Configure Telnet, Console, and AUX Port Passwords on Routers

Contents

Introduction
Prerequisites
Requirements
Components Used
Conventions
Background Information
Configure Passwords on the Line
Configuration Procedure
Verify the Configuration
Troubleshoot Log in Failure
Configure Local User-Specific Passwords
Configuration Procedure
Verify the Configuration
Troubleshoot User-specific Password Failure
Configure AUX Line Password
Configuration Procedure
Verify Configuration
Configure AAA Authentication for Log In
Configuration Procedure
Verify the Configuration
Troubleshoot AAA log in Failure
Related Information

Introduction

This document describes sample configurations to configure password protection for inbound EXEC connections to the router.

Prerequisites

Requirements

In order to perform the tasks described in this document, you must have privileged EXEC access to the router command line interface (CLI). For information about the command line and to understand command modes, see Use the Cisco IOS Command-Line Interface.

For instructions on connection of a console to your router, refer to the documentation that accompanied your router, or refer to the online documentation for your equipment.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 2509 router
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

**Conventions**

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

**Background Information**

The use of password protection to control or restrict access to the command line interface (CLI) of your router is one of the fundamental elements of an overall security plan.

To protect the router from unauthorized remote access, typically Telnet, is the most common security that needs to be configured, but to protect the router from unauthorized local access cannot be overlooked.

---

**Note:** Password protection is just one of the many steps to use in an effective in-depth network security regimen. Firewalls, access-lists, and control of physical access to the equipment are other elements that must be considered when you implement your security plan.

---

Command line, or EXEC, access to a router can be made in a number of ways, but in all cases the inbound connection to the router is made on a TTY line. There are four main types of TTY lines, as seen in this sample `show line` output:

```plaintext
<#root>
2509#
show line
  Tty
  Typ
    Tx/Rx A Modem Roty Acc0 AccI Uses Noise Overruns Int
    * 0 - - - - - 0 0 0/0 -
  
  CTY
    1 - - - - - 0 0 0/0 -

  TTY
    9600/9600 - - - - - 0 0 0/0 -
      2

  TTY
    9600/9600 - - - - - 0 0 0/0 -
      3

  TTY
    9600/9600 - - - - - 0 0 0/0 -
      4
```
<table>
<thead>
<tr>
<th>TTY</th>
<th>9600/9600</th>
<th>-</th>
<th>-</th>
<th>-</th>
<th>-</th>
<th>0</th>
<th>0</th>
<th>0/0</th>
<th>-</th>
</tr>
</thead>
<tbody>
<tr>
<td>TTY 5</td>
<td>9600/9600</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
</tr>
<tr>
<td>TTY 6</td>
<td>9600/9600</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
</tr>
<tr>
<td>TTY 7</td>
<td>9600/9600</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
</tr>
<tr>
<td>TTY 8</td>
<td>9600/9600</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
</tr>
<tr>
<td>TTY 9</td>
<td>9600/9600</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
</tr>
<tr>
<td>AUX 10</td>
<td>9600/9600</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
</tr>
<tr>
<td>VTY 11</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>VTY 12</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>VTY 13</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>VTY 14</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>VTY 15</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>

The **CTY** line-type is the Console Port. On any router, it appears in the router configuration as `line con 0` and in the output of the `show line` command as **cty**. The console port is mainly used for local system access with a console terminal.

The **TTY** lines are asynchronous lines used for inbound or outbound modem and terminal connections and can be seen in a router or access server configuration as `line x`. The specific line numbers are a function of the hardware built into or installed on the router or access server.
The **AUX** line is the Auxiliary port, seen in the configuration as `line aux 0`.

The **VTY** lines are the Virtual Terminal lines of the router, used solely to control inbound Telnet connections. They are virtual, in the sense that they are a function of software - there is no hardware associated with them. They appear in the configuration as `line vty 0 4`.

Each of these types of lines can be configured with password protection. Lines can be configured to use one password for all users, or for user-specific passwords. User-specific passwords can be configured locally on the router, or you can use an authentication server to provide authentication.

