คู่มือการปฏิบัติงานการเพิ่มโดเมนเนมสำหรับผู้ดูแลระบบ

ระบบโดเมนเนม (Domain Name System : DNS) เป็นระบบที่ให้บริการบริการแปลงชื่อเว็บไซต์หรือชื่อเครื่องคอมพิวเตอร์ปลายทางเป็นหมายเลข IP Address เช่น http://www.ubru.ac.th แปลงเป็น http://202.29.20.33 ซึ่งการแปลงชื่อนี้อาจเกิดในเครื่องผู้ใช้งานเอง (local) หรือจากเครื่องที่ให้บริการระบบโดเมนเนม (DNS Server) ของผู้ให้บริการระบบเครือข่ายอินเตอร์เน็ต เพราะเลข IP Address เป็นตัวเลขที่ใช้ไม่ค่อยสะดวกและจดจำยาก ด้วยเหตุนี้จึงมีการคิดระบบตั้งชื่อแบบที่เป็นตัวอักษร ให้มีความหมายเพื่อการจดจำได้ง่ายกว่า เวลาอ้างถึงเครื่องคอมพิวเตอร์ที่อยู่บนระบบเครือข่ายอินเตอร์เน็ต แทนระบบหมายเลข IP Address ซึ่งจดจำได้ยาก

บางครั้งจะพบกรณีคอมพิวเตอร์ที่เป็น Domain Name Server นั้นไม่ทำงานได้หรือมีเหตุขัดข้องทำให้ผู้ใช้งานระบบเครือข่ายอินเตอร์เน็ตไม่สามารถติดต่อเครื่องอื่นบนอินเตอร์เน็ตได้โดยใช้ระบบชื่อ(โดเมนเนม) แต่หากเราทราบ IP Address ของเครื่องปลายทางที่เราต้องการติดต่อ เราก็สามารถใช้หมายเลข IP Address เพื่อเชื่อมต่อกับเครื่องปลายทางได้เช่นกัน

การทำงานของระบบโดเมนเนม (DNS)

DNS ทำหน้าที่คล้ายสมุดโทรศัพท์คือ เมื่อมีคนต้องการจะโทรศัพท์หาใครคนนั้นก็จะเปิดสมุดโทรศัพท์ดูเพื่อค้นหาหมายเลขโทรศัพท์ของคนที่ต้องการติดต่อ ในระบบเครือข่ายคอมพิวเตอร์เมื่อเครื่องคอมพิวเตอร์ต้องการสื่อสารกับคอมพิวเตอร์เครื่องอื่นโดยใช้ระบบชื่อ เครื่องคอมพิวเตอร์นั้นก็จะทำการสอบถามว่าชื่อที่ต้องการติดต่อมีหมายเลข IP Address ใดกับ DNS Server ซึ่ง DNS Server ก็จะทำการค้นหาชื่อดังกล่าวในระบบฐานข้อมูลของ DNS Server ว่ามีหมายเลข IP Address ใด หากพบในฐานข้อมูลของระบบ ก็จะแจ้งให้เครื่องคอมพิวเตอร์ที่ทำการสอบถามว่าเครื่องคอมพิวเตอร์ปลายทางมีหมายเลข IP Address ใด หรือถ้าหากไม่พบในฐานข้อมูลก็จะแจ้งเครื่องคอมพิวเตอร์ที่สอบถามข้อมูลว่าไม่พบข้อมูลชื่อเครื่องคอมพิวเตอร์ในระบบ ก็จะทำให้ไม่สามารถติดต่อเครื่องคอมพิวเตอร์ที่ต้องการติดต่อโดยใช้ระบบชื่อได้ โดยจะแจ้งข้อผิดพลาดนี้ว่า DNS Cannot resolve name

ระบบ DNS แบ่งออกเป็น 3 ส่วนคือ

1. Name Resolvers : ดังที่ได้กล่าวมาแล้วว่าจุดประสงค์หลักของ DNS คือการแปลงชื่อคอมพิวเตอร์ให้เป็นหมายเลข IP ในระบบ DNS เครื่องไคลเอนท์ที่ต้องการสอบถามหมายเลข IP จะเรียกว่า "รีโซล์ฟเวอร์ (resolver)" ซอฟแวร์ที่ทำหน้าที่เป็นรีโซล์ฟเวอร์นั้นจะถูกสร้างมากับแอพพลิเคชันหรืออาจจะเป็นไลบรารีที่มีอยู่ในเครื่องไคลเอนท์

2. Domain Name Space : ฐานข้อมูลระบบ DNS มีโครงสร้างเป็นต้นไม้ ซึ่งจะเรียกว่า "โดเมนเนมสเปซ (Domain Name Space)" แต่ละโดเมนจะมีชื่อและสามารถมีโดเมนย่อยหรือซับโดเมน (Subdomain) การเรียกชื่อจะใช้จุด (.) เป็นตัวแบ่งแยกระหว่างโดเมนหลักและโดเมนย่อย เช่น http://www.ubru.ac.th

