تكوين نظام أسماء النطاقات (DNS) على الموجّهات

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين نظام تسمية المجال (DNS) لموجّهات Cisco.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- واجهة سطر الأوامر (CLI) ®IOS من Cisco
- سلوك DNS العام

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

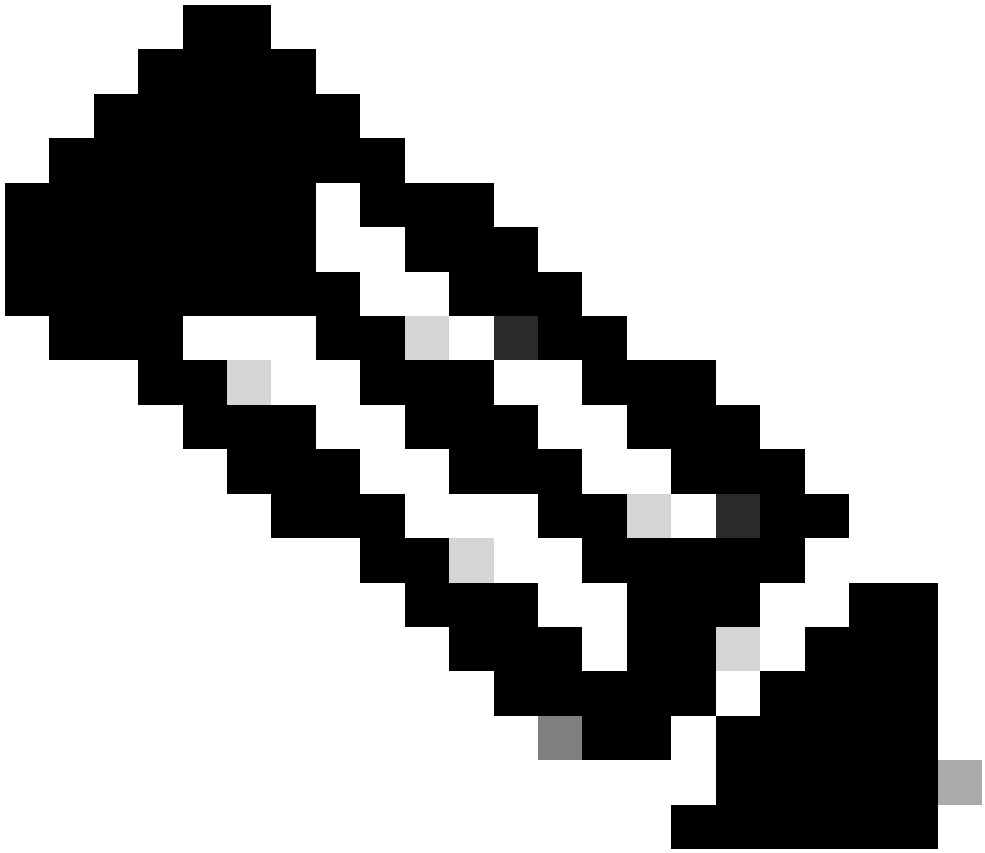
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

إعداد موجه الاستخدام عمليات بحث DNS

يمكن تكوين الموجه الخاص بك الاستخدام عمليات بحث DNS إذا كنت ترغب في إستخدام الأوامرping **traceroute**و مع اسم مضيف بدلا من عنوان IP. أستخدم هذه الأوامر للقيام بذلك:

	الوصف
البحث عن مجال ip	تمكين ترجمة اسم المضيف إلى عنوان المستندة إلى DNS. يتم تمكين هذا الأمر بشكل افتراضي.
ip name-server	تحديد عنوان خادم اسم واحد أو أكثر.
قائمة مجالات ip	تعريف قائمة بالمجالات، كل منها ليتم تجربته بالتناوب.  ملاحظة: في حالة عدم وجود قائمة مجالات، يتم إستخدام اسم المجال الذي حددته باستخدام أمر التكوين العام ip domain-name . في حالة وجود قائمة مجالات، لا يتم إستخدام اسم المجال الافتراضي.