There is no prohibition against a configuration of different lines with different types of password protection. It is, in fact, common to see routers with a single password for the console and user-specific passwords for other inbound connections.

This is an example of router output from the `show running-config` command:

```
<#root> 2509#
show running-config
Building configuration...
Current configuration : 655 bytes
!
version 12.2
.
.
.
!--- Configuration edited for brevity

line con 0
line 1 8
line aux 0
line vty 0 4
!
end
```

**Configure Passwords on the Line**

To specify a password on a line, use the `password` command in line configuration mode. To enable a password check at the log in, use the `login` command in line configuration mode.

**Configuration Procedure**

In this example, a password is configured for all users who attempt to use the console.

1. From the privileged EXEC (or `enable`) prompt, enter configuration mode and then switch to line configuration mode with these commands. Notice that the prompt changes to reflect the current mode.

```
<#root>
```
router#

configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

router(config)#

line con 0

router(config-line)#

2. Configure the password, and enable password checking at log in.

<#root>

router(config-line)#

password letmein

router(config-line)#

login

3. Exit configuration mode.

<#root>

router(config-line)#

end

router#

%SYS-5-CONFIG_I: Configured from console by console

---

**Note**: Do not save configuration changes to line con 0 until your ability to log in has been verified.

**Note**: Under the line console configuration, `login` is a required configuration command to enable a password check when logging in. Console authentication requires both the `password` and the `login` commands to work.

---

**Verify the Configuration**

Examine the configuration of the router to verify that the commands have been properly entered:

- `show running-config` - displays the current configuration of the router.
show running-config

Building configuration...
...

!--- Lines omitted for brevity

!
line con 0

password letmein
login

line 1 8
line aux 0
line vty 0 4
!
end

To test the configuration, log off the console and log in again, and use the configured password to access the router:

<#root>

router#

exit

router con0 is now available
Press RETURN to get started.

User Access Verification
Password:

!--- Password entered here is not displayed by the router

router>

Note: Before you perform this test, ensure that you have an alternate connection into the router, such as Telnet or dial-in, in case there is a problem during log in back into the router.

Troubleshoot Log in Failure

If you cannot log back into the router and you have not saved the configuration, reload the router to eliminate any configuration changes you have made.

If the configuration changes were saved and you cannot log in to the router, perform a password recovery. See Password Recovery Procedures to find instructions for your particular platform.

Configure Local User-Specific Passwords
To establish a username-based authentication system, use the `username` command in global configuration mode. To enable a password check at log in, use the `login local` command in line configuration mode.

**Configuration Procedure**

In this example, passwords are configured for users who attempt to connect to the router on the VTY lines with Telnet.

1. From the privileged EXEC (or `enable`) prompt, enter configuration mode and enter username/password combinations, one for each user for whom you want to allow access to the router:

```
<#root>
router#
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#
username russ password montecito
username cindy password belgium
username mike password rottweiler
```

2. Switch to line configuration mode, and use these commands. Notice that the prompt changes to reflect the current mode.

```
<#root>
router(config)#
line vty 0 4
router(config-line)#
```

3. Configure a password check at log in.

```
<#root>
router(config-line)#
login local
```

4. Exit configuration mode.
Note: In order to disable auto Telnet when you type a name on the CLI, configure `no logging preferred` on the line that is used. While `transport preferred none` provides the same output, it also disables auto Telnet for the defined host that are configured with the `ip host` command. This is unlike the `no log preferred` command, which stops it for undefined hosts and lets it work for the defined ones.

Verify the Configuration

Examine the configuration of the router to verify that the commands have been properly entered:

- `show running-config` - displays the current configuration of the router.

```
<#root>
router#
  show running-config
Building configuration...
!
!--- Lines omitted for brevity
!

username russ password 0 montecito
username cindy password 0 belgium
username mike password 0 rottweiler
!
!--- Lines omitted for brevity
!
line con 0
line 1 8
line aux 0
line vty 0 4

login local
!
end
```
To test this configuration, a Telnet connection must be made to the router. This can be done if you connect from a different host on the network, but you can also test from the router itself through telnet to the IP address of any interface on the router that is in an up/up state as seen in the output of the `show interfaces` command.

