คู่มือการปฏิบัติงานการเพิ่มโดเมนเนมสำหรับผู้ดูแลระบบ

โดเมนเนม (Domain Name System : DNS) เป็นเครื่องบริการแปลงชื่อเว็บไซต์เป็นหมายเลข IP ซึ่งการแปลงชื่อนี้อาจเกิดในเครื่อง local เอง จาก cache ในเครื่อง local หรือจากเครื่องบริการของผู้ให้บริการ เพราะ เบอร์ IP Address เป็นตัวเลขที่ใช้ไม่ค่อยสะดวกและจำยาก ด้วยเหตุนี้จึงมีการคิดระบบตั้งชื่อแบบที่เป็นตัวอักษร ให้มีความหมายเพื่อการจดจำได้ง่ายกว่ามาก เวลาเราอ้างถึงเครื่องใดบน

บางครั้งจะพบกรณีคอมพิวเตอร์ที่เป็น Name Server นั้นไม่ทำงาน ไม่สามารถติดต่อเครื่องอื่นบนอินเตอร์เน็ตได้อีกโดยใช้ชื่อ DNS Server หากเราทราบ IP Address เราสามารถใช้ IP Address ได้ตรงๆ ทำให้เราไม่จำเป็นต้องพึ่งสมุดโทรศัพท์ของ Name Server ด้วยเหตุนี้เราจึงทำการเก็บชื่อและ IP Address ไว้ในสมุดโทรศัพท์ส่วนตัวประจำเครื่อง เช่นบนระบบยูนิกซ์มีไฟล์ /etc/hosts เอาไว้เก็บชื่อ DNS ที่ใช้บ่อยๆ

การทำงานของระบบ DNS

DNS ทำหน้าที่คล้ายสมุดโทรศัพท์คือ เมื่อมีคนต้องการจะโทรศัพท์หาใครคนนั้นก็จะเปิดสมุดโทรศัพท์ดูเพื่อค้นหาหมายเลขโทรศัพท์ของคนที่ต้องการติดต่อ คอมพิวเตอร์ก็เช่นกัน เมื่อต้องการสื่อสารกับคอมพิวเตอร์เครื่องอื่น เครื่องนั้นก็จะทำการสอบถามหมายเลข IP ของเครื่องที่ต้องการสื่อสารด้วยกับ DNS server ซึ่งจะทำการค้นหาหมายเลขดังกล่าวในฐานข้อมูลแล้วแจ้งให้โฮสต์ดังกล่าว ทราบ ระบบ DNS แบ่งออกเป็น 3 ส่วน คือ

1. Name Resolvers : ดังที่ได้กล่าวมาแล้วว่าจุดประสงค์หลักของ DNS คือการแปลงชื่อคอมพิวเตอร์ให้เป็นหมายเลข IP ในเทอมของ DNS แล้วเครื่องไคลเอนท์ที่ต้องการสอบถามหมายเลข IP จะเรียกว่า "รีโซล์ฟเวอร์ (resolver)" วอฟแวร์ที่ทำหน้าที่เป็นรีโซล์ฟเวอร์นั้นจะถูกสร้างมากับแอพพลิเคชันหรืออาจจะเป็นไลบรารีที่มีอยู่ในเครื่องไคลเอนท์

2. Domain Name Space : ฐานข้อมูลระบบ DNS มีโครงสร้างเป็นต้นไม้ ซึ่งจะเรียกว่า "โดเมนเนมสเปซ (Domain Name Space)" แต่ละโดเมนจะมีชื่อและสามารถมีโดเมนย่อยหรือซับโดเมน (Subdomain) การเรียกชื่อจะใช้จุด (.) เป็นตัวแบ่งแยกระหว่างโดเมนหลักและโดเมนย่อย

