

# Применение списков доступа к интерфейсам вызова с использованием сервера RADIUS

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Схема сети](#)

[Определите нумерованные списки доступа на маршрутизаторе](#)

[Команды для других Cisco IOS Software Release](#)

[Конфигурации сервера – списки доступа на маршрутизаторе](#)

[Пример отладки маршрутизатора](#)

[Определите списки доступа на сервере](#)

[Команды для других Cisco IOS Software Release](#)

[Конфигурации сервера](#)

[Пример отладки маршрутизатора](#)

[Команды "debug"](#)

[Дополнительные сведения](#)

## Введение

Этот документ демонстрирует, как применить списки доступа для набора номера интерфейсов с сервером RADIUS. Существует два возможных метода:

- Определите нумерованный список доступа на маршрутизаторе, затем сошлитесь на нумерованный список доступа на сервере RADIUS. Большинство Версий программного обеспечения Cisco IOS поддерживает это. Например, определите нумерованный список доступа на маршрутизаторе и сошлитесь на них на сервере.
- Определите весь список доступа на сервере. Программное обеспечение Cisco IOS версии 11.3 или позже требуется для этого способа для каждого пользователя. Например, определите список доступа на сервере RADIUS (а не на NAS). Когда вызов соединяется, NAS аутентифицирует вызов с сервером RADIUS. Наряду с любой информацией для аутентификации, сервер возвращает список доступа к NAS, который это тогда применяется к набираемому интерфейсу.

**Примечание:** Для ISDN необходимо использовать способ для каждого пользователя, и необходимо настроить виртуальные профили на маршрутизаторе. Они описаны для программного обеспечения Cisco IOS версии 11.3 в [Виртуальных профилях Настройки](#).

## Предварительные условия

### Требования

Для этого документа отсутствуют особые требования.

### Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования.

- Программное обеспечение Cisco IOS версии 11.1 или позже (определяют списки доступа на маршрутизаторе),
- Программное обеспечение Cisco IOS версии 11.3 или позже (определяют списки доступа на сервере),
- Cisco Secure ACS UNIX или Cisco Secure ACS для Windows 2.x или Livingston RADIUS или MERIT RADIUS

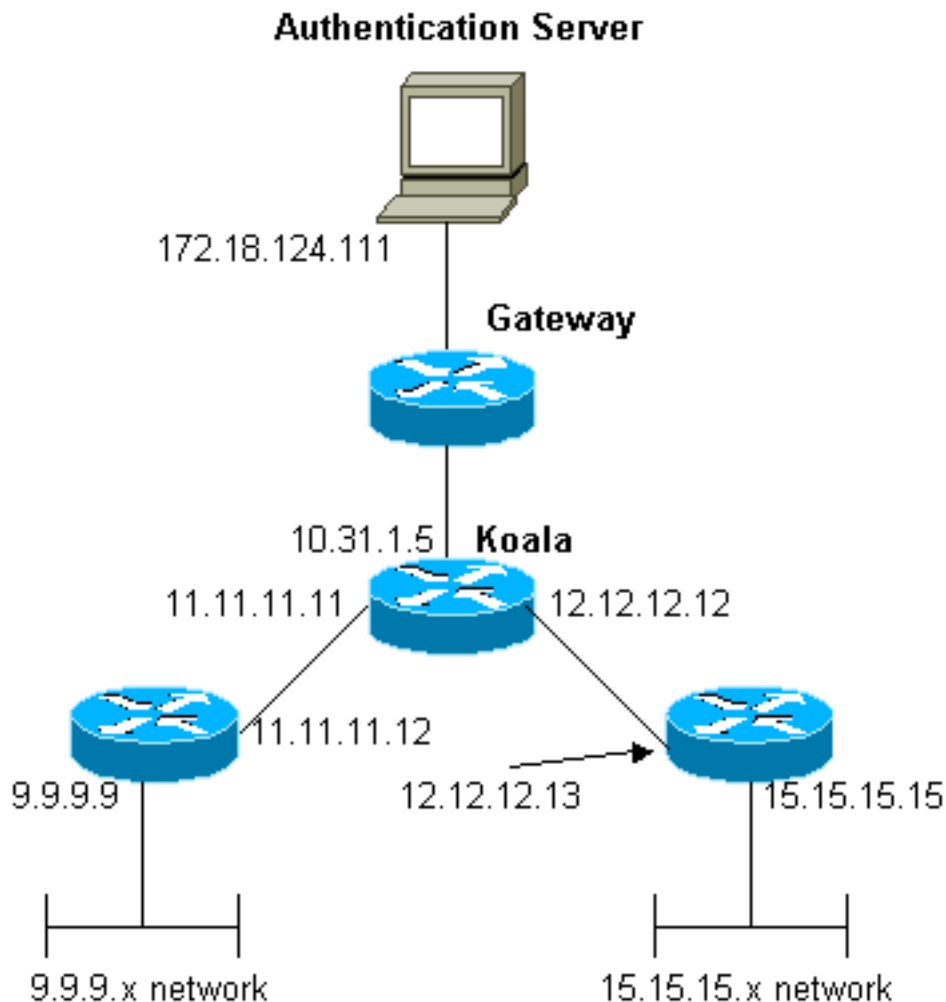
Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе с реальной сетью необходимо полностью осознавать возможные результаты использования всех команд.

### Условные обозначения

[Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.](#)

## Схема сети

Эта сеть используется в обоих примерах:



## Определите нумерованные списки доступа на маршрутизаторе

### Настройка маршрутизатора

```

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname koala
!
aaa new-model
!
!--- The following three lines of the configuration !---
!--- are specific to Cisco IOS Software Release 12.0.5.T and
!--- later. !--- See below this configuration for commands !-
!- for other Cisco IOS Software Releases. ! aaa
authentication login default local group radius aaa
authentication ppp default if-needed group radius aaa
authorization network default group radius enable secret
5 $1$mnZQ$g6XdsgVnnYjEa.17v.Pij1 enable password ww !
username john password 0 doe ! ip subnet-zero ! cns
event-service server ! interface Ethernet0 ip address
10.31.1.5 255.255.255.0 no ip directed-broadcast no mop
enabled ! interface Serial0 ip address 11.11.11.11

