Chapter 41

User Authentication

Introduction

This chapter describes:

- the different privilege levels at which users can log into the router
- the router's security operating mode
- using the router's built-in User Authentication Database to authenticate users
- using external RADIUS, TACACS, or TACACS+ authentication servers to authenticate users

Privilege Levels

Commands that someone is permitted to execute depend on their privilege level and whether the router is in normal mode or security mode. The router supports the following levels of privilege:

- **User Level**
- **Manager Level**
- **Security Officer Level**
- **Remote Security Officer Level**

By default, the router has one account (*manager*) defined with manager privilege and the password *friend*.

The prompt typically changes when the user's privilege level changes. A user level prompt looks like:

```
>
```

A manager level prompt looks like:

```
Manager >
```

A security officer prompt looks like:

```
SecOff >
```

However, for a connection to an asynchronous port, you can change the prompt to a user-defined string by using the **set asyn** command on page 9-40 of Chapter 9, Interfaces. Once changed, the prompt no longer reflects the security level of the user, and does not change when the security level changes.

For information about the security operating mode, see "Operating Modes" on page 41-7.

User Level

User level gives access to a limited set of commands, regardless of whether the router is in normal or security mode. User level commands affect the user's own session or asynchronous port. User privilege applies to a user who has not logged in—someone using a terminal connected to an asynchronous port that is **not** in security mode—or a user who has logged in with a user name with user privilege.

Manager Level

Manager level gives access to commands for configuring and viewing all aspects of the router that are not specifically security related.

To gain manager privilege, do one of the following:

- Login at the prompt with a username that has manager privilege. This is the usual method of gaining manager privilege, especially when managing remote routers.

  You are prompted for a password. The password is case-sensitive and must be entered exactly as defined. If you enter the password correctly, the port or Telnet connection gains manager privilege.

- If you are already logged in with user or security officer privilege, use the following command from a port or Telnet session to login under a name that has manager privilege:

  ```
  login
  ```

  If you enter the password correctly, the port or Telnet connection gains manager privilege and the prompt changes to the manager level prompt.

- Use the following command to set a port as a semipermanent manager port:

  ```
  set manager asyn
  ```

  Any terminal connected to the specified port has manager privilege. The **set manager asyn** command on page 41-53 is a manager level command and can only be entered from a port or a Telnet session that already has manager privilege. Only one port at a time can be defined as a manager port.

To change from manager to user level, use the command:

```
logoff
```

When the router is in normal mode, manager privilege is equivalent to security officer privilege. However, when the router is in security mode, **only** users with security officer privilege can successfully execute the subset of commands called *security commands*, and produce complete output about the network. When a manager or user enters one of these commands, a message is displayed that the switch is in secure mode and security officer privilege is required *(see* "Operating Modes" on page 41-7).

Security timer

In normal mode, a user with manager privilege can create and delete accounts for users of any privilege level. Therefore, unauthorised use of a manager session gives access to the User Authentication Database. Make sure that you do not leave a manager session unattended.

To reduce the risk of unauthorised activity, a subset of manager commands have a security timer. These commands are shown in Table 41-1 on page 41-5. When you enter one of these commands from a manager session, the security timer is started, and is restarted each time you enter another of these commands. If you enter one of these commands after the timer has expired, you are prompted to re-enter the password. The security delay timer is by default 60 seconds. If the password is not entered correctly, the password prompt is repeated a set number of times. If the correct password is still not entered, a log message is generated and the session is logged off.

The security timer enables a manager to make successive additions and modifications to the database at one time without having to re-enter the password for every command.

The security timer does **not** provide a foolproof security mechanism. managers should always log out of a manager session before leaving a terminal unattended.

When the router is in security mode, the manager must also log in with security officer privilege in order to execute commands controlled by the security timer (Table 41-1).

Table 41-1: Security commands controlled by the security timer

Command	Description
add tacacs server	Adds a TACACS server to the list of TACACS servers used for user authentication.
add user	Adds a user to the User Authentication Database.
delete tacacs server	Deletes a TACACS server from the list of TACACS servers used for user authentication.
delete user	Deletes a user from the User Authentication Database.
purge user	Deletes all users except managers from the User Authentication Database.
set manager asyn	Assigns a port semipermanent manager privilege.
set user	Modifies a user record in the User Authentication Database.

Security Officer Level

The security officer level has access to the full set of commands regardless of whether the router is in normal or security mode.

When the router is in security mode, **only** a user with security officer privilege can execute commands that affect router security. These commands are noted in individual chapters. A message that Security Office privilege is required is typically displayed. See "Operating Modes" on page 41-7.

A user must login under a name with security officer privilege from a terminal directly connected to an asynchronous port on the router or a Telnet session originating from an authorised IP address (see "Remote Security Officer Level" on page 41-6).

Security timer

A security timer operates while a user is logged in with security officer privilege to minimise the risk of unauthorised access to an unattended terminal or Telnet session. Every time a command is entered, the security timer restarts. If the timer expires, the user's privilege is reset to manager level, but the user remains logged in. Any attempt to execute a security command requires the user to re-enter the security officer password. Configure the timeout period in seconds by using the command:

```
set user securedelay=10..3600
```

The security timer is **not** a foolproof security mechanism. managers should always log out of a security officer session before leaving a terminal unattended.

Remote Security Officer Level

The *remote security officer* (RSO) feature lets a remote user connect to a router via Telnet from an authorised IP address or range of IP addresses, and login using a name with security officer privilege as if the user were at a terminal connected directly to the router. By default the remote security officer feature is disabled.

The RSO feature can be enabled or disabled with the commands:

```
enable user rso
disable user rso
```

Authorised IP addresses can be added and deleted with the commands:

```
add user rso ip=ipadd [mask=ipadd]
add user rso ip=ipadd[-ipadd]
add user rso ip=ipv6add[/prefix-length]
add user rso ip=ipv6add[-ipv6add]
delete user rso ip=ipadd[-ipadd]
delete user rso ip=ipv6add/prefix-length
delete user rso ip=ipv6add[-ipv6add]
```

The current state of the RSO feature and the list of authorised IP addresses can be displayed by using the command:

```
show user rso
```

All RSO commands require security officer privilege and therefore must be executed from a terminal directly attached to the router or from a Telnet session originating from a previously configured RSO address. RSO must be enabled, and the first address added, from a terminal directly attached to the router. If RSO is disabled (either from a terminal or a Telnet session) it must be re-enabled from a terminal directly attached to the router.

Once RSO has been enabled and configured with one or more IP addresses, a Telnet session from one of the authorised addresses can login as a user with security officer privilege.

Operating Modes

The router operates in either normal mode or security mode. When the router is in normal mode, privileges for a manager and security officer are the same. The router is in normal mode by default.

Security mode provides additional protection to routers with encryption hardware or configured to provide sensitive security functions with:

- **Secure Shell**
- **Secure Sockets Layer (SSL)**
- **Compression and Encryption Services**
- **IP Security (IPsec)**
- **Public Key Infrastructure (PKI)**)

When the router is in security mode, **only** users with security officer privilege can successfully use the subset of router commands called *security commands*. These commands impact the integrity of the network and include commands such as **add user** and **rename file**. Sensitive data files, such as encryption keys, can be stored in the file system only when the router is in security mode.

Security officers can display sensitive data about the network in output from commands such as **show system** and **show log**. When a non-security Officer enters one of these commands, a message advises that the router is in secure mode and security officer privilege is required. Security commands are documented in the Command Reference in individual chapters.

To enable security mode, first create a user with security officer privilege, then enter the command:

```
enable system security_mode
```

To access secure functionality you must log in again as a security officer. This command creates a security mode enabler file in the router's file system. This file cannot be manually modified, displayed, deleted, copied, or renamed. If the router is restarted, the startup process checks for the enabler file. If it is present, the router boots up in security mode; otherwise, the router starts in normal mode.

To restore the router to normal operating mode, enter the command:

```
disable system security_mode
```

Caution When security mode is disabled, the router automatically deletes the enabler file and all sensitive data files, including encryption keys.

To display the current operating mode, enter the command:

```
show system
```

User Authentication Facility

The User Authentication Facility (UAF) controls access to the router's command line interface (CLI), GUI, and dial-up services through a login name and password.

Login prompt

The UAF automatically prompts for a login name and password when a user tries to:

- access the router's command line interface (CLI) via a terminal or terminal emulator connected directly to an asynchronous port
- access the router's CLI via a Telnet connection
- access a dial-up service via an asynchronous modem connected to an asynchronous port
- access the router's GUI

The user must enter appropriate responses, pressing the Enter key after each response. Characters entered at the password prompt are not echoed to the screen for security reasons (Figure 41-1).

Figure 41-1: A typical login session for user Bruce on router CMD

```
CMD login: bruce
password:


CMD >
```

The password prompt is displayed regardless of whether a password is required for the login name entered by the user. This makes it more difficult for an intruder to discover valid login name/password combinations.

Users authenticated by the UAF can be operators, or other routers. If the user is another router, the authentication occurs without appearing on a terminal screen.

Logging in and out manually

A user who is already logged in may need to log in as another user to acquire different rights, such as manager or security officer privilege.

To manually log into the router, use one of these synonymous commands:

```
login
logon
logi
```

To log out of a session, use one of these synonymous commands:

```
logoff
logout
lo
```

Login failures and lockout

If the user enters an invalid login name or password, the login sequence is repeated. If successive login failures occur, the login prompt is withheld for a specified lockout period, and the terminal or Telnet session is locked out for a period of time. You can specify both the number of allowable login attempts, and the length of the lockout period.

If a user starts a Telnet session but does not log in within one minute, the router automatically terminates the Telnet connection.

Authentication methods

The UAF supports the following methods of user authentication:

- **User Authentication Database**
- **RADIUS**
- **TACACS**
- **TACACS+**

The UAF tries each authentication method in sequence until the user is authenticated or all methods have been tried. When the user is successfully authenticated, the process stops immediately and the login is accepted. If the user is not authenticated by any of the supported methods, the login is rejected.

The order in which the authentication methods are tried depends on whether any RADIUS backup users are defined in the User Authentication Database.

RADIUS backup users

You can configure users in the User Authentication Database as RADIUS backup users. RADIUS backup users provide a backup for RADIUS authentication and are used only when a RADIUS server is unreachable. They are not used if RADIUS rejects the authentication request, or for normal authentication using the User Authentication Database.

Authentication without RADIUS backup users

If no RADIUS backup users are defined in the User Authentication Database, the authentication process is as follows:

1. The UAF attempts TACACS+ authentication first.
2. If no TACACS+ servers are defined, or all the TACACS+ servers return a *reject* response, the UAF queries the User Authentication Database.
3. If the login name and password do not match an entry in the User Authentication Database, the UAF attempts RADIUS authentication.
4. If no RADIUS servers are defined, or all the RADIUS servers return a *reject* response, the UAF attempts TACACS authentication.
5. If no TACACS servers are defined, or all the TACACS servers return a *reject* response, authentication fails and the login is rejected.
6. If the user is authenticated using a login with security officer privilege, the login is only accepted if the user is accessing the router via asyn0, SSH or Telnet from an approved IP address. See "Remote Security Officer Level" on page 41-6 for more information.

Authentication with RADIUS backup users

If one or more RADIUS backup users are defined in the User Authentication Database, the authentication process is as follows:

1. The UAF attempts TACACS+ authentication first.
2. If no TACACS+ servers are defined, or all the TACACS+ servers return a *reject* response, the UAF attempts RADIUS authentication.
3. If no RADIUS servers are reachable, the UAF queries the User Authentication Database for users who have **radiusbackup** set to **yes**.
4. If all the RADIUS servers return a *reject* response, the UAF queries the User Authentication Database for users who have **radiusbackup** set to **no**.
5. If the login name and password do not match an entry in the User Authentication Database, the UAF attempts TACACS authentication.
6. If no TACACS servers are defined, or all the TACACS servers return a *reject* response, authentication fails and the login is rejected.
7. If the user is authenticated using a login with security officer privilege, the login is only accepted if the user is accessing the router via asyn0, SSH or Telnet from an approved IP address. See "Remote Security Officer Level" on page 41-6 for more information.

User Authentication Database

The User Authentication Database stores information about those users who are permitted access to the router's command prompt, asynchronous services, and dial up services. Users are identified by login names. Each login name has an associated record in the database that specifies the following:

- the password that the user must enter to log into the router
- the privilege level for the user: User, Manager, or Security Officer
- whether the user is permitted to use the **telnet** command on page 61-34 of Chapter 61, Terminal Server, or to connect to a Telnet service from a Telnet session
- the IP address, network mask, and Maximum Transmission Unit (MTU) to use for PPP connections to the router via an asynchronous port
- a callback number for use with the PPP callback facility
- whether the user is permitted to log into the router and enter commands.

Adding Entries to the User Authentication Database

When the router is started up for the first time one account is created automatically. This account has the login name Manager, the password "friend", login = yes, and manager level privilege. This account cannot be deleted although the password may—and should—be changed.

The manager should change the password of the manager account at the earliest opportunity. Leaving the manager account with the default password is a security risk because the account name and default password are well documented.

The **create config** command writes the MD5 digest, not the plaintext, of passwords in commands to the configuration file. When a configuration script is executed the command processor determines whether the password is plaintext or an MD5 digest.

To add more users to the User Authentication Database, use the command:

```
add user=login-name password=password
    [privilege={user|manager|securityofficer}]
    [telnet={yes|no}] [other-options]
```

The number of entries in the database is limited only by the amount of memory available. Only the login name and password are required. The default privilege level is **user**. Other information may be specified about a user, including a description (such as the user's full name), the privilege level, whether the user is permitted to use the **telnet** command on page 61-34 of Chapter 61, Terminal Server or connect to a Telnet service, and an IP number, network mask and Maximum Transmission Unit (MTU). The IP number, network mask and MTU are required if the user is to run asynchronous PPP or SLIP over an asynchronous modem connected to an asynchronous port. The callback number is required if the user is to make a PPP callback request with user authentication. See Chapter 15, Point-to-Point Protocol (PPP) for more information. The calling number is used for L2TP and ISDN services that provide caller ID information.

Modifying Entries in the User Authentication Database

To modify an entry in the database, use the command:

```
set user=login-name [password=password] [other-options]
```

To delete an entry in the database, use the command:

```
delete user=login-name
```

To delete all entries in the database, except the manager account, use the command:

```
purge user
```

To display the contents of the database, use the command:

```
show user[=login-name]
```

A manager can alter the password for any user by using the command:

```
set user=username password=password
```

This may be necessary if a user forgets the password. A log message is generated whenever the password for a manager account is changed.