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

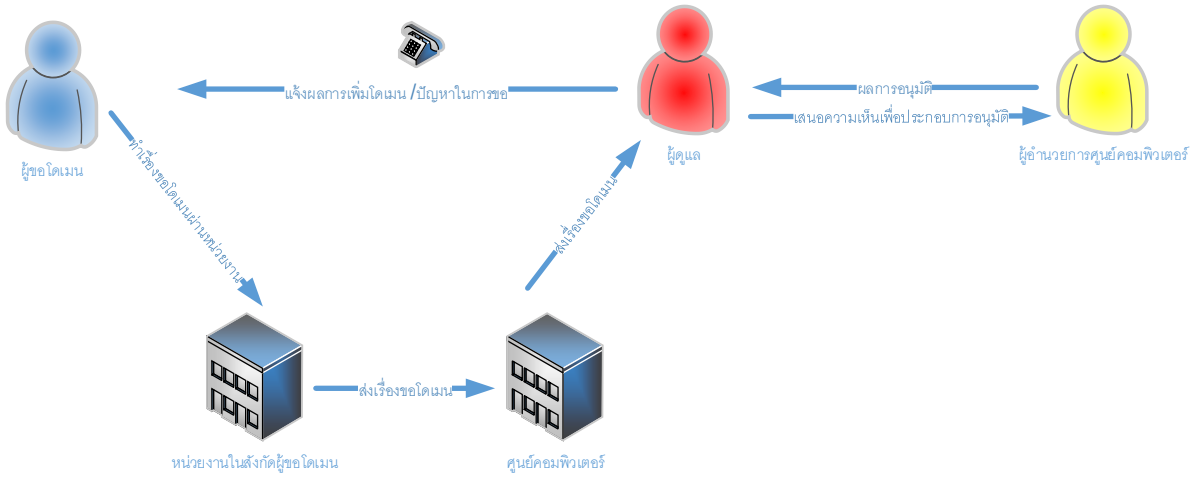
DNSSEC ทำงานอย่างไร DNSSEC จัดให้มีกระบวนการตรวจสอบคำตอบที่ Resolver ได้รับ ว่ามาจาก Name server ที่เป็นปลายทางตัวจริงหรือไม่ จากเดิมที่ Resolver จะรับหมายเลขระบุที่อยู่ของข้อมูล (หมายเลข IP) จาก Name Server ผู้ตอบ(authoritative name server) มาโดยไม่เฉลียวใจใดๆ กระบวนการตรวจสอบนี้ดำเนินไปโดยใช้ระบบคู่กุญแจแบบ 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

ขั้นตอนการขอโดเมนเนมสำหรับหน่วยงานและบุคลากร



1. หน่วยงานหรือบุคลากรที่ต้องการขอโดเมนเนม ต้องทำหนังสือราชการผ่านผู้บริหารของหน่วยงาน พร้อมแนบรายละเอียดที่ต้องการและเหตุผลในการขอใช้บริการ และจะสามารถขอโดเมนเนมภายใต้ โดเมน ubru.ac.th ที่มหาวิทยาลัยเป็นเจ้าของโดเมนได้เท่านั้น เช่น xxx.ubru.ac.th หรือ xxx.xxx.ubru.ac.th

2. ส่งหนังสือที่ขอใช้บริการโดเมนเนมที่ศูนย์คอมพิวเตอร์เพื่อดำเนินการตามขั้นตอน

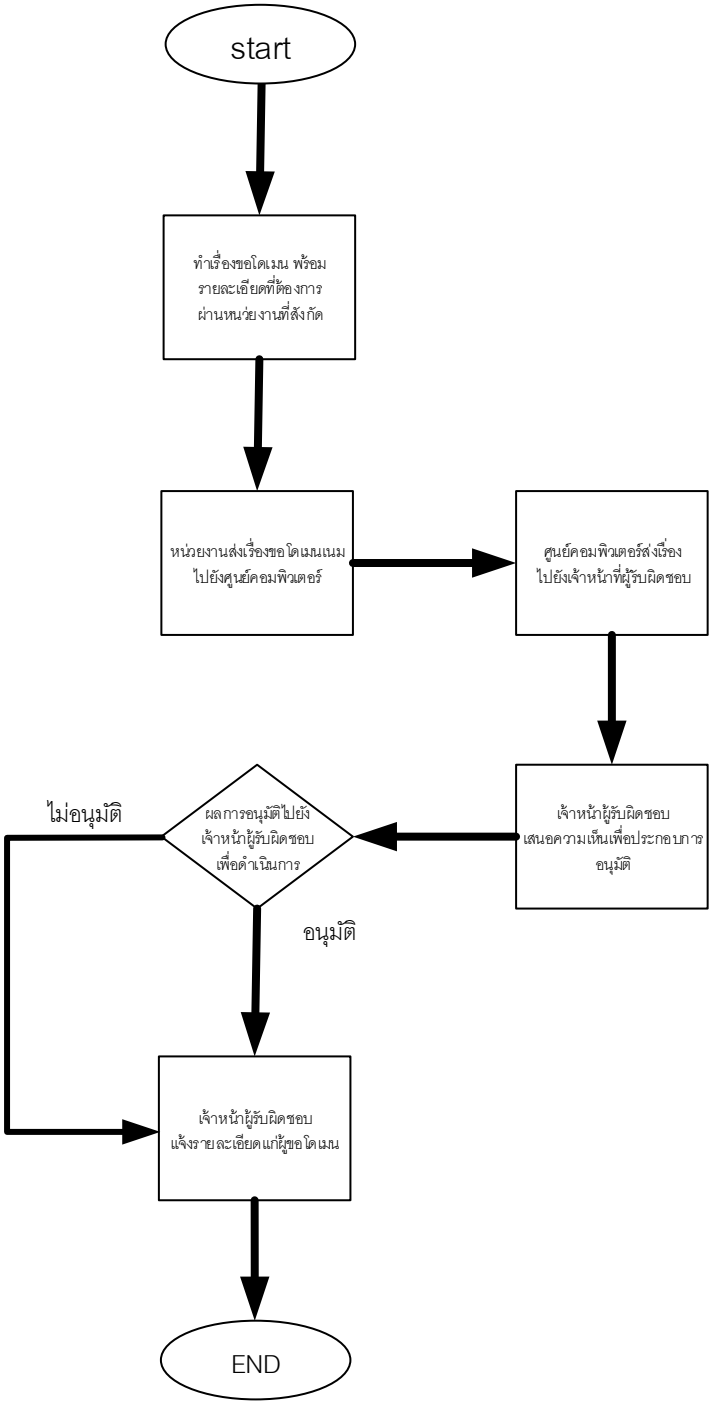
3. ส่งเรื่องให้เจ้าหน้าที่ผู้รับผิดชอบทำการตรวจสอบข้อมูล

