



รายงาน

เรื่อง Configuring NTP & Syslog

จัดทำโดย

1. นายทวี ฐินใหม่ B5803569
2. นายภูชิต วงศรีไช B5809820
3. นายชุมทรัพย์ แก้วแสงอินทร์ B5814251
4. นายเฉลิมชัย เหลืองสกุลไทย B5814985

เสนอ

อาจารย์ ดร.นันทวุฒิ คะอังกู

รายงานนี้เป็นส่วนหนึ่งของรายวิชา 523353 Computer Networks

ภาคเรียนที่ 3 ปีการศึกษา 2560

มหาวิทยาลัยสุรนารี

คำนำ

รายงานฉบับนี้จัดทำขึ้นเพื่อเป็นส่วนหนึ่งของวิชา Computer Networks โดยมีจุดประสงค์เพื่อให้ผู้สนใจได้เข้าใจใน Network Time Protocol และ Syslog ได้มีการสืบค้นข้อมูลการจำลอง Router , Switch , Server และคอมพิวเตอร์ ได้นำความรู้ที่ได้จากการศึกษา ค้นคว้า และ การเชื่อมต่อแบบจำลองต่างๆของโปรแกรม cisco packet tracer ความหมายของ Network Time Protocol และ Syslog การทำงาน รูปแบบ NTP server Log server ซึ่งสามารถนำไปใช้ในศึกษาต่อสำหรับผู้สนใจ

ทั้งเนื้อหา และ ขั้นตอนการออกแบบจำลอง ผู้จัดทำหวังเป็นอย่างยิ่งว่ารายงานเล่มนี้จะเป็นประโยชน์แก่ผู้ที่สนใจ หากมีข้อบกพร่องประการใด ก็ขออภัย ณ โอกาสนี้

ผู้จัดทำ

กลุ่ม 3

| สารบัญ | |
|---------------------------|------|
| เรื่อง | หน้า |
| คำนำ | 1 |
| สารบัญ | 2 |
| ที่มาและความสำคัญ | 3 |
| Stratum layer | 4 |
| ระดับของ Stratum | 5 |
| ความจำเป็นที่จะต้องมี NTP | 6 |
| Syslog หรือ Log message | 7 |
| โจทย์ที่ได้รับมา | 11 |
| ขั้นตอนการ Configuring | 13 |
| เพิ่มเติมต่อจากโจทย์ | 20 |
| อ้างอิง | 25 |

ที่มาและความสำคัญ

กลุ่ม 3 project8 ได้เรื่อง Configuring NTP & Syslog จึงได้นำเสนอเรื่อง Configuring NTP & Syslog ซึ่งเป็นเนื้อหาส่วนหนึ่งของวิชา 523353 - Computer Networks ดังนี้

Network Time Protocol หรือ NTP คือ networking protocol ที่ใช้สำหรับ sync time ของ server ทุกเครื่องใน network ให้ตรงกัน ผ่าน packet-switch ซึ่ง NTP เป็น protocol ที่เก่าแก่มากและมีมาตั้งแต่ 1985 และใช้จนถึงปัจจุบัน เริ่มต้นคิดค้นโดย David L. Mills ที่ University of Delaware โดย Protocol ที่ใช้จะอยู่ในรูป client-server หรือ peer-to-peer โดยจะทำการรับส่งข้อมูล timestamps ผ่านทาง UDP (port 123)

ลักษณะการให้บริการเทียบเวลาของโปรโตคอล NTP จะแบ่งออกเป็นลำดับชั้นเรียกว่า Clock Strata โดยในแต่ละลำดับชั้นจะเรียกว่า Stratum โดยจะเริ่มต้นอยู่ที่ Stratum 0 ไปจนถึงลำดับชั้นที่ยอมรับว่ายังมีความเที่ยงตรง คือ Stratum 4 หากมากกว่านี้จะไม่ได้รับการยอมรับตามมาตรฐานที่กำหนดขึ้นมาจากหน่วยงาน ANSI (American National Standards Institute) สำหรับอุปกรณ์คอมพิวเตอร์ที่เทียบเวลากับ Stratum 0 เรียกว่า Stratum 1 ถ้ามีอุปกรณ์คอมพิวเตอร์อื่น ๆ ขอเทียบเวลากับ Stratum 1 จะเรียกว่า Stratum 2 ตามลำดับ จนถึง Stratum 4 นั้นหมายถึงลำดับของ Stratum ที่มากขึ้นจะมีค่าเวลาที่มีความห่างกับเวลามาตรฐานสากล Stratum 0 มากขึ้นด้วย