A user who is logged in can change their own password by using the command:

```
set password
```

The command prompts for the old password, the new password, and confirmation of the new password. The new password and the confirmation must be identical for the change to take effect. This reduces the chance of a typing error causing the password to be different from what the user intended.

Important When you change the password for the manager account, ensure that you remember the new password because you cannot retrieve a lost password. Accessing the router again is complex.

Choosing Passwords

All users, including managers, should take care in selecting passwords. Tools exist that enable hackers to guess or test many combinations of login names and passwords easily. The User Authentication Facility (UAF) provides some protection against such attacks by allowing the manager to set the number of consecutive login failures allowed and a lockout period when the limit is exceeded.

However, the best protection against password discovery is to select a good password and keep it secret. When choosing a password:

- Do make it six or more characters in length. The UAF enforces a minimum password length, which the manager can change. The default is six characters.
- Do include both alphabetic (a–z) and numeric (0–9) characters.
- Do include both uppercase and lowercase characters. The passwords stored by the router are case-sensitive, so “bgz4kal” and “Bgz4Kal” are different.
- Do avoid words found in a dictionary, unless combined with other random alphabetic and numeric characters.
- **Do not** use the login name, or the word “password” as the password.
- **Do not** use your name, your mother’s name, your spouse’s name, your pet’s name, or the name of your favourite cologne, actor, food or song.
- **Do not** use your birth date, street number or telephone number.
- **Do not** write down your password anywhere.

Recovering passwords

If a user forgets their password, the password can be reset from an account with manager privilege by using the command:

```
set user=login-name password=password
```

Passwords for accounts with manager privilege can be reset with the same command, provided the manager can login to at least one account with manager privilege. Passwords for accounts with security officer privilege can be reset from any other account with security officer privilege.

If passwords for all accounts with manager or security officer privilege are lost, recovery is complex. Contact your authorised distributor or reseller for assistance.

Asynchronous Port Security

To set asynchronous ports to security mode, use the command:

```
set asyn secure=on
```

See Chapter 9, Interfaces for a detailed description of the **set asyn** command on page 9-40 of Chapter 9, Interfaces. By default, all asynchronous ports are set to security mode. Telnet sessions are always in security mode. A user accessing the router via a terminal connected to an asynchronous port in security mode or via Telnet, must login before the router accepts any commands.

When a user Telnets to a router the login and password prompts are always displayed. The password prompt is displayed even when the login name does not match an entry in the User Authentication Database. This makes it more difficult to discover a valid login name. When a login name and password are

entered that do not match an entry in the database, and is not accepted by any defined TACACS servers, the login sequence is repeated. If successive login failures occur, the login prompt is withheld for a specified lockout period. This makes it very difficult for an intruder to gain entry with random login names and passwords. A log message is generated when the number of retries for a connection is exceeded and the lockout period is instigated. Telnet logins from an offending IP address are also locked out for this period once the permitted number of failures is exceeded. The number of login attempts permitted and the length of the lockout period can be configured with the command:

```
set user [loginfail=1..10] [lockoutpd=1..30000]
```

Telneting from the Router

The router provides the following modes of access to host services:

- Use the **connect** command on page 61-16 of Chapter 61, Terminal Server to access asynchronous services. These are typically hosts connected directly to asynchronous ports on the router and defined as services using the **set service** command on page 61-23 of Chapter 61, Terminal Server.
- Use the **connect** command on page 61-16 of Chapter 61, Terminal Server to access Telnet services. These are typically Telnet hosts defined as services using the **set service** command on page 61-23 of Chapter 61, Terminal Server.
- Use the **telnet** command on page 61-34 of Chapter 61, Terminal Server to access Telnet hosts.

When a user is authenticated using TACACS+, they can only Telnet from the switch if their TACACS+ privilege level is equal to or higher than the minimum TACACS+ privilege level required for using Telnet on the router. By default, no TACACS+ users can use Telnet on the router. See "TACACS+" on page 41-18 for more information about TACACS+. See "TACACS+ and Telneting from the router" on page 41-21 for more information about how to allow TACACS+ authorised users to Telnet from the router.

If the user is authenticated from the user database, each entry in the database has a **telnet** attribute that determines the capability of the user to Telnet from the switch. If the user is authenticated through RADIUS or TACACS, they cannot Telnet from the router.

All users can use the **connect** command on page 61-16 of Chapter 61, Terminal Server to access asynchronous services, although users accessing the router via Telnet or a terminal attached to an asynchronous port in security mode must login first to gain access to the command prompt.

Users logged into the router via a terminal attached to an asynchronous port can also use the **connect** command on page 61-16 of Chapter 61, Terminal Server to access Telnet services. In addition, if the user is logged into an account with the **telnet** attribute set to **on**, the user can use the **telnet** command on page 61-34 of Chapter 61, Terminal Server to Telnet to remote hosts.

Users logged into the router via Telnet can, by default, use the **connect** command on page 61-16 of Chapter 61, Terminal Server to access asynchronous services. If the user is logged in to an account with the **telnet** attribute set to **on**, the user can also use the **connect** command on page 61-16 of Chapter 61, Terminal Server to access Telnet services and the **telnet** command on page 61-34 of Chapter 61, Terminal Server to Telnet to remote hosts.

A manager can use the **telnet** attribute to allow users connected to the router via a terminal to access a restricted set of Telnet hosts, by defining those hosts as Telnet services (see the description of the **set service** command on page 61-23 of Chapter 61, Terminal Server) and setting the **telnet** attribute to **off** for selected accounts. Users logged into one of these accounts can use the **connect** command on page 61-16 of Chapter 61, Terminal Server to access the Telnet services but cannot use the **telnet** command on page 61-34 of Chapter 61, Terminal Server to access other Telnet hosts.

Counters

A number of counters record activity associated with the User Authentication Database. Counters relating to specific users in the database can be displayed with the command:

```
show user[=login-name]
```

To display global counters and configuration parameters, use the command:

```
show user configuration
```

All counters are stored in non-volatile storage so that they are retained across router reboots and power cycles.

To reset counters to zero for a specific user, use the command:

```
reset user=login-name
```

To reset counters to zero for all users, the global counters, or all counters, use the command:

```
reset user counter={user|global|all}
```

Semipermanent Manager Port

It is sometimes desirable to have an asynchronous port that has manager privilege after a router reboots, without the manager having to log on. To set an asynchronous port from default to manager privilege, use the command:

```
set manager asyn=port-number
```

Only one port may be a semipermanent manager port. By default, no semipermanent manager port is defined. This command requires a user with security officer privilege when the switch is in security mode.

When the router boots with a semipermanent manager port configured, the manager account is automatically logged into the port. The port has full manager privileges except that Telneting is not permitted from the port. The security timer is reset so that the first time a security command is entered, the user is prompted for the password for the manager account.

RADIUS

RADIUS (Remote Authentication Dial In User Service) is a protocol for transferring authentication, configuration, and accounting information between a Network Access Server (e.g. a router) that desires to authenticate its links, and a shared RADIUS Server. The RADIUS authentication server manages a database of users and provides authentication (verifying user name and password) and configuration information (for example, IP address, subnet mask, etc.) to the client. The RADIUS accounting server stores accounting information about past sessions.

RADIUS allows user-definable timers. When set, these improve response times in environments where some servers may be unavailable.

The following timer parameters are set with the **set radius** command:

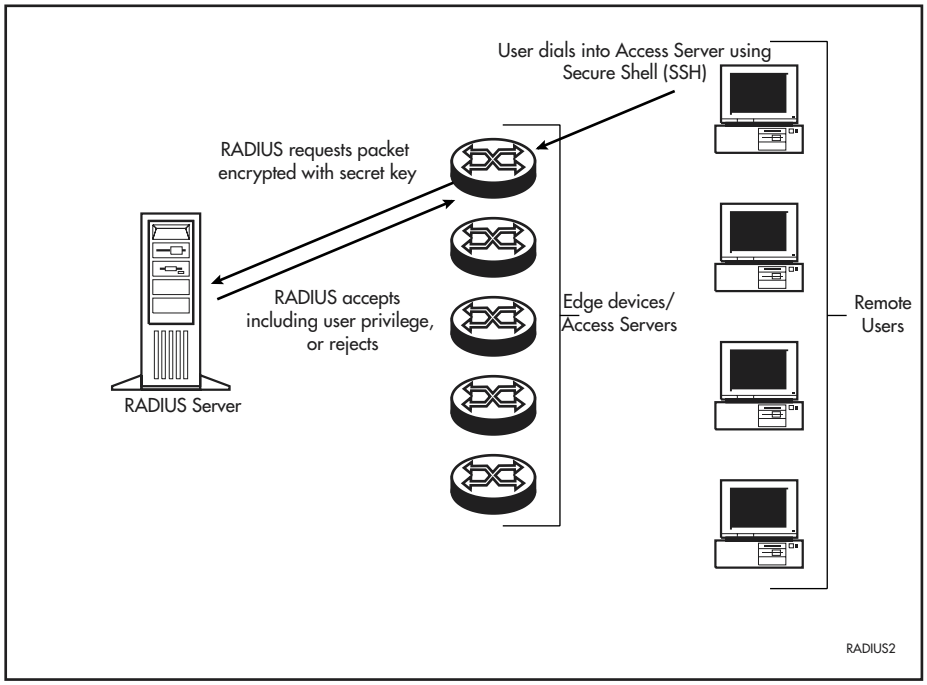
- **timeout** specifies how long the device should wait for a response from the RADIUS server, before assuming the communication has failed. The default is 6 seconds.
- **retransmitcount** is the number of times that the device will attempt to contact the RADIUS server, before it goes on to the next server. The default is 3 attempts.
- **deadtime** the length of time for which the server should be considered dead. The default is 0 minutes. When a RADIUS server cannot be contacted, it is considered 'dead' for a period of time.

Privilege levels of users can be stored on the RADIUS server and returned with the user authentication so that the user database can be centrally administered from the RADIUS server. For information about privilege levels, see "Privilege Levels" on page 41-3.

The router acts as a RADIUS client, sending requests to a RADIUS server. To enable the RADIUS server to authenticate users and include their privilege level, set up the server so that it returns an appropriate value, explained in the following table.

For this privilege level...	Set the Service-Type attribute to...
User	Login (1)
Manager	NAS Prompt (7)
Security Officer and Remote Security officer	Administrative (6)

Figure 41-2: Using a RADIUS server for user authentication.



To add or delete a RADIUS server, use the commands:

```
add radius server=ipadd secret=secret
delete radius server=ipadd
```

To change RADIUS timer attributes, use the command:

```
set radius
```

The list of known RADIUS servers is displayed using the command:

```
show radius
```

Table 41-2 lists the RADIUS attributes supported by the router.

Table 41-2: RADIUS attributes supported by the router

RADIUS Attribute Name	When Used	Description
User-Name	Authentication request Accounting request	The name of the user to be authenticated.
User-Password	Authentication request	The password of the user to be authenticated, or the user's input following an Access-Challenge.
CHAP-Password	Authentication request	The response value provided by a PPP CHAP user in response to a challenge.
NAS-IP-Address	Authentication request Accounting request	The identifying IP Address of the NAS that is requesting authentication of the user.
NAS-PORT	Authentication request	The physical port number of the NAS that is authenticating the user.
Service-Type	Authentication accept	Used to specify the privilege level where the user is logged into the router.
Calling-Station-Id	Authentication request	The number that the call to the NAS came from, using Automatic Number Identification (ANI) or similar technology.
Framed-IP-Address	Authentication accept	The address to be configured for the user.

Table 41-2: RADIUS attributes supported by the router (Continued)

RADIUS Attribute Name	When Used	Description
Framed-IP-Netmask	Authentication accept	The IP Netmask to be configured for the user when the user is a router to a network. If Framed-IP-Address is configured without Framed-IP-Netmask, a default mask of 255.255.255.255 is used.
Callback-Number	Authentication accept	A dialling string to be used for callback.
Framed-Route	Authentication accept	Provides routing information to be configured for the user on the NAS.
Framed-IPX-Network	Authentication accept	The IPX Network number to be configured for the user.
Session-Timeout	Authentication accept	The maximum number of seconds of service to be provided to the user before the session terminates.
Idle-Timeout	Authentication accept	The maximum number of consecutive seconds of idle connection allowed to the user before prompt or termination of the session.
Framed-AppleTalk-Network	Authentication accept	The AppleTalk Network number that the NAS should probe to allocate an AppleTalk node for the user.
Framed-AppleTalk-Zone	Authentication accept	The AppleTalk Default Zone to be used for this user.
CHAP-Challenge	Authentication request	The CHAP Challenge sent by NAS to a PPP CHAP user.
Acct-Status-Type	Authentication start	Whether the Accounting Request marks the beginning (Start) or end (Stop) of the user service.
Acct-Input-Octets	Authentication stop	The number of octets received from the port over the course of this service.
Acct-Output-Octets	Accounting stop	The number of octets sent to the port over the course of this service.
Acct-Session-Id	Accounting start Accounting stop	A unique accounting ID used to match start and stop records in a log file.
Acct-Session-Time	Accounting stop	The number of seconds that the user has received service.
Acct-Authentic	Accounting start	The method by which the user was authenticated.
Acct-Input-Packets	Accounting stop	The number of packets received from the port in the course of delivering this service to a Framed User.
Acct-Output-Packets	Accounting stop	The number of packets sent to the port in the course of delivering this service to a Framed User.
Acct-Terminate-Cause	Accounting stop	The mechanism or reason for terminating the session.
Tunnel-Type	Authentication accept	The protocol to be used for the tunnel specified by Tunnel-Private-Group-Id.
Tunnel-Medium-Type	Authentication accept	The transport medium to be used for the tunnel specified by Tunnel-Private-Group-Id.
Tunnel-Private-Group-Id	Authentication accept	The ID of the tunnel to be used by the authenticated user.

TACACS

The router supports the use of TACACS (Terminal Access Controller Access Control System) servers as an alternative method of user authentication. The router sends a TACACS request, which includes the username and password, to each TACACS server in turn. The TACACS server responds with an *accept* or *reject* response. When the server accepts, the user is authenticated. When the server rejects, it sends a request to the next server in the list until all are queried. When all servers on the list reject the request, user authentication is rejected.

