Konfigurieren von DNS auf Routern

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie ein Domain Name System (DNS) für Cisco Router konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco IOS® Befehlszeilenschnittstelle (CLI)
- Allgemeines DNS-Verhalten

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

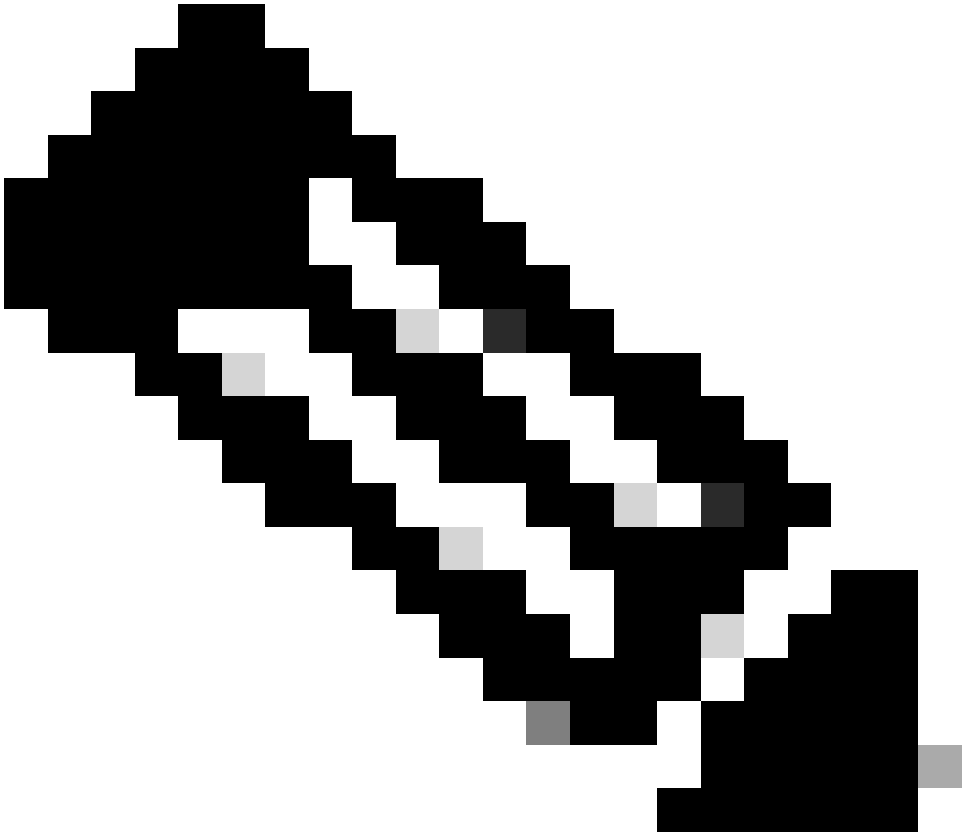
Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Einrichten eines Routers für die Verwendung von DNS-Lookups

Der Router kann so konfiguriert werden, dass er DNS-Lookups verwendet, wenn Sie die ping oder **traceroute** Befehle mit einem Hostnamen anstelle einer IP-Adresse verwenden möchten. Verwenden Sie dazu die folgenden Befehle:

Command	Beschreibung
ip domain lookup	Aktiviert die DNS-basierte Übersetzung des Hostnamens in die Adresse. Dieser Befehl ist standardmäßig aktiviert.
ip name-server	Gibt die Adresse eines oder mehrerer Nameserver an.
ip domain list	Definiert eine Liste von Domänen, die nacheinander getestet werden sollen.

	 **Hinweis: Wenn keine Domänenliste vorhanden ist, wird der Domänenname verwendet, den Sie mit dem globalen Konfigurationsbefehl ip domain-name angegeben haben.** Wenn es eine Domänenliste gibt, wird der Standard-Domänenname nicht verwendet.
ip domain name	Definiert einen Standarddomänennamen, der von der Cisco IOS-Software zur Vervollständigung nicht qualifizierter Hostnamen verwendet wird (Namen ohne Domänennamen mit Punkten). Lassen Sie den Punkt weg, der einen nicht qualifizierten Namen vom Domänennamen trennt.
ip ospf name-lookup	Konfiguriert Open Shortest Path First (OSPF), um DNS-Namen zur Verwendung in allen OSPF show EXEC-Befehlsanzeigen zu suchen. Diese Funktion erleichtert die Identifizierung eines Routers, da der Router nicht anhand seiner Router-ID oder Nachbar-ID, sondern anhand des Namens angezeigt wird.