Stratum layer

NTP ทำงานเป็นลำดับชั้น หรือ layer โดยแต่ละ layer จะเรียกว่า “stratum” และเรียงตามตัวเลขจากบนสุดคือ 0 ลงไปเรื่อย ๆ หมายความว่า stratum1 ทำการ sync กับ server บนสุด และ stratum2 ก็จะทำ sync กับ computer ที่อยู่ใน stratum1 ต่อมาอีกที ซึ่งจะเห็นว่ายิ่ง stratum มีค่าต่ำจะยิ่งมีความแม่นยำมากกว่า stratum สูง ๆ สำหรับวง telecom ตัว NTP จะมีความสำคัญมากเพราะ signaling ที่ส่งกันภายใน network มีความเร็วสูงกว่าระบบ TCP ที่เราใช้กันปกติ รูปแบบของ stratum ที่ใช้งานจึงมีลักษณะนี้

- **Stratum 0** เป็นลำดับชั้นแรกในการเทียบเวลามีความแม่นยำสูงสุด เพราะเหมือน master clock ซึ่งใช้อุปกรณ์ที่ทำหน้าที่ Synchronize เวลามาตรฐานสากล โดยไม่มีค่าหน่วยเวลาใด ๆ โดยใช้เทคโนโลยีต่าง ๆ ได้แก่ Atomic Clock, คลื่นยาว (Long wave radio), การส่งสัญญาณ GP, เทคโนโลยี CDMA (เทคโนโลยีแบบที่ค่ายมือถือ) หรืออุปกรณ์เกี่ยวกับเวลาอื่น ๆ เช่น WWV, DCF77, GPS clock หรือ radio clock โดยจะสร้าง signal pulse ทุกวินาที เพื่อ sync ให้กับ computer ที่ต่อเข้ามา เราเรียกกันว่า “reference clock” อุปกรณ์ที่เป็น Stratum 0 จะไม่ได้ต่อในระบบ Network แต่จะเชื่อมโดยตรงกับเครื่องที่ทำหน้าที่เป็น Stratum 1 ดังนั้นเครื่องแม่ข่าย ที่ต่อโดยตรงกับ อุปกรณ์พวก Stratum-0 จะเรียกว่าเป็น Stratum-1 server ซึ่ง Stratum-1 server ถือว่าเป็น Time server ระดับต้น (Primary Time Server) ที่อยู่ในระบบ Network ที่ผู้ให้บริการ Network Time Protocol (NTP) สามารถมาเชื่อมผ่าน Network มาอ้างอิง เวลาได้

- **Stratum 1** เป็นลำดับที่ใช้คอมพิวเตอร์เครื่องแม่ข่าย ที่ ทำการ sync เชื่อมต่อเข้ากับ Stratum 0 ทุกๆ ไม่นานกว่า microsecond ซึ่ง Stratum 1 server ทำการ sync กับ Stratum 1 server ตัวอื่นๆ เพื่อเป็นการเช็ค และ backup อีกที เราเรียกว่า “Primary Time Server” เพื่อขอเทียบเวลา โดยใช้โปรโตคอล NTP ในประเทศไทยมีหน่วยงานที่ทำหน้าที่ระดับ Stratum 1 ได้แก่ สถาบันมาตรวิทยาแห่งชาติ และ กรมอุตุนิยมวิทยากรุงเทพ

- **Stratum 2** เป็นลำดับที่ขอเทียบเวลาจากเครื่องแม่ข่าย ในระดับ Stratum 1 โดยใช้เครื่องแม่ข่าย เชื่อมผ่าน ระบบเครือข่ายอินเทอร์เน็ต สามารถร้องขอการเทียบเวลาได้มากกว่าหนึ่งแหล่ง Stratum เพื่อรองรับการทำงานกรณีที่ Stratum 1 เครื่องใดเครื่องหนึ่งไม่สามารถให้บริการได้

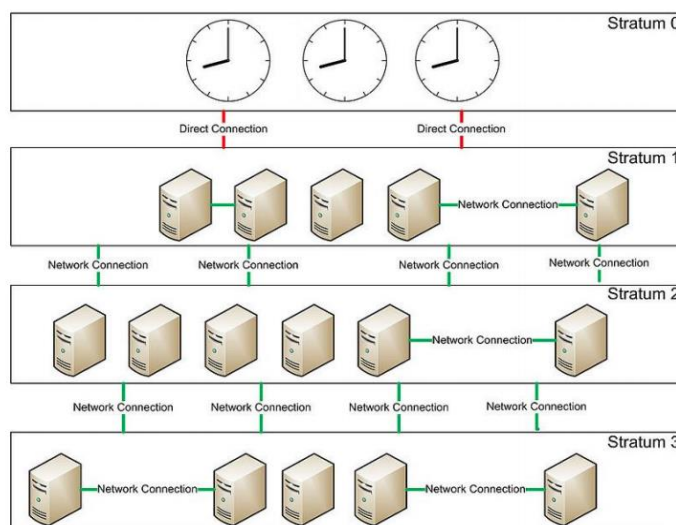
โดยทำการ sync ข้าม network มายัง stratum 1 server พวก stratum 2 นี้จะทำการ sync กับ stratum 1 server และเช็กกับ stratum 2 ตัวอื่นๆเพื่อความแม่นยำ

