


วิธีการทดสอบ EDNS เบื้องต้น

1.เข้าไปที่ Website: <https://dnsflagday.net>

 <https://dnsflagday.net>



What is happening?

The current [DNS](#) is unnecessarily slow and suffers from inability to deploy new features. To remediate these problems, [vendors of DNS software](#) and also big [public DNS providers](#) are going to remove certain workarounds on February 1st, 2019.

This change affects only sites which operate software which is not following published standards.
Are you affected?

2.พิมพ์ Domain ที่ต้องการทดสอบแล้วกดปุ่ม Test

Domain owners

Please check if your domain is affected:

Test your domain

Domain name (without www):

3.ผลจากการทดสอบ

3.1. All Ok! หมายความว่า DNS Server ที่ เป็น Authoritative ของ Domain ที่เราดูแล สามารถรองรับมาตรฐาน ENDS แล้ว

Domain owners

Please check if your domain is affected:

Test your domain

Domain name (without www):

Testing completed:

dga.or.th: All Ok!



This domain is perfectly ready, congratulations!

3.2. Minor problems detected! หมายความว่า DNS Server ที่เป็น Authoritative ของ Domain ที่เราดูแล อาจมีค่าบางอย่างที่ทำให้การทดสอบไม่ผ่านทั้งหมด ดังนั้นสามารถเข้าไปดู technical report ตาม Link ด้านล่าง

Domain owners

Please check if your domain is affected:

Test your domain

Domain name (without www):

ac.th

Test!

Testing completed:

.ac.th: Minor problems detected!



This domain is going to work after the 2019 DNS flag day BUT it does not support the latest DNS standards. As a consequence this domain cannot support the latest security features and might be an easier target for network attackers than necessary, and might face other issues later on. We recommend your domain administrator to fix issues listed in the following

technical report <https://ednscomp.isc.org/ednscomp/2c4686b4de>

3.2.1. เมื่อเข้าไปตาม Link แล้วจะพบรายละเอียดเพิ่มเติมว่าติดขัดในการทดสอบอย่างไรตามภาพตัวอย่าง EDNS สามารถใช้งานได้”แต่มีค่า Return บางอย่างออกมาทำให้ระบบทดสอบแจ้งเตือน เบื้องต้นจะพบใน DNS Server ฝั่ง Microsoft ตั้งแต่ Windows Server 2012 ขึ้นไป



Internet Systems
Consortium

EDNS Compliance Tester

Checking: ' .ac.th' as at 2019-01-15T07:05:13Z

```
.ac.th. @202.29. ( ac.th.): dns=ok edns=ok edns1=ok edns@512=ok ednsopt=echoed
edns1opt=echoed do=ok ednsflags=ok docookie=ok edns512tcp=ok optlist=ok,subnet
.ac.th. @2001:3c8: ( ac.th.): dns=ok edns=ok edns1=ok edns@512=ok ednsopt=echoed
edns1opt=echoed do=ok ednsflags=ok docookie=ok edns512tcp=ok optlist=ok,subnet

.ac.th. @202.29. ( ac.th.): dns=ok edns=ok edns1=ok edns@512=ok ednsopt=echoed edns1opt=echoed
do=ok ednsflags=ok docookie=ok edns512tcp=ok optlist=ok,subnet
.ac.th. @2001:3c8: ( ac.th.): dns=ok edns=ok edns1=ok edns@512=ok ednsopt=echoed
edns1opt=echoed do=ok ednsflags=ok docookie=ok edns512tcp=ok optlist=ok,subnet

.ac.th. @202.28. ( net.th.): dns=ok edns=ok edns1=ok edns@512=ok ednsopt=ok edns1opt=ok do=ok
ednsflags=ok docookie=ok edns512tcp=ok optlist=ok
```

The Following Tests Failed

Warning: test failures may indicate that some DNS clients cannot resolve the zone or will get a unintended answer or resolution will be slower than necessary.

Warning: failure to address issues identified here may make future DNS extensions that you want to use ineffective. In particular echoing back unknown EDNS options and unknown EDNS flags will break future signaling between DNS client and DNS server. We already have examples of this where you cannot depend on the AD flag bit meaning anything in replies because too many DNS servers just echo it back. Similarly the EDNS Client Subnet (ECS) option cannot just be sent to everyone in part because of servers just echoing it back.