3. Name Servers : เนมเซิร์ฟเวอร์ คือเครื่องคอมพิวเตอร์ที่รันโปรแกรมที่จัดการฐานข้อมูลบางส่วนของระบบ DNS เนมเซิร์ฟเวอร์จะตอบกลับการร้องขอทันทีโดยการค้นหาข้อมูลในฐานของมูลตัวเอง หรือจะส่งต่อการร้องขอ ไปยังเนมเซิร์ฟเวอร์อื่น ถ้าเนมเซิร์ฟเวอร์มีเร็คคอร์ดของส่วนของโดเมน แสดงว่าเนมเซิร์ฟเวอร์นั้นเป็นเจ้าของโดเมนนั้น (Authoritative) ถ้าไม่มีก็จะเรียกว่า Non-Authoritative

DNSSEC : Domain Name System Security Extensions

DNSSEC มีเป้าหมายเพื่อป้องกันผู้ใช้ (end user) จากการเข้าถึงปลายทางข้อมูลที่ถูกบิดเบือนผ่านระบบโดเมนเนม DNSSEC คือการเพิ่มความปลอดภัยให้แก่ระบบโดเมนเนม ซึ่งทั่วไปแล้วมีความเสี่ยงจากการที่อาจถูกนักเทคนิคผู้ไม่ประสงค์ดีลอบ แทรกแซง Name resolution ซึ่งเป็นกระบวนการถามตอบ (client-server) ระหว่าง Name server เพื่อสืบค้นชื่อโดเมนในระบบ (Domain space) ผ่านทางการทำงานของตัว

Resolver อันเป็นโปรแกรมตัวสำคัญที่ทำหน้าที่ ประสานการติดต่อระหว่าง Name server ตัวหนึ่งกับ Name server ตัวอื่นๆภายในระบบโดเมน ทำให้ Resolver ได้รับคำตอบของที่อยู่ปลายทางที่บิดเบือนอันนำไปสู่การแสดงผลที่ช้าลง หรือเข้าเว็บไซต์อื่นที่ผู้แทรกแซงเตรียมไว้ ที่ในท้ายที่สุดอาจสร้างความเสียหายแก่ผู้ใช้ได้ในหลายรูปแบบ

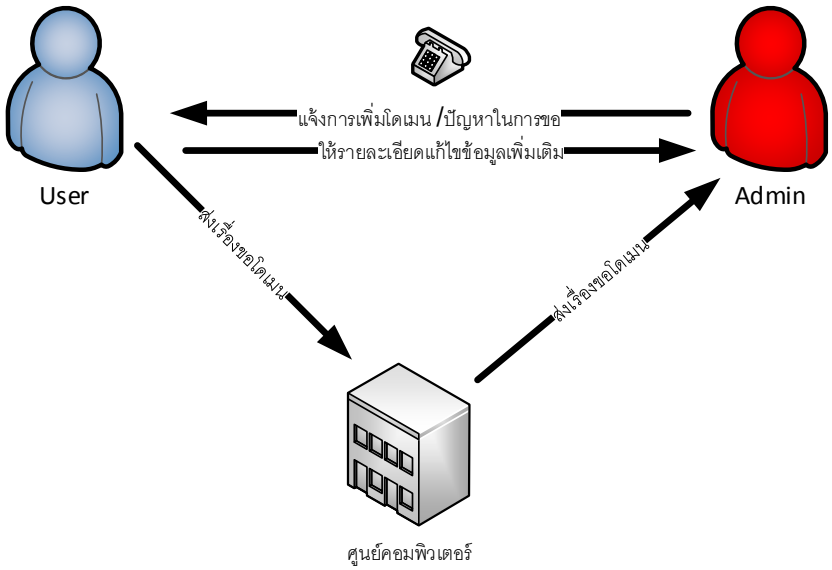
DNSSEC ทำงานอย่างไร DNSSEC จัดให้มีกระบวนการตรวจสอบคำตอบที่ Resolver ได้รับ ว่ามาจาก Name server ที่เป็นปลายทางตัวจริงหรือไม่ จากเดิมที่ Resolver จะรับหมายเลขระบุที่อยู่ของข้อมูล (หมายเลข IP) จาก Name Server ผู้ตอบ(authoritative name server) มาโดยไม่เฉลียวใจใดๆ กระบวนการตรวจสอบนี้ดำเนินไปโดยใช้ระบบคู่กุญแจแบบ asymmetric key ที่ประกอบไปด้วย private key และ public key