• **Stratum 3** เป็นลำดับที่ขอเทียบเวลาจากเครื่องแม่ข่าย ในระดับ Stratum 2 computer ที่ทำการ sync กับ stratum 2 server ใช้วิธีการ sync แบบเดียวกับ stratum 2 และก็สามารถเปิดให้ stratum 3 เข้ามา sync กับตนได้

ระดับของ Stratum

ระดับของ Stratum ที่สูงขึ้นจะหมายถึง NTP server จะมีระยะห่างจาก Stratum-1 server มากขึ้น เช่น Stratum-2 หมายถึง NTP Server ที่อ้างอิงเวลามาจาก NTP Server ระดับ Stratum-1, Stratum-3 Server หมายถึง NTP Server ที่อ้างอิงเวลามาจาก NTP Server ระดับ Stratum-2 เป็นอย่างนี้ไปเรื่อย ๆ โดยเวลา มาตรฐานโลก ที่เรียกว่า “Universal Time Clock (UTC) นับเริ่มต้นที่เมืองกรีนิช ประเทศอังกฤษ เป็น UTC+0 (ประเทศไทย UTC+7)

- Stratum-0 แต่ละระดับจะมีความผิดเพี้ยนจาก UTC ได้มากน้อยเพียงใด?
- Stratum-1 มีค่าความผิดเพี้ยนไม่เกิน 1 มิลลิวินาที จาก UTC
- Stratum-2 มีค่าความผิดเพี้ยนประมาณ 10-100 มิลลิวินาที จาก UTC



ภาพขั้นที่ ตอนของ NTP

ที่มา <http://xmodulo.com/setup-ntp-server-centos.html>

ความจำเป็นที่จะต้องมี NTP

เพื่อให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ ข้อ 9

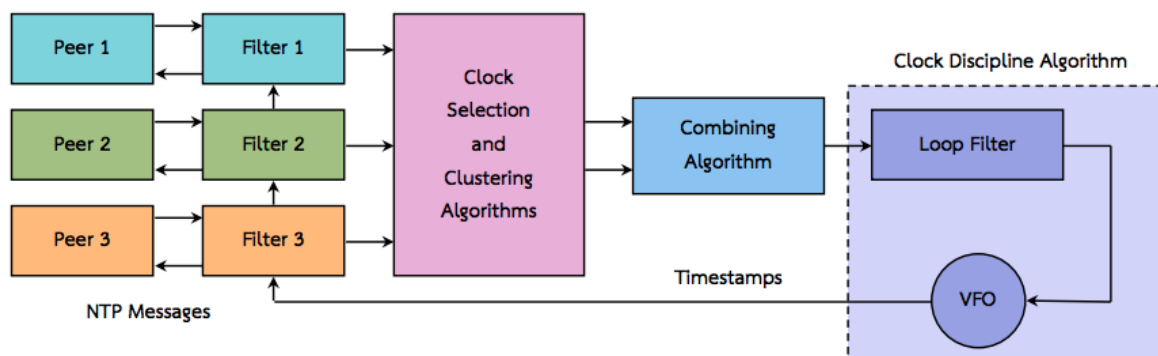
- เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริง ผู้ให้บริการต้องตั้งนาฬิกาของอุปกรณ์บริการทุกชนิดให้ตรง กับเวลาอ้างอิง สาทล (Stratum 0) โดยผิดพลาดไม่เกิน 10 มิลลิวินาที

- แนวทางแรกคือ ตั้ง NTP Server Stratum-1 ขึ้นมาเองในองค์กร ซึ่งจะทำให้เวลาผิดเพี้ยนน้อยกว่า 10 มิลลิวินาที อย่างแน่นอน

- แนวทางที่สองคือ ตั้ง NTP Server Stratum-2 ขึ้นมา ซึ่งยอมให้เวลาผิดเพี้ยนได้ในระดับ 10-100 มิลลิวินาที แล้วให้ NTP Server ของเราไป Synchronize time กับ Stratum-1 Server จาก Internet และควรเลือก Stratum-1

- NTP Server ในประเทศไทย NTP Server ที่เราตั้งขึ้นมาจะนับเป็น Stratum-2 Server จากนั้นก็กำหนดให้ อุปกรณ์ Network หรือ Servers ทุกชนิดในองค์กร Synchronize time มาจาก NTP Server ของเราเอง

- แนวทางที่สามคือ ไม่ตั้ง NTP Server โดยยังคงกำหนดให้อุปกรณ์ Network หรือ Server ไป Synchronize time ผ่าน Internet โดย พยายามเลือก Stratum-1 Server ซึ่งเวลาก็อาจจะเพี้ยนไปบ้าง เกินกว่า 10 มิลลิวินาทีขึ้นไป