There is a timeout period for TACACS requests; when a response is not received within the specified time, the request is retried. To configure the timeout period and the number of permissible retries, use the command:

```
set user [tacretries=0..10] [tactimeout=1..60]
```

Requests are sent to the TACACS servers on the list in a round-robin fashion until one server accepts it, or all servers reject it, or each server reaches its maximum number of retries.

To add a TACACS server to the list of defined servers, use the command:

```
add tacacs server=ipadd
```

where *ipadd* is the IP address of the TACACS server in dotted decimal notation.

To delete a TACACS server from the list of servers, use the command:

```
delete tacacs server=ipadd
```

To display a list of currently defined TACACS servers, use the command:

```
show tacacs server
```

TACACS+

The TACACS+ protocol is a simple TCP-based access control protocol. It supports authentication and authorisation services, and improves TACACS by:

- separating the functions of authentication, authorisation and accounting
- encrypting all traffic between the Network Access Server (NAS) and the daemon
- using TCP as the transport protocol for reliable delivery
- allowing authentication exchanges of arbitrary length and content, which allow any authentication mechanism to be used with TACACS+ clients
- being extensible to provide for site customisation and future development features.

TACACS+ allows authentication, authorisation, and accounting services to be provided independently on separate access servers (TACACS+ servers). Each service can be tied into its own database, or can use other services available on that server or on the network.

Authentication services

The TACACS+ protocol forwards many types of username and password information. This information is encrypted over the network with MD5 (Message Digest 5). TACACS+ can forward the password types for ARAP, SLIP, PAP, CHAP, and standard Telnet. This lets clients use the same username and password for different protocols.

TACACS+ authentication supports multiple challenge and response demands from the TACACS+ server. This allows token card vendors to provide advanced features like sending back a second token-generated number after the first one was manipulated by a security server.

Authorisation services

Authorisation occurs after authentication. It is here that an *attribute value (AV) pair* is returned when configured. AV pairs are configured on the TACACS+ server and passed to the router. The router takes the appropriate action based upon the pair passed to the router and the value of that pair. When the TACACS+ server sends an AV pair that is not supported by the router, that attribute is ignored.

The following AV pairs are supported:

- Timeout

  This value specifies the length of time for which the session can exist. After this value has expired, the session is either disconnected or the privilege of the user is reduced. The valid timeout range is 0 to 65535 (minutes).

- Idletime

  If no input or output traffic is received in this time period, the session is disconnected. The valid idletime range is 0 to 65535 (minutes).

- Privilege Level

  TACACS+ privilege level 0 is not mapped. Privilege levels 1-6 are mapped to User, levels 7-14 are mapped to manager, and level 15 is mapped to Security Officer.

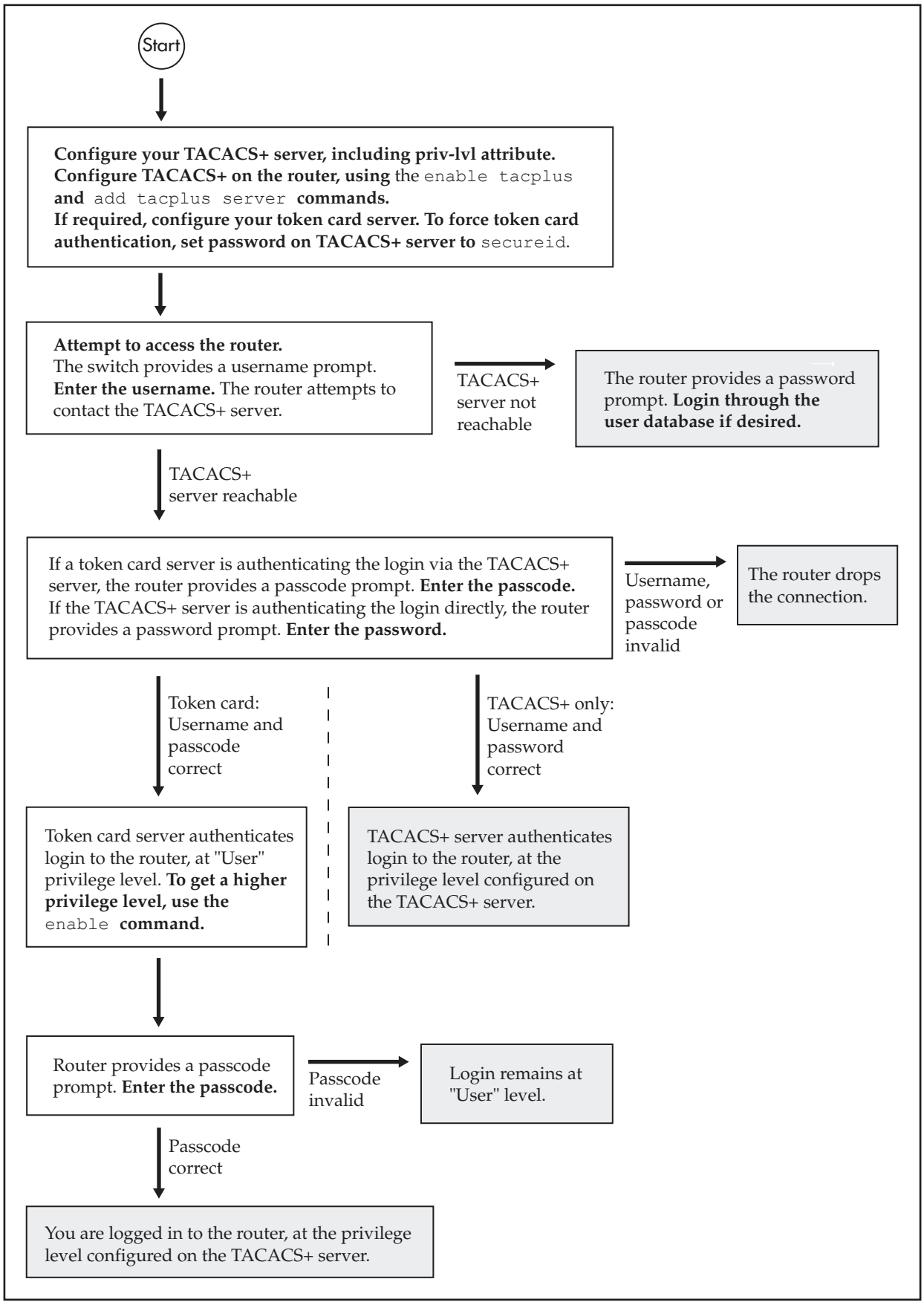
Configuring TACACS+

Use TACACS+ in one of the following ways:

- authentication through a TACACS+ server by itself, with a username/password pair
- in conjunction with a token card server, with a username/password pair. This provides stronger security.

Both procedures are summarised in Figure 41-3 on page 41-20, including the router's actions if the login fails. For more information about token card servers, and about using a TACACS+ server and a token card server together, see "Token Card Authentication" on page 41-22. For more information about using a TACACS+ server by itself, see "Logging onto the router" on page 41-21.

Figure 41-3: Logging into the router and being authenticated with TACACS+



Configuring the router

To enable TACACS+, use the command:

```
enable tacplus
```

To tell the router to attempt authentication through a TACACS+ server, use the command:

```
add tacplus server=ipaddress [key=key] [port=port]
   [singleconnection={yes|no] [timeout=1..10]
```

For example, to add a TACACS+ server with IP address 192.168.0.1, key ABCD123 and a timeout of 5, use the command:

```
add tacplus server=192.168.0.1 key=abcd123 timeout=5
```

Configuring the TACACS+ server

To determine the appropriate privilege level for the user, the router uses the TACACS+ **priv-lvl** value. You must set the server to return an appropriate value, listed in the following table.

Privilege Level	Value of TACACS+ priv-lvl
Security Officer	15
Manager	7-14
User	1-6
not mapped	0

Logging onto the router

To access the router's CLI securely over a network, you must also use secure shell. See Chapter 44, Secure Shell for information and command syntax. Follow these steps to log on with the privilege level specified on the TACACS+ server:

1. **Enter your username.**

   On your terminal, terminal emulator or SSH window, enter your username at the username prompt.

2. **Enter your password.**

Results

The username/password pair is either accepted or rejected. If the TACACS+ server accepts the pair, you are logged in at the appropriate security level. If the TACACS+ server rejects the pair, the router breaks the connection. To increase security, the router checks only the username/password against another authentication system (such as the user database) if the TACACS+ server is unavailable.

This procedure and its results are summarised in Figure 41-3 on page 41-20, including the router's actions if the login fails.

TACACS+ and Telneting from the router

If your login to the router is authenticated by TACACS+, you can Telnet from the router only if your TACACS+ privilege level is also equal to or higher than the minimum TACACS+ privilege level required for using Telnet on the router. By default, no TACACS+ users can use Telnet on the router. To set a privilege level, use the command:

```
set tacplus telnet={0..15|none}
```

A value of **none** is the default and disables Telnet for all TACACS+ authenticated users. A value of **1** indicates that all users can Telnet. A value of **7** indicates that manager privilege or better is required. A value of **15** is equivalent to security officer privilege.

Note that a user can have a TACACS+ privilege level that is equivalent to user or manager, but be unable to use Telnet on the router if the required TACACS+ privilege level is higher than the user's assigned privilege level. For example, if the required privilege level is 10, and there are two users with manager privileges, one with privilege level 9 and one with privilege level 10, only the user with privilege level 10 can use Telnet on the router.

To see the required privilege level, use the command:

```
show tacplus telnet
```

Token Card Authentication

Token card authentication is an authentication process that uses three pieces of information to authenticate users. This makes it more secure than systems that use two forms of identification. The three pieces of information are:

- username
- 4-digit PIN, which the user must remember
- token card

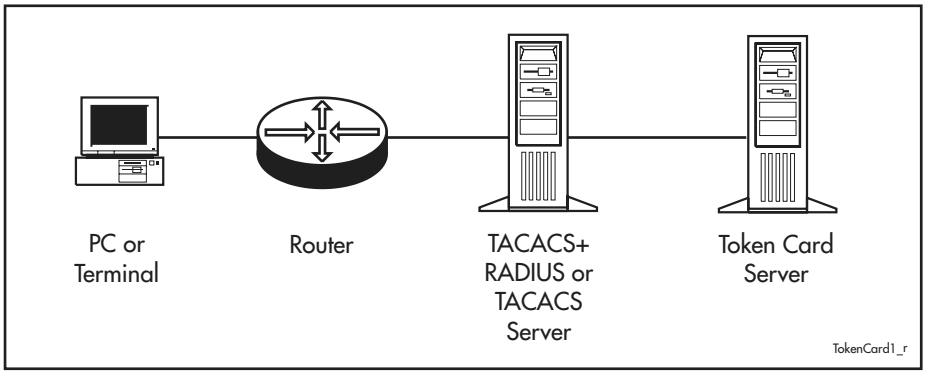
The *token card* is a form of identification that is about the size of a credit card and has a 9-digit LCD display. The number on the LCD display changes every 30 seconds and is synchronised to the token card server so the server can authenticate the 9-digit number.

The user's 4-digit PIN followed by the number displayed on the token card forms a *passcode*. The token card server authenticates users based on their usernames and passcodes.

Token Card Authentication on the Router

The router communicates with a token card server through a TACACS+, RADIUS or TACACS server (Figure 41-4).

Figure 41-4: The elements of an authentication system that uses token card authentication.



The TACACS+, RADIUS or TACACS server is between the token card server and the router, and may hold further information about the user. For TACACS+ and RADIUS servers, this information can include a privilege level, so that the user can be authenticated on the router at manager or security officer level. Token card servers return an accept or reject message, and therefore do not support different privilege levels.

Using Token Card with TACACS+

You can use a token card server in conjunction with a TACACS+ server to log users onto the router at user, manager or security officer privilege level.

Configuring the TACACS+ server

To determine the appropriate privilege level for the user, the router uses the TACACS+ **priv-lvl** value. You need to set the server to return an appropriate value (see "Configuring the TACACS+ server" on page 41-21).

To ensure that the TACACS+ server uses the token card server for authentication, set the password attribute on the TACACS+ server to "secureid".

Logging on with user privilege

To access the router securely over a network using secure shell, configure secure shell on the router. See the Secure Shell chapter of the Software Reference for information and command syntax. Follow these steps to log on with user privileges:

1. **Enter your username.**

   On your terminal, terminal emulator, or SSH window, enter your username at the username prompt.

2. **Enter your passcode.**

   The passcode is your 4-digit pin followed by the 9-digit token card number.

Results

The username/passcode pair is either accepted or rejected. In summary, the message exchange between the router and the servers is:

1. The router sends the username and passcode to the TACACS+ server.
2. The server checks its database for a match, but does not find one, because it does not have a record of the passcode.
3. The server sends the username and passcode to the token card server.
4. The token card server checks its database for a match. If a match exists, it sends an accept message to the TACACS+ server. If no match exists, it sends a reject message.
5. The TACACS+ server returns the appropriate accept or reject message to the router.
6. If the token card server accepts the username/passcode pair, the user is logged into the router with "user" privilege.

   If the token card server rejects the username/passcode pair, the router drops the connection.

This procedure and its results are summarised in Figure 41-3 on page 41-20, including the router's actions if the login fails.

Logging on with higher privilege

The TACACS+ server can also hold user privilege level information. See "Configuring the TACACS+ server" on page 41-23 for information on appropriate settings for the server. Follow these steps to log on with manager or security officer privileges:

1. **Log into the router with user privilege.**

   See "Logging on with user privilege" on page 41-23.

2. **Request a higher privilege level.**

   Enter the command:

   ```
   enable
   ```

   Then enter the passcode at the passcode prompt.

Results

The message exchange between the router and the server is:

1. The router queries the TACACS+ server.
2. The server returns the priv-lvl value that matches this username.
3. The user is logged into the router with the privilege level indicated by the priv-lvl value

Using Token Card with RADIUS or TACACS

You can use a token card server in conjunction with one of the following:

- RADIUS server to log users onto the router at user, manager, or security officer privilege level
- TACACS server to log users onto the router at user privilege level only

Configuring a RADIUS server

To determine the appropriate privilege level for the user, the router uses the RADIUS Service-Type attribute value. You must set the server to return an appropriate value shown in the following table.

Privilege Level	Value of RADIUS Service-Type Attribute
Security Officer	Administrative (6)
Manager	NAS prompt (7)
User	any other value, or no value

Logging on with user privilege

To access the router securely over a network by using secure shell, configure secure shell on the router. See Chapter 44, Secure Shell for information and command syntax. Follow these steps to log on with user privileges:

1. **Enter your username.**

   On your terminal, terminal emulator, or SSH window, enter your username at the username prompt.