4. เจ้าหน้าที่ผู้รับผิดชอบเสนอความเห็นต่อผู้อำนวยการศูนย์คอมพิวเตอร์เพื่อประกอบการพิจารณาอนุมัติ

5. เมื่อผู้อำนวยการศูนย์คอมพิวเตอร์อนุมัติแล้วผู้รับผิดชอบจะดำเนินการเพิ่มดำเนินการเพิ่มโดเมนเนมตามเงื่อนไขที่กำหนด

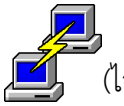
6. แจ้งให้ผู้ขอใช้บริการทราบ ในกรณีที่ไม่อนุมัติการขอใช้บริการโดเมนเนม ผู้ได้รับมอบหมายจะดำเนินการแจ้งผู้ขอใช้บริการว่าไม่อนุมัติด้วยเหตุผลใด เช่น โดเมนนี้มีการใช้งานแล้ว, ชื่อไม่เหมาะสมหรือส่อไปในทางที่จะผิดกฎหมาย

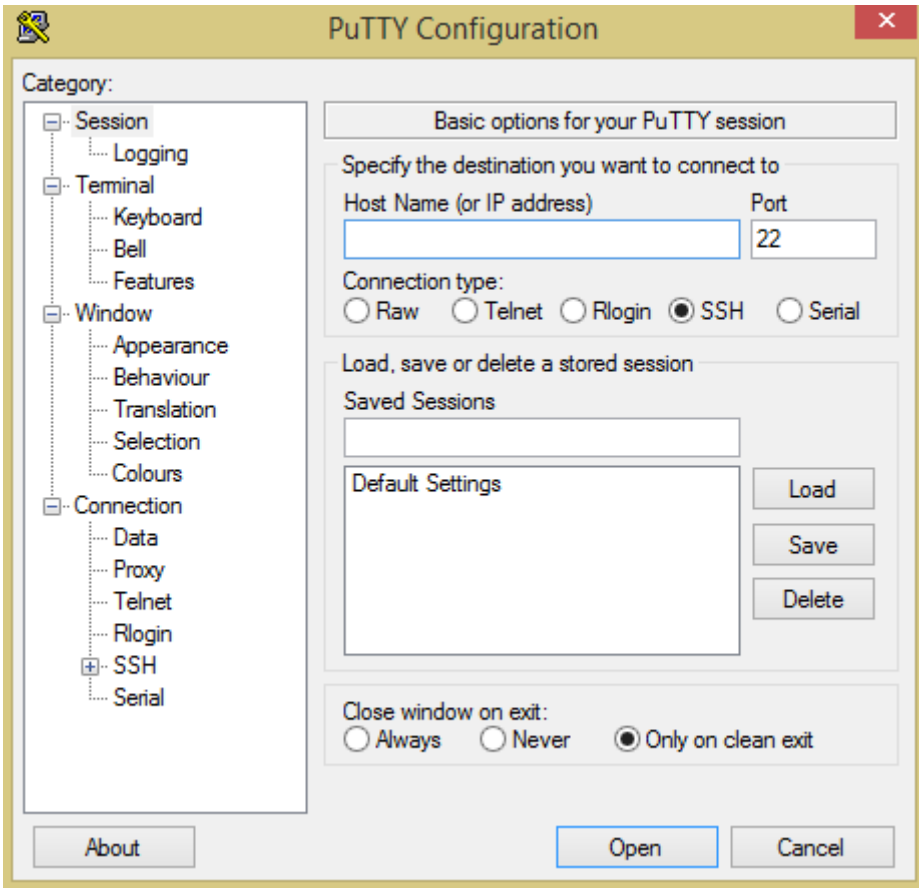
Flowchart ขั้นตอนการขอเพิ่มโดเมนเนม



ขั้นตอนการเพิ่มโดเมนเนมสำหรับผู้ดูแลระบบ

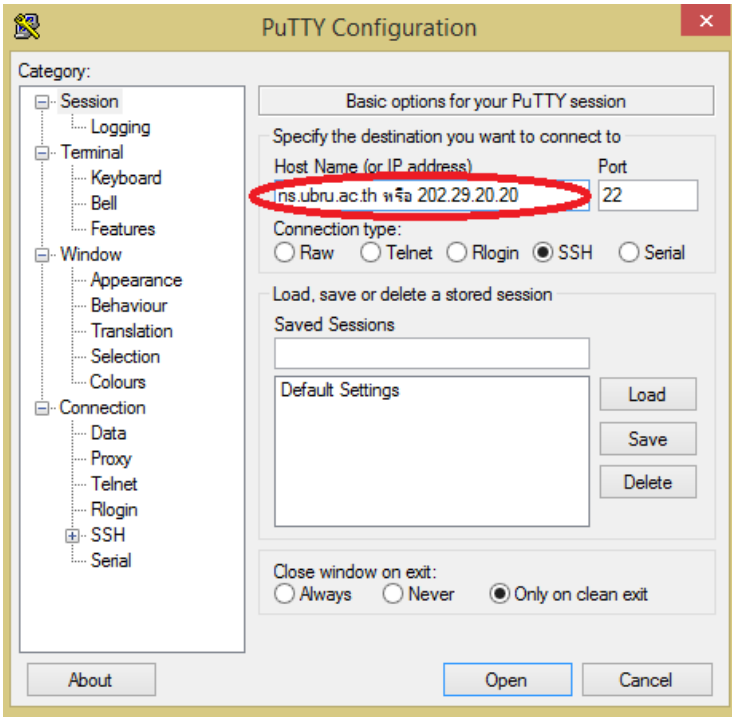
1. ผู้ดูแลระบบติดตั้งโปรแกรม Putty ในเครื่องคอมพิวเตอร์ โปรแกรม Putty (สามารถ Download Putty ได้จาก https://www.putty.org) การเพิ่มโดเมนเนมจะใช้โปรแกรม Putty เพื่อการเชื่อมต่อเข้าถึงระบบ โดเมนเนม

