

# Troubleshooting Access Lists on Dial Interfaces

Document ID: 13867

---

**Introduction**

**Prerequisites**

Requirements

Components Used

Conventions

**Troubleshoot Tips**

**NetPro Discussion Forums – Featured Conversations**

**Related Information**

---

## Introduction

This document contains information about how to troubleshoot access lists on dial interfaces.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

The information in this document is based on Cisco 2500 routers and Cisco IOS® Software Release 12.0.5.T.

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

Refer to Cisco Technical Tips Conventions for more information on document conventions.

## Troubleshoot Tips

- If the access-list does not work properly, try to apply the list directly to the interface, for example:

```
interface async 1
ip access-group 101 in|out
```

If the logic does not work applied directly to the interface, it does not work passed down from the server. The **show ip interface [name]** command can be used to see if the access-list is on the interface. Output varies based on how the access-list command is applied but can include:

```
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
```

- Some access-list debugging can be done with the temporarily removal of route-cache from the interface:

```
interface async 1
no ip route-cache
```

and then, while you are in enable mode, type:

```
debug ip packet access-list #
```

With the **terminal monitor** command enabled, this usually sends output to the screen for hits:

```
ICMP: dst (15.15.15.15) administratively prohibited unreachable sent to 1.1.1.2
```

- You can also do **show ip access-list 101**, which shows increments in hits. The log parameter can also be added at the end of the access-list command in order to cause the router to show denies:

```
access-list 101 permit icmp 1.1.1.0 0.0.0.255 9.9.9.0 0.0.0.255 log
```

- If you are satisfied that the logic works when applied directly to the interface, remove the access list from the interface, add the **aaa authorization network default tacacs|radius, debug aaa author** (and the **debug aaa per-user** command if you use per-user access control lists) commands with the **terminal monitor** command enabled and observe the access list sent down.

For RADIUS only: If the RADIUS server does not allow for attribute 11 (Filter-id) to be specified as #.in or #.out, the default is out. For example, if the server sends attribute 111, this is presumed by the router to be "111.out."

- Show the contents of an access-list:

For a non-per-user type of list, use the **show ip access-list 101** command in order to view the contents of the access list:

```
Extended IP access list 101
deny tcp any any (1649 matches)
deny udp any any (35 matches)
deny icmp any any (36 matches)
```

For a per-user type of list, use the **show ip access-lists**, or the **show ip access-list | per-user** or **show ip access-list Async1#1**:

```
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
```

- If all of the debug looks good, but the **access-list** command does not work as anticipated:
  - ◆ If too little is blocked, try to change the access-list to **deny ip any any**. If that works but the earlier one did not, the problem is in the logic of the list.
  - ◆ If too much is blocked, try to change the access-list to **permit ip any any**. If that works but the earlier one did not, the problem is in the logic of the list.

## NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the

most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

---

## Related Information

- **TACACS/TACACS+ Support**
  - **RADIUS Support**
  - **Requests for Comments**
  - **Technical Support & Documentation – Cisco Systems**
- 

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

---

Updated: Sep 14, 2005

Document ID: 13867

---