Console Port, Telnet, and SSH Handling

This chapter includes the following sections:

Notes and Restrictions for Console Port, Telnet, and SSH

- • Telnet and Secure Shell (SSH) settings configured in the transport map override any other Telnet or SSH settings when the transport map is applied to the Ethernet management interface.

- • Only local usernames and passwords can be used to authenticate users entering a Ethernet management interface. AAA authentication is not available for users accessing the router through a Ethernet management interface using persistent Telnet or persistent SSH.

- • Applying a transport map to a Ethernet management interface with active Telnet or SSH sessions can disconnect the active sessions. Removing a transport map from an interface, however, does not disconnect any active Telnet or SSH session.

- • Configuring the diagnostic and wait banners is optional, but recommended. The banners are especially useful as indicators to users about the status of their Telnet or SSH attempts.

Console Port Overview

The console port on the router is an EIA/TIA-232 asynchronous, serial connection with no flow control and an RJ-45 connector. The console port is used to access the router and is located on the front panel of the Route Processor.

For information on accessing the router using the console port, see Using Cisco IOS XE Software.

Console Port Handling Overview

If you are using the console port to access the router, you are automatically directed to the Cisco IOS command-line interface (CLI).

If you are trying to access the router through the console port and send a break signal (by entering **Ctrl-C** or **Ctrl-Shift-6**, or by entering the **send break** command at the Telnet prompt) before connecting to the CLI, you are directed to a diagnostic mode if the non-RPIOS subpackages are accessible. These settings can be changed by configuring a transport map for the console port and applying that transport map to the console interface.

Telnet and SSH Overview

Telnet and SSH on the router can be configured and handled like Telnet and SSH on other Cisco platforms. For information on traditional Telnet, see the line command in the Cisco IOS Terminal Services Command Reference, Release 12.2 document. For more information on AAA authentiction methods, see the line command in the Authentication Commands chapter.

For information on configuring traditional SSH, see the "Configuring Secure Shell" chapter in the Cisco IOS Terminal Services Command Reference, Release 12.2 document.

On the router, persistent Telnet and persistent SSH allow network administrators to more clearly define the treatment of incoming traffic when users access the router through the management ethernet port using Telnet or SSH. Notably, persistent Telnet and persistent SSH provide more robust network access by allowing the router to be configured to be accessible through the Ethernet management port using Telnet or SSH even when the Cisco IOS process has failed.

Persistent Telnet and Persistent SSH Overview

In traditional Cisco routers, accessing the router using Telnet or SSH is not possible if the Cisco IOS software fails. When Cisco IOS fails on a traditional Cisco router, the only method of accessing the router is through the console port. Similarly, if all the active Cisco IOS processes have failed on a router that is not using persistent Telnet or persistent SSH, the only method of accessing the router is through the console port.

However, with persistent Telnet and persistent SSH, you can configure a transport map that defines the treatment of incoming Telnet or SSH traffic on the Ethernet management interface. Among the many configuration options, a transport map can be configured to direct all traffic to the Cisco IOS CLI, diagnostic mode, or to wait for a Cisco IOS VTY line to become available and then direct users to diagnostic mode when a user sends a break signal while waiting for the IOS VTY line to become available. If a user uses Telnet or SSH to access diagnostic mode, that Telnet or SSH connection will be usable even in scenarios when no Cisco IOS process is active. Therefore, persistent Telnet and persistent SSH introduce the ability to access the router via diagnostic mode when the Cisco IOS process is not active. For information on diagnostic mode, see Using Cisco IOS XE Software. For information on the options that are can be configured using persistent Telnet or persistent SSH transport maps, see Configuring Persistent Telnet, on page 5 and Configuring Persistent SSH, on page 7.