โดเมนภายใต้บริการ DNSSEC จะถูกใส่รหัสลับด้วย private key จากทาง Registry ที่ดูแลฐานข้อมูลของโดเมนนั้นๆที่เข้ารหัส zone ข้อมูลโดเมนภายใต้ดอทที่ Registry นั้นๆดูแลอยู่ และจะแจกจ่าย public key สำหรับการเข้าถึงโดเมนภายในโซนที่ได้รับการเข้ารหัสอีกที

Resolver ที่เป็น DNSSEC-awear จะมี public key สำหรับตรวจสอบความถูกต้องของโดเมนปลายทางที่มีการใช้บริการ DNSSEC ด้วยการเข้าคู่กับ private key

การให้บริการ DNSSEC ในประเทศไทย .th เป็นโดเมนระดับบนสุดตัวแรกในเอเชียที่มีการปฏิบัติการลงใช้ (implement) DNSSEC

ขั้นตอนการขอ DNS สำหรับหน่วยงานและบุคลากร



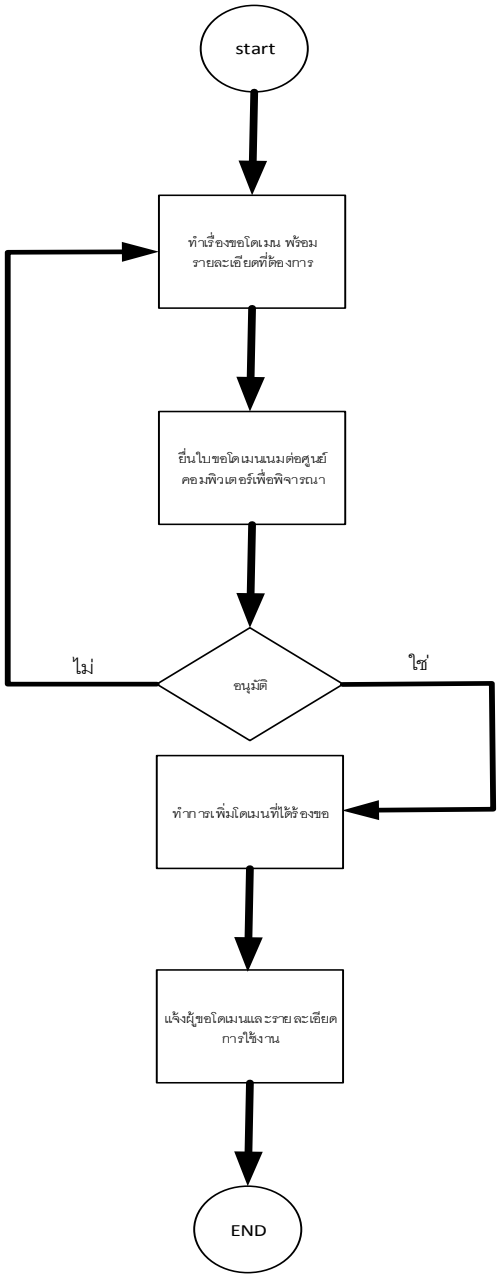
1. หน่วยงานหรือบุคลากรที่ต้องการขอโดเมนเนม ต้องทำหนังสือราชการผ่านผู้บริหารของหน่วยงานพร้อมแนบรายละเอียดที่ต้องการและเหตุผลในการขอใช้บริการ