รูปแบบการทำงานของ NTP

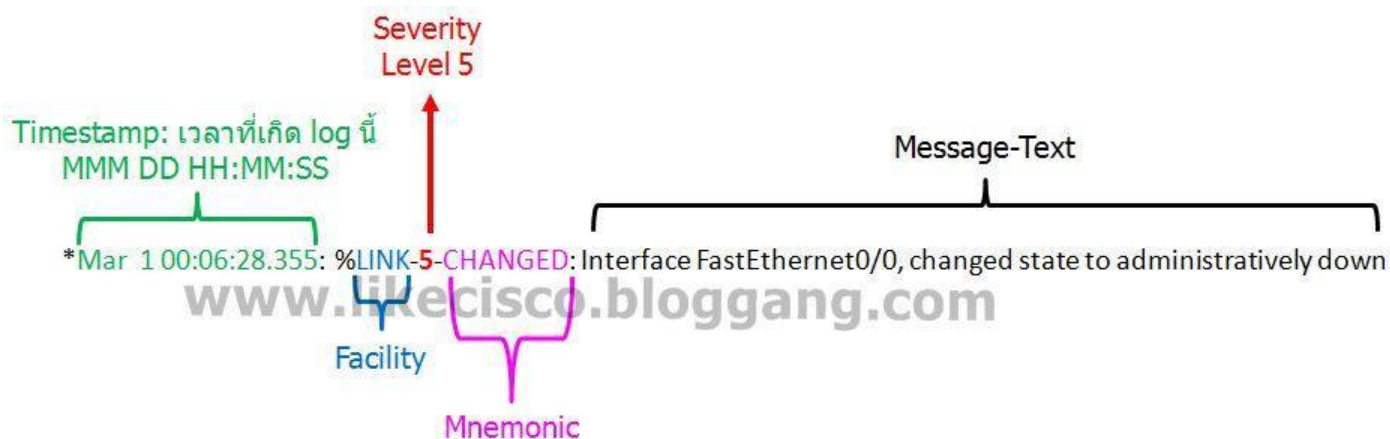
Syslog หรือ Log Message

Log Message คือ เวลาเกิดเหตุอะไรเกิดขึ้นกับ switch หรือ router แล้ว มันจะมี logging message คอย alert ให้ network administrator อย่างพวกเราทราบถึงสถานการณ์ต่างๆ ที่เกิดขึ้นกับตัวของมัน เพื่อให้เราเข้าไปตรวจสอบปัญหาต่างๆ ณ. ขณะนั้น หรือสามารถตรวจสอบปัญหาย้อนหลังได้ Logging message ได้จัดระดับความรุนแรงไว้ 8 ระดับดังตารางข้างล่างระดับความรุนแรง (severity level) ของ log

| Level | Keyword | Description |
|-------|---------------|---|
| 0 | emergencies | System is unusable |
| 1 | alerts | Immediate action is needed |
| 2 | critical | Critical conditions exist |
| 3 | errors | Error conditions exist |
| 4 | warnings | Warning conditions exist |
| 5 | notification | Normal, but significant, conditions exist |
| 6 | informational | Informational messages |
| 7 | debugging | Debugging messages |

- Level 0 จะเป็นระดับของ log ที่มีความรุนแรงมากที่สุด
- Level 7 จะเป็นระดับของ log ที่มีความรุนแรงน้อยที่สุด

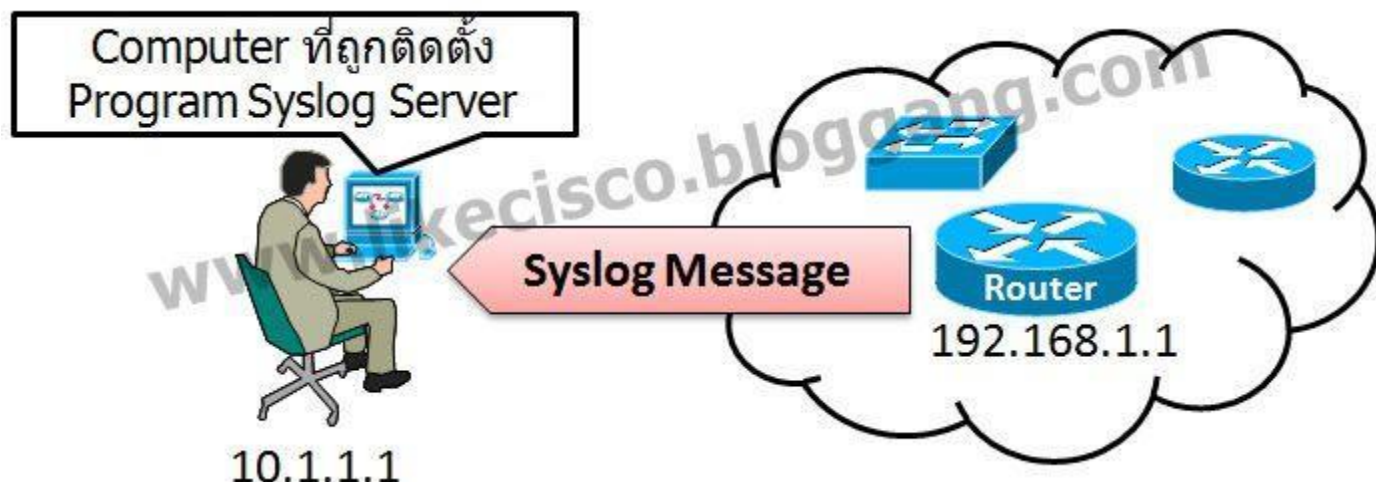
ตัวอย่าง และตำแหน่งที่บ่งบอกถึงระดับความรุนแรง (severity) ของ logging message ที่แฝง