Configuring a Console Port Transport Map

This task describes how to configure a transport map for a console port interface on the router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **transport-map type console** *transport-map-name*
4. **connection wait** [**allow** [**interruptible**] | **none** [**disconnect**]]
5. (Optional) **banner** [**diagnostic** | **wait**] *banner-message*
6. **exit**
7. **transport type console** *console-line-number* **input** *transport-map-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> **enable**	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# **configure terminal**	Enters global configuration mode.
Step 3	**transport-map type console** *transport-map-name* **Example:** Router(config)# **transport-map type console consolehandler**	Creates and names a transport map for handling console connections, and enters transport map configuration mode.
Step 4	**connection wait** [**allow** [**interruptible**]	**none** [**disconnect**]] **Example:** Router(config-tmap)# **connection wait none**	Specifies how a console connection will be handled using this transport map. • **allow interruptible**—The console connection waits for a Cisco IOS VTY line to become available, and also allows users to enter diagnostic mode by interrupting a console connection that is waiting for a Cisco IOS VTY line to become available. This is the default setting. **Note** Users can interrupt a waiting connection by entering **Ctrl-C** or **Ctrl-Shift-6**. • **none**—The console connection immediately enters diagnostic mode.

	Command or Action	Purpose

Step 5	(Optional) **banner** [**diagnostic**	**wait**] *banner-message*
		
		Example:
		
		`Router(config-tmap)# `**`banner diagnostic X`**
		`Enter TEXT message. End with the character 'X'.`
		`--Welcome to Diagnostic Mode--`
		`X`
		`Router(config-tmap)#`
			(Optional) Creates a banner message that will be seen by users entering diagnostic mode or waiting for the Cisco IOS VTY line because of the console transport map configuration.
			
			• **diagnostic**—Creates a banner message seen by users directed to diagnostic mode because of the console transport map configuration.
			
			Note Users can interrupt a waiting connection by entering **Ctrl-C** or **Ctrl-Shift-6**.
			
			• **wait**—Creates a banner message seen by users waiting for Cisco IOS VTY to become available.
			
			• *banner-message*—Banner message, which begins and ends with the same delimiting character.

Step 6	**exit** **Example:** `Router(config-tmap)# `**`exit`**	Exits transport map configuration mode to re-enter global configuration mode.
Step 7	**transport type console** *console-line-number* **input** *transport-map-name* **Example:** `Router(config)# `**`transport type console 0 input consolehandler`**	Applies the settings defined in the transport map to the console interface. The *transport-map-name* for this command must match the *transport-map-name* defined in the **transport-map type console** command.

Examples

The following example shows how to create a transport map to set console port access policies and attach to console port 0:

```
Router(config)# transport-map type console consolehandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to diagnostic mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
Waiting for IOS vty line
X
Router(config-tmap)# exit
Router(config)# transport type console 0 input consolehandler
```

Configuring Persistent Telnet

For a persistent Telnet connection to access an Cisco IOS vty line on the router, local login authentication must be configured for the vty line (the **login** command in line configuration mode). If local login authentication is not configured, users will not be able to access Cisco IOS using a Telnet connection into the management Ethernet interface with an applied transport map. Diagnostic mode will still be accessible in this scenario.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **transport-map type persistent telnet** *transport-map-name*
4. **connection wait** [**allow** [**interruptible**] | **none** [**disconnect**]]
5. (Optional) **banner** [**diagnostic** | **wait**] *banner-message*
6. **transport interface gigabitethernet 0**
7. **exit**
8. **transport type persistent telnetinput** *transport-map-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> **enable**	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# **configure terminal**	Enters global configuration mode.
Step 3	**transport-map type persistent telnet** *transport-map-name* **Example:** Router(config)# **transport-map type persistent telnet telnethandler**	Creates and names a transport map for handling persistent Telnet connections, and enters transport map configuration mode.
Step 4	**connection wait** [**allow** [**interruptible**]	**none** [**disconnect**]] **Example:** Router(config-tmap)# **connection wait none**	Specifies how a persistent Telnet connection will be handled using this transport map: • **allow**—The Telnet connection waits for a Cisco IOS vty line to become available, and exits the router if interrupted. • **allow interruptible**—The Telnet connection waits for the Cisco IOS vty line to become available, and also allows user to enter diagnostic mode by interrupting

	Command or Action	**Purpose**
		a Telnet connection waiting for the Cisco IOS vty line to become available. This is the default setting.
		Note Users can interrupt a waiting connection by entering **Ctrl-C** or **Ctrl-Shift-6**.
		• **none**—The Telnet connection immediately enters diagnostic mode.
		• **none disconnect**—The Telnet connection does not wait for the Cisco IOS vty line and does not enter diagnostic mode, so all Telnet connections are rejected if no vty line is immediately available in the Cisco IOS software.

