Configuración de DNS en los routers

Contenido

Introducción

En este documento se describe cómo configurar un Domain Naming System (DNS) para routers de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Interfaz de línea de comandos (CLI) de Cisco IOS®
- Comportamiento general de DNS

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

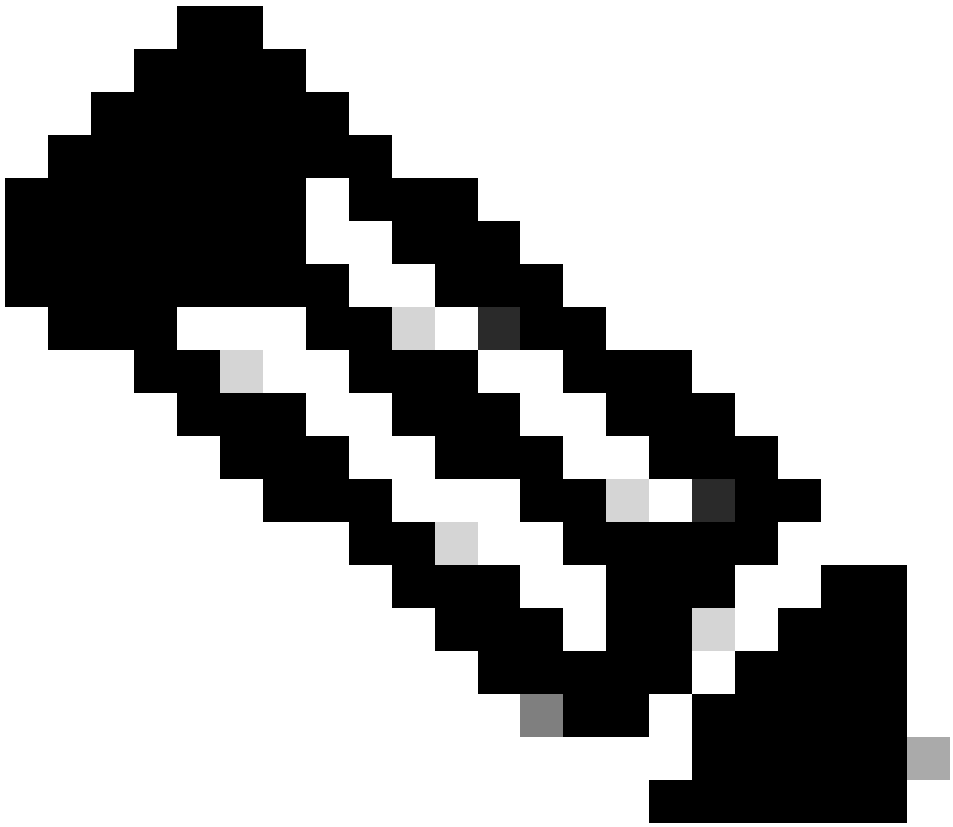
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Convenciones

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

Configuración de un router para utilizar búsquedas de DNS

El router se puede configurar para utilizar búsquedas DNS si desea utilizar los comandos`ping` o**`traceroute`**con un nombre de host en lugar de una dirección IP. Utilice estos comandos para hacerlo:

Comando	Descripción
ip domain lookup	Habilita la traducción de nombre a dirección basado en DNS del host. Este comando está activado como opción predeterminada.
ip name-server	Especifica la dirección de uno o más nombres de servidores.
ip domain list	Define una lista de dominios, que se probarán a la vez.  Nota: Si no hay lista de dominios, se utiliza el nombre de dominio que especificó con el comando de configuración global ip domain-name. Si hay lista de dominio, el nombre de dominio predeterminado no se utiliza.
ip domain name	Define un nombre de dominio predeterminado que el Cisco IOS Software utiliza para completar los nombres del host incompetentes (nombres sin un nombre de dominio

	con punto decimal). No incluya el período inicial que separa un nombre incompetente del nombre de dominio.
ip ospf name-lookup	Configura Open Shortest Path First (OSPF) para que busque nombres DNS para utilizar con el comando OSPF show EXEC. Esta característica facilita la identificación del router ya que éste se muestra por nombre en lugar de por ID de router o ID de vecino.