Dieses Beispiel zeigt eine Beispielkonfiguration auf einem Router, der für die grundlegende DNS-Suche konfiguriert ist:

Beispiel für eine grundlegende DNS-Lookup-Konfiguration

```
     <#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#
```

Fehlerbehebung

Unter seltenen Umständen können Sie eine der folgenden Fehlerbedingungen sehen:

```
<#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.

Gehen Sie folgendermaßen vor, um dieses Problem zu beheben:

1. Stellen Sie sicher, dass der Router den DNS-Server erreichen kann. Senden Sie einen Ping an den DNS-Server vom Router mit seiner IP-Adresse, und stellen Sie sicher, dass der Befehl **ip name-server** zum Konfigurieren der IP-Adresse des DNS-Servers auf dem Router verwendet wird.

2.

Gehen Sie folgendermaßen vor, um sicherzustellen, dass der Router die Suchanfragen weiterleitet:

a.

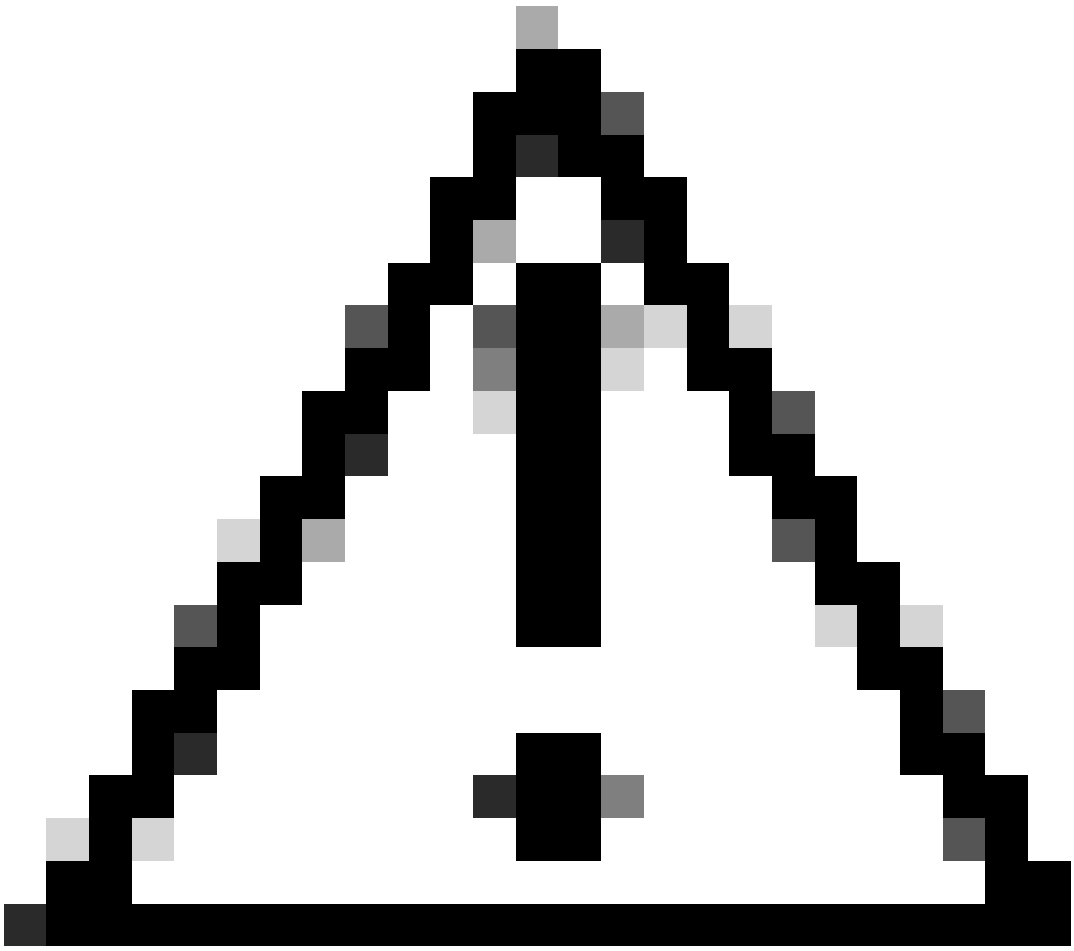
Definieren Sie eine Zugriffskontrollliste (ACL), die mit DNS-Paketen übereinstimmt:

<#root>

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

b.

Verwenden Sie **den Befehl debug ip packet 101**.



Vorsicht: Stellen Sie sicher, dass Sie die ACL angeben. Wenn Sie den Befehl **debug ip packet** ohne ACL aktivieren, kann dies zu einer großen Menge an Ausgabe an die Konsole führen und den Zugriff auf das Gerät beeinträchtigen.

3.

Stellen Sie sicher, dass der Befehl **eip domain-**lookup auf dem Router aktiviert ist.

Sie können einen Webserver anpingen, aber Sie können die HTML-Seiten nicht anzeigen

In seltenen Fällen können Sie nicht über den Namen auf bestimmte Websites zugreifen. Dieses Problem resultiert normalerweise aus den unzugänglichen Websites, die eine umgekehrte DNS-Suche nach der Quell-IP-Adresse durchführen, um sicherzustellen, dass die Adresse nicht gefälscht ist. Wenn ein falscher Eintrag oder kein Eintrag zurückgegeben wird (d. h. es gibt keinen zugehörigen Namen für den IP-Bereich), kann die HTTP-Anfrage blockiert werden.

Wenn Sie Ihren Internet-Domain-Namen erhalten, müssen Sie sich auch für eine inaddr.arpa-Domain bewerben. Diese spezielle Domäne wird manchmal als Reverse-Domäne bezeichnet. Die Reverse-Domäne ordnet numerische IP-Adressen Domänennamen zu. Wenn Ihr ISP Ihren Namensserver bereitstellt oder Ihnen von Ihrem ISP eine Adresse aus einem Block seiner eigenen Adressen zugewiesen wird, müssen Sie keine eigene in-addr.arpa-Domäne beantragen. Erkundigen Sie sich bei Ihrem ISP.

Hier ist ein Beispiel, das www.cisco.com verwendet. Diese nächste Ausgabe wurde von einer UNIX-Workstation erfasst. Das nslookup Programm und das Grabprogramm werden verwendet. Beachten Sie die Unterschiede in der Ausgabe:

