



RADIUS Attribute 104

First Published: March 1, 2004

Last Updated: September 8, 2009

The RADIUS Attribute 104 feature allows private routes (attribute 104) to be specified in a RADIUS authorization profile. The private routes affect only packets that are received on an individual interface. The routes are stored apart from the global routing table and are not injected into any routing protocols for redistribution.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for RADIUS Attribute 104” section on page 9](#).

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. An account on Cisco.com is not required.

Contents

- [Prerequisites for RADIUS Attribute 104, page 2](#)
- [Restrictions for RADIUS Attribute 104, page 2](#)
- [Information About RADIUS Attribute 104, page 2](#)
- [How to Apply RADIUS Attribute 104, page 3](#)
- [Configuration Examples for RADIUS Attribute 104, page 6](#)
- [Additional References, page 7](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for RADIUS Attribute 104

- You must be using a Cisco RADIUS server.
- You should be familiar with configuring RADIUS.
- You should be familiar with policy-based routing (PBR) and private routes.
- You should be familiar with configuring access control lists (ACLs).
- Before using the RADIUS Attribute 104 feature, you must configure RADIUS AAA authorization and RADIUS route download.
- The following memory bytes are required:
 - One route map—50 bytes.
 - One match-set clause—600 bytes.
 - One extended ACL—366 bytes.
 - For N number of attribute 104s, the memory requirement is $(600+366)*N+50=1000*N$ (approximate) per user.

Restrictions for RADIUS Attribute 104

- If you already have PBR locally (statically) configured under the interface, and you specify attribute 104, the locally configured PBR will be disabled.
- If a pseudo next-hop address is involved, there must be a route available in the routing table for the next-hop address. If a route is not available, the packet will not be policy routed.
- Policy routing does not order the match-set clauses and relies on the first match, so you should specify the attributes in the order in which you want them to be matched.
- Metric numbers cannot be used in the attribute.

Information About RADIUS Attribute 104

Before using the RADIUS Attribute 104 feature, you should understand the following concepts:

- [Policy-Based Routing: Background, page 2](#)
- [Attribute 104 and the Policy-Based Route Map, page 3](#)

Policy-Based Routing: Background

PBR provides a mechanism for the forwarding, or routing of, data packets on the basis of defined policies. The policies are not wholly dependent on the destination address but rather on other factors, such as type of service, source address, precedence, port numbers, or protocol type.

Policy-based routing is applied to incoming packets. All packets that are received on an interface that has policy-based routing enabled are considered for policy-based routing. The router passes the packets through enhanced packet filters called route maps. On the basis of the criteria that are defined in the route maps, the packets are forwarded to the appropriate next hop.

Each entry in a route map statement contains a combination of match clauses and set clauses or commands. The match clauses define the criteria for whether appropriate packets meet the particular policy (that is, whether the conditions are met). The set clauses provide instruction for how the packets should be routed after they have met the match criteria. The match clause specifies which set of filters a packet must match for the corresponding set clause to be applied.

Attribute 104 and the Policy-Based Route Map

This section discusses the attribute 104 feature and how it works with policy-based route maps.

RADIUS Attribute 104 Overview

Using the RADIUS Attribute 104 feature, you can specify private routes in your RADIUS authorization profile. The private routes you specify will affect only packets that are received on an individual interface. The routes are stored apart from the global routing table and are not injected into any routing protocols for redistribution.

Permit Route Map

Route map statements can be marked as “permit” or “deny.” If the statement is marked “permit,” the set clause is applied to the packets that match the match criteria. For attribute 104, when you are configuring the route map, you need to mark the route map as “permit,” as follows. See [“Related Documents” section on page 7](#) for where to find information on configuring a route map.

Default Private Route

The policy routing process proceeds through the route map until a match is found. If no match is found in the route map, the global routing table is consulted. If you have specified a default route in your user profile, any further routes beyond the default route are effectively ignored.

Route Map Order

You need to specify route maps on the server in the order that you want them to be applied.

How to Apply RADIUS Attribute 104

This section contains the following procedures:

- [Applying RADIUS Attribute 104 to Your User Profile, page 4](#)
- [Verifying Route Maps, page 4](#)
- [Troubleshooting the RADIUS Profile, page 5](#)

Applying RADIUS Attribute 104 to Your User Profile

You can apply RADIUS attribute 104 to your user profile by adding the following to the RADIUS server database.

SUMMARY STEPS

1. Apply RADIUS attribute 104 to your user profile.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Apply RADIUS attribute 104 to your user profile.	Ascend-Private-Route="dest_addr/netmask next_hop" The destination network address of the router is "dest_addr/netmask", and the address of the next-hop router is "next_hop."

