío (sin secreto)
SOURCE-INTERFACE	Se asocian los paquetes RADIUS al interfaz de salida.

2.14. PRIMARY-ADDRESS

Este comando se utiliza para fijar la dirección IP del Servidor RADIUS primario al que el equipo va a comenzar a enviar las peticiones de autenticación RADIUS. Esta dirección se configura de la siguiente forma:

Ejemplo:

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

La dirección que aparece en el mensaje entre corchetes corresponde al valor de la dirección IP configurado anteriormente, o si no se ha configurado el de la dirección IP del Servidor altenativo.

En el caso de introducir una dirección IP no válida aparece el mensaje de error

```
Bad address, try again
```

y se solicita una nueva dirección IP.

2.15. PRIMARY-PORT

Con este comando se configura el puerto UDP del Servidor RADIUS primario al que el equipo envía sus peticiones de autenticación, y el puerto UDP donde recibe las respuestas a esas peticiones. La forma de configurar este puerto es la siguiente:

Ejemplo:

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

El valor que aparece entre corchetes es el oficialmente asignado para el protocolo RADIUS, aún así, se puede configurar el valor de 1645 por estar su uso extendido en la comunidad RADIUS. Si se cambia el valor del puerto, entre corchetes se muestra el valor actualmente configurado.

Si se introduce un número de puerto diferente a estos valores, aparece el mensaje de error

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

2.16. PRIMARY-SECRET

Mediante este comando se configura el "secreto" del equipo, que debe coincidir con el del Servidor RADIUS primario establecido. Se configura de la siguiente forma.

Ejemplo:

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

Como se puede observar en el ejemplo, el secreto debe ser tecleado dos veces por el usuario para garantizar que se ha introducido correctamente. Si ambos valores no coinciden aparece el mensaje

```
Different secrets
```

por lo que se debe configurar nuevamente.

En el caso de solicitar configurar secreto y no introducir ningún valor se genera el mensaje de error

```
Null secret
```

Este parámetro puede contener hasta 32 caracteres, todos ellos distintos de tabulaciones y espacios en blanco.

2.17. SOURCE-INTERFACE

Mediante este comando se asocia un interfaz origen a los paquetes RADIUS. La dirección IP origen de estos es la que esté asociada a ese interfaz. Si ese interfaz no tiene configurada ninguna IP, se utiliza la configuración por defecto (IP asociada al interfaz de salida).

Si el interfaz asociado tiene configurada más de una IP, se usa la última configurada.

Si se borra el interfaz, se usa la configuración por defecto.

Ejemplo:

```
RADIUS config>SOURCE-INTERFACE ?
  <INTERFACE>    Interface name
RADIUS config>
```

2.18. TELNET

Este comando habilita o deshabilita la autenticación del acceso por terminal remoto TELNET al equipo mediante el protocolo RADIUS.

Sintaxis:

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

a) TELNET ENABLED

Este comando habilita la autenticación del acceso por terminal remoto TELNET al equipo mediante el protocolo RADIUS.

Ejemplo:

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

b) TELNET DISABLED

Este comando deshabilita la autenticación del acceso por terminal remoto TELNET al equipo mediante el protocolo RADIUS.

Ejemplo:

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

2.19. EXIT

Este comando, como ya se ha mencionado anteriormente, se utiliza para salir del entorno de configuración RADIUS y retornar al prompt anterior, que corresponde al ámbito de Configuración de Usuario. Se ejecuta de la siguiente forma:

Sintaxis:

```
RADIUS config>EXIT
```

Ejemplo:

```
RADIUS config>EXIT
Config>
```

Capítulo 3
Monitorización

1. Acceso a la monitorización del Protocolo Radius

En este capítulo se describen los comandos de monitorización del protocolo RADIUS. Para poder acceder a estos comandos, hay que situarse en el entorno de Monitorización RADIUS (prompt RADIUS>) y teclear los siguientes comandos:

```
*P 3

+FEATURE RADIUS

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

2. Comandos de monitorización

Una vez situados en el ámbito de monitorización adecuado se puede ejecutar cualquiera de los siguientes comandos:

Comando	Función
? (AYUDA)	Muestra todos los comandos u opciones disponibles.
LIST	Permite visualizar los estadísticos y el valor de algunos parámetros.
EXIT	Retorna al prompt anterior.

Se explica a continuación, cada uno de los comandos mencionados de forma más detallada.

2.1. ? (AYUDA)

El comando **?** (AYUDA) en este entorno permite obtener un listado de todos los comandos disponibles en el ámbito de monitorización RADIUS. Para ello, se teclea **?** en el prompt "RADIUS>"

Sintaxis:

```
RADIUS>?
```

Ejemplo:

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

Este comando también se puede utilizar para visualizar las opciones disponibles del comando **LIST** de este menú. En este caso se escribe **LIST** seguido del signo de interrogación **?**.

Ejemplo:

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

2.2. LIST

El comando **LIST** se utiliza para consultar el valor de los parámetros configurados y los estadísticos del protocolo. Las opciones de este comando se pueden ver de la forma indicada en el ejemplo anterior.

Sintaxis:

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

a) LIST PARAMETERS

Mediante el comando **LIST PARAMETERS** es posible visualizar el valor de todos los parámetros configurados a excepción de los secretos, además del estado en el que se encuentra el protocolo RADIUS. Se procede de la siguiente forma:

Ejemplo:

```
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

Tecleando este comando podemos acceder a los estadísticos de los paquetes correspondientes a los diferentes procesos de autenticación lanzados desde la última vez que se reinició el equipo. Esta información se consulta de la siguiente forma:

Ejemplo:

```
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>
```

Como se puede observar, en primer lugar aparece el identificador configurado del equipo junto con los paquetes recibidos de Servidores RADIUS desconocidos. Seguidamente, se listan los estadísticos de los paquetes RADIUS intercambiados primero con el Servidor primario y luego con el Servidor alternativo.

Si estos Servidores tienen configurado el mismo secreto, la misma dirección IP y el mismo puerto UDP, se considerará que sólo hay un Servidor RADIUS disponible a la hora de enviar las peticiones de autenticación, por lo que únicamente se listarán los estadísticos de los paquetes intercambiados con este Servidor.

Si sólo uno de ellos tiene configurado la dirección IP y el secreto, independientemente de si es el Servidor primario o alterno, se considerará como Servidor primario y sólo se listarán sus paquetes asociados.

Por último, si ninguno de los Servidores tiene configurados la dirección y el secreto, aparecerá el mensaje:

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

detrás del identificador del Servidor de Terminales.

c) LIST ALL

Mediante esta opción se pueden visualizar los parámetros y los estadísticos de la siguiente forma:

Ejemplo:

```
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

Este comando, como ya se ha mencionado anteriormente, se utiliza para salir del entorno de monitorización RADIUS y retornar al prompt anterior, que corresponde al Operador de Consola. Se ejecuta de la siguiente forma:

Sintaxis:

```
RADIUS>EXIT
```

Ejemplo:

```
RADIUS>EXIT
+
```

3. Visualización de Eventos del Protocolo Radius

Para visualizar los eventos que suceden durante los procesos de autenticación RADIUS, es necesario activar el sistema de eventos para este protocolo.

La forma en que se habilita desde el menú de configuración es la siguiente:

```
*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>
```

También es posible habilitar los eventos desde el menú de monitorización en cualquier momento, sin necesidad de guardar la configuración y reiniciar. La secuencia de comandos a introducir sería la siguiente:

```
*P 3
+EVENT

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