Here is a sample output if the address of `interface ethernet 0` were 10.1.1.1:

```
<#root>
router#
telnet 10.1.1.1
Trying 10.1.1.1 ... Open

User Access Verification

Username: mike
Password:
!--- Password entered here is not displayed by the router

router
```

**Troubleshoot User-specific Password Failure**

Usernames and passwords are case-sensitive. Users who attempt to log in with an incorrectly cased username or password are rejected.

If users are unable to log into the router with their specific passwords, reconfigure the username and password on the router.

**Configure AUX Line Password**

In order to specify a password on the AUX line, issue the `password` command in line configuration mode. In order to enable a password check at log in, issue the `login` command in line configuration mode.

**Configuration Procedure**

In this example, a password is configured for all users who attempt to use the AUX port.

1. Issue the `show line` command in order to verify the line used by the AUX port.

```
<#root>
R1#
show line

Tty Typ Tx/Rx A Modem Roty AccO AccI Uses Noise Overruns Int
```
In this example, the AUX port is on line 65. Issue these commands in order to configure the router AUX line:

```bash
<#root>
R1# configure terminal
R1(config)# line 65
R1(config-line)# modem inout
R1(config-line)# speed 115200
R1(config-line)# transport input all
R1(config-line)# flowcontrol hardware
R1(config-line)# login
R1(config-line)# password cisco
R1(config-line)# end
R1#
```

### Verify Configuration

Examine the configuration of the router in order to verify that the commands have been properly entered:

- The `show running-config` command displays the current configuration of the router:

```bash
<#root>
R1# show running-config
```
Configure AAA Authentication for Log In

To enable authentication, authorization, and accounting (AAA) authentication for log ins, use the `login authentication` command in line configuration mode. AAA services must also be configured.

Configuration Procedure

In this example, the router is configured to retrieve users' passwords from a TACACS+ server when users attempt to connect to the router.

**Note:** Configuration of the router to use other types of AAA servers (RADIUS, for example) is similar. See Configure Authentication for additional information.

**Note:** This document does not address configuration of the AAA server itself.

1. From the privileged EXEC (or `enable`) prompt, enter configuration mode and enter the commands to configure the router to use AAA services for authentication:

```
<#root>
router#
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#
aaa new-model
router(config)#
aaa authentication login my-auth-list tacacs+
router(config)#
tacacs-server host 192.168.1.101
```
router(config)#
  tacacs-server key letmein

2. Switch to line configuration mode and use these commands. Notice that the prompt changes to reflect the current mode.

    <#root>
    router(config)#
    line 1 8
    router(config-line)#

3. Configure a password check at log in.

    <#root>
    router(config-line)#
    login authentication my-auth-list

4. Exit configuration mode.

    <#root>
    router(config-line)#
    end
    router#
    %SYS-5-CONFIG_I: Configured from console by console

Verify the Configuration

Examine the configuration of the router to verify that the commands have been properly entered:

  - show running-config - displays the current configuration of the router.

    <#root>
    router#
    write terminal
    Build configuration...
    Current configuration:
    !
To test this particular configuration, an inbound or outbound connection must be made to the line. See the [Modem - Router Connection Guide](#) for specific information on configuration of asynchronous lines for modem connections.

Alternately, you can configure one or more VTY lines to perform AAA authentication and perform your test thereupon.

**Troubleshoot AAA log in Failure**

Before you issue `debug` commands, see [Important Information on Debug Commands](#).

To troubleshoot a failed log in attempt, use the `debug` command appropriate to your configuration:

- `debug aaa authentication`
- `debug radius`
- `debug kerberos`

**Related Information**

- [Cisco IOS Debug Command Reference](#)
- [Cisco Technical Support and Downloads](#)