Configurazione di DNS sui router

Sommario

Introduzione

In questo documento viene descritto come configurare un sistema DNS (Domain Naming System) sui router Cisco.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Interfaccia a riga di comando (CLI) di Cisco IOS®
- Comportamento DNS generale

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

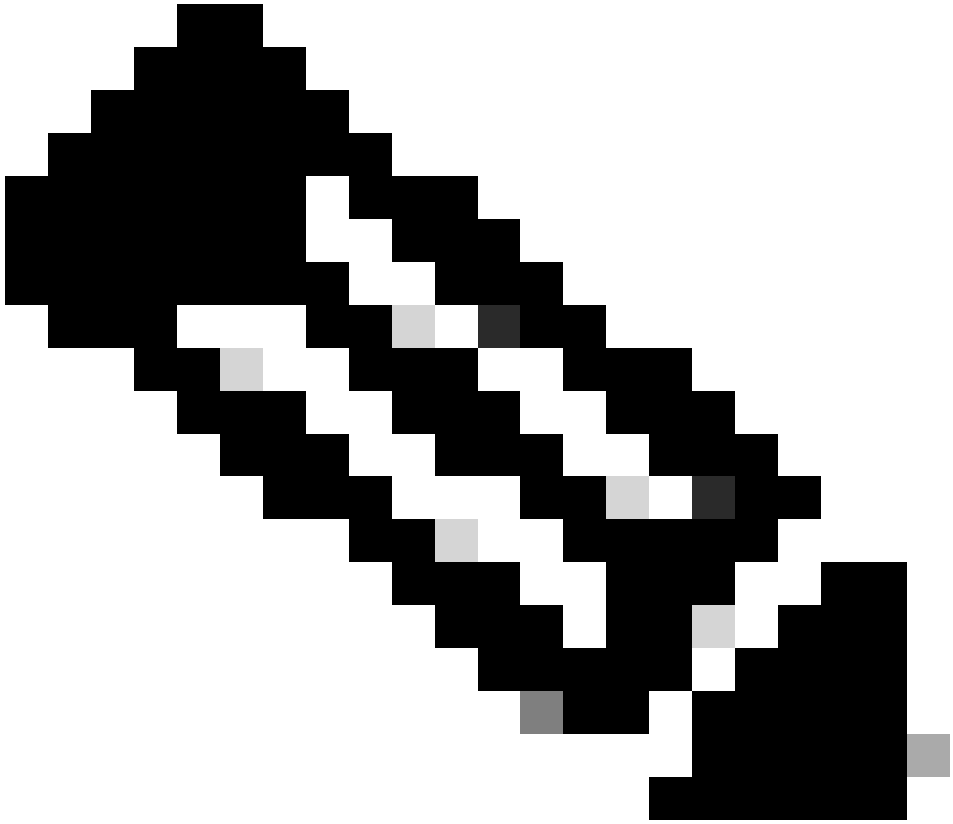
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Configurazione di un router per le ricerche DNS

Se si desidera utilizzare i comandi o con un nome host anziché un indirizzo IP, è possibile configurare il router in modo che effettui ricerche DNS.ping **traceroute** Utilizzare questi comandi:

Comando	Descrizione
ip domain lookup	Abilita la conversione tra nome host basato su DNS e indirizzo. Questo comando è abilitato per impostazione predefinita.
ip name-server	Specifica l'indirizzo di uno o più server dei nomi.
ip domain list	Definisce un elenco di domini, che verranno provati a turno.  Nota: Se non è presente alcun elenco di domini, viene utilizzato il nome di dominio specificato con il comando di configurazione globale ip domain-name. Se è presente un elenco di domini, il nome di dominio predefinito non viene utilizzato.
ip domain name	Definisce un nome di dominio predefinito utilizzato da Cisco IOS Software per completare i nomi host non completi (nomi di dominio con notazione decimale puntata). Non includere il punto iniziale che separa un nome non completo dal nome di dominio.

ip ospf name-lookup	Configura il protocollo OSPF (Open Shortest Path First) in modo che cerchi i nomi DNS da utilizzare in tutti gli output del comando OSPF show EXEC. Questa funzione facilita l'identificazione di un router perché il router viene visualizzato per nome anziché per ID del router o ID del dispositivo vicino.