```

```
255.255.255.0 no ip directed-broadcast no ip mroute-
cache no fair-queue ! interface Serial1 ip address
12.12.12.12 255.255.255.0 no ip directed-broadcast !
interface Async1 ip unnumbered Ethernet0 no ip directed-
broadcast encapsulation ppp no ip route-cache no ip
mroute-cache async mode dedicated peer default ip
address pool mypool fair-queue 64 16 0 no cdp enable ppp
authentication chap ! ip local pool mypool 1.1.1.1
1.1.1.5 ip classless ip route 0.0.0.0 0.0.0.0 10.31.1.1
ip route 9.9.9.0 255.255.255.0 11.11.11.12 ip route
15.15.15.0 255.255.255.0 12.12.12.13 no ip http server !
access-list 101 permit icmp 1.1.1.0 0.0.0.255 9.9.9.0
0.0.0.255 access-list 101 permit tcp 1.1.1.0 0.0.0.255
15.15.15.0 0.0.0.255 !--- This is the access-list that
is specified by the RADIUS server. dialer-list 1
protocol ip permit dialer-list 1 protocol ipx permit !
radius-server host 172.18.124.111 auth-port 1645 acct-
port 1646 radius-server key cisco ! line con 0 transport
input none line 1 modem InOut transport input all
stopbits 1 speed 115200 flowcontrol hardware line 2 16
line aux 0 line vty 0 4 password ww ! end
```

## [Команды для других Cisco IOS Software Release](#)

**Примечание:** Для использования этих команд удалите команды полужирным из вышеупомянутой конфигурации и вставьте эти команды в, как продиктовано Cisco IOS Software Release.

## [Cisco IOS Software Release 11.3. 3. T до 12.0.5. T](#)

```
aaa authentication login default radius local
aaa authentication ppp default if-needed radius local
aaa authorization network default radius
```

## [Программное обеспечение Cisco IOS версии 11.1 до 11.3.3. T](#)

```
aaa authentication login default radius
aaa authentication ppp default if-needed radius
aaa authorization network radius
```

## [Конфигурации сервера – списки доступа на маршрутизаторе](#)

Эта процедура включает конфигурацию самого списка доступа на маршрутизаторе. Сервер RADIUS настроен с номером списка доступа, который применен. Когда вызов аутентифицируется, сервер RADIUS возвращает номер списка доступа к NAS, который тогда применяет соответствующий список доступа.

## [Конфигурация сервера - Cisco Secure ACS для Windows 2. X - RADIUS](#)

Выполните следующие действия:

1. В Параметрах пользователя заполните имя (имена) и пароль.
2. В Параметрах группы проверьте: Атрибут 6 - **обрамленный** Атрибут 7 - **PPP** Атрибут 11 - **Filter-Id**. В области ниже, **тип 101.in** **Примечание:** Атрибут 11 указывает, что применен список доступа 101. Гарантируйте, что access-list 101 настроен на маршрутизаторе.

## Конфигурация сервера - Cisco Secure ACS UNIX - RADIUS

```
rtp-evergreen# ./ViewProfile -p 9900 -u chaprtr
User Profile Information
user = chaprtr{
profile_id = 51
profile_cycle = 1
radius=Cisco {
check_items= {
2="chaprtr"
}
reply_attributes= {
6=2
7=1
11=101.in } } }
```

**Примечание:** Атрибут 11 указывает, что применен access-list 101. Гарантируйте, что access-list 101 настроен на маршрутизаторе.

## Конфигурация сервера - Livingston RADIUS

```
chaprtr Password = chaprtr
User-Service-Type = Framed-User,
Framed-Protocol = PPP,
Framed-Filter-Id = 101.in
```

**Примечание:** Это указывает, что применен access-list 101. Гарантируйте, что access-list 101 настроен на маршрутизаторе.

## Пример отладки маршрутизатора

```
koala#show debug General OS: AAA Authentication debugging is on AAA Authorization debugging is
on PPP: PPP protocol negotiation debugging is on Radius protocol debugging is on koala# *Mar 1
00:55:36.307: As1 LCP: I CONFREQ [Closed] id 0 len 23 *Mar 1 00:55:36.311: As1 LCP: ACCM
0x00000000 (0x020600000000) *Mar 1 00:55:36.311: As1 LCP: MagicNumber 0x00004CDD
(0x050600004CDD) *Mar 1 00:55:36.315: As1 LCP: PFC (0x0702) *Mar 1 00:55:36.319: As1 LCP: ACFC
(0x0802) *Mar 1 00:55:36.319: As1 LCP: Callback 6 (0x0D0306) *Mar 1 00:55:36.323: As1 LCP: Lower
layer not up, Fast Starting *Mar 1 00:55:36.323: As1 PPP: Treating connection as a dedicated
line *Mar 1 00:55:36.327: As1 PPP: Phase is ESTABLISHING, Active Open [0 sess, 0 load] *Mar 1
00:55:36.331: As1 AAA/AUTHOR/FSM: (0): LCP succeeds trivially *Mar 1 00:55:36.335: As1 LCP: O
CONFREQ [Closed] id 26 len 25 *Mar 1 00:55:36.339: As1 LCP: ACCM 0x000A0000 (0x0206000A0000)
*Mar 1 00:55:36.343: As1 LCP: AuthProto CHAP (0x0305C22305) *Mar 1 00:55:36.343: As1 LCP:
MagicNumber 0xE0512B4A (0x0506E0512B4A) *Mar 1 00:55:36.347: As1 LCP: PFC (0x0702) *Mar 1
00:55:36.347: As1 LCP: ACFC (0x0802) *Mar 1 00:55:36.355: As1 LCP: O CONFREQ [REQsent] id 0 len
7 *Mar 1 00:55:36.355: As1 LCP: Callback 6 (0x0D0306) 00:55:36: %LINK-3-UPDOWN: Interface
Asyncl, changed state to up *Mar 1 00:55:36.479: As1 LCP: I CONFACK [REQsent] id 26 len 25 *Mar
1 00:55:36.483: As1 LCP: ACCM 0x000A0000 (0x0206000A0000) *Mar 1 00:55:36.483: As1 LCP:
AuthProto CHAP (0x0305C22305) *Mar 1 00:55:36.487: As1 LCP: MagicNumber 0xE0512B4A
(0x0506E0512B4A) *Mar 1 00:55:36.491: As1 LCP: PFC (0x0702) *Mar 1 00:55:36.491: As1 LCP: ACFC
(0x0802) *Mar 1 00:55:36.495: As1 LCP: I CONFREQ [ACKrcvd] id 1 len 20 *Mar 1 00:55:36.499: As1
LCP: ACCM 0x00000000 (0x020600000000) *Mar 1 00:55:36.503: As1 LCP: MagicNumber 0x00004CDD
(0x050600004CDD) *Mar 1 00:55:36.503: As1 LCP: PFC (0x0702) *Mar 1 00:55:36.507: As1 LCP: ACFC
(0x0802) *Mar 1 00:55:36.511: As1 LCP: O CONFACK [ACKrcvd] id 1 len 20 *Mar 1 00:55:36.515: As1
LCP: ACCM 0x00000000 (0x020600000000) *Mar 1 00:55:36.515: As1 LCP: MagicNumber 0x00004CDD
(0x050600004CDD) *Mar 1 00:55:36.519: As1 LCP: PFC (0x0702) *Mar 1 00:55:36.519: As1 LCP: ACFC
(0x0802) *Mar 1 00:55:36.523: As1 LCP: State is Open *Mar 1 00:55:36.527: As1 PPP: Phase is
AUTHENTICATING, by this end [0 sess, 1 load] *Mar 1 00:55:36.531: As1 CHAP: O CHALLENGE id 8 len
26 from "koala" *Mar 1 00:55:36.647: As1 LCP: I IDENTIFY [Open] id 2 len 18 magic 0x00004CDD
MSRASV4.00 *Mar 1 00:55:36.651: As1 LCP: I IDENTIFY [Open] id 3 len 21 magic 0x00004CDD MSRAS-1-
ZEKIE *Mar 1 00:55:36.655: As1 CHAP: I RESPONSE id 8 len 28 from "chaprtr" *Mar 1 00:55:36.663:
AAA: parse name=Asyncl idb type=10 tty=1 *Mar 1 00:55:36.667: AAA: name=Asyncl flags=0x11 type=4
```

