



DNS Spoofing

The DNS Spoofing feature is designed to allow a router to act as a proxy Domain Name System (DNS) server and “spoof” replies to any DNS queries using either the configured IP address in the **ip dns spoofing** *ip-address* command or the IP address of the incoming interface for the query. This feature is useful for devices where the interface toward the Internet service provider (ISP) is not up. Once the interface to the ISP is up, the router forwards DNS queries to the real DNS servers.

Feature History for the DNS Spoofing Feature

Release	Modification
12.3(2)T	This feature was introduced.
12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Restrictions, page 2](#)
- [How to Configure DNS Spoofing, page 2](#)
- [Configuration Examples for DNS Spoofing, page 3](#)
- [Additional References, page 4](#)
- [Command Reference, page 6](#)
- [Glossary, page 8](#)



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

Copyright © 2006 Cisco Systems, Inc. All rights reserved.

Restrictions

Addresses returned with this feature will not be sortable via Distributed Director.

How to Configure DNS Spoofing

This section contains the following procedure:

- [Configuring DNS Spoofing](#) (required)

Configuring DNS Spoofing

This feature turns on DNS spoofing and is functional if any of the following conditions are true:

- The **no ip domain-lookup** command is configured.
- IP name server addresses are not configured.
- There are no valid interfaces or routes for sending to the configured name server addresses.

If these conditions are removed, DNS spoofing will not occur.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dns server**
4. **ip dns spoofing** [*ip-address*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: Router# configure terminal	Enters global configuration mode.
Step 3	<code>ip dns server</code> Example: Router(config)# ip dns server	Activates the DNS server on the router.
Step 4	<code>ip dns spoofing [ip-address]</code> Example: Router(config)# ip dns spoofing 192.168.15.1	Enables DNS spoofing. <ul style="list-style-type: none"> The router will respond to the DNS query with the configured <i>ip-address</i> when queried for any host name other than its own. The router will respond to the DNS query with the IP address of the incoming interface when queried for its own host name. The host name used in the DNS query is defined as the exact configured host name of the router specified by the <code>hostname name</code> command

Configuration Examples for DNS Spoofing

This section provides the following configuration example:

- [DNS Spoofing: Example](#)

DNS Spoofing: Example

In the following example, the router is configured to spoof replies to any DNS queries:

```
ip dns server
ip dns spoofing
no ip domain-lookup
interface e3/1
 ip address 10.1.1.1 255.255.255.0
```

Additional References

The following section provides additional information related to the DNS Spoofing feature.

Related Documents

Related Topic	Document Title
Commands related to DNS	<i>Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services</i> , Release 12.3 T
Mapping host names to IP addresses	“Configuring IP Addressing” chapter of the <i>Cisco IOS IP Configuration Guide</i>

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	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
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents a new command. All other commands used with this feature are documented in the Cisco IOS Release 12.3T command reference publications.

- [ip dns spoofing](#)

ip dns spoofing

To enable Domain Name System (DNS) spoofing, use the **ip dns spoofing** command in global configuration mode. To disable DNS spoofing, use the **no** form of this command.

ip dns spoofing [*ip-address*]

no ip dns spoofing [*ip-address*]

Syntax Description	<i>ip-address</i> (Optional) IP address used in replies to DNS queries.
---------------------------	---

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.3(2)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.	

Usage Guidelines

DNS spoofing allows a router to act as a proxy DNS server and “spoof” replies to any DNS queries using either the configured IP address in the **ip dns spoofing** command or the IP address of the incoming interface for the query. This functionality is useful for devices where the interface toward the ISP is not up. Once the interface to the ISP is up, the router forwards DNS queries to the real DNS servers.

The router will respond to the DNS query with the configured IP address when queried for any host name other than its own but will respond to the DNS query with the IP address of the incoming interface when queried for its own host name.

The host name used in the DNS query is defined as the exact configured host name of the router specified by the **hostname** command, with no default domain appended. For example, in the following configuration:

```
ip domain name cisco.com
hostname host1
```

The system would respond with a DNS spoofing reply if queried for “host1” but not for “host1.cisco.com”.

Examples

In the following example, the router will respond to a DNS query with an IP address of 192.168.15.1:

```
ip dns spoofing 192.168.15.1
```

Glossary

DNS—Domain Name System. System used in the Internet for translating names of network nodes into addresses.

**Note**

Refer to [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0711R)

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

Copyright © 2006 Cisco System s, Inc. All rights reserved.