

# ダイヤルインターフェイスのアクセスリストの トラブルシューティング

## 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[トラブルシュートのヒント](#)

[関連情報](#)

## 概要

このドキュメントでは、ダイヤル インターフェイスのアクセス リストをトラブルシューティングする方法について説明します。

## 前提条件

### 要件

このドキュメントに関する固有の要件はありません。

### 使用するコンポーネント

この文書の情報は、Cisco 2500 ルータおよび Cisco IOS(R) ソフトウェア リリース 12.0.5.T に基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

### 表記法

ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

## トラブルシュートのヒント

- access-list がきちんとはたらかない場合、インターフェイスにリストを直接追加することを

試みて下さいたとえば:`interface async 1`

`ip access-group 101 in|out`ロジックが直接インターフェイスに適用されてはたらかない場合、サーバから渡されてはたつきません。 `show ip interface [name]` コマンドを使用すると、インターフェイスにアクセス リストが適用されているかどうかを確認できます。出力は基づいて `access-list` コマンドが適用するどのようにに変わりましたりしかし下記のものを含むことができますか:`Outgoing access list is not set`  
`Inbound access list is 101`

`Outgoing access list is not set`  
`Inbound access list is 101, default is not set`

`Outgoing access list is Async1#1, default is not set`  
`Inbound access list is Async1#0, default is not set`

- **access-list デバッグはと削除インターフェイスからのルートキャッシュの一時的にすることができます**:`interface async 1`

`no ip route-cache`イネーブル モードで次のように入力します。 `debug ip packet access-list`  
#有効になる **terminal monitor** コマンドでこれは通常ヒット用の画面に出力を送ります:`ICMP: dst (15.15.15.15) administratively prohibited unreachable sent to 1.1.1.2`

- **ヒットで増分を示すまた示します IPアクセスリスト 101 をすることができます**。 ログ パラメータはまた `access-list` コマンドの終わりにルータを示すために引き起こすために否定し  
追加することができます:`access-list 101 permit icmp 1.1.1.0 0.0.0.255 9.9.9.0 0.0.0.255`  
`log`

- **直接インターフェイスに適用されてとロジックは、取除くアクセス リストをはたらくインターフェイスからこと満足したら、AAA認証ネットワーク デフォルト tacacs を追加して下さい**|ユーザごとのアクセスコントロール アクセス・ コントロール・ リストを使用する場合半径は、 **terminal monitor** コマンドでデバッグ AAA 著者 ( および `debug aaa per-user` コマンド ) コマンド送信された アクセス リストを有効にし、観察します。RADIUS だけに関しては: RADIUSサーバがアトリビュート 11 ( フィルタid ) を #.in か #.out として規定されることを可能にしない場合デフォルトはあります。たとえば、サーバがアトリビュート 111 を送信すれば、これはルータによって "111.out." であると推定されます

- **access-list のコンテンツを示して下さい**:ユーザごとでないタイプのリストに関しては、アクセス リストのコンテンツを表示するために `show ip access-list 101` コマンドを使用して下さい:`Extended IP access list 101`  
`deny tcp any any (1649 matches)`  
`deny udp any any (35 matches)`

`deny icmp any any (36 matches)`リストのユーザごとの型に関しては、 `show ip access-lists`、か  
提示 IPアクセスリストを使用して下さい | ユーザごとまたは IPアクセスリスト Async1#1 を  
示して下さい:`Extended IP access list Async1#1 (per-user)`

`deny icmp host 171.68.118.244 host 9.9.9.10`  
`deny ip host 171.68.118.244 host 9.9.9.9`  
`permit ip host 171.68.118.244 host 9.9.9.10`  
`permit icmp host 171.68.118.244 host 9.9.9.9`

- **デバッグすべてがよく、検知するが access-list コマンドに予想されるようにはたつきません**  
:ほんのわずかがブロックされる場合、 `deny ip any any` に `access-list` を変更することを試みて下さい。それがはたらけばが、より早い1つが、問題はリストのロジックにあります。あまりがブロックされる場合、 `permit ip any any` に `access-list` を変更することを試みて下さい。それがはたらけばが、より早い1つが、問題はリストのロジックにあります。

## [関連情報](#)

- [TACACS/TACACS+ サポート](#)

- [RADIUS のサポート](#)
- [RFC](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)