



# Selecting AAA Servers Using DNIS Numbers

---

## Feature Summary

You can now authenticate users to a particular AAA server based on the session's Dialed Number Identification Service (DNIS) number. RADIUS directed-request support has been implemented to support this capability.

Any phone line (a regular home phone or a commercial T1/PRI line) can be associated with several phone numbers. The DNIS number identifies the number that was called to reach you.

For example, suppose you want to share the same phone number with several customers, but you want to know which customer is calling before you pick up the phone. You can customize how you answer the phone because DNIS allows you to know which customer is calling when you answer.

Cisco routers with either ISDN or internal modems (5200/5300) can receive the DNIS number. This functionality allows users to assign different RADIUS servers for different customers (that is, different RADIUS servers for different DNIS numbers).

## Benefits

The DNIS number identifies which number is called to reach you. This capability lets you know who is calling when you answer. You can also assign specific RADIUS servers to different DNIS numbers. In other words, you can assign specific RADIUS servers to individual users dialing into the network.

## Platforms

This feature is supported on all Cisco routers supporting ISDN or internal modems.

## Supported MIBs and RFCs

None.

## Configuration Tasks

To configure DNIS mapping, use the following commands in global configuration mode:

**Table 1**            **Configuring DNIS**

Step	Command	Purpose
1	<code>aaa dnis map {dnis-number ip-address}</code>	Map each DNIS number to a valid RADIUS server. Repeat for as many servers and numbers supported.
2	<code>aaa dnis map enable</code>	Enable DNIS.
3	<code>radius-server host x.x.x.x auth-port yyyy acct-port zzzz</code>	Defines a RADIUS server, which can be used in a DNIS map.

## Configuration Example

The following example maps the DNIS number 77777 to the RADIUS server at IP address 2.2.2.2, DNIS number 88888 to the RADIUS server at IP address 3.3.3.3, and DNIS number 99999 to the RADIUS server at IP address 4.4.4.4. Valid RADIUS hosts are defined to be IP addresses 1.1.1.1, 2.2.2.2, and 3.3.3.3.

```
AS5300(config)# aaa dnis map 77777 2.2.2.2
AS5300(config)# aaa dnis map 88888 3.3.3.3
AS5300(config)# aaa dnis map 99999 4.4.4.4
AS5300(config)# radius-server host 1.1.1.1
AS5300(config)# radius-server host 2.2.2.2
AS5300(config)# radius-server host 3.3.3.3
```

The network access server contains the configuration described above and receives a connection with DNIS=77777. Because **aaa dnis map enable** is not configured, the network access server contacts the first RADIUS server (1.1.1.1) on the list to authenticate the user.

When you enable DNIS mapping by entering the **aaa dnis map enable** command, the user calling in on 77777 will be authenticated using the RADIUS server at 2.2.2.2 because the session's DNIS number (77777) is mapped to that server. If the RADIUS server at 2.2.2.2 does not respond, the call will *not* go to another server because the session's DNIS number is mapped to that server only.

If the network access server receives a connection with the DNIS number 99999, it attempts to authenticate the user by connecting to the RADIUS server at 4.4.4.4. Because a server has not been configured for this location, the network access server will fail to find the address in your list of RADIUS servers at authentication time. The network access server will query the first server on the list (as if it never tried to choose the RADIUS server based on the DNIS number).

DNIS mapping produces the same effect as the **radius-server directed-request restricted** command.

## Command Reference

This section documents new or modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.0 command references.

- **aaa dnis map**
- **aaa dnis map enable**
- **radius-server directed-request**

## aaa dnis map

To map a DNIS number to a RADIUS server, use the **aaa dnis map** global configuration command. Use the **no** form of this command to disable DNIS mapping.

```
aaa dnis map {dnis-number ip-address}  
no aaa dnis map {dnis-number ip-address}
```

### Syntax Description

<i>dnis-number</i>	Dial in phone number.
<i>ip-address</i>	IP address of the RADIUS server.

### Default

Disabled

### Command Mode

Global configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.3(6) AA.

### Example

The following example maps the DNIS number 77777 to the RADIUS server at IP address 2.2.2.2, DNIS number 88888 to the RADIUS server at IP address 3.3.3.3, and DNIS number 99999 to the RADIUS server at IP number 4.4.4.4. Valid RADIUS hosts are defined to be IP address, 1.1.1.1, 2.2.2.2, and 3.3.3.3.

```
AS5300(config)# aaa dnis map 77777 2.2.2.2  
AS5300(config)# aaa dnis map 88888 3.3.3.3  
AS5300(config)# aaa dnis map 99999 4.4.4.4  
AS5300(config)# radius-server host 1.1.1.1  
AS5300(config)# radius-server host 2.2.2.2  
AS5300(config)# radius-server host 3.3.3.3
```

The network access server contains the configuration described above and receives a connection with DNIS=77777. Because **aaa dnis map enable** is not configured, the network access server contacts the first RADIUS server (1.1.1.1) on the list to authenticate the user.