2. **Enter your passcode.**

   The passcode is your 4-digit pin followed by the 9-digit token card number.

   Enter your passcode at the password prompt if appropriate. The router does not provide separate password and passcode prompts for RADIUS or TACACS servers.

Results

The username/passcode pair is either accepted or rejected. In summary, the message exchange between the router and the servers is:

1. The router sends the username and passcode to the RADIUS or TACACS server.
2. The server checks its database for a match, but does not find one, because it does not have a record of the passcode.
3. The server sends the username and passcode to the token card server.
4. The token card server checks its database for a match. If a match exists, it sends an accept message to the RADIUS or TACACS server. If no match exists, it sends a reject message.
5. The RADIUS or TACACS server returns the appropriate accept or reject message to the router.
6. If the token card server accepts the username/passcode pair, the user is logged into the router with user privilege.

   If the token card server rejects the username/passcode pair, the router's User Authentication Facility attempts to authenticate the user using the next possible approach (see "User Authentication Facility" on page 41-8).

Logging on with higher privilege

If the router communicates with a token card server via a RADIUS server, the server can hold user privilege level information. See "Configuring a RADIUS server" on page 41-24 for information on appropriate settings for the server. Follow these steps to log on with manager or security officer privileges:

1. **Log into the router with user privilege.**

   See "Logging on with user privilege" on page 41-24.

2. **Request a higher privilege level.**

   For TACACS+, enter the command:

   ```
   enable
   ```

   For RADIUS, login with another username/password pair that has the appropriate privilege level by using the command:

   ```
   login username
   ```

   Then enter the password at the prompt.

Results

The message exchange between the router and the server is:

1. The router sends the username/password pair to the server.
2. The server checks its database for a match. When a match exists, it sends an accept message to the router, including the Service-Type attribute value. When no match exists, it sends a reject message.
3. If the server accepts the username/password pair, the user is logged into the router with the privilege level indicated by the Service-Type attribute value.

If required, you can use a TACACS server to access the router at user level, and then a RADIUS server to obtain a higher privilege level.

Debug Support for RADIUS, TACACS and TACACS+

Access control packet debugging allows the contents of the packets to be viewed. The debugging commands allow both raw (hexadecimal dumps) and/or decoded (human-readable) packet displays. Information on any errors occurring in the transactions can be displayed once the appropriate debugging command is issued.

RADIUS and TACACS+ debugging can be enabled only by users with security officer privilege when the system is in security mode. Use the command:

```
enable tacplus debug
```

S/Key and OTP One-Time Password Systems

S/key and OTP are *one-time password* systems designed to protect networks from attacks via electronic eavesdropping during user authentication. With both systems, a user never logs into a server on the network using the same password more than once. Since a specific one-time password can authenticate a user only once, even if the password is intercepted by a malicious user enroute to the authentication server (via a sniffer), by the time they try to gain access to the system with it, it is no longer valid.

The S/Key system generates one-time passwords by applying a one-way MD4 hash function to the concatenation of a user-specified *seed* and secret password. A seed is a user-defined string utilised during initialisation of the one-time password system on the authentication server. The secret password should never be transmitted across the network and hence is safe from eavesdroppers. At initialisation time, the S/Key system is given a user-specified sequence number, and the one-way function is applied that number of times to produce the first one-time password. The sequence number decrements each time the user logs in. The hash function is described as one-way since it is almost impossible to apply the inverse function to calculate the next password in the sequence.

The OTP system is based on the original S/Key implementation. In both systems, the one-time password generation process is similar, but with OTP, the user-specified seed is internally converted to lower case, and there are more stringent requirements on the length of the initialisation password (it must be 10-63 characters long as opposed to S/Key, where it must be 8 or more characters long).

This implementation provides support for both S/Key and OTP using the following one-way hash functions:

- OTP using MD4
- OTP using MD5.
- S/Key using MD4.
- S/Key using MD5.

Initialising the S/Key or OTP System on the Authentication Server

The authentication server must support either S/Key or OTP. The server must be initialised for each user requiring access to the router using one-time passwords. Initialisation should take place either on the server itself, or via a secure local terminal so that there is no chance of the S/Key or OTP initialisation password being intercepted during transit across a network. At initialisation time, each user must specify:

- A secret initialisation password
- A seed, made up of 1-16 alphanumeric characters
- An initialisation sequence number, from 1-999

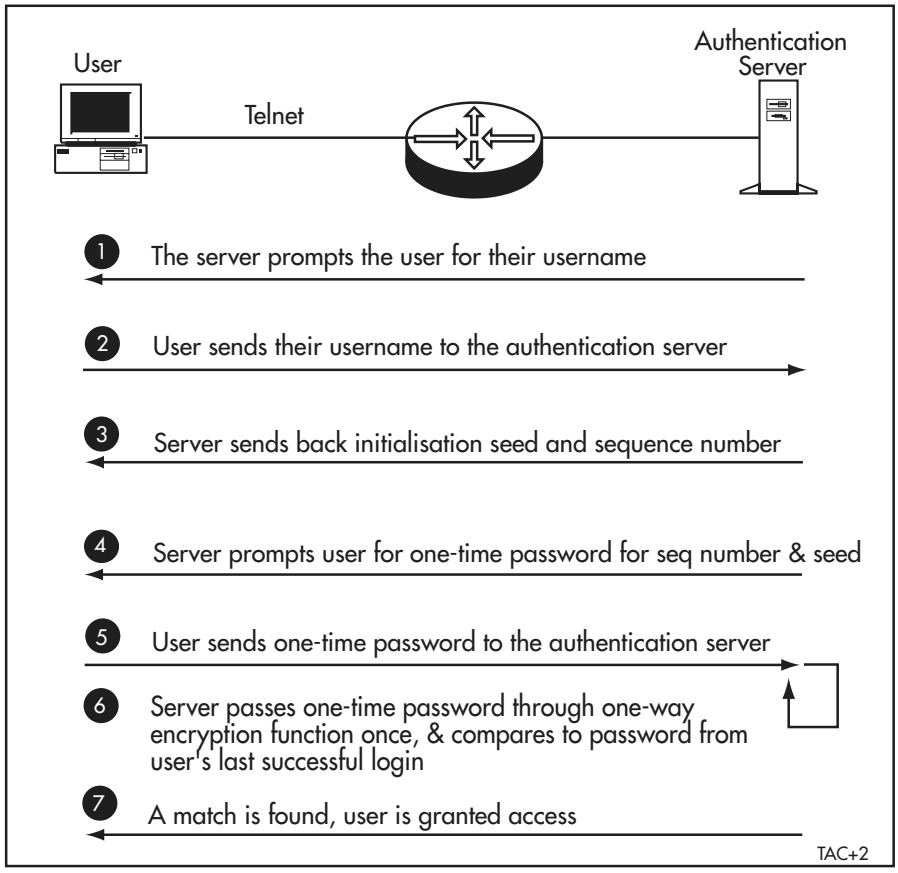
The server now accepts user authentication requests.

The steps for logging into a client are described below. The numbers correspond to those in Figure 41-5 on page 41-28.

1. The user is prompted for their username.
2. The client transmits the username to the authentication server.
3. The server searches through its database to find the current username. If the username is found, the server transmits the user's initialisation seed and current sequence number back to the client. If the username is not found the login is rejected.
4. The user is prompted to supply the one-time password for the given seed, and sequence number.
5. The one-time password is transmitted to the authentication server.
6. The server passes the received one-time password through the one-way encryption function once, and compares the result to the one-time password from the user's last successful login.
7. If they match, the authentication passes and the user is granted access.

The current sequence number is decremented by one each time a user successfully logs in to the system. The user must reinitialise the S/Key server before the sequence number equals zero.

Figure 41-5: Steps for logging into a client.



Configuring S/Key and OTP on the Router

To set the method of authentication that the router is to use and the type of encryption, use the command:

```
set skey [method={skey|otp}] [encryption={md4|md5]
```

To calculate and display one-time passwords, use the **sequence** and **seed** parameters in the command:

```
show skey [sequence=seq_no seed=seed_name [number=value]]
```

where:

- *seq_no* is an integer from 1 to 9999 representing the sequence number of the last S/Key or OTP password to be generated.
- *seed_name* is the 1-16 alphanumeric user-defined string used to initialise the one-time password system on the authentication server.
- *value* is an integer from 1 to 99 representing the number of consecutive S/Key or OTP passwords to generate, finishing at *seq_no.*

To display the correct one-time passwords, users must supply their current sequence number and seed. They are then asked to enter the password used when initialising their current sequence of one-time passwords on the authentication server. The password is not echoed to the screen when entered. The output shows the sequence of S/Key or OTP one-time passwords to be used for a user's subsequent login attempts.

Figure 41-6: Example output from the **show skey seq=n seed=seed** command.

```
Enter S/KEY initialisation password :
Computing SKEY passwords using MD4....
-------------------------------------------
Seq No        One-Time Password
95            IT DOLT ROOM NET GLUT ROWE
96            DARE MOS SARA GOAD MAO LEO
97            GUN TAIL MEND EAT INCH JOHN
98            EARN KID CARE HELD GIRD WINE
99            ADAM WARD DECK PLY EGAN WEED
-------------------------------------------
```

Command Reference

This section describes the commands available on the router to support day-to-day operational and management activities.

The shortest valid command is denoted by capital letters in the Syntax section. See "Conventions" on page lxv of About this Software Reference for details of the conventions used to describe command syntax. See Appendix A, Messages for a complete list of messages and their meanings.

add radius server

Syntax

```
ADD RADius SERVER=ipadd SECret=secret [POrt=port-number]
   [ACCPort=port-number] [LOCal={NONE|1..15}]
```

where:

- *ipadd* is an IP address in dotted decimal notation.
- *secret* is a string 1 to 63 characters long that is case-sensitive. It may contain uppercase and lowercase letters, digits (0–9), and the underscore character. If the string contains spaces, it must be in double quotes.
- *port-number* is a port number from 0 to 65535.

Description

This command adds a RADIUS server to the list of known RADIUS servers. RADIUS servers are used for user authentication.

The **server** parameter specifies the IP address of the RADIUS server in dotted decimal notation. The server must not already be in the list of known RADIUS servers. If **server** is specified but **port** and **accport** are not, then the RADIUS server is used for both authentication and accounting, and requests are sent to the default ports (1645 and 1646). Use the **port** and **accport** parameters to prevent the RADIUS server being used for authentication or accounting, or to specify a different port number to use.

The **secret** parameter specifies a shared secret used in communications between the router and the RADIUS server. The secret is used by the router to encrypt the password field in authentication requests sent to the RADIUS server, and by the RADIUS server to authenticate the router's request. The secret is case-sensitive.

The **port** parameter specifies a non-standard port number for communication with the RADIUS server. Setting the port number to zero means that the server is not to be used for RADIUS authentication (it may be required for RADIUS accounting).

The **accport** parameter specifies a port number for communication with the RADIUS server running RADIUS accounting (RFC 2139). Setting the port number to zero means that the server is not to be used for RADIUS accounting (it may be required for RADIUS authentication).

By default the RADIUS server uses port number 1645 to connect to RADIUS servers for authentication, and port number of 1646 for RADIUS accounting. The RADIUS accounting port is not the official port number (1813) but is the port number used by a number of commonly available packages.

The **local** parameter specifies a local interface to be used as the source for all RADIUS packets the router generates and subsequently sends to this RADIUS server. The local interface IP address will also be used as the NAS IP address in these outgoing packets. The local interface must already be configured and be in the range 1 to 15. If **none** is specified, the router will select a source from the current available interfaces instead. The default is **none**.

Examples To add a RADIUS server with an IP address of 192.168.17.11 and "Valid8Me" as the shared secret, use the command:

```
add radius server=192.16817.11 secret=Valid8Me local=5
```

To add a RADIUS server for accounting with an IP address of 192.168.17.12 and "Valid8Me" as the shared secret, use the command:

```
add rad server=192.16817.11 sec=Valid8Me po=0 accp=1813
```

Related Commands **delete radius server**
show radius

add tacacs server

Syntax `ADD TACacs SERVER=`*`ipadd`*

where *ipadd* is an IP address in dotted decimal notation

Description This command adds a TACACS server to the list of TACACS servers used for authenticating login names.

The **server** parameter specifies the IP address of the server in dotted decimal notation. An unlimited number of TACACS servers may be defined, although two or three is a sensible maximum.

Examples To add a TACACS server with the IP address 172.16.8.5 use the command:

```
add tac server=172.16.8.5
```

Related Commands **delete tacacs server**
show tacacs server

add tacplus server

Syntax

```
ADD TACPlus SERVer=ipaddress [Key=key]
   [LOCal={NONE|1..15}] [PORT=port]
   [SINGLEconnection={Yes|No] [TIMEOUT=1..10]
```

where:

- *ipaddress* is an IP address in dotted decimal notation.
- *key* is a string of up to 64 characters.
- *port* is an integer value.

Description

This command adds a TACACS+ server.

The **server** parameter specifies the IP address of the TACACS+ server to identify. A network can have different TACACS+ servers for the purposes of authentication, authorization and accounting.

The **key** parameter specifies the encryption key to be used for encrypting and decrypting all traffic between the router and the TACACS+ server. It is a shared secret key between the router and the TACACS+ server. It overrides the default key, which is a global key.

The **local** parameter specifies a local interface to be used as the source for all TACACS+ packets the device sends to this TACACS+ server. The local interface must already be configured. If **none** is specified the router will select a source from the current available interfaces instead. The default is **none**.

The **port** parameter specifies the TCP port number to be used when making connections to the TACACS+ server. The default port number is 49.

The **timeout** parameter specifies the period of time (in seconds) that the router waits for a response from the TACACS+ server before it times out. The default is 5 seconds.

The **singleconnection** parameter specifies whether multiple TACACS+ sessions are supported on a single TCP session. If **yes** is specified, the router opens and maintains a single TCP connection for multiple TACACS+ sessions. If **no** is specified, the router opens one TCP connection for each TACACS+ session. It is more efficient for one TCP connection to support multiple TACACS+ sessions. The default is **no**.