Este ejemplo muestra una configuración de muestra en un router configurado para una búsqueda básica del DNS:

Configuración básica de búsqueda de DNS de ejemplo

```
<#root>

Router#

show running-config

Building configuration...

Current configuration : 3922 bytes
!
! Last configuration change at 16:24:57 UTC Fri May 12 2023
!
version 17.3
service timestamps debug datetime msec
service timestamps log datetime msec
! Call-home is enabled by Smart-Licensing.
service call-home
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
platform console serial
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
!
!
!
!

ip name-server 192.168.1.1



!--- Configures the IP address of the name server. !--- Domain lookup is enabled by default.

!
!
interface GigabitEthernet1
 ip address 192.168.1.10 255.255.255.0
```

```
 negotiation auto
 no mop enabled
 no mop sysid
!
!

!--- Output Suppressed.
end
```

<#root>

Router#

ping www.cisco.com

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.37.145.84, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Router#
```

Troubleshoot

En condiciones poco comunes, puede ver una de estas condiciones de error:

<#root>

Router#

debug ip udp

UDP packet debugging is on
Router#

ping www.cisco.com

*Mar 8 06:26:41.732: UDP: sent src=10.69.16.66(5476), dst=

10.250.35.250(53)

, length=59
*Mar 8 06:26:44.740: UDP: sent src=10.69.16.66(5476), dst=10.250.35.250(53), length=59
*Mar 8 06:26:47.744: UDP: sent src=10.69.16.66(5476), dst=10.250.35.250(53), length=59

% Unrecognized host or address, or protocol not running.

```
Router#undebug all
All possible debugging has been turned off

Router#
```

ping www.cisco.com

Translating "www.cisco.com"...domain server (172.16.249.4) ¡¦
Not process