อยู่ใน message ดังภาพข้างล่าง (โดยเอา logging message ข้างบนมาแจกแจงให้ดูนะครับ)

แม้ว่า logging message ต่างๆ จะถูกเก็บไว้ใน memory ของอุปกรณ์ก็ตาม แต่มันจะไม่สามารถถูกเก็บไว้ได้ทั้งหมด เพราะเมื่อ memory ที่ถูกกัน buffer ไว้สำหรับการเก็บ logging message ได้เต็มแล้ว logging message เก่าๆ จะถูกแทนที่ด้วย logging message ใหม่ๆ ดังนั้นหากเราต้องการดู log ย้อนหลังไปสัก 3 เดือน เราก็อาจจะไม่สามารถดูได้

ด้วยปัญหาดังกล่าวข้างต้น เราจึงต้องทำการส่ง "logging message" ไปเก็บไว้บน Syslog Server ที่ใดที่หนึ่งใน network โดยเราจะต้องทำการติดตั้ง program Syslog Server (เช่น Kiwi Syslog - www.kiwisyslog.com) ไว้บน Server ตัวใดตัวหนึ่ง จากนั้นก็ให้มา configure บนอุปกรณ์ให้ทำการส่ง "logging message" ไปยัง Syslog Server ดังกล่าว เช่น



1. Server หรือ Computer - IP address 10.1.1.1 ทำการ install program Syslog Server เช่น Kiwi Syslog
2. ที่ switch หรือ router ตัวที่ต้องการจะ transfer "Syslog message", ให้ทำการ ping ไปยัง Syslog Server เพื่อตรวจสอบ Layer 3 connectivity ซึ่งจากตัวอย่างนี้ คือ ให้ ping ไปยัง 10.1.1.1 และจะต้อง ping สำเร็จ

3. จากนั้น ที่ switch หรือ router, ให้ทำการ configure command ดังต่อไปนี้ เพื่อที่จะทำให้อุปกรณ์ดังกล่าวสามารถส่ง Syslog message ไปเก็บไว้บน Syslog server ได้ ดังนี้

Step 1: ระบุ IP address ของ Syslog server ที่จะกลายเป็น destination สำหรับ Syslog messages

Router#configure terminal

Router(config)#logging 10.1.1.1

Command "logging 10.1.1.1" หมายถึง ให้ส่ง Syslog message ไปยัง Syslog Server IP address 10.1.1.1

Step 2: จำกัดกลุ่ม หรือระดับของ Syslog message ที่จะถูกส่งไปยัง Syslog server โดยอยู่บนพื้นฐานของระดับของความรุนแรงของ logging message (Severity Level)

Router(config)#logging trap

Command "logging trap notifications" จะหมายถึงการกำหนดให้อุปกรณ์ตัวนี้ทำการส่ง Syslog message ที่มีความรุนแรงตั้งแต่ระดับ Severity Level 5 (Notifications) ไปจนถึง Severity Level 0 (Emergencies) เท่านั้น นั่นก็คือ