Examples

To add a TACACS+ server to IP address 192.168.196.22, with the key "*akey4tacacsplus*" and a timeout of 3 seconds, use the command:

```
add tacp serv=192.168.196.22 K=akey4tacacsplus timeout=3
   single=n
```

Related Commands

delete tacplus server
set tacplus server
show tacplus server

add user

Syntax

```
ADD USEr=login-name LOgin={Yes|No|ON|OFf|True|False}
   PAssword=password [APPLENetwork=atk-network]
   [APPLEZone=zone-name] [CALLingnumber=number]
   [CBNUMber=e164number] [Description=description]
   [Ipaddress=ipadd] [MASk=ipadd] [NETmask=ipadd]
   [MTu=40..1500] [IPXnetwork=ipx-network]
   [PRivilege={USer|MAnager|SEcurityofficer}]
   [RAdiusbackup={Yes|No|ON|OFf|True|False}]
   [TElnet={Yes|No}]
```

where:

- *login-name* is a string 1 to 64 characters long. Valid characters are uppercase and lowercase letters and decimal digits (0–9). The string cannot contain spaces.
- *password* is a character string up to 32 characters long. The default minimum length is 6 characters. Valid characters are any printable character. If the string contains spaces, it must be in double quotes.
- *atk-network* is an AppleTalk network number from 1 to 65535.
- *zone-name* is a character string 1 to 32 characters long. Valid characters are uppercase and lowercase letters, and decimal digits (0-9).
- *number* is an ISDN number or L2TP number 1 to 32 characters long. Valid characters are any printable characters, but the calling number it should match is likely to contain only decimal digits. If the string contains spaces, it must be in double quotes.
- *e164number* is a valid phone number. It may contain digits (0–9) and should be a valid phone number as described in CCITT standard E.164.
- *description* is a string 1 to 23 characters long. Valid characters are any printable character. If the string contains spaces, it must be in double quotes.
- *ipadd* is an IP address in dotted decimal notation.
- *ipx-network* is a valid Novell network number, expressed as a hexadecimal number. Leading zeros may be omitted.

Description

This command adds a user to the User Authentication Database, and requires a user with security officer privilege when the router is in security mode. The **user** parameter specifies the login name for the user. It is not case sensitive.

The **login** parameter specifies whether users with user privilege can log into the router. If **false**, the user is authenticated by the User Authentication Database but is not allowed to log into the router. If **true**, the user can log into the router and enter commands. The default is **false**.

The **password** parameter specifies the password for the user. The password is case sensitive. The user can change the password at any time by using the **set password** command on page 41-54. By default, the password must be at least 6 characters long. You can change the minimum length by using the command **set user minpwdlen=1..23**.

The **applenetwork** parameter specifies the AppleTalk network number assigned to the user accessing an AppleTalk internetwork. See Chapter 35, AppleTalk for more information.

The **applezone** parameter specifies the AppleTalk zone assigned to the user accessing an AppleTalk internetwork. See Chapter 35, AppleTalk for more information.

The **callingnumber** parameter specifies the calling number to be used to authenticate incoming calls from L2TP and ISDN services that provide caller ID information.

The **cbnumber** parameter specifies the ISDN number to use when making a callback to a remote user using the PPP callback facility.

The **description** parameter specifies a descriptive text for the entry, such as the full name and location of the user. This string may contain any printing character and the case is preserved in output.

The **ipaddress** parameter specifies an IP address for the user. The value must be a valid IP address in dotted decimal form.

The **mask** parameter specifies the address mask which extends the range of IP addresses. If the mask parameter is not present, a mask of 255.255.255.255 is used. The address and mask must be internally consistent in that the result of ANDing the address and mask should be the address.

The **netmask** parameter and the **mask** parameter are synonymous.

The **mtu** parameter specifies a Maximum Transmission Unit value for the user. The value must be a decimal integer from 40 to 1500 inclusive.

The **ipaddress**, **mask** and **mtu** parameters are required if the user is to login in order to make a PPP or SLIP connection to the router over a modem connected to an asynchronous port.

The **ipxnetwork** parameter specifies the Novell network number assigned to the user accessing a Novell internetwork. See Chapter 36, Novell IPX for more information.

The **privilege** parameter specifies the privilege level for the user. The default is **user**. User privilege entitles someone access to a subset of commands, generally those that affect the user's own session or asynchronous port. manager privilege entitles someone access to all commands when the router is in normal mode, and to a smaller set when the router is in security mode. security officer privilege entitles someone access to the full set of commands regardless of the operating mode.

The **radiusbackup** parameter specifies whether the user account is used only as a backup when RADIUS authentication fails because the RADIUS server is unreachable (either due to a network communication problem or because the server itself is down). Specify **on**, **yes** or **true** if you want to use this account as a backup for RADIUS authentication. Specify **off**, **no** or **false** if you want to use this account as a normal user. The default is **off**.

If you configure one or more users in the User Authentication Database as RADIUS backup users then:

- RADIUS authentication will be attempted before checking the User Authentication Database. Normally, the User Authentication Database is checked before RADIUS.
- If the RADIUS server is unreachable, the login attempt is authenticated against users in the User Authentication Database who have **radiusbackup** set to **on**.
- If the RADIUS server is reachable but rejects the authentication request, the login attempt is authenticated against users in the User Authentication Database who have **radiusbackup** set to **off**.

The **telnet** parameter specifies whether the user is permitted to use the **telnet** command on page 61-34 of Chapter 61, Terminal Server to Telnet to another host, or the **connect** command on page 61-16 of Chapter 61, Terminal Server to access a Telnet service when logged in via Telnet.

Examples

To add a user with the login name “bruce”, the password “sbfd4Q”, login=yes, and manager privilege, use the command:

```
add use=bruce description="Bruce Wilson" pa=sbfd4Q pr=ma lo=y
```

To add a user with the login name “accounts”, the password “Cash4Cast”, and user privilege without access to the command line, and specify an IP address, network mask, and MTU so that the user can make SLIP connection to the router, use the command:

```
add use=accounts description="Accounting Data Entry"
   pa=Cash4Cast pr=us ipaddress=192.168.35.17
   netmask=255.255.255.0 mt=1500 lo=n
```

To add a user with the login name “cipher”, password “sbr4y3”, login=yes, and security officer privilege, use the command:

```
add user=cipher password=sbr4y3 privilege=security officer
   login=yes
```

Related Commands

delete user
disable system security_mode
disable user
enable system security_mode
enable user
purge user
reset user
set user
show user

add user rso

Syntax

```
ADD USEr RSO IP=ipadd [MASK=ipadd]

ADD USEr RSO IP=ipadd[-ipadd]

ADD USEr RSO IP=ipv6add[/prefix-length]

ADD USEr RSO IP=ipv6add[-ipv6add]
```

where:

- *ipadd* is an IPv4 address in dotted decimal notation.
- *ipv6add* is a valid IPv6 address (see "IPv6 Addresses and Prefixes" on page 31-4 of Chapter 31, Internet Protocol version 6 (IPv6)).
- *prefix-length* is an integer from 1 to 128.

Description

This command adds an IP address or address range to the list of remote access users eligible for remote security officer access. The specified address or range must not already exist in the list, but it may overlap other addresses or ranges already in the list. This command requires a user with security officer privilege when the router is in security mode.

The **ip** parameter specifies the base IP address for this range of remote security officer addresses. Base IP addresses defined with successive invocations of this command should be unique since the base IP address identifies the remote security officer access entry. The **ip** parameter may be one of the following:

- an IPv4 address and optional mask
- an IPv4 address range
- an IPv6 address and optional prefix length
- an IPv6 address range

If a single IPv6 address is specified without a prefix length, the default prefix length is 128. If a range of IPv6 addresses is specified, a prefix length is not required.

The **mask** parameter specifies an address mask that extends the range of IPv4 addresses. This parameter is only valid if the **ip** parameter specifies a single base IPv4 address. The address and mask must be internally consistent such that the result of ANDing the address and mask should be the address. The default is 255.255.255.255.

Examples

To add the IPv4 address 192.168.11.7 as a remote security officer, use the command:

```
add user rso ip=192.168.11.7
```

To add the IPv4 address range 192.168.13.1 to 192.168.13.45 as remote security officers, use the command:

```
add user rso ip=192.168.13.1-192.168.13.45
```

To add all IP addresses in the network 172.30.1.0 as remote security officers, use the command:

```
add user rso ip=172.30.1.0 mask=255.255.255.0
```

To add the IPv6 address 3ffe::1:1 as a remote security officer, use the command:

```
add user rso ip=3ffe::1:1
```

To add the IPv6 address range 3ffe::1:/64 as remote security officers, use the command:

```
add user rso ip=3ffe::1:/64
```

To add the IPv6 address range 2ffe::1:13 to 2ffe::1:72 as remote security officers, use the command:

```
add user rso ip=2ffe::1:13-2ffe::1:72
```

Related Commands

delete user rso
disable user rso
enable user rso
show user rso

delete radius server

Syntax

`DELete RADius SERVer=`*`ipadd`*

where *ipadd* is an IP address in dotted decimal notation

Description

This command deletes a RADIUS server from the list of known RADIUS servers. RADIUS servers are used for user authentication.

The **server** parameter specifies the IP address of the RADIUS server, in dotted decimal notation. The server must be in the list of known RADIUS servers.

Examples

To delete the RADIUS server with the IP address of 192.168.17.11, use the command:

```
del rad serv=192.168.17.11
```

Related Commands

add radius server
show radius

delete tacacs server

Syntax `DELete TACacs SERVer=`*`ipadd`*

where *ipadd* is an IP address in dotted decimal notation

Description This command deletes a TACACS server from the list of TACACS servers used for authenticating login names. The **server** parameter specifies the IP address of the server in dotted decimal notation.

Examples To delete the TACACS server with the IP address 172.16.8.5 use the command:

```
del tac serv=172.16.8.5
```

Related Commands
add tacacs server
show tacacs server

delete tacplus server

Syntax `DELete TACPlus SERVer=`*`ipaddress`*

where *ipaddress* is an IP address in dotted decimal notation

Description This command deletes a TACACS+ server.

The **server** parameter specifies the IP address of the TACACS+ server, which must already be defined using the **add tacplus server** command.

Example To delete the TACACS+ server with IP address 192.168.196.22, use the command:

```
del tacp serv=192.168.196.22
```

Related Commands
add tacplus server
set tacplus server
show tacplus server

delete user

Syntax

`DELete USEr=`*`login-name`*

where *login-name* is a string 1 to 64 characters long. Valid characters are uppercase and lowercase letters and digits (0–9). The string cannot contain spaces.

Description

This command deletes a user from the User Authentication Database. The **user** parameter specifies the login name for the user. This command requires a user with security officer privilege when the router is in security mode.

If the router is operating in security mode, you cannot delete every user with security officer privilege. At least one user with security officer privilege must exist in the User Authentication Database for the router to operate in security mode.

Related Commands

add user
disable user
enable user
purge user
reset user
set user
show user

delete user rso

Syntax

```
DELete USEr RSO IP=ipadd[-ipadd]

DELete USEr RSO IP=ipv6add/prefix-length

DELete USEr RSO IP=ipv6add[-ipv6add]
```

where:

- *ipadd* is an IPv4 address in dotted decimal notation.
- *ipv6add* is a valid IPv6 address in slash notation (see "IPv6 Addresses and Prefixes" on page 31-4 of Chapter 31, Internet Protocol version 6 (IPv6)).
- *prefix-length* is an integer from 1 to 128.

Description

This command deletes an IP address or range of addresses from the list of remote access users eligible for remote security officer access. The specified address or range must already exist in the list. Remote security officers who currently have security officer privilege lose it immediately. This command requires a user with security officer privilege when the router is in security mode.

The **ip** parameter specifies the base IP address for this range of remote security officer addresses. It must match exactly an entry in the list of remote access users. Other overlapping but non-identical entries in the list are not affected. The **ip** parameter may be one of the following:

- an IPv4 address
- an IPv4 address range
- an IPv6 address and prefix length
- an IPv6 address range

If a single IPv6 address is specified, the prefix length must also be specified. If a range of IPv6 addresses is specified, a prefix length is not required.

Examples

To delete the IPv4 address 192.168.11.7 from the list of remote security officers, use the command:

```
del user rso ip=192.168.11.7
```

To delete all IP addresses in the network 172.30.1.0 from the list of remote security officers, use the command:

```
delete user rso ip=172.30.1.0 mask=255.255.255.0
```

To delete the IPv6 address 3ffe::1:/64 from the list of remote security officers, use the command:

```
del user rso ip=3ffe:1:/64
```

To delete the IPv6 address range 2ffe::1:13 to 2ffe::1:72 from the list of remote security officers, use the command:

```
del user rso ip=2ffe::1:13-2ffe::1:72
```

Related Commands

add user rso
disable user rso
enable user rso
show user rso

disable radius debug

Syntax `DISable RADius DEBug={ALL|PKT|DECODE|ERROR} [,...]`

Description This command disables the debugging option for all RADIUS servers.

Examples To disable the debugging of raw packets sent to and received from all RADIUS servers, use the command:

```
dis rad deb=pkt
```

Related Commands
enable radius debug
show radius debug
disable debug active in Chapter 4, Configuring and Monitoring the System
show debug active in Chapter 4, Configuring and Monitoring the System

disable system security_mode

Syntax `DISable SYStem SECurity_mode`

Description This command disables security mode on the router. When the router is in security mode, a subset of commands, called *security commands*, requires security officer privilege. Sensitive data files such as encryption key files can be stored in the router's file system when the router is in security mode.

Caution Disabling security mode deletes sensitive data files, such as encryption keys, from the router's file system.

Examples To disable security mode, use the command:

```
dis sys sec
```

Related Commands
add user
enable system security_mode
set user
show user

disable tacacs debug

Syntax `DISable TACacs DEBug={ALL|PKT|DECode|ERRor} [,...]`

Description This command disables the debugging option for all TACACS servers.

Examples To disable the debugging of raw packets sent to and received from all TACACS servers, use the command:

```
dis tac deb=pkt
```

Related Commands **enable tacacs debug**
show tacacs debug
disable debug active in Chapter 4, Configuring and Monitoring the System
show debug active in Chapter 4, Configuring and Monitoring the System

disable tacplus

Syntax `DISable TACPlus`

Description This command disables TACACS+ operation on the router.

Example To disable TACACS+, use the command:

```
dis tacp
```

Related Commands **enable tacplus**

disable tacplus debug

Syntax `DISable TACPlus DEBug`

Description This command disables debugging for all TACPLUS servers.

Examples To disable the debugging of all TACACS+ servers, use the command:

```
disa tacp deb
```

Related Commands **enable tacplus debug**
disable debug active in Chapter 4, Configuring and Monitoring the System
show debug active in Chapter 4, Configuring and Monitoring the System

disable user

Syntax

```
DISable USEr=login-name
```

where *login-name* is a string 1 to 64 characters long. Valid characters are uppercase and lowercase letters and decimal digits (0–9). The string cannot contain spaces.

