Telnet/SSHが機能するのは、拡張アクセスリストで宛先ホストが「Any」として指定されている場合のみ

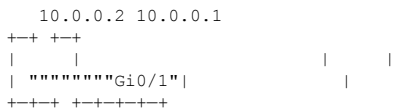
内容

概要

このドキュメントでは、スイッチへのTelnetアクセスを制御する、サポートされているアクセスコントロールリスト(ACL)構造について説明します。この制限はSSHにも適用されますが、次に示す特定の例はtelnet専用です。

問題

ユーザは、ネットワーク内の1つのホストからスイッチへのTelnetを許可したいと考えています。たとえば、ホスト10.0.0.2だけがスイッチIP 10.0.0.1にtelnetできます。



Cisco Bug ID CSCuw89081（登録ユーザ専用）の修正が適用されていないCisco IOS®バージョンで動作しない設定の例を次に示します。

```
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
```

Cisco Bug ID CSCuw89081の修正が適用されたCisco IOSバージョンでは、特定の宛先IPアドレスに一致する機能が追加されており、この問題は発生しません。

解決方法

設計上、access-classはアクセスリストの送信元IPアドレスだけに一致します。アクセスクラスは、特定のルータアドレス上のルータだけにアクセスするのではなく、ルータ全体へのアクセスを許可します。この動作は、Cisco Bug ID CSCuw89081で変更されました。

Cisco Bug ID CSCuw89081の修正がないCisco IOSで動作する設定例を次に示します。

```
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
```