2. ดับเบิลคลิกที่ไอคอน  (ไอคอนโปรแกรม Putty) จะแสดงโปรแกรมดังรูป



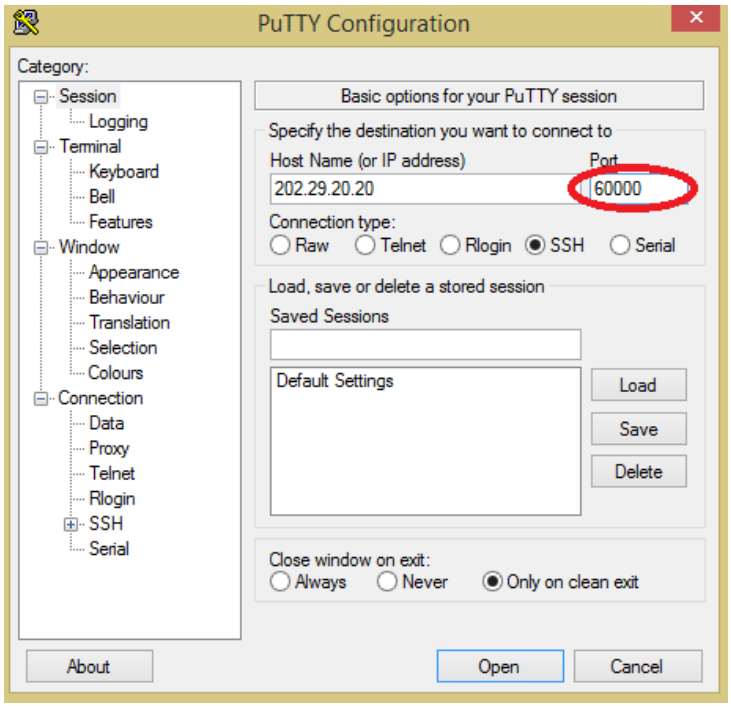
รูปแสดงหน้าต่างโปรแกรม Putty

3. ในช่อง Host Name (or IP address) ให้ใส่ชื่อ ns.ubru.ac.th หรือหมายเลข IP 202.29.20.20 ดังรูป (ใส่เพียงอย่างใดอย่างหนึ่งเท่านั้น)



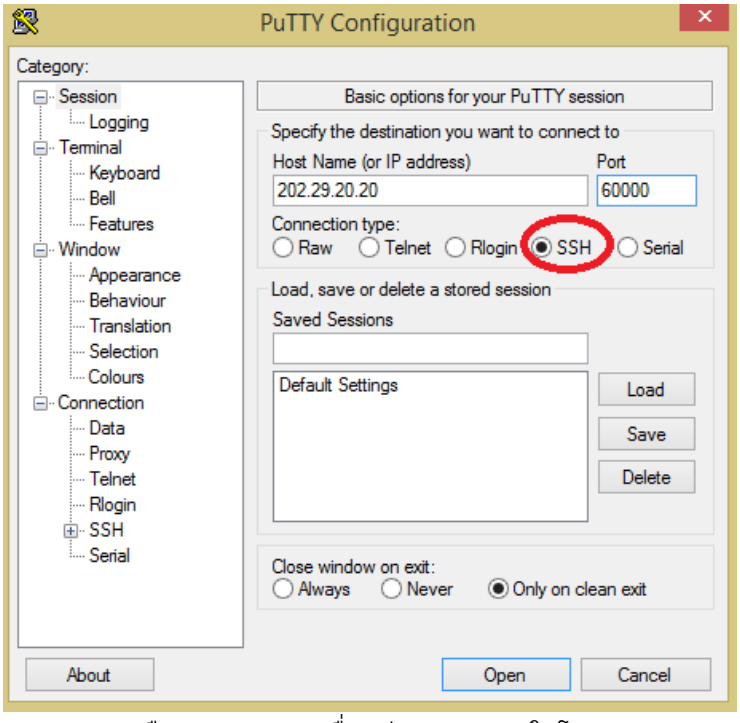
รูปแสดงการใส่ค่า Host Name ในโปรแกรม Putty

4. ในช่อง port ให้ใส่ค่า 60000 ดังรูป (เป็น ค่า port ที่กำหนดขึ้นมาในการ SSH เพื่อเข้าสู่ Server DNS)



