



TELNET Protocol

bintec-Dm 738-I

Copyright© Version 11.01 bintec elmeg

Legal Notice

Warranty

This publication is subject to change.

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

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

Table of Contents

| | | |
|-----------|-----------------------------------|---|
| I | Related Documents | 1 |
| Chapter 1 | Introduction | 2 |
| 1.1 | TELNET Protocol | 2 |
| Chapter 2 | Configuration | 3 |
| 2.1 | Configuration Commands | 3 |
| 2.1.1 | ? (HELP) | 3 |
| 2.1.2 | ACCOUNTING | 3 |
| 2.1.3 | AUTHORIZATION | 4 |
| 2.1.4 | LIST | 4 |
| 2.1.5 | LOGIN | 4 |
| 2.1.6 | SET. | 5 |
| 2.1.7 | EXIT | 5 |
| 2.2 | Configuring the Console | 6 |
| 2.2.1 | SET. | 6 |
| Chapter 3 | Monitoring | 7 |
| 3.1 | Monitoring Commands | 7 |
| 3.1.1 | SYSTEM TELNET | 7 |

I Related Documents

bintec-Dm 800-I AAA Feature

Chapter 1 Introduction

1.1 TELNET Protocol

The purpose of the TELNET protocol is to provide a general, bi-directional, byte-oriented communications system. It can therefore be thought of as a standard method for interconnecting terminal devices with terminal-oriented processes.

TELNET is one of the first attempts to develop a virtual terminal protocol (VTP) and was developed as part of the TCP/IP suite of protocols.

TELNET is built upon three basic principles:

- The concept of a Network Virtual Terminal or NVT.
- A symmetric view of terminals and processes.
- The principal of negotiated options.

An NVT is an imaginary device which provides an intermediate representation of a canonical terminal. If the communication entity is a process, a module is needed (TELNET server) to perform the conversion between the NVT representation and the process representation. If the communication entity is a terminal, a module is needed (TELNET client) to convert the terminal characteristics to those of the NVT.

The communication is expected to be made over a TCP connection. TELNET assumes that the ASCII code will be used for the communication. All TELNET connections start with a negotiation phase where options indicating the connection characteristics are agreed upon. After said negotiation, the data to be transmitted is transmitted. Escape characters can be used to include commands along with the data.

Our devices include a Telnet server (see below for details on how to configure and monitor it) that provides remote access to the consoles of the devices. This allows users to remotely configure and monitor the devices as if they were locally connected. They also contain a Telnet client to be able to connect to any other device that supports a Telnet server.

Chapter 2 Configuration

2.1 Configuration Commands

This section describes the commands to configure the TELNET protocol.

To access the TELNET protocol configuration environment, enter the following commands:

```
*process 4
Config>set telnet
-- Telnet user configuration --
Telnet config>
```

The following table lists the TELNET protocol configuration commands.

| Command | Function |
|---------------|---|
| ? (HELP) | Lists the commands or their options. |
| ACCOUNTING | Configures the AAA accounting options. |
| AUTHORIZATION | Configures the AAA authorization options. |
| LIST | Lists the TELNET configuration. |
| LOGIN | Configures the AAA login options. |
| SET | Configures the protocol parameters. |
| EXIT | Returns to the previous prompt. |

2.1.1 ? (HELP)

This command allows you to list the available commands from the current prompt level. You can also type a question mark (?) after a specific command to list its options.

Syntax:

```
Telnet config>?
```

Example:

```
Telnet config>?
 accounting      Set AAA accounting options
 authorization    Set AAA authorization options
 list            List configuration
 login          Set AAA login options
 set            Set telnet options
 exit
```

2.1.2 ACCOUNTING

This command associates an *accounting exec* or *commands* method list configured through the AAA facility. In this way, the Telnet service applies the methods from the *accounting exec* list when it registers a Shell access, and the methods from the *accounting commands* list when it registers an executed command.

Syntax:

```
Telnet config>accounting {commands <level> | exec} <listname>
```

- **commands** indicates that the method list type is *accounting commands*.
- **<level>** indicates the access level of the commands to be logged.
- **exec** indicates that the method list type is *accounting exec*.
- **<listname>** is the identifier of the accounting method list.

Example 1:

```
Telnet config>accounting commands 15 AccCmds
Telnet config>
```

In example 1, the *AccCmds* method list is configured to be used when accounting for a level 15 command.

Example 2:

```
Telnet config>accounting exec AccExec
Telnet config>
```

In example 2, the *AccExec* method list is configured to be used when accounting for a Shell access.

Method lists can only be applied if the AAA facility is enabled. Therefore, once the AAA configuration is complete, it must be enabled in order to apply the lists to the different services. For more information on how to set up the AAA facility, see the following manual: *bintec-Dm800-I AAA Feature*.

2.1.3 AUTHORIZATION

This command associates an *authorization exec* or *commands* method list configured through the AAA facility. In this way, the Telnet service applies the methods from the *authorization exec* list when it requires Shell authorization and from the *authorization commands* list when it requires command authorization.

Syntax:

```
Telnet config>authorization {commands <level> | exec} <listname>
```

- **commands** indicates that the method list is *authorization commands*.
- **<level>** indicates the access level for the commands requiring authorization.
- **exec** indicates that the method list is *authorization exec*.
- **<listname>** this is the authorization method list identifier.

Example 1:

```
Telnet config>authorization commands 15 AuthorCmds
Telnet config>
```

Example 1 specifies that the *AuthorCmds* method list will be used for authorizing level 15 commands.

Example 2:

```
Telnet config>authorization exec AuthorExec
Telnet config>
```

Example 2 specifies that the *AuthorExec* method list will be used for Shell authorization.