2. ส่งหนังสือที่ขอใช้บริการที่ศูนย์คอมพิวเตอร์เพื่อดำเนินการตามขั้นตอน

3. เจ้าหน้าที่ผู้เกี่ยวข้องทำการตรวจสอบข้อมูลและเสนอความเห็นต่อผู้อำนวยการศูนย์คอมพิวเตอร์เพื่อประกอบการพิจารณาอนุมัติ

4. ผู้ได้รับมอบหมายติดต่อผู้ขอใช้บริการเพิ่มดำเนินการเพิ่มโดเมนเนมตามเงื่อนไขที่กำหนด

Flowchart ขั้นตอนการขอเพิ่ม DNS



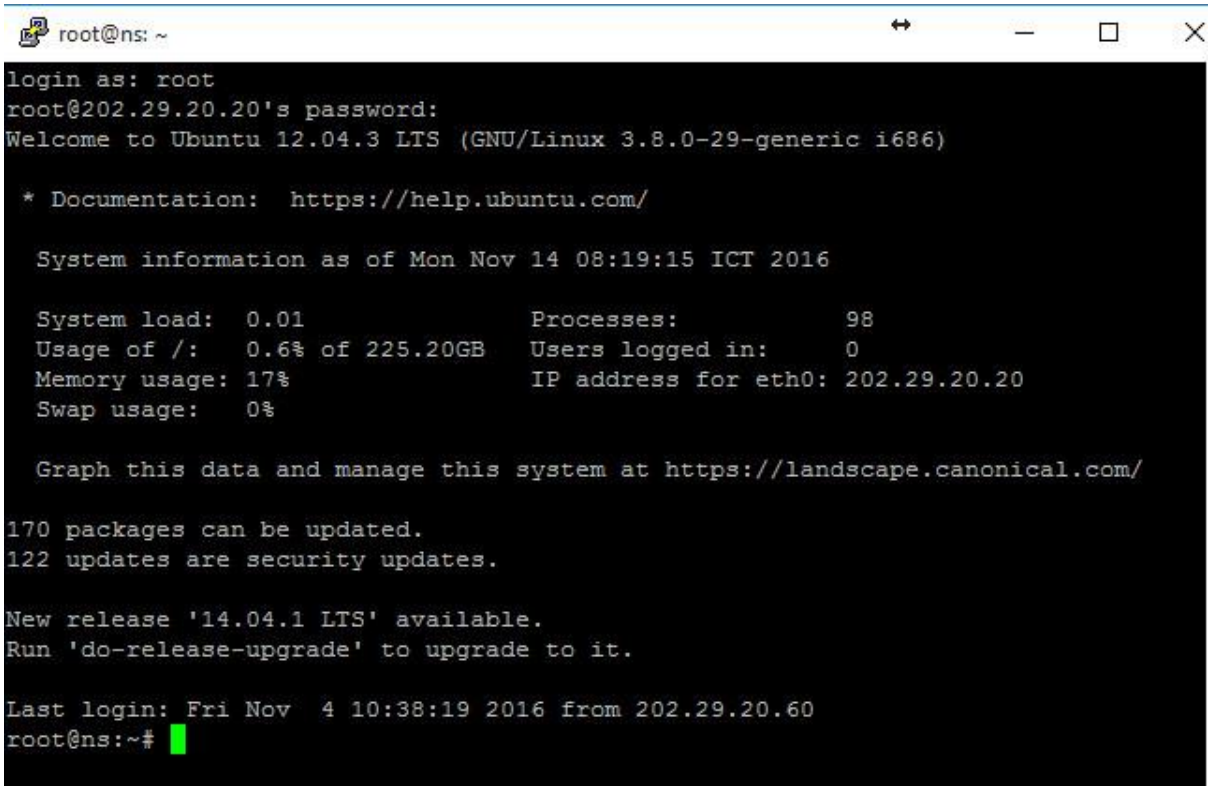
ขั้นตอนการเพิ่มโดเมนเนมสำหรับผู้ดูแลระบบ

