# Диагностика списков доступа к интерфейсам вызова

## Содержание



## Введение

Этот документ содержит информацию о том, как устранить неполадки списков доступа на набираемых интерфейсах.

## Предварительные условия

### Требования

Для этого документа отсутствуют особые требования.

### Используемые компоненты

Сведения в этом документе основаны на маршрутизаторах Cisco 2500 с Cisco IOS® Software Release 12.0.5.T.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

### Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

## Советы устранения неполадок

- Если access-list не работает должным образом, попытайтесь применить список

непосредственно к интерфейсу, например:`interface async 1`
`ip access-group 101 in|out`Если логика не работает примененная непосредственно к интерфейсу, она не работает переданная от сервера. **Команда show ip interface [name]** может использоваться, чтобы видеть, находится ли access-list на интерфейсе. Выходные данные варьируются на основе того, как команда access-list применена, но может включать:
```
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
```

- Некоторая отладка access-list может быть сделана со временно удаление route-cache от интерфейса:`interface async 1`
`no ip route-cache`и далее, пока находитесь в режиме включения, введите:`debug ip packet access-list #`С включенной **командой terminal monitor** это обычно передает выходные данные к экрану для соответствий:`ICMP: dst (15.15.15.15) administratively prohibited unreachable sent to 1.1.1.2`
- **Вы можете так же просмотреть список доступа IP 101, показывающий увеличения попаданий.** Регистрационный параметр может также быть добавлен в конце команды access-list, чтобы заставить маршрутизатор показывать, запрещает:`access-list 101 permit icmp 1.1.1.0 0.0.0.255 9.9.9.0 0.0.0.255 log`
- Если вы удовлетворены, что логика работает, когда применено непосредственно к интерфейсу, удалите список доступа из интерфейса, добавьте **по умолчанию сети с проверкой подлинности AAA tacacs|radius**, **автор debug aaa** (и **команда debug aaa per-user**, если вы используете списки контроля доступа для каждого пользователя) команды с включенной **командой terminal monitor** и наблюдает список доступа, передаваемый вниз.Для RADIUS только: Если сервер RADIUS не обеспечивает атрибут 11 (Filter-Id), который будет задан как #.in или #.out, по умолчанию отсутствует. Например, если сервер передает атрибут 111, это, как предполагает маршрутизатор, "111.out".
- Покажите содержание access-list:Для типа недля каждого пользователя списка используйте **команду show ip access-list 101** для просмотра содержания списка доступа:
```
Extended IP access list 101
deny tcp any any (1649 matches)
deny udp any any (35 matches)
```
`deny icmp any any (36 matches)`Для типа для каждого пользователя списка используйте **show ip access-lists**, или **show ip access-list | для каждого пользователя** или **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
```
- Если вся отладка выглядит хорошей, но **команда access-list** не работает как предполагалось:Если слишком мало заблокировано, попытайтесь изменить access-list для **запрета ip любой любой**. Если это работает, но более ранний не сделал, проблема находится в логике списка.Если слишком много заблокировано, попытайтесь изменить access-list на **permit ip any any**. Если это работает, но более ранний не сделал, проблема находится в логике списка.

## Дополнительные сведения

- TACACS/TACACS + Поддержка
- Поддержка RADIUS
- Request For Comments
- Cisco Systems – техническая поддержка и документация