EDNS - Unknown Option Handling (ednsopt)

```
dig +nocommand +nored +noad +edns=100 soa zone @server
expect: SOA
expect: NOERROR
expect: OPT record with version set to 0
expect: that the option will not be present in response
See RFC6891, 6.1.2 Wire Format
```

EDNS - Unknown Version with Unknown Option Handling (edns1opt)

```
dig +nocommand +nored +noad +edns=1 +noednsneg +edns=100 soa zone @server
expect: BADVERS
expect: OPT record with version set to 0
expect: not to see SOA
expect: that the option will not be present in response
See RFC6891
```

3.3. Fatal error detected! หมายความว่า DNS Server ที่เป็น Authoritative ของ Domain ที่เราดูแล รองรับ EDNS (หรือไม่สามารถติดต่อ DNS Server ได้)

Domain owners

Please check if your domain is affected:

Test your domain

Domain name (without www):

Testing completed:

.or.th: Fatal error detected!



This domain is going to STOP WORKING after the 2019 DNS flag day! Please retry the test to eliminate random network failures. If the problem persists you really need to request a fix from your domain administrator. You can refer them to <https://dnsflagday.net/> and technical report <https://ednscomp.isc.org/ednscomp/d374f6a4f3>

3.3.1. ตามตัวอย่างแรกคือไม่สามารถติดต่อ DNS Server ได้



Internet Systems
Consortium

EDNS Compliance Tester

Checking: ' or.th' as at 2019-01-15T08:30:16Z

or.th. @164.116. (or.th.): dns=timeout edns=timeout edns1=timeout edns@512=timeout ednsopt=timeout
edns1opt=timeout do=timeout ednsflags=timeout docookie=timeout edns512tcp=timeout optlist=timeout

The Following Tests Failed

Warning: test failures may indicate that some DNS clients cannot resolve the zone or will get a unintended answer or resolution will be slower than necessary.

Warning: failure to address issues identified here may make future DNS extensions that you want to use ineffective. In particular echoing back unknown EDNS options and unknown EDNS flags will break future signaling between DNS client and DNS server. We already have examples of this where you cannot depend on the AD flag bit meaning anything in replies because too many DNS servers just echo it back. Similarly the EDNS Client Subnet (ECS) option cannot just be sent to everyone in part because of servers just echoing it back.

Plain DNS (dns)

dig +norec +noad +noedns soa zone @server
expect: SOA
expect: NOERROR

Plain EDNS (edns)

This is the style of the initial query that BIND 9.0.x sends.

dig +nocoookie +norec +noad +edns=0 soa zone @server
expect: SOA
expect: NOERROR
expect: OPT record with version set to 0
expect: EDNS over IPv6
[See RFC6891](#)

EDNS - Unknown Version Handling (edns1)

dig +nocoookie +norec +noad +edns=1 +noednsneg soa zone @server
expect: BADVERS
expect: OPT record with version set to 0
expect: not to see SOA
[See RFC6891, 6.1.3. OPT Record TTL Field Use](#)

3.3.2. ตัวอย่างที่สอง EDNS “ไม่สามารถใช้งานได้” เนื่องจากมีบาง Option ที่ส่งผลให้ไม่ได้
คำตอบ(ตัวอย่างเพิ่มเติมจะอยู่ในเรื่อง DIG Command) บน Windows Server 2008 R2



Internet Systems
Consortium

EDNS Compliance Tester

Checking: 'edns12.com' as at 2019-01-15T09:07:34Z

edns12.com. @164.115.50.211 dns=ok edns=ok edns1=ok edns@512=ok **ednsopt=formerr,echoed edns1opt=formerr,version-not-zero,echoed** do=ok ednsflags=ok **docookie=formerr** edns512tcp=ok **optlist=formerr,subnet**

The Following Tests Failed

Warning: test failures may indicate that some DNS clients cannot resolve the zone or will get a unintended answer or resolution will be slower than necessary.