1. ผู้ดูแลระบบใช้โปรแกรม Putty ในการเข้าถึงระบบ โดยกำหนดข้อมูล ดังนี้

   DNS : IP 202.29.20.20 SSH port 60000

   USER/PASS :: xxx/xxxx

2. ดำเนินการ login ระบบ



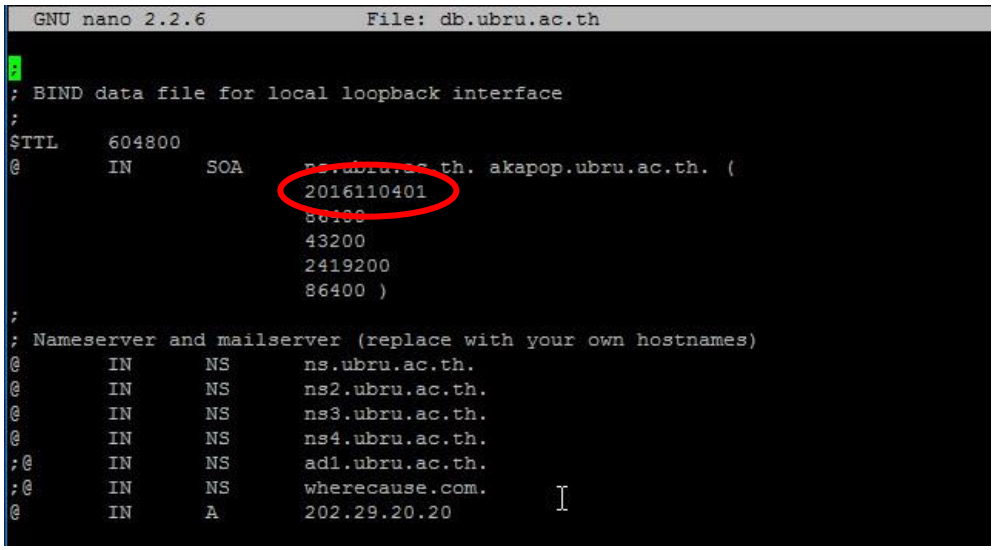
เข้า จัดการ โดเมน โดยใช้คำสั่งเข้าถึง

cd /etc/bind

pico db.ubru.ac.th

แก้ไขช่วงเวลาในการเพิ่ม

แก้ไข ค่า ตามรายละเอียด ดังนี้ 2016:ปี คศ. 11: เดือน 04 : วัน 01 : จำนวนครั้งที่แก้ไข



ทำการเพิ่ม โดเมน

(ชื่อโดเมน) IN A (IPAdress เครื่อง server ที่ต้องการใส่ โดเมน)

```
  GNU nano 2.2.6               File: db.ubru.ac.th

rdcs            IN      A       202.29.20.38
www.ieiapp      IN      AAAA    2001:3c8:d109::202:29:20:38
www.ieiapp      IN      A       202.29.20.38
pramote         IN      AAAA    2001:3c8:d109::202:29:20:38
pramote         IN      A       202.29.20.38
dss-school      IN      AAAA    2001:3c8:d109::202:29:20:38
dss-school      IN      A       202.29.20.38
rasppimedia     IN      AAAA    2001:3c8:d109::202:29:20:38
rasppimedia     IN      A       202.29.20.38

www.mambo       IN      A       202.29.20.50
www.qad         IN      A       202.29.20.50
www.exchstd     IN      A       202.29.20.50
www.gs          IN      A       202.29.20.50
www.sciencecenter       IN      A       202.29.20.50
thaihealth      IN      A       202.29.20.50
asx             IN      A       202.29.20.51
elearning.edltv IN      A       202.29.20.52
```

กด Ctrl X เพื่อบันทึก

pico db.202.29.20 (reverse)