```
Router#
ping www.cisco.com


*May 12 16:48:36.302: Reserved port 43478 in Transport Port Agent for UDP IP type 1
*May 12 16:48:36.302: UDP: sent src=0.0.0.0(43478), dst=
255.255.255.255(53)
, length=50
*May 12 16:48:37.303: Reserved port 56191 in Transport Port Agent for UDP IP type 1
*May 12 16:48:37.303: UDP: sent src=0.0.0.0(56191), dst=255.255.255.255(53), length=50
*May 12 16:48:37.304: Released port 43478 in Transport Port Agent for IP type 1
*May 12 16:48:37.304: Released port 43478 in Transport Port Agent for IP type 1%
Unrecognized host or address, or protocol not running.
```

Siga estos pasos para resolver este problema:

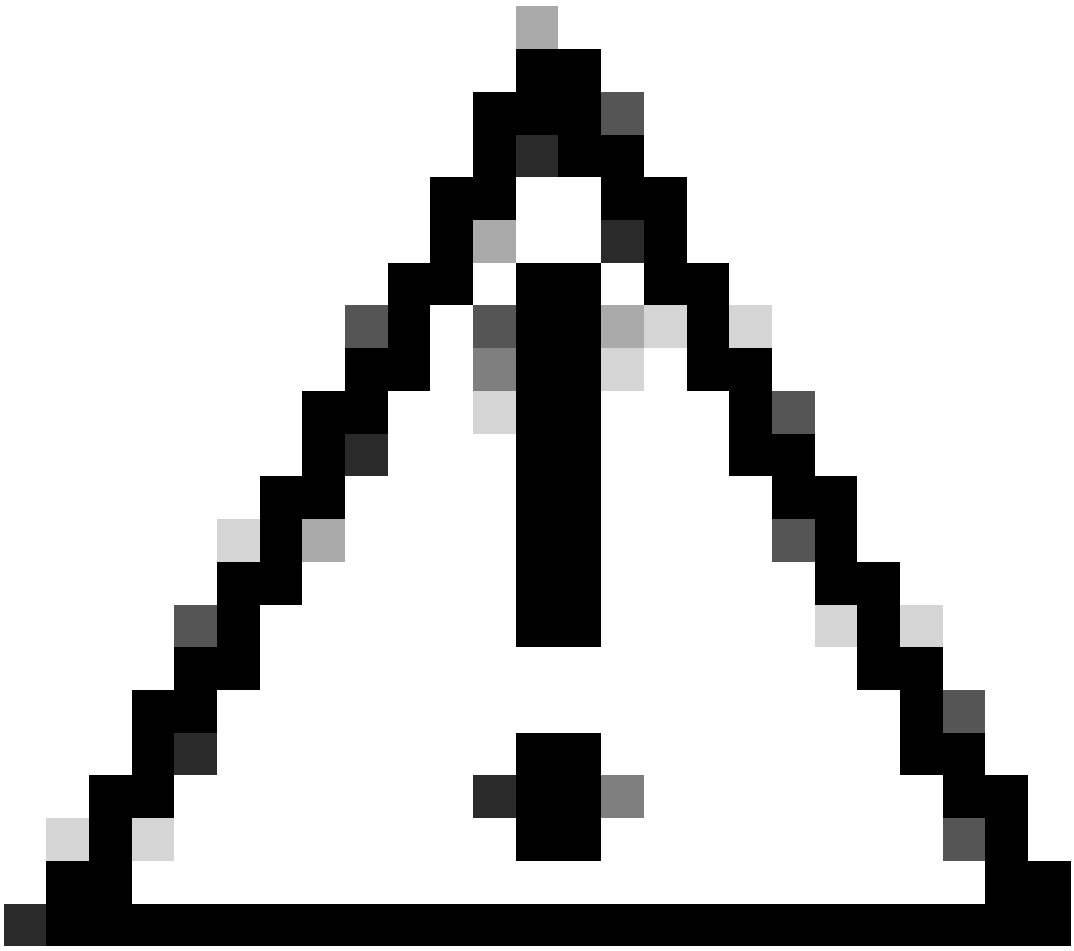
1. Asegúrese de que el router pueda alcanzar el servidor DNS. Haga ping al servidor DNS desde el router con su dirección IP y asegúrese de que el comando ip name-server se utiliza para configurar la dirección IP del servidor DNS en el router.
2. Utilice estos pasos para asegurarse de que el router envía los pedidos de búsqueda:

    a. Defina una lista de control de acceso (ACL) ese que coincida con los paquetes DNS:

    <#root>

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

    b. Utilice el comando debug ip packet 101.



Precaución: Asegúrese de especificar la ACL. Si habilita el comando debug ip packet sin una ACL, puede producir una gran cantidad de salida a la consola y afectar el acceso al dispositivo.

3. Asegúrese de tener el comando ip domain-lookup habilitado en el router.

Puede hacer un ping a un servidor web, pero no puede visualizar las páginas HTML

En raras ocasiones, no puede tener acceso a determinados sitios Web por su nombre. Este problema suele deberse a los sitios inaccesibles que realizan una búsqueda de DNS inversa en la dirección IP de origen para comprobar que la dirección no está suplantada. Si se devuelve una entrada incorrecta o ninguna entrada (es decir, no hay ningún nombre asociado para el intervalo IP), se puede bloquear la solicitud HTTP.

Cuando obtenga su nombre de dominio de Internet, también debe solicitar un dominio inaddr.arpa. Este dominio especial algunas veces se llama dominio inverso. El dominio inverso asigna direcciones IP numéricas a los nombres de dominio. Si su ISP le proporciona su servidor de nombres o su ISP le ha asignado una dirección de un bloque de sus propias direcciones, usted

no puede necesitar solicitar un dominio in-addr.arpa por su cuenta. Verifique su ISP.

Este es un ejemplo que utiliza www.cisco.com. El siguiente resultado se capturó desde una estación de trabajo UNIX. Se utilizan el`nslookup`programa y el programa dig. Observe las diferencias en el resultado:

<#root>