Warning: failure to address issues identified here may make future DNS extensions that you want to use ineffective. In particular echoing back unknown EDNS options and unknown EDNS flags will break future signaling between DNS client and DNS server. We already have examples of this where you cannot depend on the AD flag bit meaning anything in replies because too many DNS servers just echo it back. Similarly the EDNS Client Subnet (ECS) option cannot just be sent to everyone in part because of servers just echoing it back.

EDNS - Unknown Option Handling (ednsopt)

dig +nocookie +nored +noad +ednsopt=100 soa zone @server
expect: SOA
expect: NOERROR
expect: OPT record with version set to 0
expect: that the option will not be present in response
[See RFC6891, 6.1.2 Wire Format](#)

EDNS - Unknown Version with Unknown Option Handling (edns1opt)

dig +nocookie +nored +noad +edns=1 +noednsneg +ednsopt=100 soa zone @server
expect: BADVERS
expect: OPT record with version set to 0
expect: not to see SOA
expect: that the option will not be present in response
[See RFC6891](#)

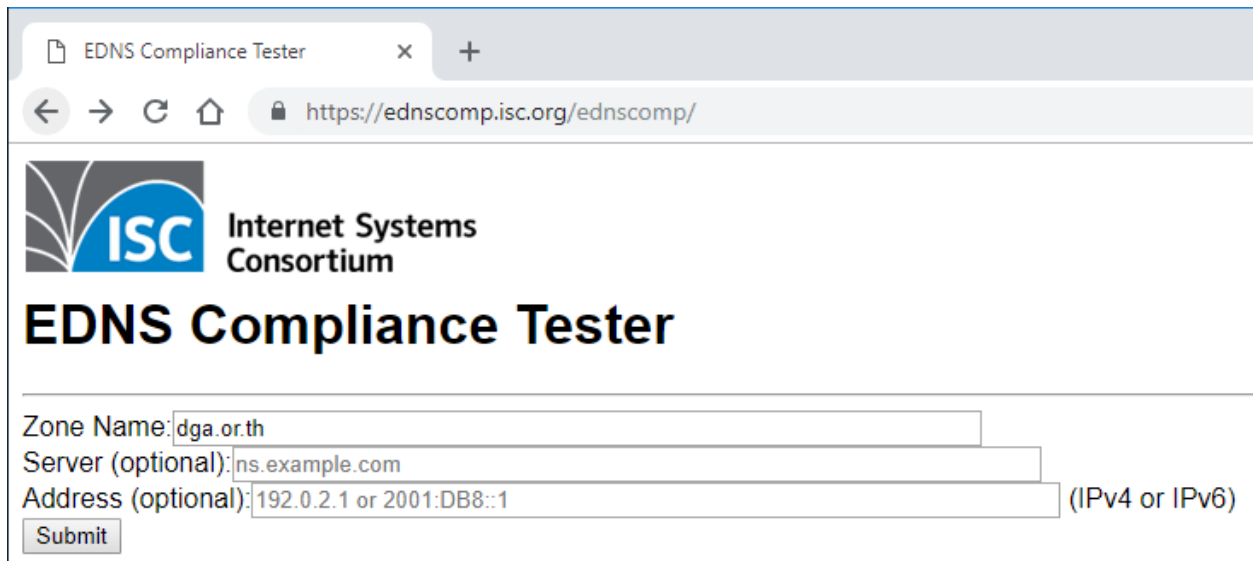
EDNS - DNSSEC with DNS COOKIE Option (docookie)

This is the style of the initial query that BIND 9.11.0 and BIND 9.10.4 Windows onwards send.

dig +cookie +nored +noad +dnssec soa zone @server
expect: SOA
expect: NOERROR
expect: OPT record with version set to 0
expect: DO flag in response if RRSIG is present in response
[See RFC3225](#), [RFC6891](#), and [RFC7873](#).