shelf=0 slot=0 adapter=0 port=1 channel=0 \*Mar 1 00:55:36.671: AAA/MEMORY: create\_user (0x4E9DF4) user='chaprttr' ruser='' port='Async1' rem\_addr='async' authen\_type=CHAP service=PPP priv=1 \*Mar 1 00:55:36.675: AAA/AUTHEN/START (128288046): port='Async1' list='' action=LOGIN service=PPP \*Mar 1 00:55:36.675: AAA/AUTHEN/START (128288046): using "default" list \*Mar 1 00:55:36.679: AAA/AUTHEN (128288046): status = UNKNOWN \*Mar 1 00:55:36.679: AAA/AUTHEN/START (128288046): Method=radius (radius) \*Mar 1 00:55:36.683: RADIUS: ustruct sharecount=1 \*Mar 1 00:55:36.687: RADIUS: Initial Transmit Async1 id 8 172.18.124.111:1645, Access-Request, len 78 \*Mar 1 00:55:36.691: Attribute 4 6 0A1F0105 \*Mar 1 00:55:36.695: Attribute 5 6 00000001 \*Mar 1 00:55:36.695: Attribute 61 6 00000000 \*Mar 1 00:55:36.695: Attribute 1 9 63686170 \*Mar 1 00:55:36.699: Attribute 3 19 08E468A8 \*Mar 1 00:55:36.699: Attribute 6 6 00000002 \*Mar 1 00:55:36.703: Attribute 7 6 00000001 \*Mar 1 00:55:36.835: RADIUS: Received from id 8 172.18.124.111:1645, Access-Accept, len 40 \*Mar 1 00:55:36.839: Attribute 6 6 00000002 \*Mar 1 00:55:36.843: Attribute 7 6 00000001 \*Mar 1 00:55:36.843: Attribute 11 8 3130312E \*Mar 1 00:55:36.851: AAA/AUTHEN (128288046): status = PASS \*Mar 1 00:55:36.855: As1 AAA/AUTHOR/LCP: Authorize LCP \*Mar 1 00:55:36.855: As1 AAA/AUTHOR/LCP (821299011): Port='Async1' list='' service=NET \*Mar 1 00:55:36.859: AAA/AUTHOR/LCP: As1 (821299011) user='chaprttr' \*Mar 1 00:55:36.859: As1 AAA/AUTHOR/LCP (821299011): send AV service=ppp \*Mar 1 00:55:36.863: As1 AAA/AUTHOR/LCP (821299011): send AV protocol=lcp \*Mar 1 00:55:36.863: As1 AAA/AUTHOR/LCP (821299011): found list "default" \*Mar 1 00:55:36.867: As1 AAA/AUTHOR/LCP (821299011): Method=radius (radius) \*Mar 1 00:55:36.871: As1 AAA/AUTHOR (821299011): Post authorization status = PASS\_REPL \*Mar 1 00:55:36.871: As1 AAA/AUTHOR/LCP: Processing AV service=ppp \*Mar 1 00:55:36.879: As1 CHAP: O SUCCESS id 8 len 4 \*Mar 1 00:55:36.883: As1 PPP: Phase is UP [0 sess, 1 load] \*Mar 1 00:55:36.887: As1 AAA/AUTHOR/FSM: (0): Can we start IPCP? \*Mar 1 00:55:36.887: As1 AAA/AUTHOR/FSM (3701006396): Port='Async1' list='' service=NET \*Mar 1 00:55:36.891: AAA/AUTHOR/FSM: As1 (3701006396) user='chaprttr' \*Mar 1 00:55:36.891: As1 AAA/AUTHOR/FSM (3701006396): send AV service=ppp \*Mar 1 00:55:36.895: As1 AAA/AUTHOR/FSM (3701006396): send AV protocol=ip \*Mar 1 00:55:36.899: As1 AAA/AUTHOR/FSM (3701006396): found list "default" \*Mar 1 00:55:36.899: As1 AAA/AUTHOR/FSM (3701006396): Method=radius (radius) \*Mar 1 00:55:36.903: As1 AAA/AUTHOR (3701006396): Post authorization status = PASS\_REPL \*Mar 1 00:55:36.907: As1 AAA/AUTHOR/FSM: We can start IPCP \*Mar 1 00:55:36.915: As1 IPCP: O CONFREQ [Closed] id 5 len 10 \*Mar 1 00:55:36.915: As1 IPCP: Address 10.31.1.5 (0x03060A1F0105) \*Mar 1 00:55:36.923: As1 AAA/AUTHOR/FSM: (0): Can we start CDPCP? \*Mar 1 00:55:36.923: As1 AAA/AUTHOR/FSM (3075092411): Port='Async1' list='' service=NET \*Mar 1 00:55:36.927: AAA/AUTHOR/FSM: As1 (3075092411) user='chaprttr' \*Mar 1 00:55:36.931: As1 AAA/AUTHOR/FSM (3075092411): send AV service=ppp \*Mar 1 00:55:36.931: As1 AAA/AUTHOR/FSM (3075092411): send AV protocol=cdp \*Mar 1 00:55:36.935: As1 AAA/AUTHOR/FSM (3075092411): found list "default" \*Mar 1 00:55:36.935: As1 AAA/AUTHOR/FSM (3075092411): Method=radius (radius) \*Mar 1 00:55:36.939: RADIUS: unknown proto "cdp" in acl-check \*Mar 1 00:55:36.943: RADIUS: Filter-Id 101 out of range for protocol cdp. Ignoring. \*Mar 1 00:55:36.943: As1 AAA/AUTHOR (3075092411): Post authorization status = PASS\_REPL \*Mar 1 00:55:36.947: As1 AAA/AUTHOR/FSM: We can start CDPCP \*Mar 1 00:55:36.951: As1 CDPCP: O CONFREQ [Closed] id 5 len 4 \*Mar 1 00:55:36.987: As1 CCP: I CONFREQ [Not negotiated] id 4 len 12 \*Mar 1 00:55:36.991: As1 CCP: OUI (0x0002) \*Mar 1 00:55:36.991: As1 CCP: MS-PPC supported bits 0x00007080 (0x120600007080) \*Mar 1 00:55:36.999: As1 LCP: O PROTREJ [Open] id 27 len 18 protocol CCP (0x80FD0104000C0002120600007080) \*Mar 1 00:55:37.003: As1 IPCP: I CONFREQ [REQsent] id 5 len 40 \*Mar 1 00:55:37.007: As1 IPCP: CompressType VJ 15 slots CompressSlotID (0x0206002D0F01) \*Mar 1 00:55:37.011: As1 IPCP: Address 0.0.0.0 (0x030600000000) \*Mar 1 00:55:37.015: As1 IPCP: PrimaryDNS 0.0.0.0 (0x810600000000) \*Mar 1 00:55:37.019: As1 IPCP: PrimaryWINS 0.0.0.0 (0x820600000000) \*Mar 1 00:55:37.023: As1 IPCP: SecondaryDNS 0.0.0.0 (0x830600000000) \*Mar 1 00:55:37.027: As1 IPCP: SecondaryWINS 0.0.0.0 (0x840600000000) \*Mar 1 00:55:37.027: As1 AAA/AUTHOR/IPCP: Start. Her address 0.0.0.0, we want 0.0.0.0 \*Mar 1 00:55:37.031: As1 AAA/AUTHOR/IPCP: Processing AV service=ppp \*Mar 1 00:55:37.035: As1 AAA/AUTHOR/IPCP: Processing AV inacl=101 !--- Note that acl 101 is applied to the dialer interface. \*Mar 1 00:55:37.035: As1 AAA/AUTHOR/IPCP: Authorization succeeded \*Mar 1 00:55:37.039: As1 AAA/AUTHOR/IPCP: Done. Her address 0.0.0.0, we want 0.0.0.0 \*Mar 1 00:55:37.043: As1 IPCP: Pool returned 1.1.1.1 \*Mar 1 00:55:37.047: As1 IPCP: O CONFREQ [REQsent] id 5 len 28 \*Mar 1 00:55:37.051: As1 IPCP: CompressType VJ 15 slots CompressSlotID (0x0206002D0F01) \*Mar 1 00:55:37.055: As1 IPCP: PrimaryWINS 0.0.0.0 (0x820600000000) \*Mar 1 00:55:37.059: As1 IPCP: SecondaryDNS 0.0.0.0 (0x830600000000) \*Mar 1 00:55:37.063: As1 IPCP: SecondaryWINS 0.0.0.0 (0x840600000000) \*Mar 1 00:55:37.067: As1 IPCP: I CONFACK [REQsent] id 5 len 10 \*Mar 1 00:55:37.071: As1 IPCP: Address 10.31.1.5 (0x03060A1F0105) \*Mar 1 00:55:37.075: As1 LCP: I PROTREJ [Open] id 6 len 10 protocol CDPCP (0x820701050004) \*Mar 1 00:55:37.079: As1 CDPCP: State is Closed \*Mar 1 00:55:37.183: As1 IPCP: I CONFREQ [ACKrcvd] id 7 len 16 \*Mar 1 00:55:37.187: As1 IPCP: Address 0.0.0.0 (0x030600000000) \*Mar 1 00:55:37.191: As1 IPCP: PrimaryDNS 0.0.0.0 (0x810600000000) \*Mar 1 00:55:37.191: As1 AAA/AUTHOR/IPCP: Start. Her address 0.0.0.0, we want 1.1.1.1 \*Mar 1

```
00:55:37.195: As1 AAA/AUTHOR/IPCP: Processing AV service=ppp *Mar 1 00:55:37.199: As1
AAA/AUTHOR/IPCP: Processing AV inacl=101 *Mar 1 00:55:37.199: As1 AAA/AUTHOR/IPCP: Authorization
succeeded *Mar 1 00:55:37.203: As1 AAA/AUTHOR/IPCP: Done. Her address 0.0.0.0, we want 1.1.1.1
*Mar 1 00:55:37.207: As1 IPCP: O CONFNAK [ACKrcvd] id 7 len 16 *Mar 1 00:55:37.211: As1 IPCP:
Address 1.1.1.1 (0x030601010101) *Mar 1 00:55:37.215: As1 IPCP: PrimaryDNS 172.18.125.3
(0x8106AC127D03) *Mar 1 00:55:37.327: As1 IPCP: I CONFREQ [ACKrcvd] id 8 len 16 *Mar 1
00:55:37.331: As1 IPCP: Address 1.1.1.1 (0x030601010101) *Mar 1 00:55:37.335: As1 IPCP:
PrimaryDNS 172.18.125.3 (0x8106AC127D03) *Mar 1 00:55:37.335: As1 AAA/AUTHOR/IPCP: Start. Her
address 1.1.1.1, we want 1.1.1.1 *Mar 1 00:55:37.343: As1 AAA/AUTHOR/IPCP (408915304):
Port='Async1' list='' service=NET *Mar 1 00:55:37.347: AAA/AUTHOR/IPCP: As1 (408915304)
user='chaprtr' *Mar 1 00:55:37.347: As1 AAA/AUTHOR/IPCP (408915304): send AV service=ppp *Mar 1
00:55:37.351: As1 AAA/AUTHOR/IPCP (408915304): send AV protocol=ip *Mar 1 00:55:37.355: As1
AAA/AUTHOR/IPCP (408915304): send AV addr*1.1.1.1 *Mar 1 00:55:37.355: As1 AAA/AUTHOR/IPCP
(408915304): found list "default" *Mar 1 00:55:37.359: As1 AAA/AUTHOR/IPCP (408915304):
Method=radius (radius) *Mar 1 00:55:37.363: As1 AAA/AUTHOR (408915304): Post authorization
status = PASS_REPL *Mar 1 00:55:37.367: As1 AAA/AUTHOR/IPCP: Reject 1.1.1.1, using 1.1.1.1 *Mar
1 00:55:37.375: As1 AAA/AUTHOR/IPCP: Processing AV service=ppp *Mar 1 00:55:37.375: As1
AAA/AUTHOR/IPCP: Processing AV inacl=101 *Mar 1 00:55:37.379: As1 AAA/AUTHOR/IPCP: Processing AV
addr*1.1.1.1 *Mar 1 00:55:37.379: As1 AAA/AUTHOR/IPCP: Authorization succeeded *Mar 1
00:55:37.383: As1 AAA/AUTHOR/IPCP: Done. Her address 1.1.1.1, we want 1.1.1.1 *Mar 1
00:55:37.387: As1 IPCP: O CONFACK [ACKrcvd] id 8 len 16 *Mar 1 00:55:37.391: As1 IPCP: Address
1.1.1.1 (0x030601010101) *Mar 1 00:55:37.395: As1 IPCP: PrimaryDNS 172.18.125.3 (0x8106AC127D03)
*Mar 1 00:55:37.399: As1 IPCP: State is Open *Mar 1 00:55:37.727: As1 IPCP: Install route to
1.1.1.1 *Mar 1 00:55:37: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async1, changed state
to up koala#
```