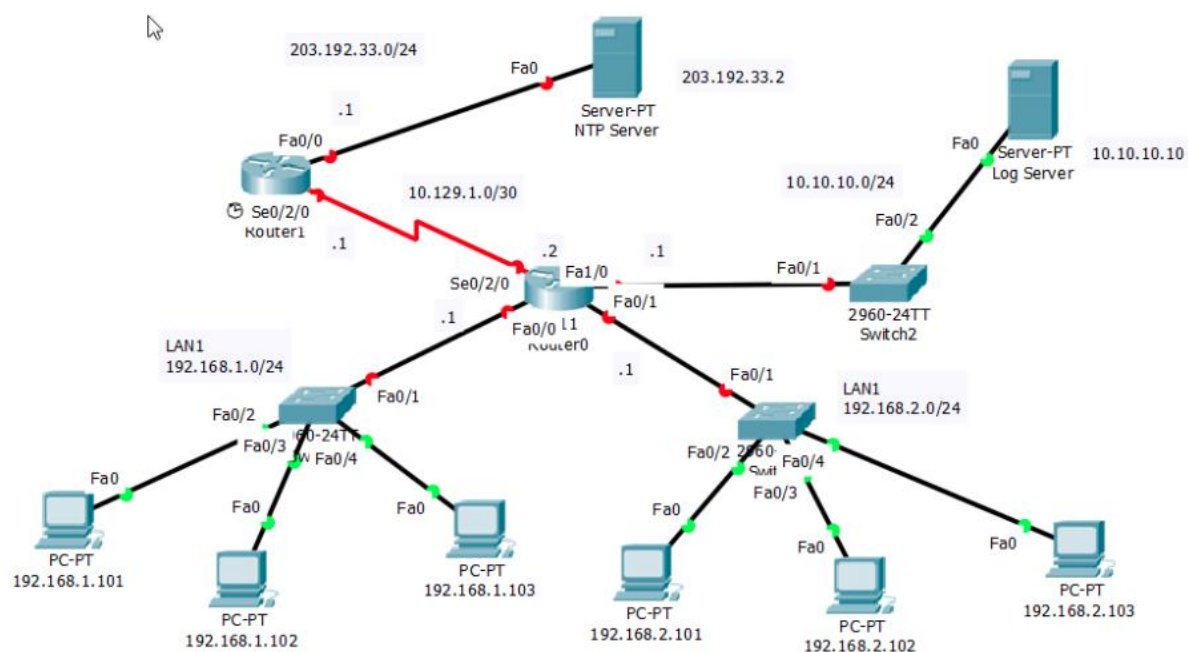
Level 5-Notification, Level 4-Warning, Level 3-Error, Level 2-Critical, Level 1-Alert, Level 0-Emergency

โดย Default แล้ว หากไม่ระบุ command "logging trap" แล้ว จะหมายถึงการส่ง logging message ตั้งแต่ระดับ Severity Level 6 (informational) เป็นต้นไป นั่นก็คือ Level 6 (informational), Level 5-Notification, Level 4-Warning, Level 3-Error, Level 2-Critical, Level 1-Alert, Level 0-Emergency

โจทย์ที่ได้รับมา

อุปกรณ์: Router 2 ตัว, Switch 2 ตัว, Computer 6 เครื่อง, Server 2 เครื่อง

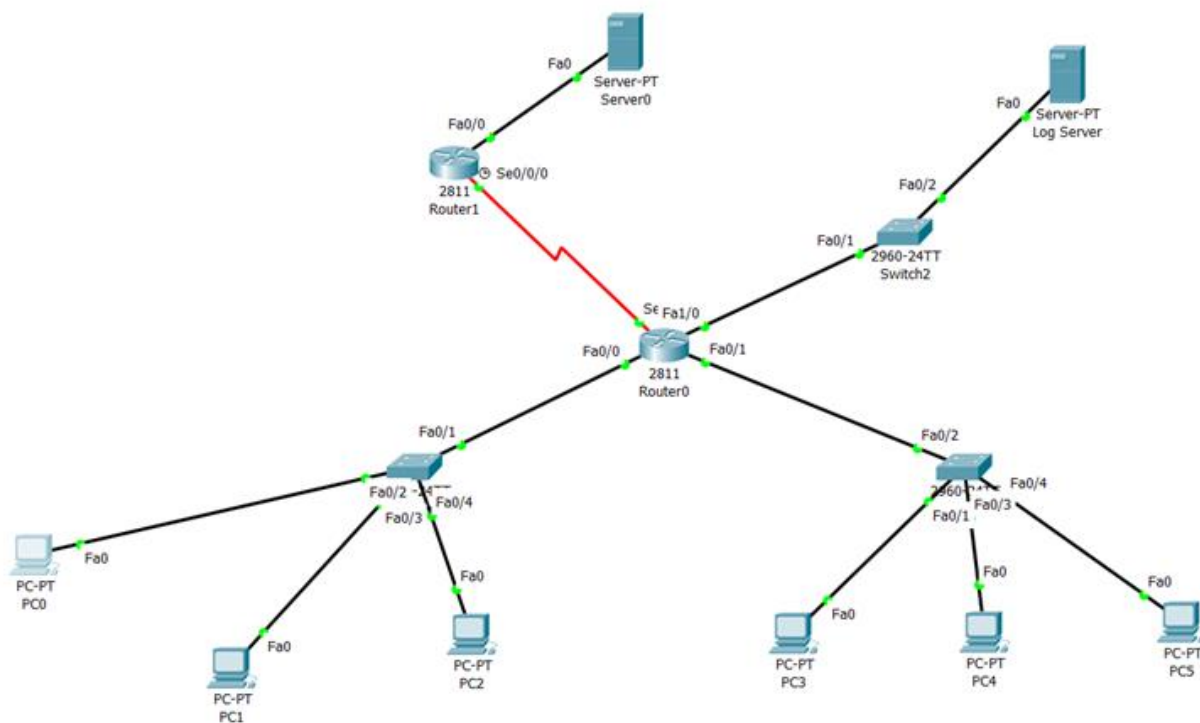
โจทย์: Configuration NTP & Syslog บนอุปกรณ์ Router และ Switch