4. การทดสอบแบบเลือก DNS Server เฉพาะเจาะจง ซึ่งเราสามารถกำหนดได้ว่าจะให้ทดสอบไปยัง DNS Server เครื่องไหน อีกทั้งยังสามารถใช้ในการทดสอบกับ DNS Server ที่เราติดตั้งใหม่ได้ด้วย เพื่อทดสอบก่อนชี้ Name Server มา โดยให้เข้าไปที่ Website :

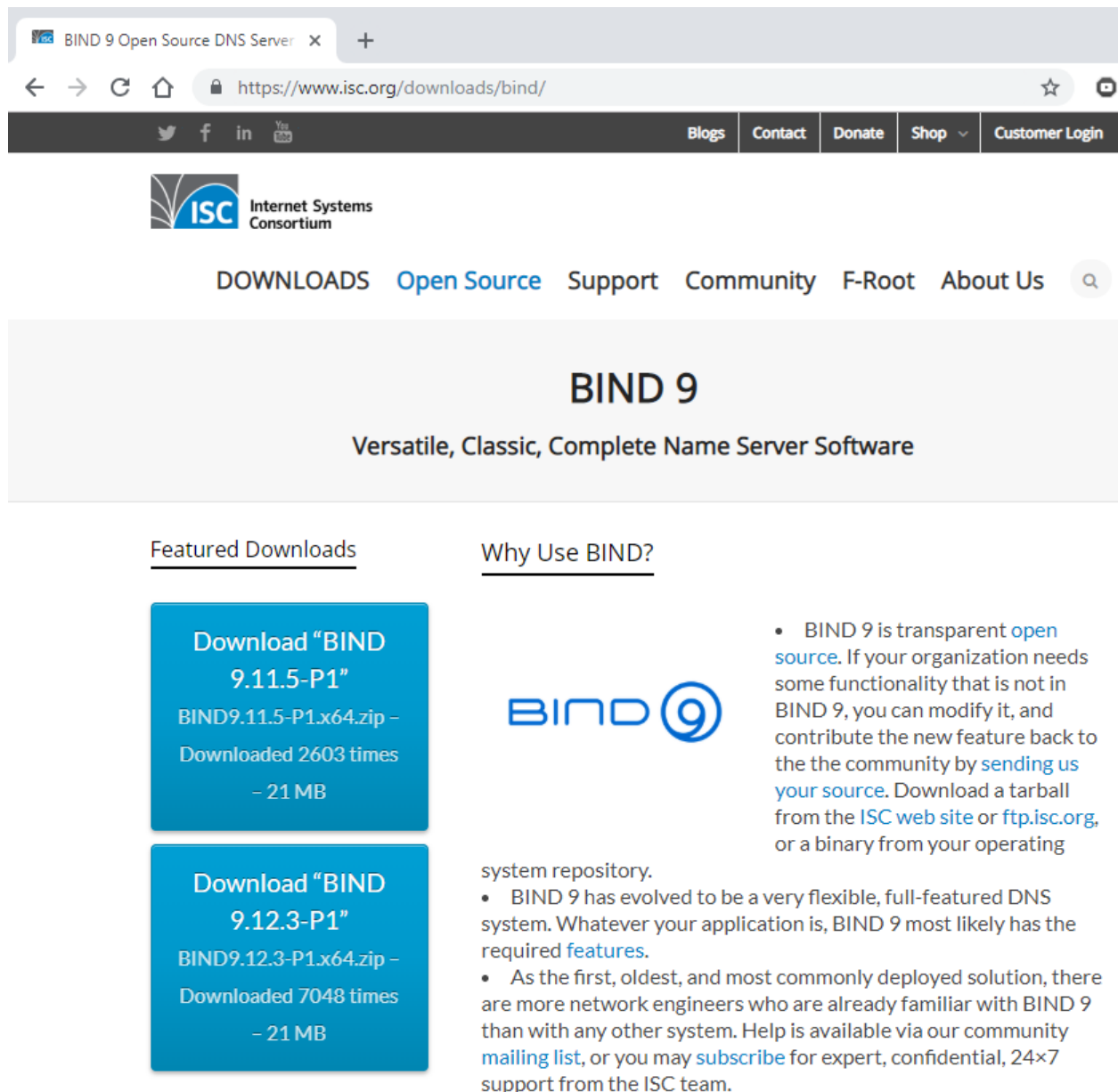
<https://ednscomp.isc.org/ednscomp/>



The screenshot shows a web browser window with the title 'EDNS Compliance Tester'. The address bar displays 'https://ednscomp.isc.org/ednscomp/'. The page features the ISC Internet Systems Consortium logo and the title 'EDNS Compliance Tester'. Below the title, there are three input fields: 'Zone Name:' with the value 'dga.or.th', 'Server (optional):' with the value 'ns.example.com', and 'Address (optional):' with the value '192.0.2.1 or 2001:DB8::1'. To the right of the 'Address (optional):' field is the text '(IPv4 or IPv6)'. A 'Submit' button is located at the bottom left of the form area.