In questo esempio viene mostrata la configurazione di un router che utilizza la ricerca DNS di base:

Esempio di configurazione della ricerca DNS di base

```
<#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#
```

Risoluzione dei problemi

In rare condizioni, potrebbero verificarsi questi errori:

<#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.
```

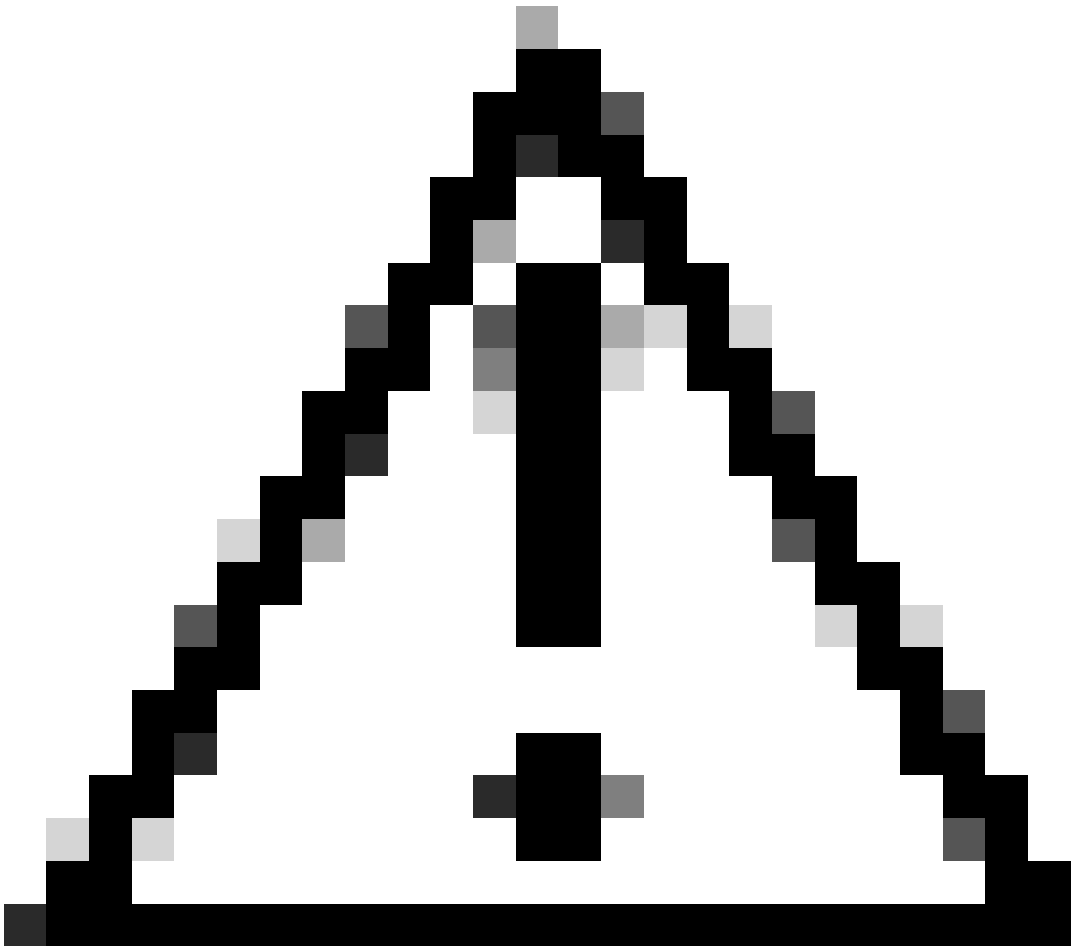
Completare questa procedura per risolvere il problema:

1. Accertarsi che il router possa raggiungere il server DNS. Eseguire il ping tra il server DNS e il router con il relativo indirizzo IP per verificare che il comando ip name-server venga utilizzato per configurare l'indirizzo IP del server DNS sul router.
2. Per accertarsi che il router inoltri le richieste di ricerca, procedere come segue:
    a. Definire un ACL (Access Control List) corrispondente per i pacchetti DNS:

    <#root>

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

    b. Utilizzare il comando debug ip packet 101.



Attenzione: Accertarsi di specificare l'ACL. Se si abilita il comando debug ip packet senza un ACL, la console potrebbe generare un elevato numero di output e compromettere l'accesso al dispositivo.

3. Accertarsi che il comando ip domain-lookup sia abilitato sul router.

Il ping sul server Web viene eseguito correttamente, ma non è possibile visualizzare le pagine HTML

In rari casi non è possibile accedere a determinati siti Web per nome. Questo problema è in genere causato da siti inaccessibili che eseguono una ricerca DNS inversa sull'indirizzo IP di origine per verificare che non sia stato falsificato. Se viene visualizzata una voce errata o non viene restituita alcuna voce (in altre parole, non esiste un nome associato per l'intervallo IP), la richiesta HTTP può essere bloccata.

Quando si ottiene il nome di dominio Internet, è necessario richiedere anche un dominio inaddr.arpa. Questo dominio speciale è talvolta chiamato dominio inverso. Il dominio inverso associa gli indirizzi IP numerici ai nomi di dominio. Se il server dei nomi o il provider di servizi Internet ha assegnato all'utente un indirizzo da un blocco di indirizzi propri, non è possibile

richiedere un dominio in-addr.arpa. Verificare questa condizione con il proprio ISP.

Ecco un esempio in cui viene utilizzato www.cisco.com. L'output successivo è stato acquisito da una postazione di lavoro UNIX. Vengono utilizzati il programma nslookupe il programma dig. Notare le differenze nell'output:

<#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.
```