รูปภาพ ได้รับมาจาก Project 5 : Configuring NTP & Syslog

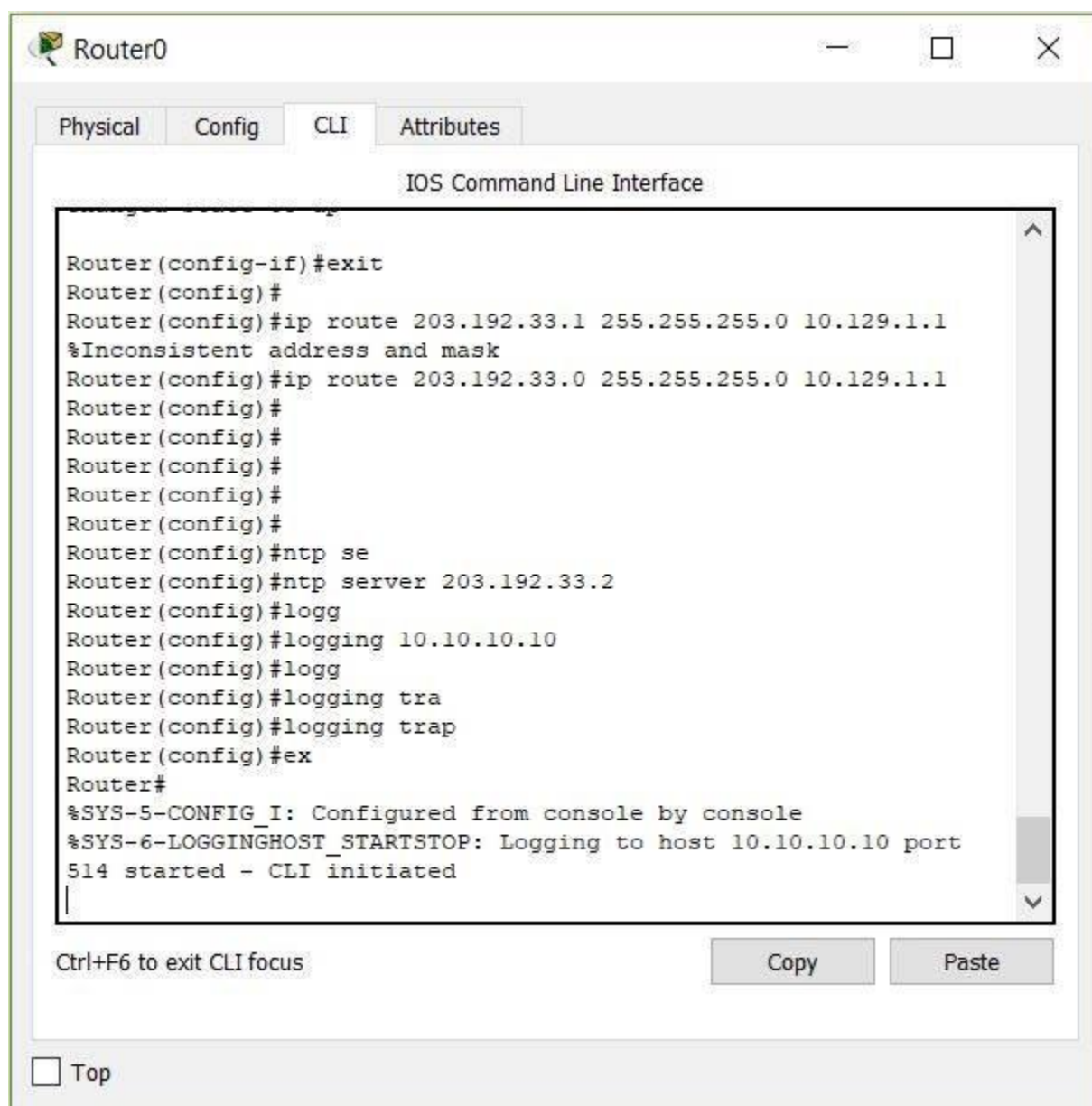
ที่มา <https://docs.google.com/viewer>

สร้างแบบจำลองเครือข่ายตามรูปผังงานการเชื่อมต่อเครือข่ายด้านบนนี้ ด้วยอุปกรณ์ที่กำหนดมาให้



รูปภาพ แบบจำลองเครือข่ายตามรูปผังงานการเชื่อมต่อเครือข่ายด้วยอุปกรณ์ที่กำหนดมาให้