โดยการระบุจะระบุ Name Server ในช่อง Server (optional) หรือ IP Address ในช่อง Address (Optional) ก็ได้ เมื่อใส่ข้อมูลแล้วกด Submit

5.การทดสอบโดยใช้ Dig Tools (BIND9) โดยบน Windows สามารถ Download ผ่าน Website:
<https://www.isc.org/downloads/bind/>




The screenshot shows the BIND 9 download page on the Internet Systems Consortium (ISC) website. The browser address bar shows the URL <https://www.isc.org/downloads/bind/>. The page header includes the ISC logo and navigation links: DOWNLOADS, Open Source, Support, Community, F-Root, About Us, and a search icon. The main heading is "BIND 9" with the subtitle "Versatile, Classic, Complete Name Server Software".

Featured Downloads

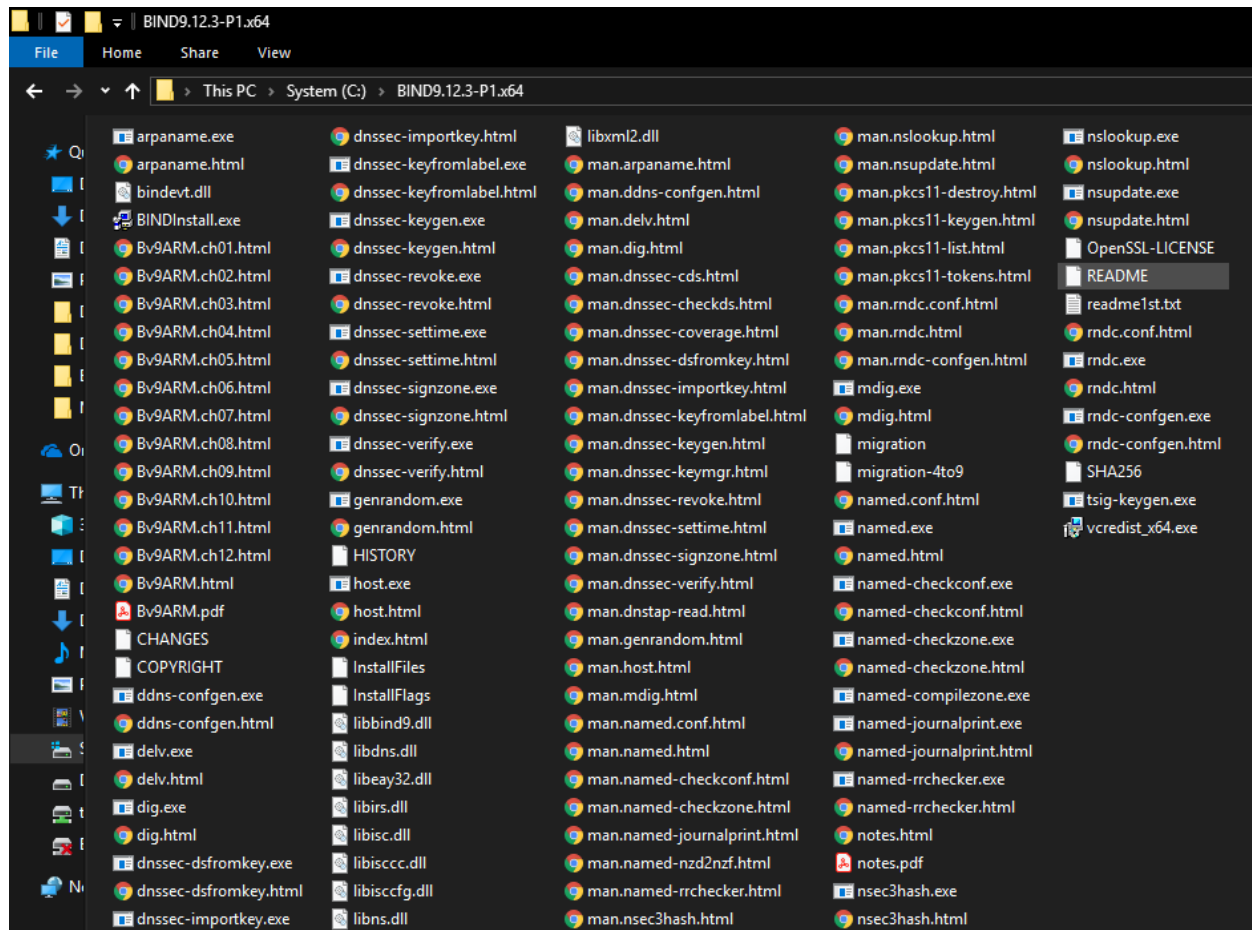
- Download "BIND 9.11.5-P1"**
BIND9.11.5-P1.x64.zip – Downloaded 2603 times – 21 MB
- Download "BIND 9.12.3-P1"**
BIND9.12.3-P1.x64.zip – Downloaded 7048 times – 21 MB