اسم مجال ip	تعريف اسم مجال افتراضي يستخدمه برنامج Cisco IOS لإكمال أسماء البيئات المضيفة غير المؤهلة (أسماء بدون اسم مجال عشري منقوط). لا تقوم بتضمين الفترة الأولية التي تفصل اسم غير مؤهل عن اسم المجال.
ip ospf name-lookup	يقوم بتكوين فتح أقصر مسار أولا (OSPF) للبحث عن أسماء DNS للاستخدام في أوامر EXEC ل OSPF. تجعل هذه الميزة من السهل تعريف الموجه لأن جميع عروض الموجه يتم عرضه بالاسم بدل من معرف الموجه الخاص به أو معرف المجاور له.

يوضح هذا المثال نموذجا للتكوين على موجه تم تكوينه للبحث الأساسي في DNS:

نموذج تكوين البحث عن DNS الأساسي

```
<#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#
```

استكشاف الأخطاء وإصلاحها

تحت حالات نادرة، يمكنك أن ترى حالة من حالات الخطأ هذه:

<#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.

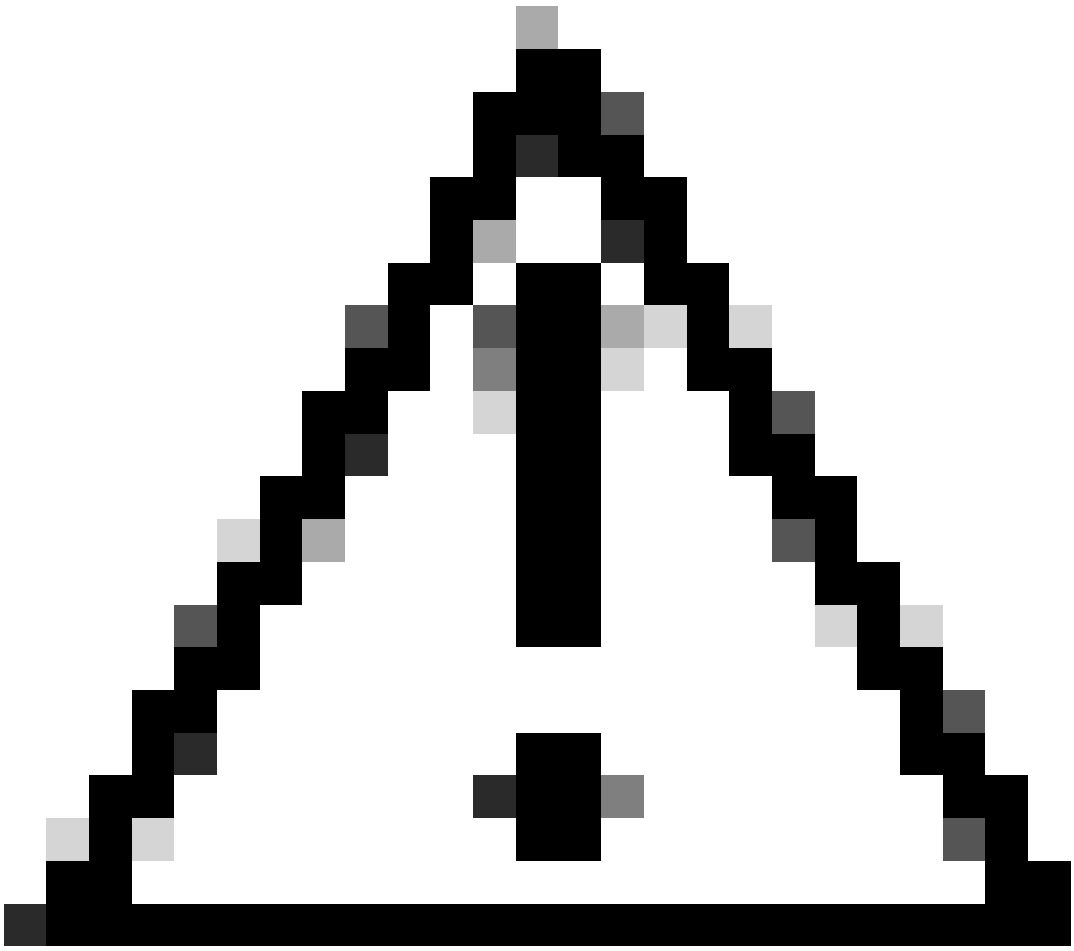
أتمت اذه steps أن يتحرى اذه مشكلة:

