

Configuring DNS on Cisco Routers

Document ID: 24182

Introduction

Prerequisites

Requirements

Components Used

Conventions

Setting Up a Router to Use DNS Lookups

Troubleshooting

You Can Ping a Web Server, But You Cannot View the HTML Pages

Router Queries Multiple Name Servers

Related Information

Introduction

The purpose of this document is to bring together certain points about Domain Name System (DNS) use by Cisco routers.

Prerequisites

Requirements

Readers of this document should have knowledge of these topics:

- Cisco IOS[®] Command Line Interface (CLI)
- General DNS behavior

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 2500 series routers
- Cisco IOS software 12.2(24a)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Setting Up a Router to Use DNS Lookups

Your router can be configured to use DNS lookups if you wish to use the **ping** or **tracert** commands with a host name rather than an IP address. Use these commands to do so:

Command	Description
---------	-------------

ip domain lookup	Enables DNS-based host name-to-address translation. This command is enabled by default.
ip name-server	Specifies the address of one or more name servers.
ip domain list	<p>Defines a list of domains, each to be tried in turn.</p> <p>Note: If there is no domain list, the domain name that you specified with the ip domain-name global configuration command is used.</p> <p>If there is a domain list, the default domain name is not used.</p>
ip domain name	Defines a default domain name that the Cisco IOS software uses to complete unqualified host names (names without a dotted-decimal domain name). Do not include the initial period that separates an unqualified name from the domain name.
ip ospf name-lookup	Configures Open Shortest Path First (OSPF) to look up DNS names for use in all OSPF show EXEC command displays. This feature makes it easier to identify a router because the router is displayed by name rather than by its router ID or neighbor ID.

This example shows a sample configuration on a router configured for basic DNS lookup:

Sample Basic DNS Lookup Configuration
<pre> Router# show running-config Building configuration... Current configuration : 470 bytes ! version 12.2 service timestamps debug datetime msec service timestamps log uptime no service password-encryption ! hostname Router ! ! ip subnet-zero ip name-server 192.168.1.100 !--- Configures the IP address of the name server. !--- Domain lookup is enabled by default. ! ! interface Ethernet0 ip address 192.168.1.1 255.255.255.0 ! </pre>

```
!  
!--- Output Suppressed.  
  
end
```

```
Router# ping www.cisco.com  
Translating "www.cisco.com"...domain server (192.168.1.100) [OK]  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 198.133.219.25, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 224/228/236 ms
```

Troubleshooting

Under rare conditions, you may see one of these error conditions:

```
Router# debug ip udp  
UDP packet debugging is on  
Router# ping www.yahoo.com  
Translating "www.yahoo.com"...domain server (129.250.35.250)  
*Mar 8 06:26:41.732: UDP: sent src=209.69.16.66(5476), dst=129.250.35.250(53), length=59  
*Mar 8 06:26:44.740: UDP: sent src=209.69.16.66(5476), dst=129.250.35.250(53), length=59  
*Mar 8 06:26:47.744: UDP: sent src=209.69.16.66(5476), dst=129.250.35.250(53), length=59  
% Unrecognized host or address, or protocol not running.  
Router#undebug allAll possible debugging has been turned off  
  
Router# ping www.yahoo.co.kr  
Translating "www.yahoo.co.kr"...domain server (169.140.249.4) ;!  
Not process  
  
Router# ping www.novell.com  
Translating "www.novell.com"...domain server (255.255.255.255)  
% Unrecognized host or address, or protocol not running.
```

Complete these steps to troubleshoot this problem:

1. Ensure the router can reach the DNS server. Ping the DNS server from the router using its IP address, and make sure that the **ip name-server** command is used to configure the IP address of the DNS server on the router.
2. Use these steps to ensure that the router forwards the lookup requests:

- a. Define an access control list (ACL) that matches on DNS packets:

```
access-list 101 permit udp any any eq domain  
access-list 101 permit udp any eq domain any
```

- b. Use the **debug ip packet 101** command.

Note: Ensure that you specify the ACL. If you enable the **debug ip packet** command without an ACL may produce a large amount of output to the console and cause the router to reload.

3. Ensure you have the **ip domain-lookup** command enabled on the router.

You Can Ping a Web Server, But You Cannot View the HTML Pages

In rare cases, you may be unable to access particular Web sites by name. This problem typically results from the inaccessible sites performing a reverse DNS lookup on the source IP address to verify that the address is not being spoofed. If an incorrect entry or no entry returns (in other words, there is no associated name for the

the IP range) then the HTTP request will be blocked.

When you obtain your Internet domain name, you also should apply for an inaddr.arpa domain. This special domain is sometimes called a reverse domain. The reverse domain maps numeric IP addresses into domain names. If your ISP provides your name server or your ISP assigned you an address from a block of its own addresses, you may not need to apply for an in-addr.arpa domain on your own. Check with your ISP.

Let us look at an example that uses www.cisco.com. The output which follows was captured from a UNIX workstation. We used the nslookup program and the dig program. Note the differences in the output:

```
sj-cse-280% nslookup www.cisco.com
Note: nslookup is deprecated and may be removed from future releases.
Consider using the 'dig' or 'host' programs instead. Run nslookup with
the '-sil[ent]' option to prevent this message from appearing.
Server:          171.68.226.120
Address:         171.68.226.120#53
Name:            www.cisco.com
Address: 198.133.219.25

sj-cse-280% nslookup 198.133.219.25
Note: nslookup is deprecated and may be removed from future releases.
Consider using the 'dig' or 'host' programs instead. Run nslookup with
the '-sil[ent]' option to prevent this message from appearing.
Server:          171.68.226.120
Address:         171.68.226.120#53
25.219.133.198.in-addr.arpa      name = www.cisco.com.
```

The dig program prints more detailed information from the DNS packets:

```
sj-cse-280% dig 198.133.219.25

; <<>> DiG 9.0.1 <<>> 198.133.219.25
;; global options: printcmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 5231
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;198.133.219.25.                IN      A

;; AUTHORITY SECTION:
.                86400   IN      SOA
A.ROOT-SERVERS.NET. nstld.verisign-grs.com.
( 2002031800 1800 900 604800 86400 )

;; Query time: 135 msec
;; SERVER: 171.68.226.120#53(171.68.226.120)
;; WHEN: Mon Mar 18 09:42:20 2002
;; MSG SIZE rcvd: 107
```

Router Queries Multiple Name Servers

Dependant upon on the network activity level, the router may query multiple name servers listed in the configuration. This is an example:

```
router> test002
Translating ?test002?...domain server (172.16.33.18) (171.70.10.78)
(171.100.20.78)
(172.16.33.18) (171.70.10.78) (171.10.20.78)
Translating ?test002?...domain server (172.16.33.18) [OK]
Trying test002.rtr.abc.com (171.68.23.130)... Open
```

This behavior is expected and occurs when the router needs to create an Address Resolution Protocol (ARP) entry for the DNS server. By default, a router maintains an ARP entry for four hours. In periods of low activity, the router needs to complete the ARP entry and then perform the DNS query. If the ARP entry for the DNS server is not in the router ARP table, then you would get a failure if sending only one DNS query. So, two queries are sent out, one to get the ARP entry, if needed, and the second to actually do the DNS query. This behavior is common with TCP/IP applications.

Related Information

- [DNS Resource Records](#)
 - [Cisco CNS Network Registrar: Appendix A – Resource Records](#)
 - [DNS Support Page](#)
 - [IP Addressing and Application Services Support Page](#)
 - [IP Routing Support Page](#)
 - [Technical Support – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Sep 30, 2008

Document ID: 24182