Why Use BIND?

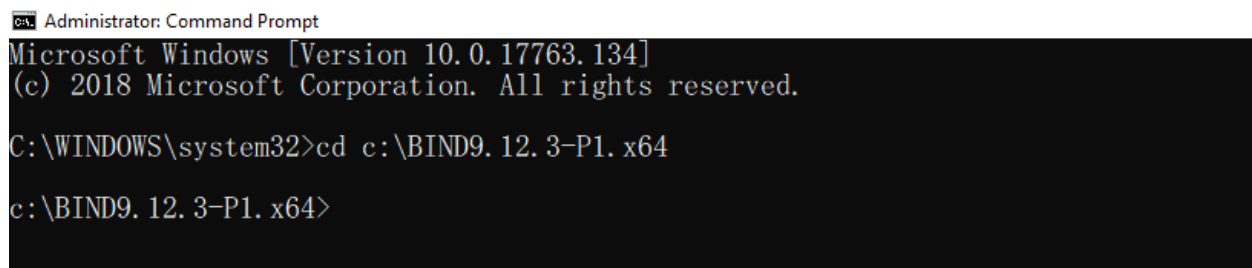


- BIND 9 is transparent [open source](#). If your organization needs some functionality that is not in BIND 9, you can modify it, and contribute the new feature back to the the community by [sending us your source](#). Download a tarball from the [ISC web site](#) or [ftp.isc.org](#), or a binary from your operating system repository.
- BIND 9 has evolved to be a very flexible, full-featured DNS system. Whatever your application is, BIND 9 most likely has the required [features](#).
- As the first, oldest, and most commonly deployed solution, there are more network engineers who are already familiar with BIND 9 than with any other system. Help is available via our community [mailing list](#), or you may [subscribe](#) for expert, confidential, 24x7 support from the ISC team.

6. เมื่อ Download แล้วให้ Extract File จะได้ดังนี้



7. เปิด Command Line ขึ้นมาแล้วไปที่ Folder ที่ Extract ไว้



8. ใช้คำสั่ง `dig +edns soa <your domain> @<domain name server>` ถ้าได้คำตอบดังภาพ ตัวอย่าง หมายความว่า DNS Server ที่เป็น Authoritative ของ Domain ที่เราดูแลรองรับ EDNS

```
c:\BIND9.12.3-P1.x64>dig +edns soa dga.or.th @ns1.dga.or.th

; <<>> DiG 9.12.3-P1 <<>> +edns soa dga.or.th @ns1.dga.or.th
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9042
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;dga.or.th.                IN      SOA

;; ANSWER SECTION:
dga.or.th.                28800   IN      SOA      ns1.dga.or.th. contact.dga.or.th. 2018068838 10800 1080 2419200 900

;; Query time: 3 msec
;; SERVER: 164.115.19.132#53(164.115.19.132)
;; WHEN: Wed Jan 16 10:37:00 SE Asia Standard Time 2019
;; MSG SIZE rcvd: 86
```