Method lists can only be applied if the AAA facility is enabled. Therefore, once the AAA configuration is complete, it must be enabled in order to apply the lists to the different services. For more information on how to set up the AAA facility, see the following manual: *bintec-Dm800-I AAA Feature*.

2.1.4 LIST

The **LIST** command allows you to view the contents of the TELNET configuration.

Syntax:

```
Telnet config>list
```

Example:

List corresponding to the default configuration:

```
Telnet config>list
Telnet port: 23
Maximum number of telnet sessions: 4
Telnet config>
```

2.1.5 LOGIN

This command associates an *authentication login* method list configured through the AAA facility. In this way, the Telnet service applies the methods from the associated list when it needs to execute authentication.

Syntax:

```
Telnet config>login authentication <listname>
```

- **<listname>** is the identifier of the authentication method list.

Example:

```
Telnet config>login authentication AutheLogin
Telnet config>
```

This example specifies that the *AutheLogin* method list will be used to authenticate users accessing the Shell.

Method lists can only be applied if the AAA facility is enabled. Therefore, once the AAA configuration is complete, it must be enabled in order to apply the lists to the different services. For more information on how to set up the AAA facility, see the following manual: *bintec-Dm800-I AAA Feature*.

2.1.6 SET

Syntax:

```
Telnet config> set ?
login          Set login options
max-telnets    Maximum number of telnet sessions you can open
port          Set port number
```

2.1.6.1 SET LOGIN ATTEMPTS

This command allows you to configure the maximum number of login attempts allowed in a telnet session.

Syntax:

```
Telnet config>set login attempts <max_attempts>
```

- **< max_attempts >** this is the maximum number of login attempts allowed.

Example:

```
Telnet config>set login attempts 2
Telnet config>
```

2.1.6.2 SET MAX-TELNETS

This command allows you to configure the maximum number of telnet sessions you can open with the device. By default, you can only open four simultaneous sessions. The maximum number of configurable sessions is 20, and using 0 disables access to the device via telnet.

Syntax:

```
Telnet config>set max-telnets ?
<0..20>      Value in the specified range
```

Example:

```
Telnet config>set max-telnets 10
Telnet config>
```

2.1.6.3 SET PORT

This command allows you to configure the port assigned to the device's Telnet server. Port 23 is used by default.

Syntax:

```
Telnet config>set port
```

Example:

```
Telnet config>set port 24
Telnet config>
```

2.1.7 EXIT

This command returns you to the previous prompt level.

Syntax:

```
Telnet config>exit
```

Example:

```
Telnet config>exit
Config>
```

2.2 Configuring the Console

A point to bear in mind is that in addition to the Telnet protocol's own configuration parameters, there are certain commands related to the console process configuration which could affect the Telnet server functionality. You can access these parameters from the general configuration prompt in the following way:

```
*process 4
Config>
```

2.2.1 SET

Syntax:

```
Config>set ?
inactivity-timer      Configure the maximum inactivity time
password              Configure the device access password
```

2.2.1.1 SET INACTIVITY-TIMER

This command allows you to configure a maximum inactivity time (i.e., without pressing a key or sending a character) in the process that allows device console access (both through TELNET and through local access). The value is provided in minutes and the permitted range is between 1 minute and 10 hours. Once this has timed out, the TELNET server for the device disconnects the user or the local console pauses. When the local console pauses due to inactivity, you need to press a key to recoup it or introduce an access password if this function is enabled (please see the **SET PASSWORD** command below).

Syntax:

```
Config>set inactivity-timer
```

Example:

```
Config>set inactivity-timer ?
<1..600>      Console inactivity timeout in minutes
disabled     Disable inactivity timer
Config>
```

2.2.1.2 SET PASSWORD

This command allows you to configure an access password to access the device using a TELNET remote terminal, local console connection, or FTP connection.

Syntax:

```
Config>set password
```

Example:

```
Config>set password hello
Config>
```

To access the device without entering a password, use the NO command to delete the password.

Example:

```
Config>no password
Config>
```

Chapter 3 Monitoring

3.1 Monitoring Commands

This section describes the commands used to monitor the TELNET server. These commands are found at the general monitoring prompt which is accessed as follows:

```
*process 3
Console Operator
+
```

3.1.1 SYSTEM TELNET

This command displays information about the users that are connected to the device.

Syntax:

```
+system telnet
```

Example:

```
+system telnet

Time unit: minutes
  ID  USER  LEVEL  IP ADDRESS:PORT  CONNECTION-TIME  INACTIV-TIME  IDLETIME  TIMEOUT
-----
  0  telat  15      Local Console  03/03/05 10:40:57      0          0          0
  2  telat  15    172.24.51.128:59671  04/05/05 16:59:46      0          10          0 *
  1  telat  15    192.168.1.1:0    04/03/05 16:57:58      2          0          0
+
```

The meaning of each of the fields is as follows:

| | |
|------------------------|---|
| ID | ID number of the Telnet session. |
| USER | Name of the user connected to the device. This field will be empty if no users have been created. |
| LEVEL | User privilege level. |
| IP ADDRESS:PORT | IP address and port from which the connection is received. |
| CONNECTION TIME | Date and time the connection occurred. |
| INACTIVITY TIME | Telnet session downtime. If this parameter is disabled in the device configuration, its value will be 0 (zero). |
| IDLETIME | Maximum idle time allowed. If not specified, the value of this parameter will be 0 (zero). |
| TIMEOUT | Maximum session time allowed. If not specified, the value of this parameter will be 0 (zero). |

An asterisk next to the idle time field indicates the session from which you are accessing.