

Telnet/SSH は宛先ホストが拡張アクセスリストで「どれでも」として規定されるときだけはたらいきまます

目次

[概要](#)

[問題](#)

[解決策](#)

概要

この資料はスイッチにサポートされた Access Control List (ACL) 構造をその制御 Telnetアクセス記述したものです。この制約事項は SSH に特定の下記の例が telnet のためだけであるけれども、同様に適用されます。

問題

ユーザはネットワークのちょうど 1 ホストからのスイッチに telnet を許可したいと思います。たとえば、ホストだけ 10.0.0.2 スイッチ IP 10.0.0.1 に Telnet で接続できますはずです。

```
10.0.0.2 10.0.0.1
+-----+ +-----+
| Host   |           |           |
|           |           |           |
|           |           |           |
+-----+ +-----+
```

Cisco バグ ID [CSCuw89081](#) のための修正がない Cisco IOS[®] バージョンで動作しない設定の例はここにあります。

```
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 バグ ID [CSCuw89081](#) のための修正がある Cisco IOSバージョンに関しては、特定の宛先 IP アドレスで一致するべき機能は追加され、この問題は見られません。

解決策

意図的に、access-class は access-list のソース IP アドレスだけと一致します。Access-class は特定のルータアドレスのだけルータにルータ全体にアクセスを、ないアクセス許可します。この動作は Cisco バグ ID [CSCuw89081](#) によって変化しました。

Cisco IOS で動作する設定の例はここにあります Cisco バグ ID [CSCuw89081](#) のための修正がない。

```
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
```