When you enable DNIS mapping by entering the **aaa dnis map enable** command, the user calling in on 77777 will be authenticated using the RADIUS server at 2.2.2.2 because the session's DNIS number (77777) is mapped to that server. If the RADIUS server at 2.2.2.2 does not respond, the call will not go to another server because the session's DNIS number is mapped to that server only.

If the network access server receives a connection with the DNIS number 99999, it attempts to authenticate the user by connecting to the RADIUS server at 4.4.4.4. Because a server has not been configured for this location, the network access server will fail to find the address in your list of RADIUS servers at authentication time. The network access server will query the first server on the list (as if it never tried to choose the RADIUS server based on the DNIS number).

Related Commands

**aaa dnis map enable**  
**radius-server directed-request**

## aaa dnis map enable

To enable AAA server selection based on DNIS, use the **aaa dnis map enable** global configuration command. Use the **no** form of this command to disable the selection.

**aaa dnis map enable**  
**no aaa dnis map enable**

### Syntax Description

This command has no arguments or keywords.

### Default

Disabled

### Command Mode

Global configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.3(6) AA.

### Example

The following example enables AAA server selection based on associations set with the **aaa dnis map** command.

```
AS5300 (config) # aaa dnis map enable
```

### Related Commands

**aaa dnis map**  
**radius-server directed-request**

## radius-server directed-request

To allow users logging into a Cisco server to select the RADIUS server for authentication, use the **radius-server directed-request** global configuration command. Use the **no** form of this command to disable the directed-request feature.

```
radius-server directed-request [restricted]  
no radius-server directed-request [restricted]
```

### Syntax Description

<b>restricted</b>	Prevents the user, who is intended to be sent to the specified server, from being sent to a secondary server if the specified server is not available.
-------------------	--

### Default

Disabled

### Command Mode

Global configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.3(6) AA.

This command sends only the portion of the username before the “@” symbol to the host specified after the “@” symbol. In other words, with this command enabled, you can direct a request to any of the configured servers, and only the username is sent to the specified server.

Disabling the **radius-server directed-request** command causes the whole string, both before and after the “@” symbol, to be sent to the default RADIUS server. The router queries the list of servers, starting with the first one in the list, sends the whole string, and accepts the first response that it gets from the server.

With the **radius-server directed-request** command enabled, only configured RADIUS servers can be specified by the user after the “@” symbol. If the host name specified by the user does not match the IP address of a RADIUS server configured by the administrator, the user input is rejected.

Use the **radius-server directed-request restricted** command to limit the user to the RADIUS server identified as part of the username.

The **no radius-server directed-request** command causes the entire username string to be passed to the default RADIUS server.

### Examples

The following example verifies that the RADIUS server is selected based on the directed request:

```
5200(config)# aaa new-model
5200(config)# aaa authentication login default radius

5200(config)# radius-server host 192.168.1.1
5200(config)# radius-server host 172.16.56.103
5200(config)# radius-server host 172.31.40.1

5200(config)# radius-server directed-request
```

The user `jdoue@172.16.56.103` logs in to the network access server using Telnet. The login authentication uses the directed server `172.16.56.103`. If `172.16.56.103` does not respond, `172.31.40.1` is tried next, as it is the next server in the **radius-server** list.

The following example shows that with the **radius-server directed-request restricted** command issued, the directed-request RADIUS server does not fail over.

```
5200(config)# aaa new-model
5200(config)# aaa authentication login default radius

5200(config)# radius-server host 192.168.1.1
5200(config)# radius-server host 172.16.56.103
5200(config)# radius-server host 172.31.40.1

5200(config)# radius-server directed-request restricted
```

The user `jsmith@192.168.1.1` logs in to the network access server using Telnet. The login authentication uses the directed server `192.168.1.1`. If `192.168.1.1` does not respond, an error occurs, and authentication does not fail over to the next RADIUS server, `172.16.,56.103`, because the restricted flag is set. The user, `jsmith`, finds that the login authentication fails with an error.

The following example sends the entire username string to the default RADIUS server:

```
5200(config)# no radius-server directed-request
```

### Related Commands

- aaa dnis map**
- aaa dnis map enable**
- tacacs-server directed-request**