```
    <#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.
```

Das Programm „dig“ gibt detailliertere Informationen aus den DNS-Paketen aus:

```
    <#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
```

Router fragt mehrere Nameserver ab

Abhängig von der Netzwerkaktivitätsebene kann der Router mehrere in der Konfiguration aufgeführte Namenserver abfragen. Dies ist ein Beispiel aus der Ausgabe **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
```

Dieses Verhalten wird erwartet und tritt auf, wenn der Router einen ARP-Eintrag (Address Resolution Protocol) für den DNS-Server erstellen muss. Standardmäßig verwaltet ein Router einen ARP-Eintrag vier Stunden lang. In Zeiten geringer Aktivität muss der Router den ARP-Eintrag vervollständigen und dann die DNS-Abfrage durchführen. Wenn sich der ARP-Eintrag für den DNS-Server nicht in der ARP-Tabelle des Routers befindet, tritt ein Fehler auf, wenn nur eine DNS-Abfrage gesendet wird. Daher werden zwei Abfragen gesendet, eine, um den ARP-Eintrag abzurufen, falls erforderlich, und die zweite, um die DNS-Abfrage durchzuführen. Dieses Verhalten ist bei TCP/IP-Anwendungen üblich.

Zugehörige Informationen

- **IP-Adressierungsunterstützung**
- **IP-Routing-Unterstützung**
- **Technischer Support und Downloads von Cisco**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.