Il programma dig restituisce informazioni più dettagliate sui pacchetti 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
```

Interrogazioni del router su più server dei nomi

A seconda del livello di attività della rete, il router può interrogare più server dei nomi elencati nella configurazione. Riportiamo un esempio di output del comando 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: info: log_nametypeclass: processQueryTargets: test002. AAAA IN**
***May 12 17:56:32.726: DNS: info: log_nametypeclass: sending query: test002. AAAA IN**
***May 12 17:56:32.726: DNS: detail: log_name_addr: sending to target: <.> 192.168.1.1#53**
***May 12 17:56:32.726: DNS: detail: cdns_get_first_hop: dst 192.168.1.1, intf GigabitEthernet1**

```
*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: info: processQueryResponse: query response was THROWAWAY

*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: DNS: detail: log_name_addr: sending to target: <.> 10.0.0.2#53
*May 12 17:56:35.730: DNS: detail: cdns_get_first_hop: dst 10.0.0.2, intf GigabitEthernet1

*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
```

Questo comportamento è normale e si verifica quando il router deve creare una voce ARP (Address Resolution Protocol) per il server DNS. Per impostazione predefinita, un router conserva una voce ARP per quattro ore. Nei periodi di scarsa attività, il router deve completare la voce ARP ed eseguire la query DNS. Se la voce ARP per il server DNS non è presente nella tabella ARP del router, l'invio di una sola query DNS genera un errore. Quindi vengono inviate due query, una per ottenere la voce ARP, se necessaria, e la seconda per eseguire effettivamente la query DNS. Questo comportamento è comune nelle applicazioni TCP/IP.

Informazioni correlate

- Supporto per l'indirizzamento IP
- Supporto per il routing IP
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).