Note

If the test timeout option is enabled and pin 18 remains high, the modem returns to idle mode at the end of the test timeout period and will not re-enter the test mode until an off-to-on transition of pin 18 has been detected.

Chapter 8
Security

GENERAL

The V.3400 series of modems provide three features to assure secure operation of the modem. These features are front panel password protection, autocallback, and secure mode of operation. The topic of front panel password protection is discussed in Chapter 4.

Two levels of major security operation are available: high and low. The AT commands for each level are explained below.

AUTOCALLBACK SECURITY

Autocallback is an additional security feature that is separate from Low and High Security. Autocallback forces an answering modem to dial the selected autodial (**AUn*) telephone number after answering a call, holding the line for one second, and then disconnecting. When autocallback is enabled the modem will not train on a direct call. Access autocallback via Main Menu #5 on the LCD. Refer to Chapter 4 for further information. *S72* enables/disables autocallback. *S78* determines the delay in seconds before autocallback is initiated.

LOW SECURITY OPERATION

Low security operation provides password protection against unauthorized dial-up access. High security is another feature which is discussed later in this chapter. The security feature can be enabled/disabled with AT commands when operating on a dial-up system.

Transmitted data and received data lines are suppressed to the host DTE during security validation; all other signals (CTS, DSR, RI, etc.) operate as selected. After the password has been validated, the modem operates normally.

Operating without Low Security

The modem is not factory set for security and operates like a standard V.34, except for additional AT command which allow access to security. With these commands a user can set passwords and turn security on. When security is enabled, a password must be used to change security options.

Operating with Low Security

A secure modem will not allow data transfer between its host and a remote host until a correct password is received from the calling party. If an incorrect password is received the secure modem disconnects. The front panel is not locked out because this type of security prevents unauthorized dial-up access.

Remote Operation

The originating modem must transmit the correct security code before the secure modem will allow data transfer. If accessing a secure remote modem, the local modem prompts the user with

PLEASE ENTER YOUR PASSWORD ⇒

To Respond to the password prompt

Enter *AT$* followed by the password.

After receiving the *$* the secure remote modem accepts the security code and waits for a carriage return. Entering more than ten characters is invalid and causes the secure modem to disconnect. Entering a valid password causes the calling party's DTE to display PASSWORD ACCEPTED.

Local Operation

When accessing the local modem, the password is not required except when the user wants to change a security option. To change a password or to turn security on or off, the user must enter a password when entering the appropriate AT commands. EIA-232 signals to the DTE are not affected by security in command mode.

Passwords

Two passwords of up to ten characters each can be stored in the modem's nonvolatile memory. AT commands change the passwords. Backspace and escape keys are not supported for password entry. The passwords can consist of any printable characters except a dollar sign, comma, or space. Passwords are case sensitive.

The passwords have the same priority level and are interchangeable with each other. This can be helpful in situations such as when the user forgets one of the passwords.

LCD Indication of Security

The front panel LCD indicates whether security is on or off. If disabled, the LCD appears as if the security does not exist. If enabled, Main Menu #1 consists of the following display:

```
SECURE 28800
XXXX
```

Restrictions In Security Operation

If the caller gives the wrong password, while security is enabled, the modem will disconnect.

LOW SECURITY COMMANDS

The following AT commands operate low security:

Set Password $S=*x*

The *$S=x* command sets an empty password location to *x*. This command only applies when no password or only one is stored in memory. It can not be used to change a password.

Changing a Password $C=*x, y*

The *$C=x, y* command changes either password where *x* represents the old password and *y* is new one.

Deleting a Password $C=*x*, -

The *$C=x*, - command deletes password *x* from memory. Security is automatically disabled if the last password is deleted.

Security Reset $DR

This command resets security to its initial state (off with no passwords stored). The option is not available in remote configuration.

Disabling Security $D=*x*

The *$D=x* command disables security where *x* is either password.

Security Status $D?, $E?

The *$D?* or *$E?* commands display the current status of security (on or off).

Enabling Security $E=x

The *$E=x* command enables security where *x* is either password.

HIGH SECURITY

Compatibility

The calling modem does not require any security capabilities to connect with a secured V.3400. Access to the V.3400 host is gained by following the appropriate logon procedure as described in following text. All security operations are controlled by the secured V.3400.