## Определите списки доступа на сервере

**Примечание:** Инструкции маршрута не должны быть переданы от сервера до маршрутизатора; набираемый пользователь обычно поднимает маршруты с маршрутизатора. Присутствие инструкций маршрута на маршрутизаторе зависит от того, должны ли маршруты быть переданы от сервера или подняты с маршрутизатора. Однако в данном примере, список доступа и инструкции маршрута переданы.

```
ip route 9.9.9.0 255.255.255.0 11.11.11.12
ip route 15.15.15.0 255.255.255.0 12.12.12.13
```

В этом примере конфигурации, передавая маршруты от сервера только для целей иллюстрации.

### Настройка маршрутизатора

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname koala
!
aaa new-model
!
!--- The following three lines of the configuration are
!--- specific to Cisco IOS Software Release 12.0.5.T and
later. !--- See below this configuration for commands !-
-- for other Cisco IOS Software Releases. ! aaa
authentication login default group radius none aaa
authentication ppp default if-needed group radius aaa
authorization network default group radius enable secret
5 $1$mNzQ$g6XdsgVnnYjEa.l7v.Pijl enable password ww !
username john password 0 doe ! ip subnet-zero ! cns
```



```
event-service server ! interface Ethernet0 ip address
10.31.1.5 255.255.255.0 no ip directed-broadcast no mop
enabled ! interface Serial0 ip address 11.11.11.11
255.255.255.0 no ip directed-broadcast no ip mroute-
cache no fair-queue ! interface Serial1 ip address
12.12.12.12 255.255.255.0 no ip directed-broadcast !
interface Async1 ip unnumbered Ethernet0 no ip directed-
broadcast encapsulation ppp no ip route-cache no ip
mroute-cache async mode dedicated peer default ip
address pool mypool fair-queue 64 16 0 no cdp enable ppp
authentication chap ! ip local pool mypool 1.1.1.1
1.1.1.5 ip classless ip route 0.0.0.0 0.0.0.0 10.31.1.1
ip route 172.17.192.0 255.255.255.0 10.31.1.1 ip route
172.18.124.0 255.255.255.0 10.31.1.1 ip route
172.18.125.0 255.255.255.0 10.31.1.1 no ip http server !
dialer-list 1 protocol ip permit dialer-list 1 protocol
ipx permit ! radius-server host 172.18.124.111 auth-port
1645 acct-port 1646 radius-server key cisco ! line con 0
transport input none line 1 autoselect during-login
autoselect ppp modem InOut transport input all stopbits
1 speed 115200 flowcontrol hardware line 2 16 line aux 0
line vty 0 4 password ww ! end
```

## [Команды для других Cisco IOS Software Release](#)

**Примечание:** Для использования этих команд удалите команды полужирным из вышеупомянутой конфигурации и вставьте эти команды в, как продиктовано Cisco IOS Software Release.

### [Cisco IOS Software Release 11.3. 3. T до 12.0.5. T](#)

```
aaa authentication login default radius local
aaa authentication ppp default if-needed radius local
aaa authorization network default radius
```

### [Программное обеспечение Cisco IOS версии 11.3 до 11.3.3. T](#)

```
aaa authentication login default radius
aaa authentication ppp default if-needed radius
aaa authorization network radius
```

## [Конфигурации сервера](#)

### [Конфигурация сервера - Cisco Secure ACS UNIX - RADIUS](#)

```
# ./ViewProfile -p 9900 -u chaprtr
User Profile Information
user = chaprtr{
profile_id = 31
profile_cycle = 1
radius=Cisco {
check_items= {
2="chaprtr"
}
reply_attributes= {
6=2
7=1
9,1="ip:route#1=9.9.9.9 255.255.255.255 11.11.11.12"
9,1="ip:route#2=15.15.15.15 255.255.255.255 12.12.12.13"
9,1="ip:route#3=15.15.15.16 255.255.255.255 12.12.12.13"
```