```
sj-cse-280%

nslookup www.cisco.com


Note:  nslookup is deprecated and can be removed from future releases.
Consider with the 'dig' or 'host' programs instead.  Run nslookup with
the '-sil[ent]' option to prevent this message from appearing.
Server:         172.16.226.120
Address:        172.16.226.120#53
Name:   www.cisco.com
Address: 192.168.219.25

sj-cse-280%

nslookup 192.168.219.25


Note:  nslookup is deprecated and can be removed from future releases.
Consider with the 'dig' or 'host' programs instead.  Run nslookup with
the '-sil[ent]' option to prevent this message from appearing.
Server:         172.16.226.120
Address:        172.16.226.120#53
10.219.133.198.in-addr.arpa     name = www.cisco.com.
```

El programa dig imprime información más detallada a partir de los paquetes de DNS.

<#root>

```
sj-cse-280%

dig 192.168.219.25



; <<>> DiG 9.0.1 <<>> 192.168.219.25
;; 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:
;192.168.219.25.                        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: 172.16.226.120#53(172.16.226.120)
;; WHEN: Mon Mar 18 09:42:20 2002
;; MSG SIZE  rcvd: 107
```

El router consulta múltiples nombres de servidores

Dependiendo del nivel de actividad de la red, el router puede consultar varios servidores de nombres incluidos en la configuración. Este es un ejemplo de la salida debug ip domain detail:

<#root>

Router#

show run | section name-server

 ip name-server 192.168.1.1 10.0.0.2 Router#
Router#

debug ip domain detail

Router#

test002

```
*May 12 17:56:32.723: DNS: detail: cdns_name_verify_internal: Checking if hostname is valid or not..
*May 12 17:56:32.723: DNS: info: cdns_name_verify_internal: Hostname is valid
*May 12 17:56:32.723: DNS: detail: cdns_get_rr_type: converting name kind 2000 to type 28
*May 12 17:56:32.723: DNS: detail: read_forwards: Forward zone server list:
*May 12 17:56:32.723: DNS: info: delegpt_log: DelegationPoint<.>: 0 names (0 missing), 2 addrs (0 result
*May 12 17:56:32.724: DNS: detail: val_operate: validator[module 0] operate: extstate:module_state_init
*May 12 17:56:32.724: DNS: info: log_nametypeclass: validator operate: query test002. AAAA IN
*May 12 17:56:32.724: DNS: detail: iter_operate: iterator[module 1] operate: extstate:module_state_init
*May 12 17:56:32.724: DNS: info: log_nametypeclass: resolving test002. AAAA IN
*May 12 17:56:32.724: DNS: detail: error_response: return error response NXDOMAIN
*May 12 17:56:32.724: DNS: detail: val_operate: validator[module 0] operate: extstate:module_wait_modul
*May 12 17:56:32.724: DNS: info: log_nametypeclass: validator operate: query test002. AAAA IN
*May 12 17:56:32.725: DNS: detail: cdns_get_rr_type: converting name kind 2000 to type 28
*May 12 17:56:32.725: DNS: detail: read_forwards: Forward zone server list:
*May 12 17:56:32.725: DNS: info: delegpt_log: DelegationPoint<.>: 0 names (0 missing), 2 addrs (0 result
*May 12 17:56:32.726: DNS: detail: val_operate: validator[module 0] operate: extstate:module_state_init
*May 12 17:56:32.726: DNS: info: log_nametypeclass: validator operate: query test002. AAAA IN
*May 12 17:56:32.726: DNS: detail: iter_operate: iterator[module 1] operate: extstate:module_state_init
```

***May 12 17:56:32.726: DNS: info: log_nametypeclass: resolving test002. AAAA IN *May 12 17:56:32.726: DNS**