Description

This command temporarily disables a user login name in the User Authentication Database. The login name must be currently enabled. Login attempts through the User Authentication Database using the login name are ignored. This command has no effect on user authentication through TACACS+, TACACS, or RADIUS servers.

This command requires a user with security officer privilege when the router is in security mode.

The **user** parameter specifies the login name for the user. It is case insensitive.

Related Commands

add user
delete user
enable user
purge user
reset user
set user
show user

disable user rso

Syntax

```
DISable USEr RSO
```

Description

This command disables remote security officer access. Remote security officers who have security officer privilege immediately lose access privilege. This command requires a user with security officer privilege when the router is in security mode.

Examples

To disable remote security officer access, use the command:

```
dis use rso
```

Related Commands

add user rso
delete user rso
enable user rso
show user rso

enable

Syntax `ENAble`

Description This command sets the privilege level of a user to the level stored on a TACACS+ server, for a user whose login has been authenticated by a token card server via the TACACS+ server. Through the TACACS+ server, this command enables token card authorisation to result in login at manager or security officer privilege level. The required privilege level must be configured on the TACACS+ server, using the TACACS+ **priv-lvl** value (see "Configuring the TACACS+ server" on page 41-21).

Before entering this command, the user has user privileges. When the user enters this command, the router queries the TACACS+ server, which returns the **priv-lvl** value that matches this username. The user is then logged into the router with the privilege level indicated by the **priv-lvl** value.

Example After authentication by the token card server, to log on at the privilege level that has been configured on the TACACS+ server, use the command:

```
ena
```

Related Commands **add tacplus server**
show tacplus server

enable radius debug

Syntax `ENAble RADius DEBug={ALL|PKT|DECODE|ERROR} [,...]`

Description This command enables the debugging option for all RADIUS servers.

The **debug** parameter specifies which debugging options are to be enabled. The value may be a single option or a comma-separated list of options.

If **all** is specified, all debugging options are enabled.

If **pkt** is specified, the raw RADIUS packets are debugged.

If **decode** is specified, decoded packets are debugged.

If **error** is specified, error messages regarding RADIUS transactions are displayed.

Examples To enable the debugging of raw packets sent to and received from all RADIUS servers, use the command:

```
ena rad deb=pkt
```

To enable the debugging of all decoded packets and error messages for all RADIUS servers, use the command:

```
ena rad deb=decode,error
```

Related Commands
disable radius debug
show radius debug
disable debug active in Chapter 4, Configuring and Monitoring the System
show debug active in Chapter 4, Configuring and Monitoring the System

enable system security_mode

Syntax `ENAble SYStem SECurity_mode`

Description This command enables security mode on the router. Security mode cannot be enabled unless at least one user with security officer privilege exists in the User Authentication Database.

When the router is in security mode, a subset of commands, called *security commands*, requires security officer privilege. Sensitive data files, such as encryption key files, can be stored in the router's file system when the router is in security mode.

Security mode should be enabled on a router with a hardware encryption device or that is configured to provide secure features like encryption, authentication, or Secure Shell.

Examples To enable security mode, use the command:

```
ena sys sec
```

Related Commands
add user
disable system security_mode
set user
show user

enable tacacs debug

Syntax `ENAble TACacs DEBug={ALL|PKT|DECode|ERRor} [,...]`

Description This command enables the debugging option for all TACACS servers.

The **debug** parameter specifies which debugging options to enable. The value may be a single option or a comma-separated list of options.

If **all** is specified, all debugging options are enabled.

If **pkt** is specified, raw TACACS packets are debugged.

If **decode** is specified, decoded packets are debugged.

If **error** is specified, error messages regarding TACACS transactions are displayed.

Examples To enable the debugging of raw packets sent to and received from all TACACS servers, use the command:

```
ena tac deb=pkt
```

To enable the debugging of all decoded packets and error messages for all TACACS servers, use the command:

```
ena tac deb=dec,err
```

Related Commands **disable tacacs debug**
show tacacs debug
disable debug active in Chapter 4, Configuring and Monitoring the System
show debug active in Chapter 4, Configuring and Monitoring the System

enable tacplus

Syntax `ENAble TACPlus`

Description This command enables TACACS+ operation on the router. TACACS+ is enabled by default.

Example To enable TACACS+, use the command:

```
ena tacp
```

Related Commands **disable tacplus**

enable tacplus debug

Syntax `ENAble TACPlus DEBug`

Description This command enables debugging for all TACACS+ servers.

Examples To enable the debugging of all TACACS+ servers, use the command:

```
ena tacp deb
```

Related Commands **disable tacplus debug**
disable debug active in Chapter 4, Configuring and Monitoring the System
show debug active in Chapter 4, Configuring and Monitoring the System

enable user

Syntax `ENAble USEr=`*`login-name`*

where *login-name* is a string 1 to 64 characters long. Valid characters are uppercase and lowercase letters and decimal digits (0–9). The string cannot contain spaces.

Description This command enables a user login name in the User Authentication Database that has been disabled. Login attempts using the login name are processed as normal.

This command requires a user with security officer privilege when the router is in security mode.

The **user** parameter specifies the login name for the user, and is not case sensitive.

Related Commands **add user**
delete user
disable user
purge user
reset user
set user
show user

enable user rso

Syntax `ENAble USEr RSO`

Description This command enables remote security officer access. Authorised IP addresses must be added with the **add user rso** command on page 41-36 before remote security officer access can be used. This command requires a user with security officer privilege when the router is in security mode.

Examples To enable remote security officer access, use the command:

```
ena use rso
```

Related Commands
add user rso
delete user rso
disable user rso
show user rso

login

Syntax `LOGIn [login-name]`

where *login-name* is a string 1 to 64 characters long. Valid characters are uppercase and lowercase letters and decimal digits (0–9). The string cannot contain spaces.

Description This command is used to login to the router. The User Authentication Facility prompts the user for a login name (if not specified) and a password. The user must enter appropriate responses, pressing the Enter key after each response. Characters entered at the password prompt are not displayed on the screen for security reasons.

The password prompt is displayed regardless of whether a password is required for the login name entered by the user. This makes it more difficult for an intruder to discover valid login name/password combinations.

If the user enters an invalid login name or password, the sequence is repeated a set number of times. If a valid login name and password has still not been entered the terminal or Telnet session is locked out for a period of time. During this period the password prompt is withheld, preventing the user from logging in or entering commands. The manager can specify the number of login attempts allowed and the length of the lockout period using the **set user** command on page 41-59.

This command is not normally required. The user is automatically prompted to enter a login name and password when accessing the router via Telnet or a terminal connected to an asynchronous port set to security mode, or when accessing a dial up service via an asynchronous modem connected to an asynchronous port.

This command might be used to login from a terminal connected to an asynchronous port that is not in security mode, in order to use facilities available to logged-in users, or to login as another user in order to acquire different rights, such as manager privilege.

The **logon** command is an alias for **login**.

If a user starts a Telnet session to the router but does not login within one minute, the router automatically times out the session and terminates the Telnet connection.

Related Commands **logoff**

logoff

Syntax `LOgoff`

Description This command is used to log out from the router. For a terminal attached to an asynchronous port, the port returns to its default prompting state, either the login prompt for a port in security mode, or the command prompt. For a Telnet session the TCP connection is terminated. The **logout** command is an alias for **logoff**.

Related Commands **login**

purge user

Syntax `PURge USEr`

Description This command deletes all users from the User Authentication Database. The manager account remains but the password is set to the default password, *friend*. Global configuration parameters and counters are not affected. To clear these counters use the **reset user** command on page 41-52.

This command requires a user with security officer privilege when the router is in security mode.

Related Commands
add user
delete user
disable user
enable user
reset user
set user
show user

reset user

Syntax `RESET USEr[=`*`login-name`*`] [COUNTER[={ALL|GLOBAL|USER}]]`

where *login-name* is a string 1 to 64 characters long. Valid characters are uppercase and lowercase letters and decimal digits (0–9). The string cannot contain spaces.

Description This command is used to reset User Authentication Database counters for one or all users, or to reset global counters for the User Authentication Facility. It requires a user with security officer privilege when the router is in security mode.

If a login name is specified with the **user** parameter, the **counter** parameter is optional (only **user** can be specified) and the activity counters for the specified user are reset. The login name is not case sensitive.

If a login name is not specified, then the **counter** parameter is required to specify which counters should be reset. If **user** is specified, activity counters for all users are reset. If **global** is specified, global counters for the User Authentication Facility are reset. If **all** is specified, all counters are reset.

Examples To reset the activity counters for user “Bruce”, use the command:

```
reset use=bruce
```

To reset the activity counters for all users, use the command:

```
reset use counter=user
```

To reset the global counters, use the command:

```
reset use counter=global
```

Related Commands

add user
delete user
disable user
enable user
purge user
set user
show user

set manager asyn

Syntax `SET MAnager ASYn={`*`port-number`*`|NONE}`

where *port-number* is the number of the port. Ports are numbered sequentially starting with `asyn` 0

Description This command sets the semipermanent manager port. If a valid port number is specified, the port becomes the semipermanent manager port. If the specified port was secure before the command was entered, it loses its secure setting. If another port is currently the semipermanent manager port, then that port loses its semipermanent manager privilege and becomes a secure port. If **none** is specified, the current semipermanent manager port loses its semipermanent manager privilege and becomes a secure port. There can be only one semipermanent manager port at a time.

This command is one of the security commands controlled by the security timer (Table 41-1 on page 41-5). When the security timer expires before the command is entered, the manager is prompted to re-enter the password for the login name where the command was issued.

Examples To set `asyn` 0 as the semipermanent manager port, use the command:

```
set ma asy=0
```

To remove the semipermanent manager port, use the command:

```
set ma asy=none
```

Related Commands

login
show manager asyn
set asyn in Chapter 9, Interfaces

set password

Syntax `SET PASSword`

Description This command changes the password for the user currently logged into the port where the command is issued. When properly logged in, the user is prompted for the current password, the new one, and confirmation of the new one. The passwords are not displayed on the screen. If the user is not logged into the port, an error message is displayed.

The password is a character string up to 32 characters long. Valid characters are any printable character. If the string contains spaces, it must be in double quotes. The default minimum length is 6 characters. To change the minimum length, use the command **set user minpwdlen=1..23**.

The new password and the confirmation must be identical for the change to take effect. This reduces the chances of a typing error causing the password to be different from what the user intended.

A log message is generated whenever the password for an account with manager privilege is changed.

Examples To change the password for the current user, enter the command:

```
set password
old password:
new password:
Confirm:
```

Related Commands **add user**
set user

set radius

Syntax

```
SET RADius [TIMEOut=1..15] [DEAdtime=0..1440]
   [RETransmitcount=1..5]
```

Description

This command sets the timeout and retry parameters for RADIUS servers.

The **timeout** parameter specifies the length of time the device waits for a server to respond to a request before the request is deemed to have timed out. The default is 6 seconds.

The **deadtime** parameter specifies a length of time that non-responsive servers cannot be used for authentication. The default is 0 minutes.

The **retransmitcount** parameter specifies the number of times the device tries to resend a given request to a RADIUS server before the server is considered non-responsive. The default is 3.

Examples

To set RADIUS to wait 15 seconds for the server to respond before timing out, use the command:

```
set rad timeo=15
```

Related Commands

add radius server
show radius

set skey

Syntax

```
SET SKEY [METhod={SKEY|OTP}] [ENCryption={MD4|MD5]
```

Description

This command sets the method of one-time password authentication to use, and the type of encryption to use during one-time password generation with the **show skey** command. S/Key commands have a user privilege level.

The **method** parameter specifies whether to use the S/Key or OTP authentication technique. The default is **skey**.

The **encryption** parameter specifies whether to use MD4 or MD5 encryption. The default is **md4**.

Examples

To set up one-time passwords using the OTP method and MD5 encryption, use the command:

```
set skey met=otp enc=md5
```

Related Commands

show skey

set tacplus key

Syntax `SET TACPlus Key=`*`key`*

where *key* is a string of up to 64 characters

Description This command sets a new global key for TACACS+ servers. The **key** parameter specifies the new global secret key.

Examples To modify the global key on the TACACS+ server, use the command:

```
set tacp k=trynot2useMe2atAll
```

Related Commands **show tacplus key**

set tacplus server

Syntax

```
SET TACPlus SERVer=ipaddress [Key=key]
   [LOCal={NONE|1..15}] [POrt=port]
   [SINGLEconnection={Yes|No}] [TIMEOUT=1..10]
```

where:

- *ipaddress* is an IP address in dotted decimal notation.
- *key* is a key string of up to 64 characters.
- *port* is an integer value.

Description

This command modifies parameters already set for a TACACS+ server.

The **server** parameter specifies the IP address of the TACACS+ server to be modified.

The **key** parameter specifies the secret key to be modified.

The **local** parameter specifies a local interface to be used as the source for all TACACS+ packets the device sends to this TACACS server. The local interface must already be configured and be from 1 to 15. If **none** is specified, the router selects a source from the current available interfaces instead. The default is **none**.

The **port** parameter specifies the TCP port to be modified.

The **timeout** parameter specifies the period of time in seconds that the router waits for a response from the TACACS+ server before it times out.

The **singleconnection** parameter specifies whether multiple TACACS+ sessions are supported.

Examples

To change timeout from 3 seconds to 2 seconds and change the **singleconnection** parameter to **yes**, use the command:

```
set tacp serv=192.168.196.22 k=newkey4atr2supportacasplus
   timeout=2 single=y
```

Related Commands

add tacplus server
delete tacplus server
show tacplus server

set tacplus telnet

Syntax `SET TACPlus TELnet={0..15|None}`

Description This command determines whether or not TACACS+ authenticated users can Telnet from the router.

The **telnet** parameter specifies the minimum TACACS+ privilege level required for using Telnet on the router. A value of **none** disables Telnet for all TACACS+ authenticated users. A value of **1** indicates that all users can Telnet. A value of **7** indicates that manager privilege or better is required. A value of **15** is equivalent to security officer privilege. The default is **none**.