แก้ไข ค่า ตามรายละเอียด ดังนี้ 2016:ปี คศ. 11: เดือน 04 : วัน 01 : จำนวนครั้งที่แก้ไข

```
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns.ubru.ac.th. akapop.ubru.ac.th. (
                        2016110402      ; Serial
                        86400           ; Refresh
                        43200           ; Retry
                        2419200         ; Expire
                        86400 )         ; Negative Cache TTL
;
;DNS Reverse
@       IN      NS      ns.ubru.ac.th.
@       IN      NS      ns2.ubru.ac.th.
@       IN      NS      ns3.ubru.ac.th.
@       IN      NS      ns4.ubru.ac.th.
0.2.0.0.0.2.0.0.9.2.0.0.2.0.2.0.0.0.0.0.0.9.0.1.d.8.c.3.0.1.0.0.2      IN      PTR     ns.ubru.ac.th.
20      IN      PTR     ns.ubru.ac.th.
2.1.0.0.0.2.0.0.9.2.0.0.2.0.2.0.0.0.0.0.0.9.0.1.d.8.c.3.0.1.0.0.2      IN      PTR     ns2.ubru.ac.th.
21      IN      PTR     ns2.ubru.ac.th.
2.2.0.0.0.2.0.0.9.2.0.0.2.0.2.0.0.0.0.0.0.9.0.1.d.8.c.3.0.1.0.0.2      IN      PTR     ns3.ubru.ac.th.
22      IN      PTR     ns3.ubru.ac.th.
23      IN      PTR     ns4.ubru.ac.th.
23      IN      PTR     udrive.ubru.ac.th.
23      IN      PTR     ad1.ubru.ac.th.
225     IN      PTR     ns1.cscl.ubru.ac.th.
58      IN      PTR     wherecause.com.
```

เพิ่ม Reverse โดเมน

(IP Reverse)IN PTR (ชื่อโดเมน)

```
8.3.0.0.0.2.0.0.9.2.0.0.2.0.2.0.0.0.0.0.9.0.1.d.8.c.3.0.1.0.0.2      IN      PTR     rspg.ubru.ac.th.
38      IN      PTR     rspg.ubru.ac.th.
8.3.0.0.0.2.0.0.9.2.0.0.2.0.2.0.0.0.0.0.9.0.1.d.8.c.3.0.1.0.0.2      IN      PTR     rdcs.ubru.ac.th.
38      IN      PTR     rdcs.ubru.ac.th.
8.3.0.0.0.2.0.0.9.2.0.0.2.0.2.0.0.0.0.0.9.0.1.d.8.c.3.0.1.0.0.2      IN      PTR     www.ieiapp.ubru.ac.th.
38      IN      PTR     www.ieiapp.ubru.ac.th.
8.3.0.0.0.2.0.0.9.2.0.0.2.0.2.0.0.0.0.0.9.0.1.d.8.c.3.0.1.0.0.2      IN      PTR     pramote.ubru.ac.th.
38      IN      PTR     pramote.ubru.ac.th.
8.3.0.0.0.2.0.0.9.2.0.0.2.0.2.0.0.0.0.0.9.0.1.d.8.c.3.0.1.0.0.2      IN      PTR     dss-school.ubru.ac.th.
38      IN      PTR     dss-school.ubru.ac.th.
8.3.0.0.0.2.0.0.9.2.0.0.2.0.2.0.0.0.0.0.9.0.1.d.8.c.3.0.1.0.0.2      IN      PTR     rasppimedia.ubru.ac.th.
38      IN      PTR     rasppimedia.ubru.ac.th.


50      IN      PTR     www.mambo.ubru.ac.th.
50      IN      PTR     www.qad.ubru.ac.th.
50      IN      PTR     www.exchstd.ubru.ac.th.
50      IN      PTR     www.gs.ubru.ac.th.
50      IN      PTR     www.sciencecenter.ubru.ac.th.
```