Step 5	(Optional) **banner** [**diagnostic** | **wait**] *banner-message*
	
	Example:
	
	`Router(config-tmap)#` **banner diagnostic X**
	`Enter TEXT message. End with the character 'X'.`
	--Welcome to Diagnostic Mode--
	X
	`Router(config-tmap)#`
		(Optional) Creates a banner message that will be seen by users entering diagnostic mode or waiting for the Cisco IOS vty line because of the persistent Telnet configuration.
		
		• **diagnostic**—Creates a banner message seen by users directed into diagnostic mode because of the persistent Telnet configuration.
		
		Note Users can interrupt a waiting connection by entering **Ctrl-C** or **Ctrl-Shift-6**.
		
		• **wait**—Creates a banner message seen by users waiting for the vty line to become available.
		
		• *banner-message*—The banner message, which begins and ends with the same delimiting character.

Step 6	**transport interface gigabitethernet 0** **Example:** `Router(config-tmap)#` **transport interface gigabitethernet 0**	Applies the transport map settings to the management Ethernet interface (interface gigabitethernet 0). Persistent Telnet can be applied only to the management Ethernet interface on the router. This step must be taken before applying the transport map to the management Ethernet interface.
Step 7	**exit** **Example:** `Router(config-tmap)#` **exit**	Exits transport map configuration mode to re-enter global configuration mode.
Step 8	**transport type persistent telnetinput** *transport-map-name* **Example:** `Router(config)#` **transport type persistent telnet input telnethandler**	Applies the settings defined in the transport map to the management Ethernet interface. The *transport-map-name* for this command must match the *transport-map-name* defined in the **transport-map type persistent telnet** command.

Examples

In the following example, a transport map that will make all Telnet connections wait for a Cisco IOS XE vty line to become available before connecting to the router, while also allowing the user to interrupt the process and enter diagnostic mode, is configured and applied to the management Ethernet interface (**interface gigabitethernet 0**).

A diagnostic and a wait banner are also configured.

The transport map is then applied to the interface when the **transport type persistent telnet input** command is entered to enable persistent Telnet.

```
Router(config)# transport-map type persistent telnet telnethandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to diagnostic mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
Waiting for IOS IOS Process--
X
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit
Router(config)# transport type persistent telnet input telnethandler
```

Configuring Persistent SSH

This task describes how to configure persistent SSH on the router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **transport-map type persistent ssh** *transport-map-name*
4. **connection wait** [**allow** [**interruptible**] | **none** [**disconnect**]]
5. **rsa keypair-name** *rsa-keypair-name*
6. (Optional) **authentication-retries** *number-of-retries*
7. (Optional) **banner** [**diagnostic** | **wait**] *banner-message*
8. (Optional) **time-out** *timeout-interval*
9. **transport interface gigabitethernet 0**
10. **exit**
11. **transport type persistent ssh input** *transport-map-name*

DETAILED STEPS

	Command or Action	**Purpose**
Step 1	enable	Enables privileged EXEC mode.
	Example:	Enter your password if prompted.