Capacity

The modem stores in nonvolatile memory the password, security level, callback phone number, and status information for 50 users.

Operating without High Security

The modem is factory set with security disabled. In this mode the local DTE is connected to the local modem as usual except that the command to enable or view the status of the security feature will be accepted and processed.

Operating with High Security

With high security enabled, each user must follow the appropriate logon procedure. The procedure for remote users is determined by their assigned security level. Upon termination of the connection, the secured modem waits for the next call and password sequence. A local user must logon to the secured V.3400 to use the unit.

If a power outage occurs the logged on user must logon again when the power is restored.

For optimum security operation a reliable connection should be used.

SECURITY LEVELS

The V.3400 provides three levels of security to prevent unauthorized access by a remote user.

Level 1: Password Only

This is the lowest level of dial-up security. The user is prompted for an ID and password; if invalid, the modem hangs up.

Level 2: Password with Callback

This security level also requires that the user call from a pre-set telephone number. After the user enters a correct ID and password, the modem looks up the telephone number and calls the user back at that number.

Level 3: Password with Callback and Password Re-Entry

This is the highest level of security and is similar to Password with Callback except that after the user answers the callback call, the modem prompts him again for the password.

SUPERUSER

The superuser has access to all user information for administrative purposes and can change user logon requirements and privileges.

Superuser status can be gained at the local modem or from a remote Motorola or UDS modem via remote configuration, if the "Remote Superuser" option is enabled.

The superuser must first logon as a regular user, then request the superuser privilege.

Incorrect attempts to gain superuser privilege are logged in the users status information field in nonvolatile memory. After seven invalid attempts, the user is suspended from access to the V.3400 until cleared by the superuser.

To reinstate a suspended user, logon as a different regular user, then request superuser privilege in order to clear the illegal attempts count.

If the local superuser disables security, the only security commands available are those used to enable security or to check security status.

Passwords

Passwords can be changed or deleted by the superuser. The regular user can change his password only if the "user changes" option has been enabled by the superuser. Refer to the Extended Features section for more details.

When calling from a remote location, the user is prompted for a password. Once the password is entered, the user is either allowed direct access or disconnected and called back depending on the assigned security level.

During password entry or logon, each password character is displayed as an "X" on the DTE screen. The backspace key can be used for editing. For remote logon, the Esc key can be pressed prior to the carriage return to clear the password entry.

Incorrect password attempts exceeding the threshold set in *S77* for a specific user will cause the modem to disconnect. Each call exceeding the threshold increments the ILLEGAL ATTEMPTS counter by one. After seven calls the ILLEGAL ATTEMPTS counter will have reached maximum and the user will be suspended.

Default Passwords

The modem is shipped from the factory with a default password for the superuser and for one regular user. They are

- SUPERUSER System administrator
- USER 1 User number 1

Passwords for users 2 through 50 are left blank.

It is recommended that the superuser change the default SUPERUSER and USER 1 passwords as soon as possible.

HIGH SECURITY COMMANDS

These commands are only allowed for a local superuser.

Enabling High Security $EH=*pw*

The *$EH=pw* command enables high security, where pw is the superuser's password.

To initialize high security for the first time enter

AT$EH=SUPERUSER

to enable security, then enter

AT$1=USER1 <CR> followed by
AT$S=SUPERUSER <CR>

to gain superuser status. Passwords, security levels, and callback numbers can now be entered or modified.

When superuser activities are completed, return to regular user status by entering *AT$$*. Once in regular user status *AT$$* becomes the final local logoff command.

Disabling High Security $D

Enter the *$D* command to disable security. The modem will operate as a nonsecure unit except that it will respond to enable and check security status commands.

Setting Passwords $P*n=pw$pw*

Select a password between 4 and 34 printable ASCII characters.

To store the password enter:

AT$Pn=pw$pw

Where *n* is the user number (0-50) and pw is the new password which is entered twice to ensure that is has been entered correctly.

The *$* character is used as the marker between the dual password entries and cannot be used as part of the password.

Passwords cannot be recalled from nonvolatile memory.

Note

Superuser password is critical because the security feature cannot be configured without it.