1. تأكد من إمكانية وصول الموجه إلى خادم DNS. زوِّي خادم DNS من الموجه باستخدام عنوان IP الخاص به، وتأكد من إستخدام الأمر ip name-server لتكوين عنوان IP الخاص بخادم DNS على الموجه.
2. أستخدم هذه الخطوات لضمان أن الموجه يقوم بإعادة توجيه طلبات البحث:
   a. تحديد قائمة تحكم في الوصول (ACL) تطابق على حزم DNS:

      <#root>

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

   b. أستخدم الأمر debug ip packet 101.



تحذير: تأكد من تحديد قائمة التحكم في الوصول (ACL). إذا قمت بتمكين الأمر debug ip packet دون قائمة تحكم في الوصول (ACL)، فيمكنه إنتاج كمية كبيرة من الإخراج إلى وحدة التحكم والتأثير على الوصول إلى الجهاز.

3. تأكد من تمكين الأمر ip domain-lookup على الموجه.

يمكنك إختبار اتصال خادم ويب، ولكن لا يمكنك عرض صفحات HTML

في حالات نادرة، يتعذر عليك الوصول إلى مواقع ويب معينة بالاسم. تنتج هذه المشكلة عادة من المواقع التي يتعذر الوصول إليها والتي تقوم بإجراء بحث DNS عكسي على عنوان IP المصدر للتحقق من عدم انتحال العنوان. إذا لم يتم إرجاع إدخال غير صحيح أو لم يتم إرجاع إدخال (بمعنى آخر، لا يوجد اسم مقترن لنطاق IP)، فيمكن حظر طلب HTTP.

عند حصولك على اسم مجال الإنترنت، يجب أيضا تقديم طلب لمجال inaddr.arpa. يسمى هذا المجال الخاص أحيانا بمجال عكسي. يعمل المجال العكسي على تعيين عناوين IP الرقمية إلى أسماء المجالات. إذا كان موزود خدمة الإنترنت (ISP) الخاص بك يوفر خادم الاسم أو قام موزود خدمة الإنترنت (ISP) بتعيين عنوان لكل من كتلة من العناوين الخاصة به، فلن يمكنك التقدم بطلب لمجال in-addr.arpa خاص بك. تحقق من ذلك مع موزود خدمة الإنترنت (ISP).

فيما يلي مثال يستخدم www.cisco.com. تم التقاط هذا الإخراج التالي من محطة عمل UNIX. يستخدم برنامج البحث وبرنامج الحفر. لاحظ الفروق في المخرجات:

<#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.
```

يطبع برنامج الحفر معلومات أكثر تفصيلا من حزم 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
```

الموجه يستعلم خوادم أسماء متعددة

يمكن للموجه، الذي يعتمد على مستوى نشاط الشبكة، الاستعلام عن خوادم أسماء متعددة مدرجة في التكوين. هذا مثال من تفاصيل مجال IP الخاص بتصحيح الإخراج:

<#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
```

هذا السلوك متوقع ويحدث عندما يحتاج الموجه إلى إنشاء إدخال بروتوكول تحليل العناوين (ARP) لخادم DNS. بشكل افتراضي، يحتفظ الموجه بإدخال ARP لأربع ساعات. في فترات النشاط المنخفض، يحتاج الموجه إلى إكمال إدخال ARP ثم تنفيذ استعلام DNS. إذا لم يكن إدخال ARP لخادم DNS في جدول ARP للموجه، فستحصل على فشل إذا قام بإرسال استعلام DNS واحد فقط. لذلك، يتم إرسال استفساريين، أحدهما للحصول على إدخال ARP، إذا لزم الأمر، والآخر للقيام باستعلام DNS بالفعل. هذا السلوك شائع مع تطبيقات TCP/IP.

معلومات ذات صلة

- دعم عنونة IP
- دعم توجيه IP
- الدعم الفني والتنزيلات من Cisco

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).