	Command or Action	Purpose
	Router> **enable**	
Step 2	**configure terminal** **Example:** Router# **configure terminal**	Enters global configuration mode.
Step 3	**transport-map type persistent ssh** *transport-map-name* **Example:** Router(config)# **transport-map type persistent telnet telnethandler**	Creates and names a transport map for handling persistent SSH connections, and enters transport map configuration mode.
Step 4	**connection wait** [**allow** [**interruptible**] | **none** [**disconnect**]] **Example:** Router(config-tmap)# **connection wait interruptible**	Specifies how a persistent SSH connection will be handled using this transport map: • **allow**—The SSH connection waits for a Cisco IOS VTY line to become available, and exits the router if interrupted. • **allow interruptible**—The SSH connection waits for the VTY line to become available, and also allows a user to enter diagnostic mode by interrupting an SSH connection waiting for the VTY line to become available. This is the default setting. **Note** Users can interrupt a waiting connection by entering **Ctrl-C** or **Ctrl-Shift-6**. • **none**—The SSH connection immediately enters diagnostic mode. • **none disconnect**—The SSH connection does not wait for the VTY line and does not enter diagnostic mode. Therefore, all SSH connections are rejected if no VTY line is immediately available.
Step 5	**rsa keypair-name** *rsa-keypair-name* **Example:** Router(config)# **rsa keypair-name sshkeys**	Names the RSA keypair to be used for persistent SSH connections. For persistent SSH connections, the RSA keypair name must be defined using this command in transport map configuration mode. The RSA keypair definitions defined elsewhere on the router, such as through the use of the **ip ssh rsa keypair-name** command, do not apply to persistent SSH connections. No *rsa-keypair-name* is defined by default.

	Command or Action	Purpose
Step 6	(Optional) **authentication-retries** *number-of-retries* **Example:** Router(config-tmap)# **authentication-retries 4**	(Optional) Specifies the number of authentication retries before dropping the connection. The default *number-of-retries* is 3.
Step 7	(Optional) **banner** [**diagnostic** | **wait**] *banner-message* **Example:** Router(config-tmap)# **banner diagnostic X** Enter TEXT message. End with the character 'X'. **--Welcome to Diagnostic Mode--** **X** Router(config-tmap)#	(Optional) Creates a banner message that will be seen by users entering diagnostic mode or waiting for the VTY line because of the persistent SSH configuration. • **diagnostic**—Creates a banner message seen by users directed to diagnostic mode because of the persistent SSH configuration. • **wait**—Creates a banner message seen by users waiting for the VTY line to become available. • *banner-message*—The banner message, which begins and ends with the same delimiting character.
Step 8	(Optional) **time-out** *timeout-interval* **Example:** Router(config-tmap)# **time-out 30**	(Optional) Specifies the SSH time-out interval, in seconds. The default *timeout-interval* is 120 seconds.
Step 9	**transport interface gigabitethernet 0** **Example:** Router(config-tmap)# **transport interface gigabitethernet 0**	Applies the transport map settings to the Ethernet management interface (interface gigabitethernet 0). Persistent SSH can be applied only to the Ethernet management interface on the router.
Step 10	**exit** **Example:** Router(config-tmap)# **exit**	Exits transport map configuration mode to re-enter global configuration mode.
Step 11	**transport type persistent ssh input** *transport-map-name* **Example:** Router(config)# **transport type persistent ssh input sshhandler**	Applies the settings defined in the transport map to the Ethernet management interface. The *transport-map-name* for this command must match the *transport-map-name* defined in the **transport-map type persistent ssh** command.

Examples

The following example shows a transport map that will make all SSH connections wait for the VTY line to become active before connecting to the router being configured and applied to the Ethernet management interface (interface gigabitethernet 0). The RSA keypair is named sshkeys.

This example only uses the commands required to configure persistent SSH.

```
Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow
Router(config-tmap)# rsa keypair-name sshkeys
Router(config-tmap)# transport interface gigabitethernet 0
Enter TEXT message. End with the character 'X'.
--Welcome to diagnostic mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
--Waiting for IOS IOS Process--
X
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit
Router(config)# transport type persistent telnet input telnethandler
```

In the following example, a transport map is configured and will apply the following settings to users attempting to access the Ethernet management port via SSH:

- SSH users will wait for the VTY line to become active, but will enter diagnostic mode if the attempt to access the Cisco IOS software through the VTY line is interrupted.