After logon as USER 1 and gaining superuser privileges, enter the *$Pn* command to modify passwords.

For the superuser enter:

AT$P0=pw$pw

For user 1 enter:

AT$P1=pw$pw

Record the passwords in your personal records.

Caution

Do not forget the superuser password. Systems administrator functions cannot be accessed without it and the modem must be returned to the factory for re-initialization.

Set Security Levels $L*n=m*

The System Administrator (superuser) assigns each user with a security level by entering the *$Ln=m* command (where *n* is the user number and *m* is the security level).

Set User Callback Number $C*n=m*

The callback number, used with level 2 or 3 security, is dialed by the modem after a user has successfully called in from a remote location and entered their password.

Level 1 security does not require a callback number; however, if the security level is changed to level 2 or 3 a callback number will be required.

The callback number should be programmed initially using the *$Cn=m* command. Where *n* is the user number and *m* is the callback number.

Extended Features $W

$W1

A regular user can change his password and callback number if the local superuser has enabled the *$W1* option.

$W2

A remote regular user can gain superuser privilege once the local superuser has enabled the *$W2* command.

$W0

The extended feature options can be cleared by a local superuser by entering the *$W0* command.

Display Extended Feature Status $W?

Enter the *$W?* command to display the status of the user changes and remote superuser options.

Display / Reset Illegal Access Attempt Counters $M, $M*n*, $M*

This command informs the superuser of any illegal attempts to gain superuser status and the users current status. The status will either be "normal," indicating the user is still able to logon to the secure V.3400, or "suspended," indicating that the user made more than seven illegal attempts to gain superuser status and has been automatically suspended.

When the superuser logs on, the secure V.3400 automatically displays any illegal attempts since the last superuser logon. If it is not reset, the illegal attempt count will remain and the superuser will not be reminded unless more illegal attempts occur. To manually request this same information enter

AT$M

The V.3400 responds by scrolling any illegal attempt information onto the screen as in the following example:

USER NUMBER: 01, ILLEGAL ATTEMPTS: 1,
STATUS: NORMAL

USER NUMBER: 14, ILLEGAL ATTEMPTS: 7,
STATUS: SUSPENDED

OK

Enter the *$Mn* command (where *n* equals user number) to reset a specific user's illegal attempt count.

Enter the *$M** command to reset all of the user's illegal attempt count.

Factory Reset $F=*pw*$*pw*

To reinitialize the security feature enter the *$F=pw$pw* command (where *pw* is the "current" superuser password). This command deletes all user information and reinstates factory default passwords. User information cannot be recalled.

Removing a User $R*n*

This superuser command removes a user from active status without deleting all of the users information. The user can be restored to active status by setting the password with the corresponding user number as previously mentioned. The command to remove a user is

AT$Rn

where *n* is the user numbers 2-50.

The superuser or user with ID #1 cannot be deleted from the user list.

Security Status $E?

System security status can be verified using the *$E?* command.

Display User Status $S?

Enter the *$S?* command to indicate whether or not the current user has superuser status.

The V.3400 responds with one of the following responses:

SUPERUSER STATUS
NORMAL STATUS

Verify User Information $I*n*, $IB*n*

Security level and callback number can be displayed using either the *$In* or *$IBn* command. To display the assigned security level and callback number for a single user enter

AT$In where *n* is the user number.

A regular user can only check his own information. A user with superuser privileges can check any user's information.

A user with superuser privileges can also display the assigned security level and callback number for each valid user within a block of ten consecutive user numbers by entering:

AT$IBn where *n* is the first user number.

Request Superuser Privilege $S=*pw*

Once logged on as a user, superuser privilege can be requested by entering the *$S=pw* command, where *pw* is the superuser password.

When the correct password has been entered, the V.3400 responds with

SUPERUSER STATUS

OK

Local Logon Command $*n*=*pw*

Enter the *$n=pw* command to logon locally to the secure V.3400. Where *n* is the user number and pw is the password.

Local Logoff Command $$

To logoff after a local session enter

AT$$

Remote Logon Procedure $*n*=*pw*

The remote logon procedure is required to access a secure V.3400. When calling into the secure V.3400 from a remote location the user is prompted to enter a password. The password must be entered as