```
9,1="ip:inacl#1=permit icmp 1.1.1.0 0.0.0.255 9.9.9.0 0.0.0.255" 9,1="ip:inacl#2=permit tcp
1.1.1.0 0.0.0.255 15.15.15.0 0.0.0.255" !--- The access-list to be applied is specified. !---
Note that the number after inacl# increments for each line of the access-list. } } }
```

## Конфигурация сервера - Cisco Secure ACS для Windows 2.x - RADIUS

Выполните следующие действия:

1. В Параметрах пользователя заполните имя (имена) и пароль.
2. В Параметрах группы проверьте: Атрибут 6 - **обрамленный** Атрибут 7 - PPP
3. Под Атрибутами сервера RADIUS для Cisco проверьте [009\001] пару значение-атрибут

и введите следующий текст в коробке внизу:  
ip:route#1=9.9.9.9 255.255.255.254  
11.11.11.12  
ip:route#2=15.15.15.15 255.255.255.255 12.12.12.13  
ip:route#3=15.15.15.16 255.255.255.255 12.12.12.13  
ip:inacl#1=permit icmp 1.1.1.0 0.0.0.255 9.9.9.0 0.0.0.255 ip:inacl#2=permit tcp 1.1.1.0  
0.0.0.255 15.15.15.0 0.0.0.255 !--- The access-list to be applied is specified. !--- Note  
that the number after inacl# increments for !--- each line of the access-list.

## Конфигурация сервера - MERIT RADIUS

**Примечание:** Это конфигурации допустимо для версии 3.6b MERIT RADIUS или более поздних версий тот Cisco поддержки ав-пары.

```
chaptrtr Password = "chaptrtr",
Service-Type = Framed,
Framed-Protocol = PPP,
Framed-IP-Address = 255.255.255.254
Cisco:Avpair="ip:route#1=9.9.9.9 255.255.255.255 11.11.11.12"
Cisco:Avpair="ip:route#2=15.15.15.15 255.255.255.255 12.12.12.13"
Cisco:Avpair="ip:route#3=15.15.15.16 255.255.255.255 12.12.12.13"
Cisco:Avpair="ip:inacl#1=permit icmp 1.1.1.0 0.0.0.255 9.9.9.0 0.0.0.255"
Cisco:Avpair="ip:inacl#2=permit tcp 1.1.1.0 0.0.0.255 15.15.15.0 0.0.0.255" !--- The access-list
to be applied is specified. ! --- Note that the number after inacl# increments for each line of
the access-list.
```

## [Пример отладки маршрутизатора](#)

Конфигурация ПОЛЬЗОВАТЕЛЯ RADIUS для отладки ниже была:

```
RADIUS user password = "radiususer",
Service-Type = Framed,
Framed-Protocol = PPP,
Framed-IP-Address = 255.255.255.254
cisco-avpair = "ip:route#1=9.9.9.0 255.255.255.0 11.11.11.12"
cisco-avpair = "ip:route#2=15.15.15.0 255.255.255.0 12.12.12.13"
cisco-avpair = "ip:inacl#1=permit icmp 1.1.1.0 0.0.0.255 9.9.9.0 0.0.0.255 log"
cisco-avpair = "ip:inacl#2=permit tcp 1.1.1.0 0.0.0.255 15.15.15 .0 0.0.0.255 log"
```

koala#

koala#

```
4d05h: As1 AAA/AUTHOR/FSM: (0): LCP succeeds trivially
4d05h: %LINK-3-UPDOWN: Interface Async1, changed state to up
4d05h: AAA: parse name=Async1 idb type=10 tty=1
4d05h: AAA: name=Async1 flags=0x11 type=4 shelf=0 slot=0
adapter=0 port=1 channel=0
4d05h: AAA/MEMORY: create_user (0x552AB4) user='radiususer'
ruser='' port='Async1' rem_addr='async' authen_type=CHAP
```