Examples To allow Telnet for TACACS+ authenticated security officers, use the command:

```
set tacp tel=15
```

Related Commands **show tacplus telnet**

set user

Syntax

```
SET USEr=login-name [APPLENetwork=atk-network]
   [APPLEZone=zone-name] [CALLingnumber=number]
   [CBNUMber=e164number] [DESCription=description]
   [Ipaddress={ipadd|OFf|NONe}] [MASk={ipadd|OFf|NONe}]
   [NETMASK={ipadd|OFf|NONe}] [MTu=40..1500]
   [IPXnetwork=ipx-network]
   [LOgin={True|False|ON|OFf|Yes|No}] [PAssword=password]
   [PRivilege={USer|MAnager|SEcurityofficer}]
   [RAdiusbackup={Yes|No|ON|OFf|True|False}]
   [TELnet={Yes|No}]

SET USEr [LOgin={True|False|ON|OFf|Yes|No}]
   [LOGINFail=1..10] [LOCkoutpd=1..30000]
   [MANpwdfail=1..5] [MInpwdlen=1..23]
   [Securedelay=10..3600] [TACRetries=0..10]
   [TACTimeout=1..60]
```

where:

- *login-name* is a string 1 to 64 characters long. Valid characters are uppercase and lowercase letters and decimal digits (0–9). The string cannot contain spaces.
- *atk-network* is an AppleTalk network number from 1 to 65535.
- *zone-name* is a character string 1 to 32 characters long. Valid characters are uppercase and lowercase letters, and decimal digits (0-9).
- *number* is an ISDN number or L2TP number 1 to 32 characters long. Valid characters are any printable characters, but the calling number it should match is likely to contain only decimal digits. If the string contains spaces, it must be in double quotes.
- *e164number* is the phone number to dial when performing callback. It may contain digits (0–9) and should be a valid phone number as described in CCITT standard E.164.
- *description* is a string 1 to 23 characters long. Valid characters are any printable character. If the string contains spaces, it must be in double quotes.
- *ipadd* is an IP address in dotted decimal notation.
- *ipx-network* is a valid Novell network number, expressed as a hexadecimal number. Leading zeros may be omitted.
- *password* is a character string up to 32 characters long. The default minimum length is 6 characters. Valid characters are any printable character. If the string contains spaces, it must be in double quotes.

Description

This command modifies a user record in the User Authentication Database or alters global parameters affecting the User Authentication Facility. It requires a user with security officer privilege when the router is in security mode.

The first variant of the command alters a user record in the User Authentication Database. The **user** parameter specifies the login name of a user in the database. Other parameters specified on the command modify the information stored in the database for that user. The second variant of the command is used to alter the global security parameters for the User Authentication Facility.

The **applenetwork** parameter specifies the AppleTalk network number assigned to the user accessing an AppleTalk internetwork. See Chapter 35, AppleTalk for more information.

The **applezone** parameter specifies the AppleTalk zone assigned to the user accessing an AppleTalk internetwork. See Chapter 35, AppleTalk for more information.

The **callingnumber** parameter specifies the calling number to be used to authenticate incoming calls from L2TP and ISDN services that provide caller ID information.

The **cbnumber** parameter specifies the ISDN number to use when making a callback to a remote user using the PPP callback facility.

The **description** parameter specifies text for the entry such as the full name and location of the user. This string may contain any printable character and the case is preserved in output.

The **ipaddress** parameter specifies an IP address for the user. The value must be a valid IP address in dotted decimal form. The IP address may be cleared by setting this parameter to **off** or **none**.

The **mask** parameter specifies the address mask that extends the range of IP addresses. If the **mask** parameter is not specified, a mask of 255.255.255.255 is used. The address and mask must be internally consistent in that the result of ANDing the address and mask should be the address. The mask may be cleared by setting this parameter to **off** or **none**.

The **netmask** parameter and the **mask** parameter are synonymous.

The **mtu** parameter specifies a Maximum Transmission Unit value for the user. The value must be a decimal integer from 40 to 1500 inclusive.

The **ipaddress**, **mask** and **mtu** parameters are required if the user is to login in order to make a PPP or SLIP connection to the router over a modem connected to an asynchronous port.

The **ipxnetwork** parameter specifies the Novell network number assigned to the user accessing a Novell internetwork. See Chapter 36, Novell IPX for more information.

The **login** parameter specifies whether users with user level privilege are permitted to log into the router. If used without a login name, it changes all login values for those with user privilege who are currently in the User Authentication Database. If a valid login name is used, the login value of that specific user is changed. If **false**, the user is authenticated by the User Authentication Database but not allowed to log into the router. If **true**, the user can log into the router and enter commands. The default is **false**.

The **password** parameter specifies a password for the user. The password is case sensitive. The user can change the password at any time by using the **set password** command on page 41-54. By default, the password must be at least 6 characters long. You can change the minimum length by using the **minpwdlen** parameter. The **password** parameter is required when the **privilege** parameter is specified.

The **privilege** parameter specifies the privilege level for the user. The default is **user**. User privilege entitles someone access to a subset of commands, generally those that affect the user's own session or asynchronous port. Manager privilege entitles someone access to all commands when the router is in normal mode, and to a smaller set when the router is in security mode. security officer privilege entitles someone access to the full set of commands regardless of the operating mode. The **password** parameter is required when the **privilege** parameter is specified.

The **radiusbackup** parameter specifies whether the user account is used only as a backup when RADIUS authentication fails because the RADIUS server is unreachable (either due to a network communication problem or the server itself is down). Specify **on**, **yes** or **true** if you want to use this account as a backup for RADIUS authentication. Specify **off**, **no** or **false** if you want to use this account as a normal user. The default is **off**.

If you configure one or more users in the User Authentication Database as RADIUS backup users then:

- RADIUS authentication will be attempted before checking the User Authentication Database. Normally, the User Authentication Database is checked before RADIUS.
- If the RADIUS server is unreachable, the login attempt is authenticated against users in the User Authentication Database who have **radiusbackup** set to **on**.
- If the RADIUS server is reachable but rejects the authentication request, the login attempt is authenticated against users in the User Authentication Database who have **radiusbackup** set to **off**.

The **telnet** parameter specifies whether the user is permitted to use the **telnet** command on page 61-34 of Chapter 61, Terminal Server to Telnet to another host, or the **connect** command on page 61-16 of Chapter 61, Terminal Server to access a Telnet service when logged in through Telnet.

The **loginfail** parameter sets the number of successive login failures a user may make before the login prompt is withheld for the lockout period. The default is 3.

The **lockoutpd** parameter sets the number of seconds that the login prompt is withheld when the number of login retries exceeds the value set by **loginfail**. The default is 600 seconds.

The **manpwdfail** parameter sets the number of successive attempts a manager may make to enter the correct password while entering a security command before the session is automatically logged off. The default is 3.

The **minpwdlen** parameter sets the minimum password length that is enforced for the **add user** and **set password** commands. The default is 6 characters.

The **securedelay** parameter sets the number of seconds that may elapse between the entry of one security command and the next without the user being required to re-enter the Security Officer password to validate the command. This only applies when the router is in security mode. The default is 60 seconds.

The **tacretries** parameter sets the number of times a TACACS request is resent when a response is not received within the timeout period. The default is 3.

The **tactimeout** parameter sets the number of seconds the router waits for a TACACS response before retransmitting the request or giving up after the number of retries is reached. The default is 5 seconds.

Examples To change the password to "BZ4gal" and the privilege level to manager for user Bruce, use the command:

```
set use=bruce pa=BZ4gal pr=ma
```

To change the minimum password length to eight characters for all users, use the command:

```
set use mi=8
```

Related Commands
add user
delete user
disable system security_mode
disable user
enable system security_mode
enable user
purge user
reset user
show user

show manager asyn

Syntax

```
SHow MAnager ASYn
```

Description This command displays the port number of the current semipermanent manager port. There can be only one semipermanent manager port at a time. When a semipermanent manager port is defined, the following message is displayed:

```
The manager port is ASYN 0
```

When no semipermanent manager port is defined, the following message is displayed:

```
No manager port is defined.
```

Related Commands
login
set manager asyn
set asyn

show radius

Syntax `SHow RADius`

Description This command displays the list of known RADIUS servers (Figure 41-7, Table 41-3 on page 41-63), and a list of user-definable RADIUS parameters. RADIUS servers are used for user authentication.

Figure 41-7: Example output from the **show radius** command

```
RADIUS Server Parameters
--------------------------------------------------------------------------------
Server Retransmit Count....... 2
Server Timeout................ 7 sec
Server Dead Time.............. 0 min
--------------------------------------------------------------------------------
Server          Port   AccPort  LocalInterface  Radius          Accounting
                                                Status          Status
--------------------------------------------------------------------------------
192.168.17.11   1645   1646     local4          Alive           Alive
172.31.253.9    1645   0        Not set         Alive           N/A
172.20.15.20    1337   0        Not set         Dead (3min)     N/A
--------------------------------------------------------------------------------
```

Table 41-3: Parameters in output of the **show radius** command

Parameter	Meaning
Server Retransmit Count	The number of times the device will attempt to contact a given RADIUS server, before moving on to the next server.
Server Timeout	The length of time the device will wait for a response from a RADIUS server for any given request.
Server Dead Time	Should a dead time be set, non responsive servers will not be used again for authentication, for a time equal to that of the Server Dead Time.
Server	IP address of this RADIUS server.
Port	Port number used to communicate with the RADIUS authentication server.
AccPort	Port number used to communicate with the RADIUS accounting server.
Local Interface	Local interface used as the source in outgoing messages to the RADIUS server.
Radius Status	The status of the server, either Alive or Dead. A value of Alive means that the server will be used for authentication. A value of Dead means that the server will not be used, until its dead period has timed out. The value in brackets for a dead server indicates the time in minutes before the dead period expires.
Accounting Status	The status of the accounting server, either Alive or Dead. A value of Alive means that the server will be used for authentication. A value of Dead means that the server will not be used, until its dead period has timed out. The value in brackets for a dead server indicates the time before the dead period expires.

Examples To display the list of known RADIUS servers, use the command:

```
sh rad
```

Related Commands **add radius server**
delete radius server

show radius debug

Syntax

```
SHow RADius DEBug
```

Description This command shows the debugging options for all RADIUS servers (Figure 41-8, Table 41-4).

Figure 41-8: Example output from the **show radius debug** command

```
RADIUS Server         Enabled Debug Modes
-------------------------------------------------------------
All Servers           PKT, DECODE, ERROR
```

Table 41-4: Parameters in output of the **show radius debug** command

Parameter	Meaning
RADIUS Server	Servers where debugging is enabled.
Enabled Debug Modes	Debugging modes enabled.

Examples To display the debugging options enabled for RADIUS, use the command:

```
sh rad deb
```

Related Commands **enable radius debug**
disable radius debug
disable debug active in Chapter 4, Configuring and Monitoring the System
show debug active in Chapter 4, Configuring and Monitoring the System

show skey

Syntax `SHow SKEY [SEQuence=`*`seq_no`* `SEED=`*`seed_name`* `[NUMber=`*`value`*`]]`

where:

- *seq_no* is an integer from 1 to 9999 representing the sequence number of the last S/Key or OTP password to be generated.
- *seed_name* is the 1-16 alphanumeric user-defined string that initialises the one-time password system on the authentication server.
- *value* is an integer from 1 to 99 representing the number of consecutive S/Key or OTP passwords to generate, finishing at *seq_no.*

Description This command shows the current S/Key configuration on the router (Figure 41-9, Table 41-5).

If the **sequence** and **seed** parameters are specified, the router calculates and displays one-time passwords for use during authentication when a user logs into the router using the S/Key or OTP system (Figure 41-10 on page 41-66, Table 41-6 on page 41-66).

To display the correct one-time passwords, the user must supply their current sequence number and seed. They are then asked to enter the password, which was used when initialising their current sequence of one-time passwords on the authentication server. The entered password is not echoed to the screen. The output shows the sequence of S/Key or OTP one-time passwords to be used for a user's subsequent login attempts.

Figure 41-9: Example output from the **show skey** command

```
Current S/Key Configuration
-------------------------------------------------------------
   Password Calculation Method ..... SKEY
   Encryption Algorithm ............ MD4
-------------------------------------------------------------
```

Table 41-5: Parameters in output of the **show skey** command

Parameter	Meaning
Password Calculation Method	Method to calculate the password: SKEY or OTP.
Encryption Algorithm	Encryption method: MD4 or MD5.

Figure 41-10: Example output from the **show skey seq=*n* seed=*seed*** command

```
Enter S/KEY initialisation password :
Computing SKEY passwords using MD4....
-------------------------------------------------------
Seq No         One-Time Password
95             IT DOLT ROOM NET GLUT ROWE
96             DARE MOS SARA GOAD MAO LEO
97             GUN TAIL MEND EAT INCH JOHN
98             EARN KID CARE HELD GIRD WINE
99             ADAM WARD DECK PLY EGAN WEED
-------------------------------------------------------
```

Table 41-6: Parameters in output of the **show skey seq=*n* seed=*seed*** command

Parameter	Meaning
Seq No	Sequence number of the S/Key password to be generated.
One-Time Password	S/Key passwords to be used when the user next logs in.

Examples

To show the next five passwords to be used when logging into a router under S/key or OTP authentication control, where the current sequence number is 99 and the seed used to generate the sequence was hs12345, use the command:

```
sh skey seq=99 seed=hs12345 num=5
```

Related Commands

set skey
login

show tacacs debug

Syntax `SHow TACacs DEBug`

Description This command shows the debugging options for all TACACS servers (Figure 41-11, Table 41-7).

Figure 41-11: Example output from the **show tacacs debug** command

```
TACACS Server          Enabled Debug Modes
-------------------------------------------------------------
All Servers            PKT, DECODE, ERROR
```

Table 41-7: Parameters in output of the **show tacacs debug** command

Parameter	Meaning
TACACS Server	Servers where debugging is enabled.
Enabled Debug Modes	Debugging modes enabled.

Examples To display the debugging options enabled for TACACS, use the command:

```
sh tac deb
```

Related Commands

enable tacacs debug
disable tacacs debug
disable debug active in Chapter 4, Configuring and Monitoring the System
show debug active in Chapter 4, Configuring and Monitoring the System

show tacacs server

Syntax `SHow TACacs SERVER`

Description This command displays the list of TACACS servers used for authenticating login names (Figure 41-12, Table 41-8).

Figure 41-12: Example output from the **show tacacs server** command

```
TACACS server addresses  Passcode prompt
---------------------------------------
192.168.35.17            On
192.168.163.30           Off
---------------------------------------
```

Table 41-8: Parameters in output of the **show tacacs server** command

Parameter	Meaning
TACACS server address	IP address of this TACACS server.
Passcode prompt	Status of the passcode prompt generation.