ใช้คำสั่งในการสร้าง DNSSEC

zonesigner -zone 20.29.202.in-addr.arpa db.202.29.20 (รอซักครู่)

```
root@ns:/etc/bind# zonesigner -zone 20.29.202.in-addr.arpa db.202.29.20

        if zonesigner appears hung, strike keys until the program completes
        (see the "Entropy" section in the man page for details)

Verifying the zone using the following algorithms: RSASHA256.
Zone signing complete:
Algorithm: RSASHA256: KSKs: 1 active, 0 stand-by, 0 revoked
                      ZSKs: 1 active, 1 stand-by, 0 revoked

zone signed successfully

20.29.202.in-addr.arpa:
        KSK (cur) 35686  -b 2048  11/14/16      (20.29.202.in-addr.arpa-signset-00003)
        ZSK (cur) 62148  -b 1024  11/14/16      (20.29.202.in-addr.arpa-signset-00001)
        ZSK (pub) 59616  -b 1024  11/14/16      (20.29.202.in-addr.arpa-signset-00002)

zone will expire in 30 days
DO NOT delete the keys until this time has passed.
root@ns:/etc/bind#
```

zonesigner -zone ubru.ac.th db.ubru.ac.th(รอซักครู่)

```
root@ns:/etc/bind# zonesigner -zone ubru.ac.th db.ubru.ac.th

        if zonesigner appears hung, strike keys until the program completes
        (see the "Entropy" section in the man page for details)

Verifying the zone using the following algorithms: RSASHA256.
Zone signing complete:
Algorithm: RSASHA256: KSKs: 1 active, 0 stand-by, 0 revoked
                      ZSKs: 1 active, 1 stand-by, 0 revoked

zone signed successfully

ubru.ac.th:
        KSK (cur) 29599  -b 2048  11/14/16      (ubru.ac.th-signset-00003)
        ZSK (cur) 47715  -b 1024  11/14/16      (ubru.ac.th-signset-00001)
        ZSK (pub) 43854  -b 1024  11/14/16      (ubru.ac.th-signset-00002)

zone will expire in 30 days
DO NOT delete the keys until this time has passed.
root@ns:/etc/bind#
```

ทำการ restrart service

service bind9 restart

```
root@ns:/etc/bind# service bind9 restart
 * Stopping domain name service... bind9
waiting for pid 4479 to die
                                                                    [ OK ]
 * Starting domain name service... bind9                           [ OK ]
root@ns:/etc/bind#
```

ทำการตรวจสอบ โดยเข้า command prompt

nslookup จาก ภาพ โดเมน rasppimedia.ubru.ac.th เป็น IP ที่ได้ประกาศไว้

```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\zero>nslookup
Default Server:  ns.ubru.ac.th
Address:  202.29.20.20

> rasppimedia.ubru.ac.th
Server:  ns.ubru.ac.th
Address:  202.29.20.20

Name:    rasppimedia.ubru.ac.th
Addresses:  2001:3c8:d109:0:202:29:20:38
          202.29.20.38

>
```

Detail server DNS

1. IP 202.29.20.20 (NS)

   DNS Master

   OS: Ubuntu 14.04.1 LTS

   HDD : 250G RAM : 4GB

   Sotfware Install : Bind9,DNSSEC

2. IP 202.29.20.21 (NS2)

   DNS Slave

   OS: Windows Server2008R2

   HDD : 250G RAM : 4GB

3. IP 202.29.20.22 (NS3)

   DNS Slave

   OS: Ubuntu 14.04.1 LTS

   HDD : 500G RAM : 2GB

Sotfware Install : Bind9,DNSSEC

4. IP 202.29.20.23 (NS4)

   DNS Slave

   OS: Windows Server2008R2

   HDD : 500G RAM : 4GB

DNS

IP:P202.29.20.20

IP:P202.29.20.21

IP:P202.29.20.22

IP:P202.29.20.23