

如何在 RADIUS 服务器的拨号接口上应用访问列表

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[网络图](#)

[在路由器上定义编号访问列表](#)

[其他Cisco IOS软件版本的命令](#)

[服务器配置 - 路由器的访问列表](#)

[路由器调试示例](#)

[在服务器上定义访问列表](#)

[其他Cisco IOS软件版本的命令](#)

[服务器配置](#)

[路由器调试示例](#)

[调试命令](#)

[相关信息](#)

简介

本文档演示如何将访问列表应用到与RADIUS服务器的拨号接口。有两个可能的方法：

- 在路由器上定义编号访问列表，然后在RADIUS服务器上引用编号访问列表。大多数Cisco IOS®软件版本都支持此功能。例如，在路由器上定义编号访问列表并在服务器上引用它们。
- 在服务器上定义整个访问列表。此每用户方法需要Cisco IOS软件版本11.3或更高版本。例如，在RADIUS服务器（而不是NAS上）上定义访问列表。当呼叫连接时，NAS会向RADIUS服务器验证呼叫。除了任何身份验证信息，服务器还会将访问列表返回到NAS，然后将其应用到拨号接口。

注意：对于ISDN，您必须使用每用户方法，并且必须在路由器上配置虚拟配置文件。在配置虚拟配置文件中，对Cisco IOS软件版本11.3进行了[说明](#)。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本。

- Cisco IOS软件版本11.1或更高版本（在路由器上定义访问列表）
- Cisco IOS软件版本11.3或更高版本（在服务器上定义访问列表）
- 适用于Windows 2.x或Livingston RADIUS或Merit RADIUS的Cisco Secure ACS UNIX或Cisco Secure ACS

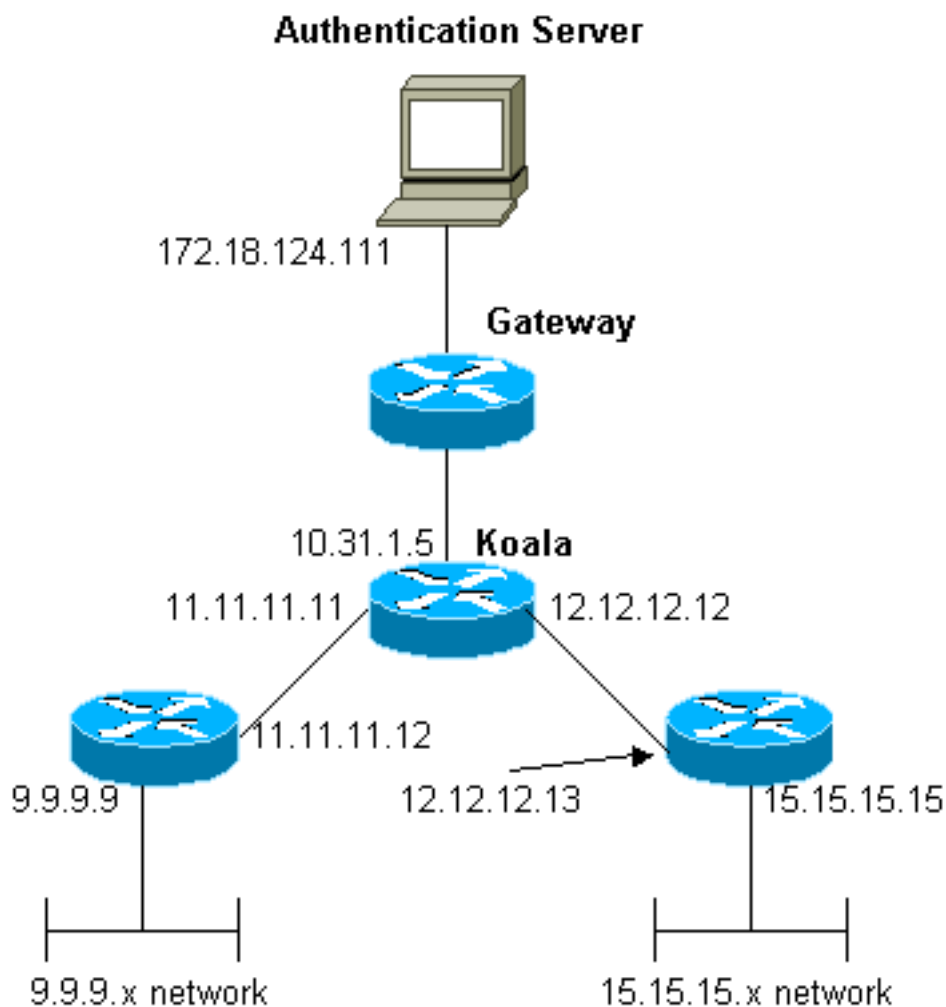
本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