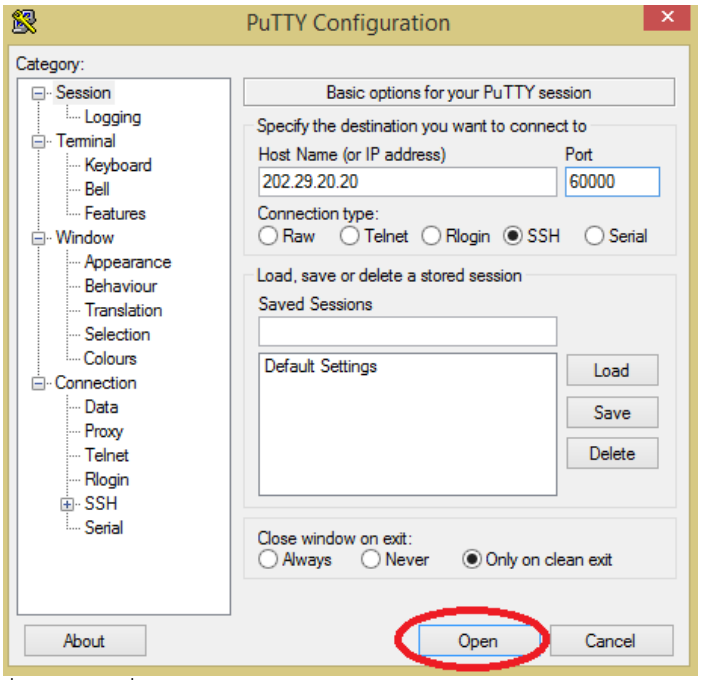
รูปแสดงการใส่ค่า port ในโปรแกรม putty

5. แถบ Connection type ให้เลือกการเชื่อมต่อแบบ SSH ดังรูป



รูปแสดงการเลือกรูปแบบการเชื่อมต่อแบบ SSH ในโปรแกรม putty

6. เมื่อใส่ค่าในโปรแกรม putty ครบแล้ว ให้ผู้ดูแลระบบ กดปุ่ม Open เพื่อเชื่อมต่อ ดังรูป



รูปแสดงการเริ่มต้นการเชื่อมต่อกับระบบ โดเมนเนม โดยกดปุ่ม Open ในโปรแกรม Putty

7. เมื่อกดปุ่ม Open ในโปรแกรม Putty แล้วจะปรากฏหน้าต่างเชื่อมต่อดังรูป

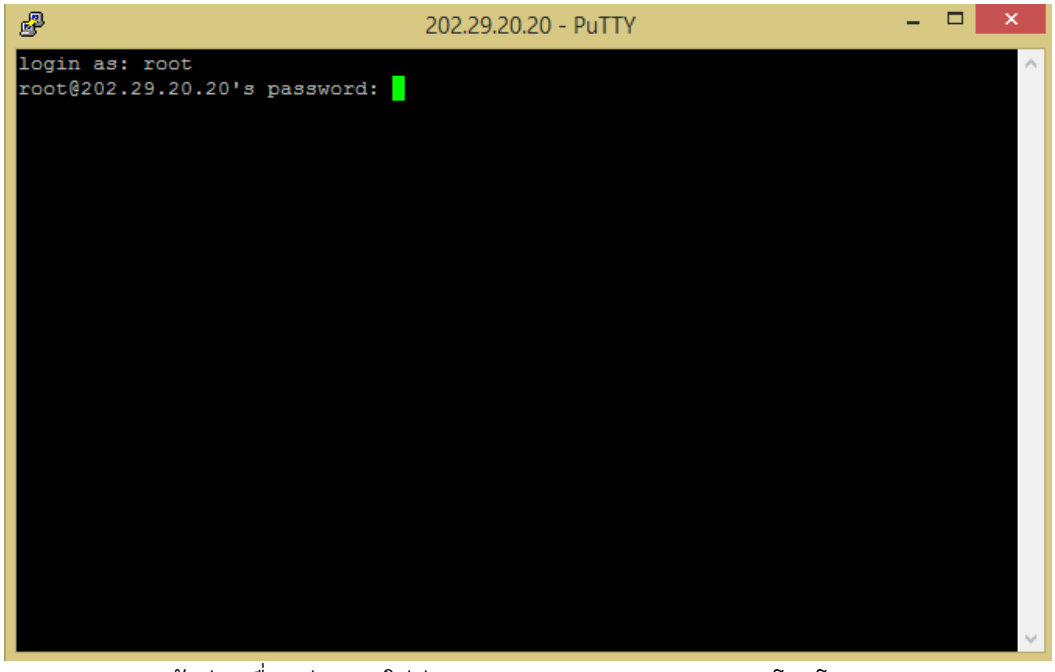
รูปแสดงหน้าต่างเชื่อมต่อโดยโปรแกรม Putty

8. ให้พิมพ์ username ที่ผู้ดูแลระบบสามารถเชื่อมต่อกับระบบได้ (ตัวอย่างจะใช้ root) หลัง login as:

ดังรูป

รูปแสดงการใส่ค่า username (root) หลัง login as: โดยโปรแกรม Putty

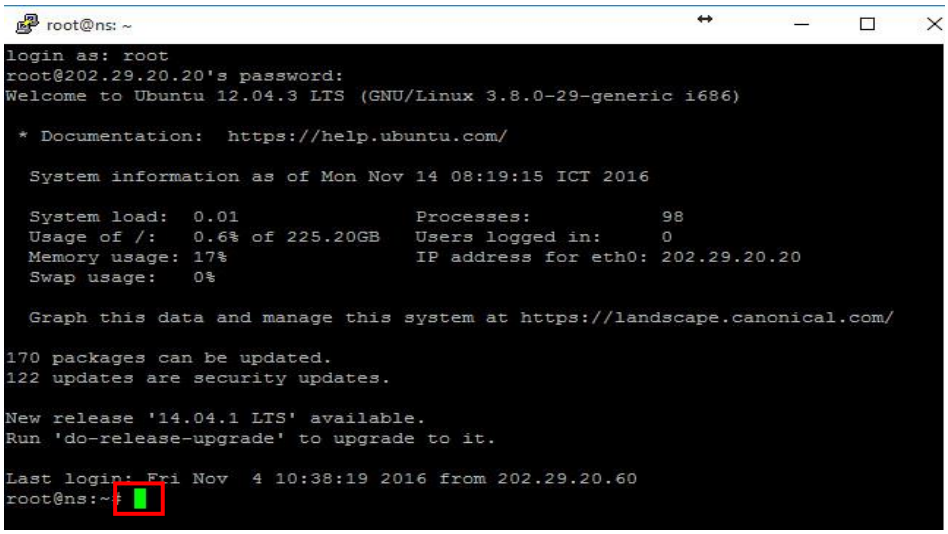
9. เมื่อใส่ username แล้วให้กด Enter จะขึ้นข้อความให้ใส่รหัสผ่าน (Password) ดังรูป