```
service=PPP priv=1
4d05h: AAA/AUTHEN/START (624846144): port='Async1' list=''
    action=LOGIN service=PPP
4d05h: AAA/AUTHEN/START (624846144): using "default" list
4d05h: AAA/AUTHEN (624846144): status = UNKNOWN
4d05h: AAA/AUTHEN/START (624846144): Method=radius (radius)
4d05h: RADIUS: ustruct sharecount=1
4d05h: RADIUS: Initial Transmit Async1 id 9 172.18.124.111:1645,
    Access-Request, len 81
4d05h: Attribute 4 6 0A1F0105
4d05h: Attribute 5 6 00000001
4d05h: Attribute 61 6 00000000
4d05h: Attribute 1 12 72616469
4d05h: Attribute 3 19 1672E16F
4d05h: Attribute 6 6 00000002
4d05h: Attribute 7 6 00000001
4d05h: RADIUS: Received from id 9 172.18.124.111:1645,
    Access-Accept, len 287
4d05h: Attribute 6 6 00000002
4d05h: Attribute 7 6 00000001
4d05h: Attribute 8 6 FFFFFFFE
4d05h: Attribute 26 52 00000009012E6970
4d05h: Attribute 26 55 0000000901316970
4d05h: Attribute 26 70 0000000901406970
4d05h: Attribute 26 72 0000000901426970
4d05h: AAA/AUTHEN (624846144): status = PASS
4d05h: As1 AAA/AUTHOR/LCP: Authorize LCP
4d05h: As1 AAA/AUTHOR/LCP (3679631149): Port='Async1' list=''
    service=NET
4d05h: AAA/AUTHOR/LCP: As1 (3679631149) user='radiususer'
4d05h: As1 AAA/AUTHOR/LCP (3679631149): send AV service=ppp
4d05h: As1 AAA/AUTHOR/LCP (3679631149): send AV protocol=lcp
4d05h: As1 AAA/AUTHOR/LCP (3679631149): found list "default"
4d05h: As1 AAA/AUTHOR/LCP (3679631149): Method=radius (radius)
4d05h: RADIUS: cisco AVPair "ip:route#1=9.9.9.0 255.255.255.0
    11.11.11.12" not applied for lcp
4d05h: RADIUS: cisco AVPair "ip:route#2=15.15.15.0 255.255.255.0
    12.12.12.13" not applied for lcp
4d05h: RADIUS: cisco AVPair "ip:inacl#1=permit icmp 1.1.1.0 0.0.0.255
    9.9.9.0 0.0.0.255 log" not applied for lcp
4d05h: RADIUS: cisco AVPair "ip:inacl#2=permit tcp 1.1.1.0 0.0.0.255
    15.15.15.0 0.0.0.255 log" not applied for lcp
4d05h: As1 AAA/AUTHOR (3679631149): Post authorization
    status = PASS_REPL
4d05h: As1 AAA/AUTHOR/LCP: Processing AV service=ppp
4d05h: As1 AAA/AUTHOR/FSM: (0): Can we start IPCP?
4d05h: As1 AAA/AUTHOR/FSM (231623628): Port='Async1' list=''
    service=NET
4d05h: AAA/AUTHOR/FSM: As1 (231623628) user='radiususer'
4d05h: As1 AAA/AUTHOR/FSM (231623628): send AV service=ppp
4d05h: As1 AAA/AUTHOR/FSM (231623628): send AV protocol=ip
4d05h: As1 AAA/AUTHOR/FSM (231623628): found list "default"
4d05h: As1 AAA/AUTHOR/FSM (231623628): Method=radius (radius)
4d05h: RADIUS: Using NAS default peer
4d05h: RADIUS: Authorize IP address 0.0.0.0
4d05h: RADIUS: cisco AVPair "ip:route#1=9.9.9.0 255.255.255.0
    11.11.11.12"
4d05h: RADIUS: cisco AVPair "ip:route#2=15.15.15.0 255.255.255.0
    12.12.12.13"
4d05h: RADIUS: cisco AVPair "ip:inacl#1=permit icmp 1.1.1.0 0.0.0.255 9.9.9.0 0.0.0.255 log"
4d05h: RADIUS: cisco AVPair "ip:inacl#2=permit tcp 1.1.1.0 0.0.0.255 15.15.15.0 0.0.0.255 log"
!--- The access list is sent down from the RADIUS server. 4d05h: As1 AAA/AUTHOR (231623628):
Post authorization status = PASS_REPL 4d05h: As1 AAA/AUTHOR/FSM: We can start IPCP 4d05h: As1
AAA/AUTHOR/IPCP: Start. Her address 0.0.0.0, we want 0.0.0.0 4d05h: As1 AAA/AUTHOR/IPCP:
```

Processing AV service=ppp 4d05h: As1 AAA/AUTHOR/IPCP: Processing AV addr=0.0.0.0 4d05h: As1  
AAA/AUTHOR/IPCP: Processing AV route#1=9.9.9.0 255.255.255.0 11.11.11.12 4d05h: As1  
AAA/AUTHOR/IPCP: Processing AV route#2=15.15.15.0 255.255.255.0 12.12.12.13 4d05h: As1  
AAA/AUTHOR/IPCP: Processing AV inacl#1=permit icmp 1.1.1.0 0.0.0.255 9.9.9.0 0.0.0.255 log  
4d05h: As1 AAA/AUTHOR/IPCP: Processing AV inacl#2=permit tcp 1.1.1.0 0.0.0.255 15.15.15.0  
0.0.0.255 log 4d05h: As1 AAA/AUTHOR/IPCP: Authorization succeeded 4d05h: As1 AAA/AUTHOR/IPCP:  
Done. Her address 0.0.0.0, we want 0.0.0.0 4d05h: As1 AAA/AUTHOR/IPCP: Start. Her address  
0.0.0.0, we want 1.1.1.3 4d05h: As1 AAA/AUTHOR/IPCP: Processing AV service=ppp 4d05h: As1  
AAA/AUTHOR/IPCP: Processing AV addr=0.0.0.0 4d05h: As1 AAA/AUTHOR/IPCP: Processing AV  
route#1=9.9.9.0 255.255.255.0 11.11.11.12 4d05h: As1 AAA/AUTHOR/IPCP: Processing AV  
route#2=15.15.15.0 255.255.255.0 12.12.12.13 4d05h: As1 AAA/AUTHOR/IPCP: Processing AV  
inacl#1=permit icmp 1.1.1.0 0.0.0.255 9.9.9.0 0.0.0.255 log 4d05h: As1 AAA/AUTHOR/IPCP:  
Processing AV inacl#2=permit tcp 1.1.1.0 0.0.0.255 15.15.15.0 0.0.0.255 log 4d05h: As1  
AAA/AUTHOR/IPCP: Authorization succeeded 4d05h: As1 AAA/AUTHOR/IPCP: Done. Her address 0.0.0.0,  
we want 1.1.1.3 4d05h: As1 AAA/AUTHOR/IPCP: Start. Her address 1.1.1.3, we want 1.1.1.3 4d05h:  
As1 AAA/AUTHOR/IPCP (2383669304): Port='Async1' list='' service=NET 4d05h: AAA/AUTHOR/IPCP: As1  
(2383669304) user='radiususer' 4d05h: As1 AAA/AUTHOR/IPCP (2383669304): send AV service=ppp  
4d05h: As1 AAA/AUTHOR/IPCP (2383669304): send AV protocol=ip 4d05h: As1 AAA/AUTHOR/IPCP  
(2383669304): send AV addr\*1.1.1.3 4d05h: As1 AAA/AUTHOR/IPCP (2383669304): found list "default"  
4d05h: As1 AAA/AUTHOR/IPCP (2383669304): Method=radius (radius) 4d05h: RADIUS: Using NAS default  
peer 4d05h: RADIUS: Authorize IP address 1.1.1.3 4d05h: RADIUS: cisco AVPair "ip:route#1=9.9.9.0  
255.255.255.0 11.11.11.12" 4d05h: RADIUS: cisco AVPair "ip:route#2=15.15.15.0 255.255.255.0  