Related Commands **add tacacs server**
delete tacacs server

show tacplus

Syntax `SHow TACPlus`

Description This command displays information about the status and use of TACACS+ (Figure 41-13, Table 41-9).

Figure 41-13: Example output from the **show tacacs server** command

```
TACACS+.................Enabled
Number of servers ............1
Number of login users ........3
```

Table 41-9: Parameters in output of the **show tacacs server** command

Parameter	Meaning
TACACS+	Whether TACACS+ is enabled.
Number of servers	The number of TACACS+ servers that the router has been configured to use for authenticating users.
Number of login users	The number of currently logged-in users who were authenticated by a TACACS+ server.

Related Commands
add tacplus server
delete tacplus server
disable tacplus
enable tacplus
set tacplus server
show tacplus server
show tacplus user

show tacplus key

Syntax `SHow TACPlus Key`

Description This command displays the global key for TACACS+ (Figure 41-14).

Figure 41-14: Example output from the **show tacplus key** command

```
Tacplus global key: thisIsTheCurrentGlobalTacplusKey
```

Examples To show the TACACS+ global key, use the command:

```
sh tacp k
```

Related Commands
set tacplus key
show tacplus server

show tacplus server

Syntax `SHow TACPlus SERVER`

Description This command displays the configured TACACS+ servers (Figure 41-15, Table 41-10).

Figure 41-15: Example output from the **show tacplus server** command

```
Tacacs Plus Server Information
IP Address       Port     Timeout Value  Sessions   Single connection Local Interface
-------------------------------------------------------------------------------
172.168.198.254    49         5              1          Yes               local7
192.168.196.254    49         8              2          No                Not set
-------------------------------------------------------------------------------
```

Table 41-10: Parameters in output of the **show tacplus server** command

Parameter	Meaning
IP Address	IP address of the TACACS+ server.
Port	TCP port being used.
Timeout Value	Length of time the router waits for a response from the TACACS+ server.
Sessions	Number of TACACS+ sessions for each server.
Single connection	Whether multiple TACACS+ sessions are supported.
Local Interface	Interface used as the source in outgoing TACACS + messages sent to the TACACS+ server.

Example To show the TACACS+ servers currently configured, used the command:

```
sh tacp server
```

Related Commands

add tacplus server
delete tacplus server
set tacplus server

show tacplus telnet

Syntax `SHow TACPlus TELnet`

Description This command displays the level of TACACS+ privilege that is currently required for using Telnet on the router (Figure 41-16, Table 41-11).

Figure 41-16: Example output from the **show tacplus telnet** command

```
TACACS+ telnet privilege level: NONE
```

Table 41-11: Parameters in output of the **show tacplus telnet** command

Parameter	Meaning
TACACS+ telnet privilege level	Level of TACACS+ privilege required for using Telnet on the router—a number from 0 to 15 or **none**. **None** indicates that no TACACS+ authenticated user can use Telnet.

Related Commands **set tacplus telnet**

show tacplus user

Syntax `SHow TACPlus USer`

Description This command displays users who are currently being authenticated by TACACS+, or those who have been authenticated very recently (Figure 41-17, Table 41-12).

To see how many of the currently logged-in users were authenticated by TACACS+, use the **show tacplus** command.

Figure 41-17: Example output from the **show tacplus user** command

```
Tacacs Plus User Information
------------------------------------------------------------
User Name: admin
Privilege: manager        Login: 12:03:08

User Name: user1
Privilege: unknown        Login: not logged in
```

Table 41-12: Parameters in output of the **show tacplus user** command

Parameter	Meaning
User Name	User's login name.
Privilege	User's privilege level.
Login	Time the user logged in, or "not logged in".

Example To display users who are currently being authenticated by TACACS+, use the command:

```
sh tacp us
```

Related Commands **show tacplus server**

show user

Syntax `SHow USEr[=`*`login-name`*`] [Configuration]`

where *login-name* is a string 1 to 64 characters long. Valid characters are uppercase and lowercase letters and decimal digits (0–9). The string cannot contain spaces.

Description This command displays the contents of the User Authentication Database or global configuration parameters and counters for the User Authentication Facility.

For a user with manager or security officer privilege, the command displays the contents of the User Authentication Database. When the router is in security mode, the command also displays the number of users currently logged in with security officer privilege. If a login name is specified, information for the specific user is displayed. If a login name is not specified, the entire database is displayed (Figure 41-18 on page 41-74, Table 41-13 on page 41-74). For users with user level privilege, parameters are not allowed and their own database record is displayed.

The **configuration** parameter displays global configuration parameters and counters for the User Authentication Facility (Figure 41-19 on page 41-76, Table 41-14 on page 41-76). A login name is not valid with this parameter.

Figure 41-18: Example output from the **show user** command

```
Number of logged in Security Officers currently active.....1

Number of Radius-backup users..... 0

User Authentication Database
---------------------------------------------------------------------------
Username: dave ()
   Status: enabled    Privilege: Sec Off   Telnet: yes   Login: yes   RBU: no
   Callback number: 0061393546786
   Calling number: 5554491
   Logins: 2          Fails: 0        Sent: 0            Rcvd: 0
   Authentications: 0 Fails: 0
Username: manager (Manager Account)
   Status: enabled    Privilege: manager   Telnet: yes   Login: yes   RBU: no
   Logins: 4          Fails: 0        Sent: 0            Rcvd: 0
   Authentications: 0 Fails: 0
Username: tony ()
   Status: enabled    Privilege: user      Telnet: no    Login: no    RBU: no
   Ip address: 192.168.1.5      Netmask: 255.255.255.0    Mtu: 1500
   IPX network: c0e7230f
   Apple network: 22   Apple zone: Finance
   Logins: 0          Fails: 2        Sent: 0            Rcvd: 0
   Authentications: 0 Fails: 0
---------------------------------------------------------------------------


Active (logged in) Users
------------------------

User           Port/Device
    Login Time               Location
---------------------------------------------------------------------------
manager        Asyn 0
    14:33:22 18-Apr-2002     local
manager        Telnet 1
    14:33:22 18-Apr-2002     10.1.1.1
---------------------------------------------------------------------------
```

Table 41-13: Parameters in output of the **show user** command

Parameter	Meaning
Number of logged in Security Officers currently active	Number of users currently logged in with security officer privilege. This counter is only displayed when security mode is enabled. It does not include users whose security officer privilege is disabled because they have not entered a security command within the secure delay period.
Number of Radius-backup users	Number of backup users configured. For more information, see "RADIUS backup users" on page 41-9.
User Authentication Database	
Username	Login name for this user.
Status	Whether the entry is enabled.
Privilege	The privilege level for this user.
Telnet	Whether the user is permitted to use the **telnet** command to open a session with a host.
Login	Whether the user can log into the router and enter commands.

Table 41-13: Parameters in output of the **show user** command (Continued)

Parameter	Meaning
RBU	Whether the user is configured as a RADIUS backup user, for authenticaton only when a RADIUS server is unreachable.
IP address	IP address for this user. This field is not present if an IP address has not been assigned.
Netmask	Network mask for this user. This field is not present if an IP address has not been assigned.
Mtu	MTU for this user. This field is not present if an IP address has not been assigned.
IPX network	Novell network number assigned to the user. This field is not present if an IPX network number has not been assigned.
Apple network	AppleTalk network number assigned to the user. This field is not present if an AppleTalk network number has not been assigned.
Apple zone	AppleTalk zone assigned to the user. This field is not present if an AppleTalk network number has not been assigned.
Callback number	ISDN phone number for this user when making a call back to a remote user. This field is not present if a callback number has not been assigned.
Calling number	Number to check against the incoming calling number of an L2TP or ISDN call when the call provides caller ID information. This field is not present if a calling number has not been assigned.
Logins	Number of times a successful login has been made by this user.
Fails	Number of times login has failed for this user.
Sent	Number of octets sent by the user to the router.
Rcvd	Number of octets set to the user from the router.
Authentications	Number of authentications.
Fails	Number of times authentication has failed for this user.
Active (logged in) Users	
User	Login name of the user.
Port/Device	Port or device on the router that the user is logged into; either Port x, Telnet x, or SSH x, where *x* is the device instance.
Login Time	Time the user logged in for this connection.
Location	Location of the user. It is local if the user is attached to an asynchronous port, or the IP address of the remote device.

Figure 41-19: Example output from the **show user configuration** command

```
User module configuration and counters
------------------------------------------------------------------------------
Security parameters
  login failures before lockout ............     4            (LOGINFAIL)
  lockout period ...........................    20 seconds    (LOCKOUTPD)
  manager password failures before logoff ..     3            (MANPWDFAIL)
  maximum security command interval ........    30 seconds    (SECUREDELAY)
  minimum password length ..................     6 characters (MINPWDLEN)
  TACACS retries ...........................     3            (TACRETRIES)
  TACACS timeout period ....................     5 seconds    (TACTIMEOUT)
  semi-permanent manager port .............. none

Security counters
  logins                          7     authentications                23
  managerPwdChanges               0     defaultAcctRecoveries           0
  unknownLoginNames               1     tacacsLoginReqs                 1
  totalPwdFails                   5     tacacsLoginRejs                 1
  managerPwdFails                 3     tacacsReqTimeouts               0
  securityCmdLogoffs              1     tacacsReqFails                  0
  loginLockouts                   1     databaseClearTotallys           0
------------------------------------------------------------------------------
```

Table 41-14: Parameters in output of the **show user configuration** command

Parameter	Meaning
Security parameters	
login failures before lockout	Default number of login failures allowed by a user before the login prompt is withheld for the lockout period.
lockout period	Default period in seconds that the login prompt is withheld from a user after a number of consecutive login failures.
manager password failures before logoff	Default number of successive failures a manager may make entering the login password before the session is logged off.
maximum security command interval	Default interval in seconds that may elapse between successive commands without the security officer being prompted to re-enter the login password.
minimum password length	Default for the minimum password length.
TACACS retries	Default number of times a TACACS request is retransmitted when a response is not received within the timeout period.
TACACS timeout period	Default in seconds that the router waits for a TACACS response before retransmitting the request.
semi-permanent manager port	Port number of the semipermanent manager port.
Security counters	
logins	Total number of logins by any user to the router.
authentications	Total number of authentications by a user, by the router.
managerPwdChanges	Number of times a manager level password has been changed.
defaultAcctRecoveries	Number of times the router was rebooted with DIP switch 3 set to restore the default account passwords.

Table 41-14: Parameters in output of the **show user configuration** command (Continued)

Parameter	Meaning
unknownLoginNames	Number of attempted logins with a login name that did not exist in the database and was not validated by a TACACS server.
tacacsLoginReqs	Number of login requests made to a TACACS server.
totalPwdFails	Total number of times an incorrect password was given for a login name that exists in the database.
tacacsLoginRejs	Number of rejects received from a TACACS server in response to a login request.
managerPwdFails	Number of times a manager entered the incorrect password when required to validate a security command.
tacacsReqTimeouts	Number of login requests to a TACACS server that terminated in a timeout.
securityCmdLogoffs	Number of times a manager was logged off because a correct password was not entered when required to validate a security command.
tacacsReqFails	Number of login attempts terminated because of TACACS server timeouts.
loginLockouts	Number of times the login lockout period was instigated because too many unsuccessful login attempts were made.
databaseClearTotallys	Number of times the database has been cleared.

Related Commands

add user
delete user
disable system security_mode
disable user
enable system security_mode
enable user
purge user
reset user
set user

show user rso

Syntax `SHow USEr RSO`

Description This command displays information about the current state of remote security officer (RSO) access and the log of access events (Figure 41-20, Table 41-15 on page 41-79). This command requires a user with security officer privilege when the router is in security mode.

Figure 41-20: Example output from the **show user rso** command

```
Remote Security Officer Access is enabled.

Remote Security Officer Log
------------------------------------------------------------------------------

Remote Security Officer range from: 3ffe::1:6
                                 to: 3ffe::1:10
Failed logins ..................... 1
Last failed login ................. 23-Feb-2004 03:28:29
Successful logins ................. 2
Last successful login ............. 23-Feb-2004 03:28:05
------------------------------------------------------------------------------

Remote Security Officer ........... 3ffe::1:2/128
Failed logins ..................... 0
Last failed login ................. **-***-**** **:**:**
Successful logins ................. 2
Last successful login ............. 23-Feb-2004 05:04:27
------------------------------------------------------------------------------

Remote Security Officer ........... 192.168.100.200/255.255.255.255
Failed logins ..................... 1
Last failed login ................. 23-Feb-2004 03:31:17
Successful logins ................. 1
Last successful login ............. 23-Feb-2004 04:04:27
------------------------------------------------------------------------------

Remote Security Officer ........... 192.168.5.0/255.255.255.0
Failed Logins ..................... 1
Last failed login ................. 18-Mar-2004 23:33:50
Successful Logins ................. 0
Last successful login ............. **-***-**** **:**:**
------------------------------------------------------------------------------

Illegal Login Attempts
------------------------------------------------------------------------------
IP Address                                Date/Time                   Attempts
------------------------------------------------------------------------------
202.175.36.132                            23-Feb-2004 04:03:48               1
172.20.1.3                                23-Feb-2004 03:27:17               3
2ffe::1:3                                 23-Feb-2004 03:26:34               6
------------------------------------------------------------------------------
```

Table 41-15: Parameters in output of the **show user rso** command

Parameter	Meaning
Remote Security Officer Access is...	Whether the remote security officer access is enabled.
Remote Security Officer Log	The list of remote security officers and a log of access events for those remote security officers.
Remote Security Officer	IPv4 address and mask, IPv4 address range, or IPv6 address and prefix length of a remote security officer. A mask other than 255.255.255.255 defines a range of remote security officer addresses.
Failed logins	Number of failed login attempts by users in the remote security officer address range.
Last failed login	Date and time of the last failed login attempt, or "**-***-**** **:**:**" when there have been no failed attempts.
Successful logins	Number of successful login attempts by users in the remote security officer address range.
Last successful login	Date and time of the last successful login attempt, or "**-***-**** **:**:**" when there have been no successful attempts.
Illegal login attempts	A log of illegal login attempts from IP addresses not in one of the defined remote security officer address ranges.
IP address	IP address where the Telnet session originated.
Date/time	Date and time of the login attempt.
Attempts	Number of attempts made from this IP address.

Examples To display the log of remote security officer access events, use the command:

```
sh use rso
```

Related Commands

add user rso
delete user rso
disable user rso
enable user rso