รูปแสดงหน้าต่างเชื่อมต่อ การใส่ค่า username และ password โดยโปรแกรม Putty

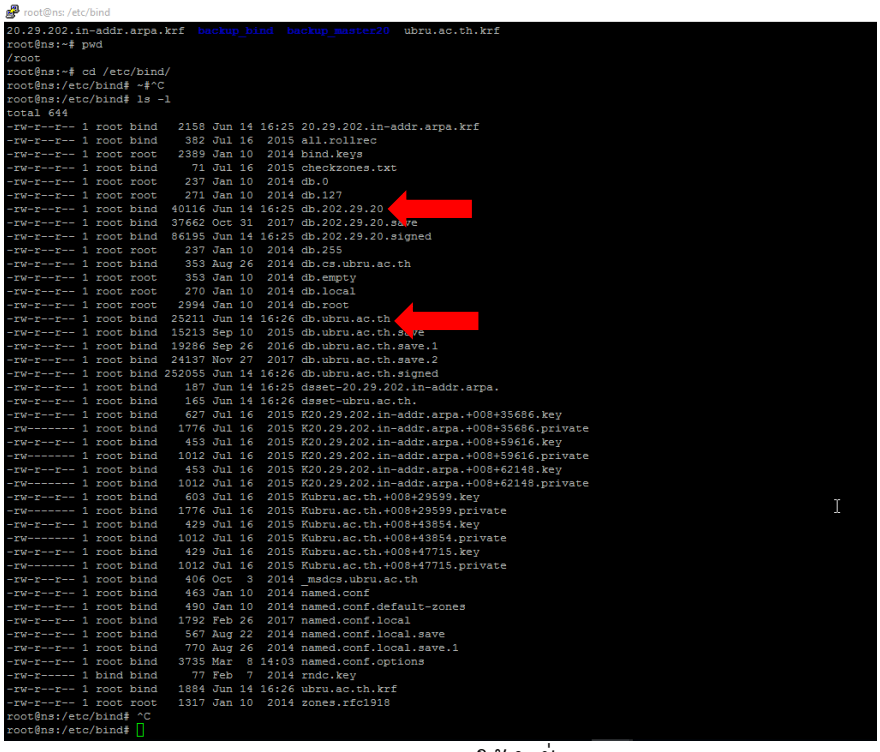
เมื่อใส่รหัสผ่าน (Password) เรียบร้อยแล้วให้กด Enter หากใส่ข้อมูลถูกต้องก็จะสามารถเข้าสู่ระบบได้

10. เมื่อเข้าระบบได้แล้ว ลักษณะหน้าตาของโปรแกรมแสดงดังภาพ ซึ่งจะเหมือนโปรแกรมที่รันบนดอส โดยมีเคอเซอร์สีเขียวรอรับคำสั่งอยู่บนหน้าจอ ผู้ดูแลระบบสามารถเข้าระบบเพื่อเพิ่มโดเมนเนมโดยย้ายไดเรคทอรี่ จาก /root (~#) ไปยังไดเรคทอรี่ /etc/bind ด้วยการพิมพ์คำสั่ง # cd /etc/bind ในระบบ ตรงที่เคอเซอร์กระพริบอยู่



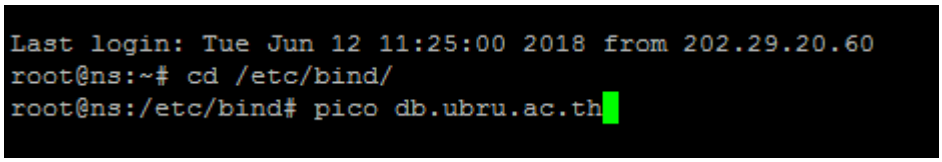
รูปแสดงจุดเคอเซอร์กระพริบ ที่อยู่ที่ไดเรคทอรี่ /root (~#)

11. ใช้คำสั่ง ls –l เพื่อดูแฟ้มข้อมูลชื่อ db.ubru.ac.th และ db.202.29.20 ว่ามีแฟ้มข้อมูลอยู่ในไดเรคทอรี่ /etc/bind หรือไม่



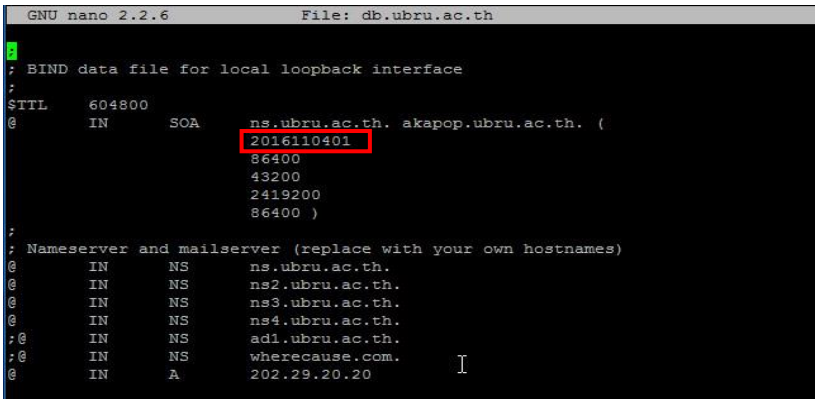
รูปแสดงการใช้คำสั่ง ls –l

12. เมื่อพบข้อมูลให้เข้าไปแก้ไข ไฟล์ db.ubru.ac.th โดยใช้คำสั่ง pico db.ubru.ac.th



