Configurer le DNS sur les routeurs

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés
- Conventions

Configuration d'un routeur pour utiliser les recherches DNS

- Dépannage

Vous pouvez envoyer un ping à un serveur Web mais vous ne pouvez pas afficher les pages HTML

Le routeur interroge différents serveurs de noms

Informations connexes

Introduction

Ce document décrit comment configurer un système de noms de domaine (DNS) pour les routeurs Cisco.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Interface de ligne de commande (CLI) Cisco IOS®
- Comportement général du système DNS

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

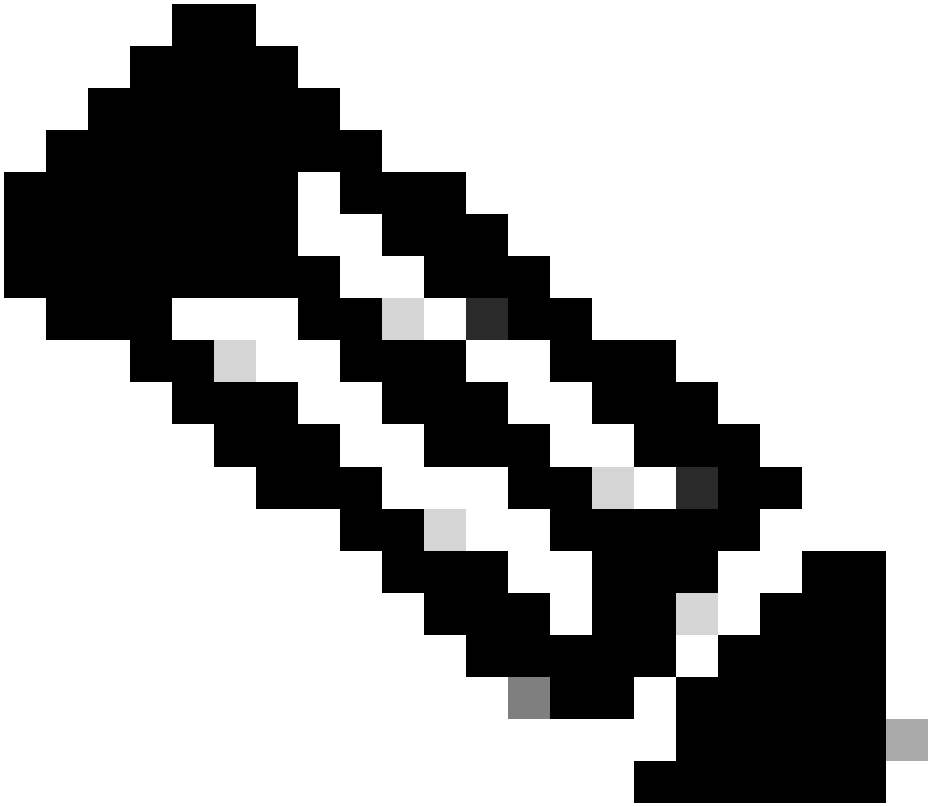
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configuration d'un routeur pour utiliser les recherches DNS

Votre routeur peut être configuré pour utiliser les recherches DNS si vous souhaitez utiliser les commandes`ping` ou**`traceroute`**avec un nom d'hôte plutôt qu'une adresse IP. Pour cela, utilisez les commandes suivantes :

Commande	Description
ip domain lookup	Active la conversion du nom d'hôte de type DNS en adresse. Cette commande est activée par défaut.
ip name-server	Spécifie l'adresse d'un ou de plusieurs serveurs de noms.
ip domain list	Définit une liste de domaines à essayer tour à tour.  Remarque : S'il n'y a aucune liste de domaines, le nom du domaine que vous avez spécifié avec la commande ip domain-name global configuration est utilisé. S'il y a une liste de domaines, le nom du domaine par défaut n'est pas utilisé.
ip domain name	Définit un nom de domaine par défaut que le logiciel Cisco IOS utilise pour compléter les noms d'hôte incomplets (noms sans nom de domaine en notation décimale

	pointée). N'incluez pas le point initial qui sépare un nom incomplet du nom du domaine.
ip ospf name-lookup	Configure Open Shortest Path First (OSPF) pour rechercher les noms DNS à utiliser dans tous les affichages de la commande EXEC ospf show. Cette fonctionnalité facilite l'identification d'un routeur, car le routeur est affiché avec son nom au lieu de son ID de routeur ou ID de voisin.

Cet exemple montre une configuration sur un routeur configuré pour la recherche DNS de base :