Examples

The following is a sample user profile that creates three private routes that are associated with the caller:

```
username Password="ascend"; User-Service=Framed-User
```

```
Framed-Protocol=PPP,
Framed-Address=10.1.1.1,
Framed-Netmask=255.0.0.0,
Ascend-Private-Route="172.16.1.1/16 10.10.10.1"
Ascend-Private-Route="192.168.1.1/32 10.10.10.2"
Ascend-Private-Route="10.20.0.0/1 10.10.10.3"
Ascend-Private-Route="10.0.0.0/0 10.10.10.4"
```

Using the above profile, the private routing table for the connection contains the following routes, including a default route:

```
Destination/Mask      Gateway
172.16.1.1/16        10.10.10.1
192.168.1.1/32       10.10.10.2
10.20.20.20/1        10.10.10.3
10.0.0.0/0           10.10.10.4
```

Verifying Route Maps

You can use the following **show** commands to verify the route maps that have been configured.

SUMMARY STEPS

1. **enable**
2. **show ip policy**
3. **show route-map** [*map-name* | **dynamic** [*dynamic-map-name* | **application** [*application-name*]] | **all**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	show ip policy Example: Router# show ip policy	Displays the route map that is used for policy routing.
Step 3	show route-map [<i>map-name</i> dynamic [<i>dynamic-map-name</i> application [<i>application-name</i>]] all] Example: Router# show route-map	Displays all route maps that are configured or only the one that is specified.

Troubleshooting the RADIUS Profile

If your private route configuration is not working properly, you may want to reread the section [“Policy-Based Routing: Background” section on page 2.](#) This section may help you determine what is happening to the packets. In addition, the following **debug** commands can be used to troubleshoot your RADIUS profile.

SUMMARY STEPS

1. **enable**
2. **debug radius**
3. **debug aaa per-user**
4. **debug ip policy**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	debug radius Example: Router# debug radius	Displays information associated with RADIUS.
Step 3	debug aaa per-user Example: Router# debug aaa per-user	Displays the attributes that are applied to each user as the user authenticates.
Step 4	debug ip policy Example: Router# debug ip policy	Displays IP routing packet activity.

Configuration Examples for RADIUS Attribute 104

This section includes the following configuration example:

- [Route-Map Configuration in Which Attribute 104 Has Been Applied: Example, page 6](#)

Route-Map Configuration in Which Attribute 104 Has Been Applied: Example

The following output is a typical route-map configuration to which attribute 104 has been applied:

```
Router# show route-map dynamic

route-map AAA-01/08/04-14:13:59.542-1-AppSpec, permit, sequence 0, identifier 1639994476
  Match clauses:
    ip address (access-lists): PBR#1 PBR#2
  Set clauses:
    Policy routing matches: 0 packets, 0 bytes
route-map AAA-01/08/04-14:13:59.542-1-AppSpec, permit, sequence 1, identifier 1640264784
  Match clauses:
    ip address (access-lists): PBR#3 PBR#4
  Set clauses:
    Policy routing matches: 0 packets, 0 bytes
route-map AAA-01/08/04-14:13:59.542-1-AppSpec, permit, sequence 2, identifier 1645563704
  Match clauses:
    ip address (access-lists): PBR#5 PBR#6
    length 10 100
  Set clauses:
    ip next-hop 10.1.1.1
    ip gateway10.1.1.1
  Policy routing matches: 0 packets, 0 bytes
Current active dynamic routemaps = 1
```

Additional References

The following sections provide references related to RADIUS Attribute 104 feature.

Related Documents

Related Topic	Document Title
Configuring RADIUS	“ Configuring RADIUS ” feature module.
Configuring policy-based routing	“ Classifying Network Traffic ” feature module.
Configuring access control lists	“ IP Access List Overview ” feature module.
Configuring RADIUS AAA authorization and RADIUS route download	“ RADIUS Route Download ” feature module.
Security commands	<i>Cisco IOS Security Command Reference</i>
Quality of Service (QoS) commands (for policy-based routing commands)	<i>Cisco IOS Quality of Service Solutions Command Reference</i>

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Feature Information for RADIUS Attribute 104

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for RADIUS Attribute 104

Feature Name	Releases	Feature Information
RADIUS Attribute 104	12.3(7)T	<p>The RADIUS Attribute 104 feature allows private routes (attribute 104) to be specified in a RADIUS authorization profile. The private routes affect only packets that are received on an individual interface. The routes are stored apart from the global routing table and are not injected into any routing protocols for redistribution.</p> <p>This feature was introduced in Cisco IOS Release 12.3(7)T.</p> <p>The following commands were introduced or modified: show ip policy, show route-map.</p>

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2004–2009 Cisco Systems, Inc. All rights reserved.