- The RSA keypair name is sshkeys.

- The connection allows one authentication retry.

- The banner `--Welcome to Diagnostic Mode--` will appear if diagnostic mode is entered as a result of SSH handling through this transport map.

- The banner `--Waiting for vty line--` will appear if the connection is waiting for the VTY line to become active.

- The transport map is then applied to the interface when the **transport type persistent ssh input** command is entered to enable persistent SSH:

```
Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# rsa keypair-name sshkeys
Router(config-tmap)# authentication-retries 1
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to diagnostic mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
--Waiting for vty line--
X
Router(config-tmap)# time-out 30
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit
Router(config)# transport type persistent ssh input sshhandler
```

Viewing Console Port, SSH, and Telnet Handling Configurations

Use the following commands to view console port, SSH, and Telnet handling configurations:

- **show transport-map**

- **show platform software configuration access policy**

Use the **show transport-map** command to view transport map configurations.

show transport-map [**all** | **name** *transport-map-name* | **type** [**console** | **persistent** [**ssh** | **telnet**]]]

This command can be used either in user EXEC mode or privileged EXEC mode.

Example

The following example shows transport maps that are configured on the router: a console port (`consolehandler`), persistent SSH (`sshhandler`), and persistent Telnet transport (`telnethandler`):

```
Router# show transport-map all
Transport Map:
Name: consolehandler
Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for the IOS CLI

bshell banner:

Welcome to Diagnostic Mode


Transport Map:
Name: sshhandler
Type: Persistent SSH Transport

Interface:
GigabitEthernet0

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for IOS prompt

Bshell banner:
Welcome to Diagnostic Mode


SSH:
Timeout: 120
Authentication retries: 5
RSA keypair: sshkeys

Transport Map:
Name: telnethandler
Type: Persistent Telnet Transport

Interface:
GigabitEthernet0

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for IOS process

Bshell banner:
```

```
Welcome to Diagnostic Mode


Transport Map:
Name: telnethandling1
Type: Persistent Telnet Transport

Connection:
Wait option: Wait Allow


Router# show transport-map type console
Transport Map:
Name: consolehandler
Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for the IOS CLI

Bshell banner:

Welcome to Diagnostic Mode


Router# show transport-map type persistent ssh
Transport Map:
Name: sshhandler
Type: Persistent SSH Transport

Interface:
GigabitEthernet0

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for IOS prompt

Bshell banner:

Welcome to Diagnostic Mode


SSH:
Timeout: 120
Authentication retries: 5
RSA keypair: sshkeys

Router# show transport-map type persistent telnet
Transport Map:
Name: telnethandler
Type: Persistent Telnet Transport

Interface:
GigabitEthernet0

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for IOS process
```

```
Bshell banner:

Welcome to Diagnostic Mode


Transport Map:
Name: telnethandling1
Type: Persistent Telnet Transport

Connection:
Wait option: Wait Allow


Router# show transport-map name telnethandler
Transport Map:
Name: telnethandler
Type: Persistent Telnet Transport

Interface:
GigabitEthernet0

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for IOS process

Bshell banner:

Welcome to Diagnostic Mode


Router# show transport-map name consolehandler
Transport Map:
Name: consolehandler
Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for the IOS CLI

Bshell banner:

Welcome to Diagnostic Mode


Router# show transport-map name sshhandler
Transport Map:
Name: sshhandler
Type: Persistent SSH Transport

Interface:
GigabitEthernet0

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for IOS prompt

Bshell banner:
```

```
Welcome to Diagnostic Mode


SSH:
Timeout: 120
Authentication retries: 5
RSA keypair: sshkeys

Router#
```

Use the **show platform software configuration access policy** command to view the current configurations for handling the incoming console port, SSH, and Telnet connections. The output of this command provides the current wait policy for each type of connection (Telnet, SSH, and console), as well as information on the currently configured banners.

Unlike the **show transport-map** command, the **show platform software configuration access policy** command is available in diagnostic mode so that it can be entered in scenarios where you need transport map configuration information, but cannot access the Cisco IOS CLI.