Exemple de configuration d'une DNS de 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#
```

Dépannage

Dans de rares cas, vous pouvez voir l'une de ces conditions d'erreur :

<#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.

Suivez ces étapes pour dépanner le problème suivant :

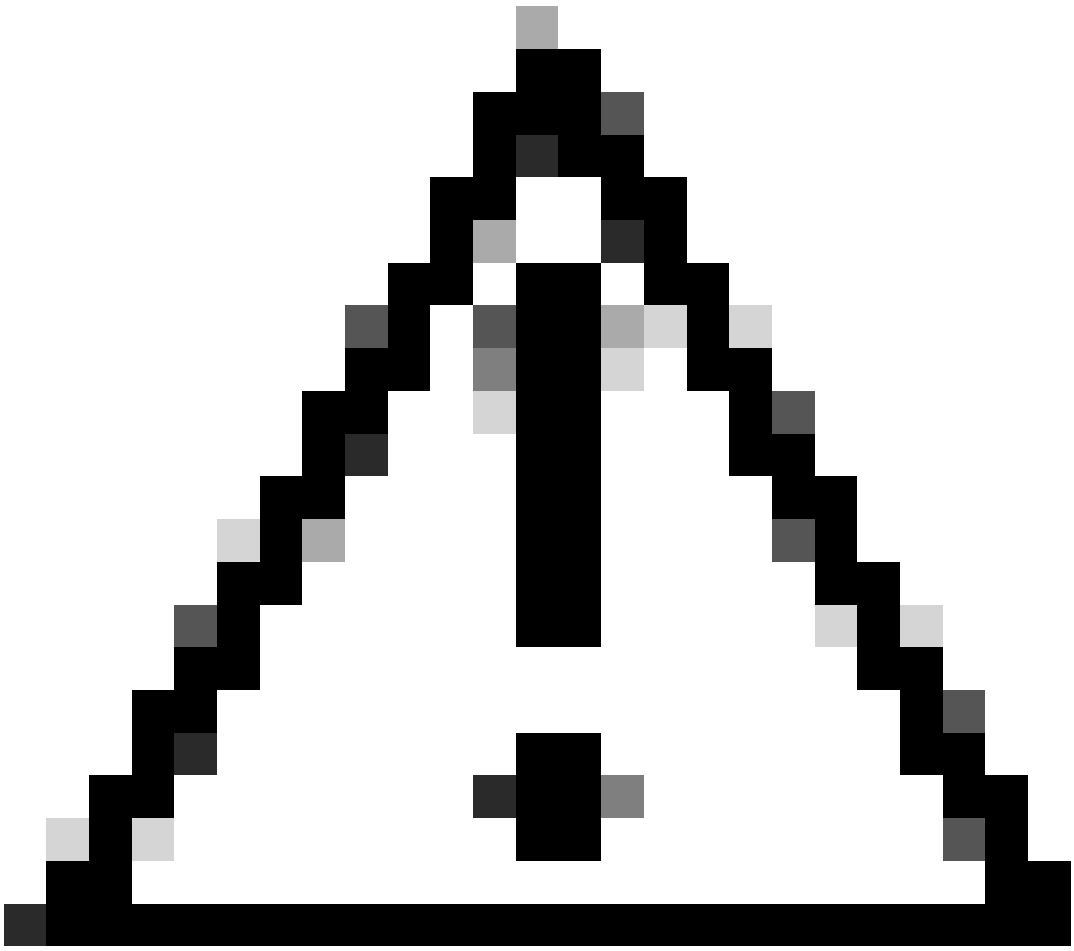
1. Assurez-vous que le routeur peut atteindre le serveur DNS. Envoyez une requête ping au serveur DNS à partir du routeur avec son adresse IP et assurez-vous que la commande ip name-server est utilisée pour configurer l'adresse IP du serveur DNS sur le routeur.
2. Suivez les étapes ci-dessous pour garantir que le routeur transmet les demandes de recherche :

    a. Définissez une liste de contrôle d'accès (ACL) appropriée sur les paquets DNS :

    <#root>

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

    b. Utilisez la commande debug ip packet 101.



Mise en garde : Veillez à spécifier l'ACL. Si vous activez la commande debug ip packet sans ACL, elle peut produire une grande quantité de sortie vers la console et affecter l'accès au périphérique.

3. Assurez-vous que la commande ip domain-lookup est activée sur le routeur.

Vous pouvez envoyer un ping à un serveur Web mais vous ne pouvez pas afficher les pages HTML

Dans de rares cas, vous ne pouvez pas accéder à des sites Web particuliers par leur nom. Ce problème provient généralement des sites inaccessibles qui effectuent une recherche DNS inverse sur l'adresse IP source pour vérifier que l'adresse n'est pas usurpée. Si une entrée incorrecte ou aucune entrée n'est renvoyée (en d'autres termes, il n'y a pas de nom associé pour la plage IP), la requête HTTP peut être bloquée.

Lorsque vous obtenez votre nom de domaine Internet, vous devez également demander un domaine inaddr.arpa. Ce domaine spécial s'appelle un domaine inverse. Le domaine inverse mappe les adresses IP numériques avec les noms de domaine. Si votre FAI vous fournit votre serveur de noms ou si votre FAI vous a attribué une adresse à partir d'un bloc de ses propres

adresses, vous ne pouvez pas demander un domaine in-addr.arpa seul. Vérifiez avec votre ISP.

Voici un exemple qui utilise www.cisco.com. Cette sortie suivante a été capturée à partir d'une station de travail UNIX. Le programme nslookup et le programme dig sont utilisés. Notez les différences contenues dans la sortie :

<#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.
```

Le programme dig imprime plus d'informations sur les paquets 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
```

Le routeur interroge différents serveurs de noms

En fonction du niveau d'activité du réseau, le routeur peut interroger plusieurs serveurs de noms répertoriés dans la configuration. Voici un exemple du résultat de la commande 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
```

Ce comportement est prévu et se produit quand le routeur a besoin de créer une entrée de Protocole de résolution d'adresse (ARP) pour le serveur DNS. Par défaut, un routeur conserve une entrée ARP pendant quatre heures. Lorsque l'activité est réduite, le routeur doit compléter l'entrée ARP puis exécuter la requête DNS. Si l'entrée ARP pour le serveur DNS ne figure pas dans la table ARP du routeur, vous obtiendrez un échec s'il envoie une seule requête DNS. Ainsi, deux requêtes sont envoyées, une pour extraire l'entrée ARP, si nécessaire, et la seconde pour exécuter effectivement la requête DNS. Ce comportement est commun aux applications TCP/IP.

Informations connexes

- Prise en charge des adresses IP
- Prise en charge du routage IP
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.