```
*May 12 17:56:32.726: DNS: detail: cdns_set_udp_source_interface: using source interface GigabitEtherne
*May 12 17:56:33.726: DNS: detail: cdns_get_first_hop: dst 192.168.1.1, intf GigabitEthernet1
*May 12 17:56:33.726: DNS: detail: cdns_set_udp_source_interface: using source interface GigabitEtherne
*May 12 17:56:34.726: DNS: detail: iter_operate: iterator[module 1] operate: extstate:module_wait_reply
*May 12 17:56:34.726: DNS: info: log_nametypeclass: iterator operate: query test002. AAAA IN
*May 12 17:56:34.726: DNS: info: log_nametypeclass: processQueryTargets: test002. AAAA IN
*May 12 17:56:34.727: DNS: info: log_nametypeclass: sending query: test002. AAAA IN
*May 12 17:56:34.727: DNS: detail: log_name_addr: sending to target: <.> 192.168.1.1#53
*May 12 17:56:34.727: DNS: detail: cdns_get_first_hop: dst 192.168.1.1, intf GigabitEthernet1
*May 12 17:56:34.727: DNS: detail: cdns_set_udp_source_interface: using source interface GigabitEtherne
```

```
*May 12 17:56:35.729: DNS: detail: iter_operate: iterator[module 1] operate: extstate:module_wait_reply
*May 12 17:56:35.729: DNS: info: log_nametypeclass: iterator operate: query test002. AAAA IN
*May 12 17:56:35.729: DNS: info: log_nametypeclass: response for test002. AAAA IN

*May 12 17:56:35.729: DNS: info: log_name_addr: reply from <.> 192.168.1.1#53 *May 12 17:56:35.729: DNS:

*May 12 17:56:35.729: DNS: info: log_nametypeclass: processQueryTargets: test002. AAAA IN

*May 12 17:56:35.729: DNS: info: log_nametypeclass: sending query: test002. AAAA IN *May 12 17:56:35.729

*May 12 17:56:35.730: DNS: detail: cdns_set_udp_source_interface: using source interface GigabitEtherne
*May 12 17:58:35.732: DNS: error: comm_point_tcp_handle_write: tcp connect: Connection refused
*May 12 17:58:35.732: DNS: detail: log_addr: remote address is ip4 10.0.0.2 port 53 (len 16)
*May 12 17:58:35.732: DNS: detail: outnet_tcp_cb: outnettcp got tcp error -1
*May 12 17:58:35.732: DNS: detail: log_addr: tcp error for address ip4 10.0.0.2 port 53 (len 16)
*May 12 17:58:35.732: DNS: detail: iter_operate: iterator[module 1] operate: extstate:module_wait_reply
*May 12 17:58:35.732: DNS: info: log_nametypeclass: iterator operate: query test002. AAAA IN
*May 12 17:58:35.732: DNS: info: log_nametypeclass: processQueryTargets: test002. AAAA IN
```

Este comportamiento se espera y ocurre cuando el router necesita crear una entrada de protocolo de resolución de direcciones (ARP) para el servidor DNS. De forma predeterminada, un router mantiene una entrada ARP durante cuatro horas. En los períodos de actividad baja, el router debe de completar la entrada ARP y realizar la interrogación DNS. Si la entrada ARP para el servidor DNS no está en la tabla ARP del router, obtendrá una falla si envía solamente una consulta DNS. Por lo tanto, se envían dos consultas, una para obtener la entrada ARP, si es necesario, y la segunda para hacer realmente la consulta DNS. Este comportamiento es común en las aplicaciones TCP/IP.

Información Relacionada

- Compatibilidad con direccionamiento IP
- Compatibilidad con routing de IP
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).