8.1. ทดสอบบน Windows Server 2008R2 เพิ่มเติม จากตัวอย่าง 3.3.2 ซึ่งผลปรากฏว่า ไม่สามารถ Resolve คำตอบออกมาได้

```
c:\BIND9.12.3-P1.x64>dig +edns soa ends12.com @164.115.50.211

; <<>> DiG 9.12.3-P1 <<>> +edns soa ends12.com @164.115.50.211
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: FORMERR, id: 7047
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: 7526a655075ff92c (echoed)
;; QUESTION SECTION:
;ends12.com.                IN      SOA

;; Query time: 5 msec
;; SERVER: 164.115.50.211#53(164.115.50.211)
;; WHEN: Wed Jan 16 10:43:53 SE Asia Standard Time 2019
;; MSG SIZE rcvd: 51
```

8.2. การทดสอบบน Windows Server 2012R2

```
c:\BIND9.12.3-P1.x64>dig +nocookie soa ends12.net @164.115.50.212
; <<>> DiG 9.12.3-P1 <<>> +nocookie soa ends12.net @164.115.50.212
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 17344
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:;, udp: 4000
;; QUESTION SECTION:
;ends12.net.                IN      SOA
;; AUTHORITY SECTION:
net.                59      IN      SOA      a.gtld-servers.net. nstld.verisign-grs.com. 1547610821 1800 900 604800 86400
;; Query time: 198 msec
;; SERVER: 164.115.50.212#53(164.115.50.212)
;; WHEN: Wed Jan 16 10:54:11 SE Asia Standard Time 2019
;; MSG SIZE  rcvd: 112
```

ข้อสังเกตเพิ่มเติมการทดสอบผ่าน <https://ednscomp.isc.org/ednscomp/> จะเห็นว่าเมื่อมี Warning/Error ออกมาจะมี Command ให้ทดสอบเพิ่มเติมด้านล่าง ซึ่งทดสอบผ่าน Dig ได้เลย

EDNS - Unknown Option Handling (ednsopt)

```
dig +nocookie +nored +noad +edns=100 soa zone @server
expect: SOA
expect: NOERROR
expect: OPT record with version set to 0
expect: that the option will not be present in response
See RFC6891, 6.1.2 Wire Format
```

EDNS - Unknown Version with Unknown Option Handling (edns1opt)

```
dig +nocookie +nored +noad +edns=1 +noednsneg +edns=100 soa zone @server
expect: BADVERS
expect: OPT record with version set to 0
expect: not to see SOA
expect: that the option will not be present in response
See RFC6891
```

EDNS - DNSSEC with DNS COOKIE Option (docookie)

This is the style of the initial query that BIND 9.11.0 and BIND 9.10.4 Windows onwards send.

```
dig +cookie +nored +noad +dnssec soa zone @server
expect: SOA
expect: NOERROR
expect: OPT record with version set to 0
expect: DO flag in response if RRSIG is present in response
See RFC3225, RFC6891, and RFC7873.
```

ข้อเสนอแนะเพิ่มเติม:

หากมีการปรับปรุงระบบ DNS ใหม่ภายในองค์กรแนะนำให้ติดตั้ง Version ล่าสุด จะดีที่สุดเพื่อจะรองรับกระบวนการการทำงานต่างๆ ได้ดีกว่าในปัจจุบัน เบื้องต้นโปรแกรมที่รองรับเป็น Windows Server 2012R2 และ BIND 9.10 ขึ้นไป

Reference:

- <https://www.isc.org/blogs/partial-edns-compliance-hampers-deployment-of-new-dns-features/>
- <https://www.ietf.org/proceedings/92/slides/slides-92-dnsop-7.pdf>
- <https://mailman.nanog.org/pipermail/nanog/2016-May/085987.html>
- <https://tools.ietf.org/html/rfc2671>
- <https://linux.die.net/man/1/dig>