12.12.12.13" 4d05h: RADIUS: cisco AVPair "ip:inacl#1=permit icmp 1.1.1.0 0.0.0.255 9.9.9.0  
0.0.0.255 log" 4d05h: RADIUS: cisco AVPair "ip:inacl#2=permit tcp 1.1.1.0 0.0.0.255 15.15.15.0  
0.0.0.255 log" 4d05h: As1 AAA/AUTHOR (2383669304): Post authorization status = PASS\_REPL 4d05h:  
As1 AAA/AUTHOR/IPCP: Processing AV service=ppp 4d05h: As1 AAA/AUTHOR/IPCP: Processing AV  
addr=1.1.1.3 4d05h: As1 AAA/AUTHOR/IPCP: Processing AV route#1=9.9.9.0 255.255.255.0 11.11.11.12  
4d05h: As1 AAA/AUTHOR/IPCP: Processing AV route#2=15.15.15.0 255.255.255.0 12.12.12.13 **4d05h:  
As1 AAA/AUTHOR/IPCP: Processing AV inacl#1=permit icmp 1.1.1.0 0.0.0.255 9.9.9.0 0.0.0.255 log  
4d05h: As1 AAA/AUTHOR/IPCP: Processing AV inacl#2=permit tcp 1.1.1.0 0.0.0.255 15.15.15.0  
0.0.0.255 log !---** Access list from the RADIUS server is applied. 4d05h: As1 AAA/AUTHOR/IPCP:  
Authorization succeeded 4d05h: As1 AAA/AUTHOR/IPCP: Done. Her address 1.1.1.3, we want 1.1.1.3  
4d05h: As1 AAA/AUTHOR/PER-USER: Event IP\_UP 4d05h: As1 AAA/AUTHOR: IP\_UP 4d05h: As1 AAA/PER-  
USER: processing author params. 4d05h: As1 AAA/AUTHOR: Parse 'IP route 9.9.9.0 255.255.255.0  
11.11.11.12' 4d05h: As1 AAA/AUTHOR: Parse returned ok (0) 4d05h: As1 AAA/AUTHOR: enqueue peruser  
IP txt=no IP route 9.9.9.0 255.255.255.0 11.11.11.12 4d05h: As1 AAA/AUTHOR: Parse 'IP route  
15.15.15.0 255.255.255.0 12.12.12.13' 4d05h: As1 AAA/AUTHOR: Parse returned ok (0) 4d05h: As1  
AAA/AUTHOR: enqueue peruser IP txt=no IP route 15.15.15.0 255.255.255.0 12.12.12.13 4d05h: As1  
AAA/AUTHOR: Parse 'ip access-list extended Async1#0' 4d05h: As1 AAA/AUTHOR: Parse returned ok  
(0) 4d05h: As1 AAA/AUTHOR: Parse 'permit icmp 1.1.1.0 0.0.0.255 9.9.9.0 0.0.0.255 log' 4d05h:  
As1 AAA/AUTHOR: Parse returned ok (0) 4d05h: As1 AAA/AUTHOR: Parse 'permit tcp 1.1.1.0 0.0.0.255  
15.15.15.0 0.0.0.255 log' 4d05h: As1 AAA/AUTHOR: Parse returned ok (0) 4d05h: As1 AAA/AUTHOR:  
enqueue peruser IP txt=no ip access-list extended Async1#0 4d05h: As1 AAA/AUTHOR: Parse  
'interface Async1' 4d05h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async1, changed state  
to up 4d05h: As1 AAA/AUTHOR: Parse returned ok (0) 4d05h: As1 AAA/AUTHOR: Parse 'IP access-group  
Async1#0 in' 4d05h: As1 AAA/AUTHOR: Parse returned ok (0) 4d05h: As1 AAA/AUTHOR: enqueue peruser  
IP txt=interface Async1 no IP access-group Async1#0 in koala#**show ip access-list** Extended IP  
access list 101 permit icmp 1.1.1.0 0.0.0.255 9.9.9.0 0.0.0.255 log (5 matches) permit tcp  
1.1.1.0 0.0.0.255 15.15.15.0 0.0.0.255 log (11 matches) Extended IP access list **Async1#0 (per-  
user) permit icmp 1.1.1.0 0.0.0.255 9.9.9.0 0.0.0.255 log permit tcp 1.1.1.0 0.0.0.255  
15.15.15.0 0.0.0.255 log !---** Verify that the access list is applied to the AS1 dial interface.  
koala#**show ip route** Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D -  
EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 -  
OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-  
IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area \* - candidate default, U -  
per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort is  
10.31.1.1 to network 0.0.0.0 1.0.0.0/32 is subnetted, 1 subnets C 1.1.1.3 is directly connected,  
Async1 172.17.0.0/24 is subnetted, 1 subnets S 172.17.192.0 [1/0] via 10.31.1.1 172.18.0.0/24 is  
subnetted, 2 subnets S 172.18.124.0 [1/0] via 10.31.1.1 S 172.18.125.0 [1/0] via 10.31.1.1  
9.0.0.0/24 is subnetted, 1 subnets **U 9.9.9.0 [1/0] via 11.11.11.12 !---** The static user route  
specified by the RADIUS server is applied. 10.0.0.0/24 is subnetted, 1 subnets C 10.31.1.0 is  
directly connected, Ethernet0 11.0.0.0/24 is subnetted, 1 subnets C 11.11.11.0 is directly  
connected, Serial0 12.0.0.0/24 is subnetted, 1 subnets C 12.12.12.0 is directly connected,  
Serial1 15.0.0.0/24 is subnetted, 1 subnets **U 15.15.15.0 [1/0] via 12.12.12.13 !---** The static

*user route specified by the RADIUS server is applied. S\* 0.0.0.0/0 [1/0] via 10.31.1.1*

## Команды "debug"

- **debug aaa authentication** - Отображает информацию об аутентификации AAA (проверка подлинности, авторизация и учет).
- **debug aaa authorization** - Отображает информацию об авторизации AAA.
- **debug aaa per-user** - Отображает информацию о настройках на базе отдельных пользователей на маршрутизаторе или сервере доступа, которые передаются от AAA-сервера.
- **debug radius** — отображаются подробные отладочные данные, связанные с RADIUS.
- **"debug ppp negotiation"** – отображаются PPP-пакеты, передаваемые при запуске PPP с согласованием параметров.

Для сведений об устранении проблем посмотрите [Списки доступа Устранения проблем на Набираемых Интерфейсах](#).

## Дополнительные сведения

- [Документация к CiscoSecure ACS для UNIX](#)
- [Страница поддержки Cisco Secure ACS для Windows](#)
- [Документация по Cisco Secure ACS для Windows](#)
- [Уведомления о дефектах продуктов безопасности \(включая Cisco Secure UNIX\)](#)
- [Страница поддержки RADIUS](#)
- [RADIUS Настройки](#)
- [Запросы комментариев \(RFC\)](#)
- [Техническая поддержка - Cisco Systems](#)