Telnet/SSH Works Only If the Destination Host Is Specified as "Any" in the Extended Access Lists

Contents

Introduction

This document describes the supported Access Control List (ACL) structure that controls telnet access to a switch. This restriction applies to SSH as well, though the specific example below is only for telnet.

Problem

The user wants to allow telnet to the switch from just one host in the network. For example, only host 10.0.0.2 should be able to telnet to the switch IP 10.0.0.1.

Here is an example of a configuration that does not work on a Cisco IOS® version that does not have the fix for Cisco bug ID CSCuw89081 .

```
ip access-list extended 100
permit tcp host 10.0.0.2 host 10.0.0.1 eq telnet

line vty 0 4
access-class 100 in
transport input telnet
login
password cisco
```

For a Cisco IOS version that has the fix for Cisco bug ID CSCuw89081, the capability to match on a specific destination IP address has been added and this problem is not seen.

Solution

By design, access-class only matches the source IP address of the access-list. Access-class allows access to the router as a whole, not access to the router only on a particular router address. This behavior has changed through Cisco bug ID CSCuw89081.

Here is an example of a configuration that works on Cisco IOS that does not have the fix for Cisco bug ID CSCuw89081.

```
ip access-list extended 100
permit tcp host 10.0.0.2 any eq telnet

line vty 0 4
access-class 100 in
transport input telnet
login
password cisco
```