รูปแสดงการใช้คำสั่ง pico ที่แฟ้มข้อมูล db.ubru.ac.th

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

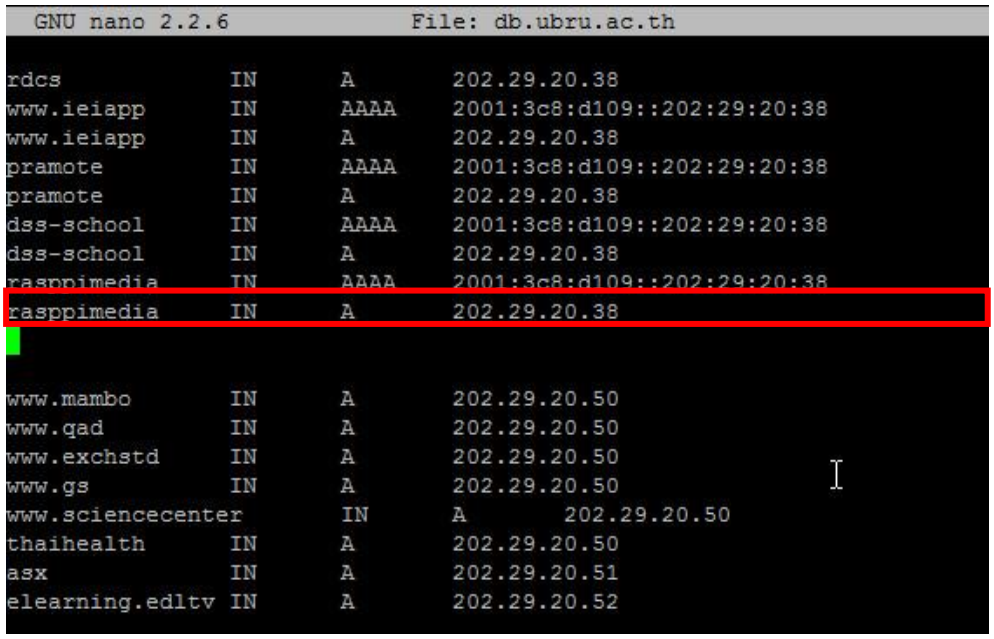


รูปแสดงรายละเอียดการตั้งค่าวันเวลาการแก้ไขแฟ้มข้อมูล

14. ทำการเพิ่ม โดเมนเนม โดยมีรูปแบบการเพิ่มข้อมูลดังนี้ดังนี้

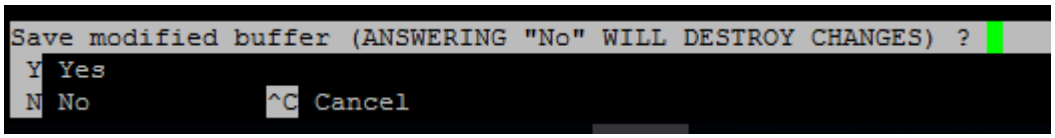
ชื่อโดเมน IN A IPAdress ดังตัวอย่าง

โดยชื่อโดเมนเนม คือชื่อที่ต้องการใช้งานภายใต้โดเมน ubru.ac.th เป็น rasppimedia และมีหมายเลข IPAdress เป็น 202.29.20.38 ดังรูป



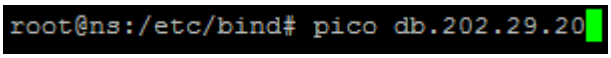
รูปแสดงรายละเอียดการเพิ่มโดเมนเนม

15. เมื่อเพิ่มโดเมนเนมเสร็จเรียบร้อย ให้กด Ctrl X เพื่อบันทึกข้อมูล และกด Y (YES) เพื่อยืนยันการบันทึกข้อมูล ดังรูป



รูปแสดงรายละเอียดการบันทึกข้อมูลที่แก้ไข

16. เมื่อทำการแก้ไขแฟ้มข้อมูล db.ubru.ac.th เสร็จเรียบร้อยแล้ว ให้แก้ไขแฟ้มข้อมูลชื่อ db.202.29.20 โดยใช้คำสั่งดังรูป



รูปแสดงคำสั่งการเข้าไปแก้ไขแฟ้มข้อมูล db.202.29.20

17. แก้ไข ค่า ตามรายละเอียด ดังนี้ 2016 : ปี คศ. 11 : เดือน 04 : วัน 01 : จำนวนครั้งที่แก้ไข โดยให้ตรงกับแฟ้ม db.ubru.ac.th

```
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns.ubru.ac.th. akapop.ubru.ac.th. (
                        2016110402      ; Serial
                          [illegible]   ; 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.
0.2.0.0.0.2.0.0.9.2.0.0.2.0.2.0.0.0.0.0.9.0.1.d.8.c.3.0.1.0.0.2        IN      PTR     ns.ubru.ac.th.
20      IN      PTR     ns.ubru.ac.th.
2.1.0.0.0.2.0.0.9.2.0.0.2.0.2.0.0.0.0.0.9.0.1.d.8.c.3.0.1.0.0.2        IN      PTR     ns2.ubru.ac.th.
21      IN      PTR     ns2.ubru.ac.th.
2.2.0.0.0.2.0.0.9.2.0.0.2.0.2.0.0.0.0.0.9.0.1.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.
```

รูปแสดงรายละเอียดการตั้งค่าวันเวลาการแก้ไขแฟ้มข้อมูล

18. เพิ่ม Reverse โดเมนเนม และ IPAdress ในแฟ้มข้อมูล db.202.29.20
โดยมีรูปแบบ ดังนี้ IP Reverse IN PTR ชื่อโดเมน ดังตัวอย่าง

```
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.
```

รูปแสดงรายละเอียดการเพิ่ม Reverse โดเมนเนม

19. เมื่อเพิ่ม Reverse โดเมนเนมเสร็จเรียบร้อย ให้กด Ctrl X เพื่อบันทึกข้อมูล และกด Y (YES) เพื่อยืนยันการบันทึกข้อมูล ดังรูป

```
Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ?
 Y Yes
 N No            ^C Cancel
```

