

Fehlerbehebung bei Zugriffslisten auf Wählschnittstellen

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Tipps zur Fehlerbehebung](#)

[Zugehörige Informationen](#)

[Einführung](#)

Dieses Dokument enthält Informationen zur Fehlerbehebung bei Zugriffslisten auf Wählschnittstellen.

[Voraussetzungen](#)

[Anforderungen](#)

Für dieses Dokument bestehen keine speziellen Anforderungen.

[Verwendete Komponenten](#)

Die Informationen in diesem Dokument basieren auf Cisco 2500-Routern und der Cisco IOS[®] Softwareversion 12.0.5.T.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

[Konventionen](#)

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

[Tipps zur Fehlerbehebung](#)

- Wenn die Zugriffsliste nicht ordnungsgemäß funktioniert, versuchen Sie, die Liste direkt auf die Schnittstelle anzuwenden, z. B.:

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

Wenn die Logik nicht direkt auf die Schnittstelle angewendet wird, funktioniert sie nicht, wenn sie vom Server übergeben wird. Mit dem Befehl **show ip interface [name]** kann überprüft werden, ob sich die Zugriffsliste auf der Schnittstelle befindet. Die Ausgabe hängt davon ab, wie der Befehl "access-list" angewendet wird, kann jedoch Folgendes beinhalten:

```
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
```

- Beim Debuggen von Zugriffslisten kann der Route-Cache vorübergehend aus der Schnittstelle entfernt werden:

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

und geben Sie im Aktivierungsmodus Folgendes ein:

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

Wenn der Befehl **terminal monitor** aktiviert ist, wird in der Regel eine Ausgabe für Treffer an den Bildschirm gesendet:

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

- Sie können auch **die ip access-list 101 anzeigen**, die die Anzahl der Treffer anzeigt. Der log-Parameter kann auch am Ende des Befehls access-list hinzugefügt werden, damit der Router eine Leugnung anzeigt:

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

- Wenn Sie sich davon überzeugt haben, dass die Logik funktioniert, wenn sie direkt auf die Schnittstelle angewendet wird, entfernen Sie die Zugriffsliste aus der Schnittstelle, fügen Sie die **AAA-Standardzugriffsdatacs|radius, debug aaa author** (und den Befehl **debug aa per user**, wenn Sie Zugriffskontrolllisten für einzelne Benutzer verwenden)-Befehle mit aktiviertem Terminalmonitor-Befehl ein, und beobachten Sie die heruntergesendete Zugriffsliste. Nur für RADIUS: Wenn der RADIUS-Server die Angabe von Attribut 11 (Filter-ID) als #.in oder #.out nicht zulässt, ist die Standardeinstellung "out" (out). Wenn der Server beispielsweise das Attribut 111 sendet, wird vom Router als "111.out" angenommen.

- Inhalt einer Zugriffsliste anzeigen: Bei Listen, die nicht benutzerspezifisch sind, verwenden Sie den Befehl **show ip access-list 101**, um den Inhalt der Zugriffsliste anzuzeigen:

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

Verwenden Sie für einen benutzerdefinierten Listentyp die **Zugriffslisten show ip** oder die **Zugriffsliste show ip. | pro Benutzer** oder **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
```

- Wenn das gesamte Debuggen gut aussieht, der Befehl **access-list** jedoch nicht wie erwartet funktioniert: Wenn zu wenig blockiert ist, versuchen Sie, die Zugriffsliste so zu ändern, dass **ip any (ip any any any) verweigert wird**. Wenn das funktioniert, aber das frühere nicht, ist das Problem in der Logik der Liste. Wenn zu viel blockiert ist, versuchen Sie, die Zugriffsliste zu

ändern, um **ip any any** zu **erlauben**. Wenn das funktioniert, aber das frühere nicht, ist das Problem in der Logik der Liste.

Zugehörige Informationen

- [Unterstützung von TACACS/TACACS+](#)
- [RADIUS-Unterstützung](#)
- [Kommentare](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)