Example

```
Router# show platform software configuration access policy
The current access-policies

Method : telnet
Rule : wait
Shell banner:
Wait banner :

Method : ssh
Rule : wait
Shell banner:
Wait banner :

Method : console
Rule : wait with interrupt
Shell banner:
Wait banner :
```

Example

The following example shows the **show platform software configuration access policy** command being issued both before and after a new transport map for SSH are configured. During the configuration, the connection policy and banners are set for a persistent SSH transport map, and the transport map for SSH is enabled.

```
Router# show platform software configuration access policy
The current access-policies

Method : telnet
Rule : wait with interrupt
Shell banner:
Welcome to Diagnostic Mode

Wait banner :
Waiting for IOS Process
```

```
Method : ssh
Rule : wait
Shell banner:
Wait banner :

Method : console
Rule : wait with interrupt
Shell banner:
Wait banner :

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
Welcome to Diag Mode
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
Waiting for IOS
X
Router(config-tmap)# rsa keypair-name sshkeys
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit
Router(config)# transport type persistent ssh input sshhandler
Router(config)# exit

Router# show platform software configuration access policy
The current access-policies

Method : telnet
Rule : wait with interrupt
Shell banner:
Welcome to Diagnostic Mode

Wait banner :
Waiting for IOS process


Method : ssh
Rule : wait with interrupt
Shell banner:
Welcome to Diag Mode

Wait banner :
Waiting for IOS


Method : console
Rule : wait with interrupt
Shell banner:
Wait banner :
```

Configuring Auxiliary Port for Modem Connection

Cisco 4000 Series ISR supports connecting a modem to the router auxiliary port for EXEC dial in connectivity. When a modem is connected to the auxiliary port, a remote user can dial in to the router and configure it. To configure a modem on the auxiliary port, perform these steps:

Step 1   Connect the RJ-45 end of the adapter cable to the black AUX port on the router.

Step 2   Use the **show line** command to determine the async interface of the AUX port:

```
Router# show  line

 Tty Typ     Tx/Rx      A Modem  Roty AccO AccI   Uses   Noise  Overruns   Int
*    0 CTY              -    -    -    - -   0    0    0/0    -
     1 AUX   9600/9600  -    -    -    - -   0    0    0/0    -
     2 VTY              -    -    -    - -   0    0    0/0    -
     3 VTY              -    -    -    - -   0    0    0/0    -
     4 VTY              -    -    -    - -   0    0    0/0    -
     5 VTY              -    -    -    - -   0    0    0/0    -
     6 VTY              -    -    -    - -   0    0    0/0    -
```

Step 3   Use the following commands to configure the router AUX line::

```
Router(config)# line 1

Router(config-line)#modem inOut
Router(config-line)#modem autoconfigure type usr_sportster
Router(config-line)#speed 115200  [Speed to be set according to the modem manual]
Router(config-line)#stopbits 1 [Stopbits to be set according to the modem manual]
Router(config-line)#transport input all
Router(config-line)#flowcontrol hardware [flowcontrol to be set according to the modem manual]
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#end
Router(config)#enable password lab
```

Step 4   Use the reverse telnet method on the modem to verify the modem connectivity and configuration string:

```
Router(config)#int loopback 0
Router(config-if)#ip add 1.1.1.1 255.255.255.0
Router(config-if)#end
Router#telnet 1.1.1.1 2001
Trying 1.1.1.1, 2001 ... Open

User Access Verification

Password: <enter the password given under line configuration>

at   <<<=== Modem command
OK  <<<=== This OK indicates that the modem is connected successully to the AUX port.
```

Step 5   Use an analog phone to verify that the phone line is active and functions properly. Then, connect the analog phone line to the modem.

Step 6   Initialize an EXEC modem call to the router from another device (PC) to test the modem connection.

Step 7   When the connection is established, the dial in client is prompted for a password. Enter the correct password.

Note: This password should match the one that is configured on the auxiliary port line.