รูปแสดงรายละเอียดการบันทึกข้อมูลที่แก้ไข

20. การสร้างระบบ DNSSEC เพื่อเข้ารหัสระบบ Reverse โดเมนเนม โดยใช้คำสั่ง zonesigner ดังตัวอย่าง # zonesigner -zone 20.29.202.in-addr.arpa db.202.29.20

```
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#
```

รูปแสดงการใช้คำสั่ง zonesigner เพื่อเข้ารหัส Reverse โดเมนเนม

21. การสร้างระบบ DNSSEC เพื่อเข้ารหัสระบบ โดเมนเนม โดยใช้คำสั่ง zonesigner ดังตัวอย่าง# zonesigner -zone ubru.ac.th db.ubru.ac.th

```
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#
```

รูปแสดงการใช้คำสั่ง zonesigner เพื่อเข้ารหัส โดเมนเนม

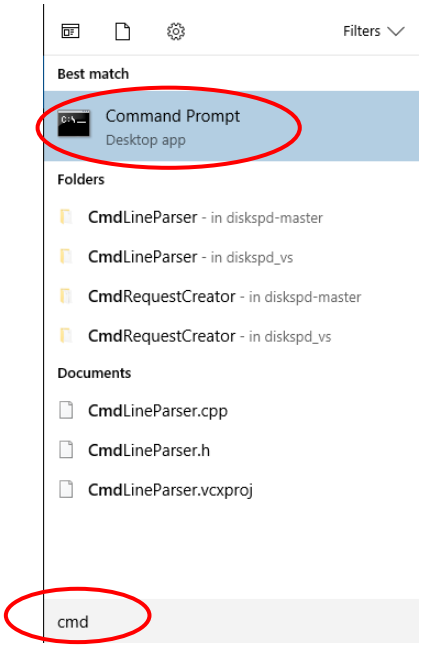
22. เมื่อทำการสร้างระ DNSSEC เสร็จเรียบร้อย ให้ทำการ restrart service โดยใช้คำสั่ง ดังนี้

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#
```

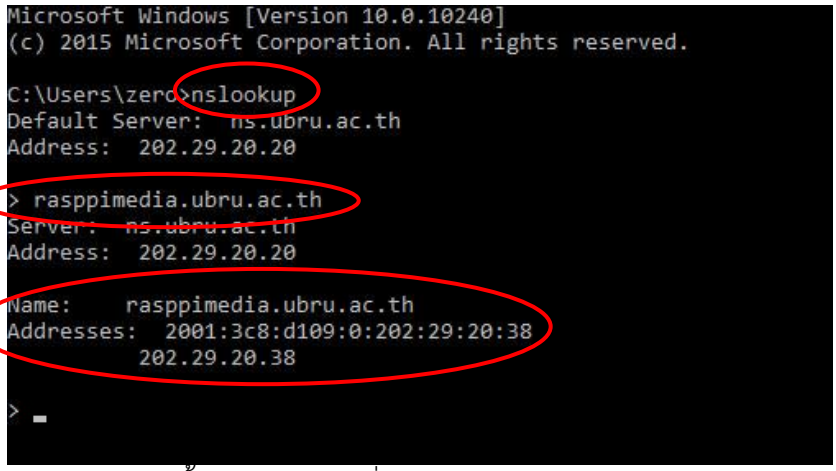
รูปแสดงการใช้คำสั่ง restrart service

23. หลังจากได้ restrart service ใหม่แล้ว ให้ตรวจสอบการใช้งานระโดเมนเนม ว่าชื่อโดเมนเนมที่เพิ่มเข้าไปในระบบ สามารถใช้งานได้แล้วหรือไม่ ทำการตรวจสอบ โดยเข้า command prompt ของระบบ Windows



รูปแสดงการเข้า ใช้งาน command prompt

24. เมื่อเข้าสู่หน้าจอ command prompt ให้พิมพ์ คำสั่ง nslookup หลังจากนั้นให้พิมพ์ชื่อโดเมนที่ได้เพิ่มเข้าไปในระบบโดเมนเนม ตรงเครื่องหมาย > rasppimedia.ubru.ac.th ระบบชื่อโดเมนเนมและหมายเลข IPAdress ดังรูป



รูปแสดงขั้นตอนการใช้คำสั่ง nslookup บนระบบ Windows

โดเมนเนมเซริฟเวอร์ของมหาวิทยาลัยราชภัฏอุบลราชธานี จะแบ่งออกเป็น 4 เซริฟเวอร์ โดยมี เซริฟเวอร์หลัก 1 เครื่อง และเซริฟเวอร์ที่เป็นเครื่องให้บริการโดเมนเนมเซริฟเวอร์ที่เป็นลูกข่ายจำนวน 3 เครื่อง ดังรายละเอียด

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

เทคนิคและแนวปฏิบัติ

1. ตรวจสอบชื่อโดเมนเนมที่ผู้ขอใช้บริการของเพิ่มโดเมนเนมว่าผิดกับ พรบ.คอมพิวเตอร์หรือพรบ.อื่นๆ ที่เกี่ยวข้องหรือไม่หรือชื่อโดเมเนมนั้นมีความไม่เหมาะสมและส่อไปในแนวไม่ดีหรือไม่

2. ตรวจสอบข้อมูลของหน่วยงานหรือบุคคลที่ขอเพิ่มโดเมนเนมว่าสังกัดหน่วยงานใดหรืออยู่ภายใต้หน่วยงานใดเพื่อเพิ่มข้อมูลโดเมนเนมให้เป็นไปตามเงื่อนไข คือ ชื่อโดเมนเนมและตามด้วยหน่วยงานที่สังกัด โดยต้องเป็นรูปแบบเดียวกันทั้งหมด

3. แจ้งข้อมูลกับผู้ขอใช้งานภายใน 2 วันทำการ ไม่ว่าการขอเพิ่มโดเมนเนมนั้นได้รับการอนุมัติหรือไม่ก็ตาม