规则

有关文件规则的更多信息请参见“Cisco技术提示规则”。

网络图

此网络用于以下两个示例：



在路由器上定义编号访问列表

路由器配置

```
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.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 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
```

[其他Cisco IOS软件版本的命令](#)

注意：要使用这些命令，请从上述配置中删除粗体命令，然后按照Cisco IOS软件版本的说明将这些命令粘贴到中。

[思科IOS软件版本11.3.3.T到12.0.5.T](#)

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

[思科IOS软件版本11.1至11.3.3.T](#)

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

[服务器配置 - 路由器的访问列表](#)

此过程涉及在路由器上配置访问列表本身。RADIUS服务器配置了所应用的访问列表编号。当呼叫进行身份验证时，RADIUS服务器将访问列表编号返回给NAS，然后NAS会应用相应的访问列表。

[服务器配置 — Cisco Secure ACS for Windows 2.X - RADIUS](#)

遵循以下步骤：

1. 在“用户设置”中，填写名称和密码。
2. 在组设置中，选中：属性6 — 已配置属性7 - PPP属性11 - Filter-Id。在下面的区域中，键入**101.in**注意：属性11指定应用访问列表101。确保在路由器上配置了access-list 101。

[服务器配置 — Cisco Secure ACS UNIX - RADIUS](#)

```
rtp-evergreen# ./ViewProfile -p 9900 -u chaptr
User Profile Information
user = chaptr{
profile_id = 51
profile_cycle = 1
radius=Cisco {
check_items= {
2="chaptr"
```

```

}
reply_attributes= {
6=2
7=1
11=101.in
}
}
}

```

注意：属性11指定应用访问列表101。确保在路由器上配置了access-list 101。

服务器配置 — Livingston RADIUS

```

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

```

注意：这指定应用访问列表101。确保在路由器上配置了access-list 101。

路由器调试示例

```

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 Async1, 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 "chaptrtr"
*Mar 1 00:55:36.663: AAA: parse name=Async1 idb type=10 tty=1
*Mar 1 00:55:36.667: AAA: name=Async1 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='chaptrtr'
    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='chaptrtr'
*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#

```

在服务器上定义访问列表

注意：Route语句不必从服务器向下传送到路由器；拨号用户通常从路由器获取路由。路由器上是否存在route语句取决于路由是从服务器向下传递还是从路由器上提取。但是，在本例中，访问列表和路由语句会向下传递。

```

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

```

在此示例配置中，从服务器向下传递路由仅用于说明目的。

路由器配置

```

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
```

[其他Cisco IOS软件版本的命令](#)

注意：要使用这些命令，请从上述配置中删除粗体命令，然后按照Cisco IOS软件版本的说明将这些命令粘贴到中。

[思科IOS软件版本11.3.3.T到12.0.5.T](#)

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

[思科IOS软件版本11.3到11.3.3.T](#)

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

[服务器配置](#)

[服务器配置 — 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. } } }
```

[服务器配置 — Cisco Secure ACS for Windows 2.x - RADIUS](#)

请完成以下步骤：

1. 在“用户设置”中，填写名称和密码。
2. 在组设置中，选中：属性6 — 已配置属性7 - PPP
3. 在Cisco RADIUS Attributes下，选中[009\001] AV-Pair，并在下面的框中键入以下文本：

```
ip:route#1=9.9.9.9 255.255.255.255 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.
```

服务器配置 — Merit RADIUS

注意：此配置对支持Cisco av-pair的Merit RADIUS版本3.6b或更高版本有效。

```
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.
```

路由器调试示例

以下调试的RADIUS用户配置为：

```
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' authn_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*

调试命令

- **debug aaa authentication** — 显示有关AAA身份验证的信息。
- **debug aaa authorization** — 显示有关AAA授权的信息。
- **debug aaa per-user** — 显示有关从AAA服务器发送的路由器或接入服务器上的每用户配置设置的信息。
- **debug radius** - 显示与 RADIUS 相关的调试详细信息。
- **debug ppp negotiation** - 显示在 PPP 启动期间传输的 PPP 数据包，在此启动期间将协商 PPP 选项。

有关故障排除信息，请参阅[对拨号接口上的访问列表进行故障排除](#)。

相关信息

- [Cisco Secure ACS for UNIX 文档](#)
- [Cisco Secure ACS for Windows 支持页](#)
- [Cisco Secure ACS for Windows 文档](#)
- [RADIUS 支持页](#)
- [配置RADIUS](#)
- [请求注解 \(RFC\)](#)