Telnet, Console and AUX Port Passwords on Cisco Routers Configuration Example

Contents

Introduction

This document provides sample configurations for configuring 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's command line interface (CLI). For information on using the command line and for understanding command modes, see Using the Cisco IOS Command-Line Interface.

For instructions on connecting 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
- Cisco IOS® Software Version 12.2(19)

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, make sure 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.

Protecting the router from unauthorized remote access, typically Telnet, is the most common security that needs configuring, but protecting the router from unauthorized local access cannot be overlooked.

Note: Password protection is just one of the many steps you should 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 implementing 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:

```
2509#show line
   Tty Typ     Tx/Rx    A Modem  Roty AccO AccI   Uses   Noise  Overruns   Int
*    0 CTY              -    -      -    -    -      0       0     0/0       -
     1 TTY   9600/9600  -    -      -    -    -      0       0     0/0       -
     2 TTY   9600/9600  -    -      -    -    -      0       0     0/0       -
     3 TTY   9600/9600  -    -      -    -    -      0       0     0/0       -
     4 TTY   9600/9600  -    -      -    -    -      0       0     0/0       -
     5 TTY   9600/9600  -    -      -    -    -      0       0     0/0       -
     6 TTY   9600/9600  -    -      -    -    -      0       0     0/0       -
     7 TTY   9600/9600  -    -      -    -    -      0       0     0/0       -
     8 TTY   9600/9600  -    -      -    -    -      0       0     0/0       -
     9 AUX   9600/9600  -    -      -    -    -      0       0     0/0       -
    10 VTY              -    -      -    -    -      0       0     0/0       -
    11 VTY              -    -      -    -    -      0       0     0/0       -
    12 VTY              -    -      -    -    -      0       0     0/0       -
    13 VTY              -    -      -    -    -      0       0     0/0       -
    14 VTY              -    -      -    -    -      0       0     0/0       -

2509#
```

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 using 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 configuring 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.

Below is an example of router output from the **show running-config** command:

```
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 password checking at login, use the **login** command in line configuration mode.

Configuration Procedure

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

1. From the privileged EXEC (or "enable") prompt, enter configuration mode and then switch to line configuration mode using the following commands. Notice that the prompt changes to reflect the current mode.
```
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 login.
```
router(config-line)#password letmein
router(config-line)#login
```

3. Exit configuration mode.

```
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 password checking at login. 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.

```
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, using the configured password to access the router:

```
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 performing this test, ensure that you have an alternate connection into the router, such as Telnet or dial-in, in case there is a problem logging back into the router.

Troubleshoot Login Failure

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

If the configuration changes were saved and you cannot login to the router, you will have to 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 password checking at login, use the **login local** command in line

configuration mode.

Configuration Procedure

In this example, passwords are configured for users attempting to connect to the router on the VTY lines using 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:
```
router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#username russ password montecito
router(config)#username cindy password belgium
router(config)#username mike password rottweiler
```

2. Switch to line configuration mode, using the following commands. Notice that the prompt changes to reflect the current mode.
```
router(config)#line vty 0 4
router(config-line)#
```
3. Configure password checking at login.
```
router(config-line)#login local
```

4. Exit configuration mode.
```
router(config-line)#end
router#
%SYS-5-CONFIG_I: Configured from console by console
```
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 logging 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.
```
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 by connecting from a different host on the network, but you can also test from the router itself by telnetting 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:

```
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 attempting to log in with an incorrectly cased username or password will be 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 password checking at login, issue the **login** command in line configuration mode.

Configuration Procedure

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

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

```
R1#show line

   Tty Typ     Tx/Rx    A Modem Roty AccO AccI  Uses  Noise  Overruns  Int
*    0 CTY                  -    -     -    -     -     0      0     0/0      -
    65 AUX  9600/9600  -    -     -    -    -    0     1     0/0             -
    66 VTY                 -    -     -    -     -     0      0     0/0      -
    67 VTY                 -    -     -    -     -     0      0     0/0      -
```

2. In this example, the AUX port is on line 65. Issue these commands in order to configure the router AUX line:

```
R1# conf t
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:

```
R1#show running-config
Building configuration...
!
!--- Lines omitted for brevity. line aux 0
 password cisco
 login
 modem InOut
 transport input all
 speed 115200
 flowcontrol hardware

!--- Lines omitted for brevity. ! end
```

Configure AAA Authentication for Login

To enable authentication, authorization, and accounting (AAA) authentication for logins, 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: Configuring the router to use other types of AAA servers (RADIUS, for example) is similar. See Configuring 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:

```
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 using the following commands. Notice that the prompt changes to reflect the current mode.

```
router(config)#line 1 8
router(config-line)#
```

3. Configure password checking at login.

```
router(config-line)#login authentication my-auth-list
```

4. Exit configuration mode.

```
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.

```
router#write terminal
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname router
!
aaa new-model
aaa authentication login my-auth-list tacacs+
!
!--- Lines omitted for brevity ... ! tacacs-server host 192.168.1.101
tacacs-server key letmein
!
line con 0
line 1 8
 login authentication my-auth-list
line aux 0
line vty 0 4
!
end
```

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 configuring async lines for modem connections.

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

Troubleshoot AAA Login Failure

Before issuing **debug** commands, see Important Information on Debug Commands.

To troubleshoot a failed login attempt, use the **debug** command appropriate to your configuration:

- debug aaa authentication
- debug radius
- debug kerberos

Related Information

- **Cisco IOS Debug Command Reference**
- **Technical Support - Cisco Systems**