ขั้นตอนการ Configuring



รูปภาพ รูปแบบ configuring NTP บน Router 0

ส่วนของโค้ดในการ configuring NTP บน Router 0

NTP setting

R0(config)#ntp server 203.192.33.2

เชื่อมต่อไปยัง server ntp

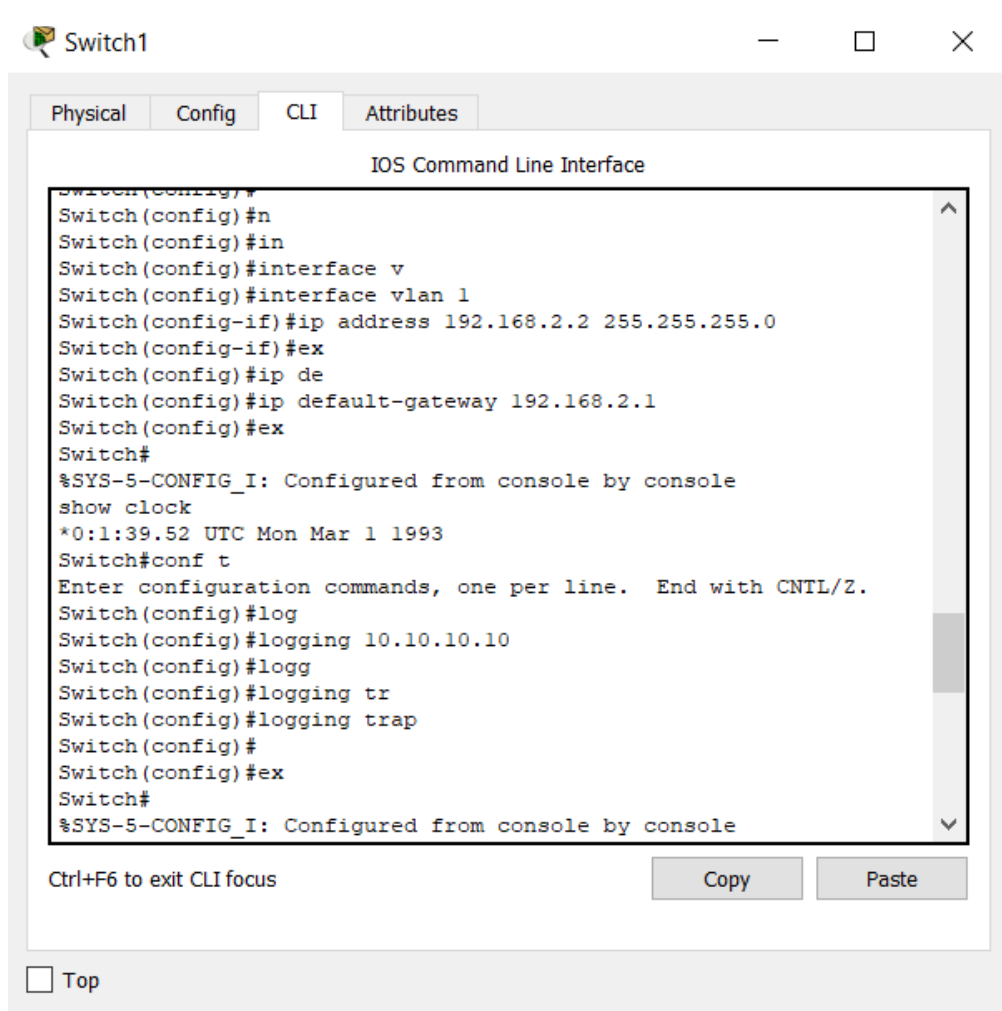
R0(config)#logging 10.10.10.10

เชื่อมต่อไปยัง Log server

R0(config)#logging trap

กำหนดให้ ส่ง log message ไปเก็บไว้ที่ log server

R0(config)#service timestamps log datetime msec แสดงเวลาและวันที่ของ log message



รูปภาพ รูปแบบ configuring บน Switch 1

ส่วนของโค้ดในการ configuring switch 1

SWitch1 configure

SW1(config)#interface vlan 1

SW1(config-if)#ip address 192.168.2.2 255.255.255.0 กำหนด ip address ให้กับ vlan 1

SW1(config)#ip default-gateway 192.168.2.1

กำหนด gateway ให้กับ vlan1

SW1(config)#logging 10.10.10.10

เชื่อมต่อไปยัง log server

SW1(config)#logging trap

กำหนดให้ส่ง log message ไปเก็บไว้ที่ log server

ภาพรวมทั้งหมด

PC0-PC5 configure

| PC | IP Address | Subnet Mask | Gateway |
|----|---------------|---------------|-------------|
| 0 | 192.168.1.101 | 255.255.255.0 | 192.168.1.1 |
| 1 | 192.168.1.102 | 255.255.255.0 | 192.168.1.1 |
| 2 | 192.168.1.103 | 255.255.255.0 | 192.168.1.1 |
| 3 | 192.168.2.101 | 255.255.255.0 | 192.168.2.1 |
| 4 | 192.168.2.102 | 255.255.255.0 | 192.168.2.1 |
| 5 | 192.168.2.103 | 255.255.255.0 | 192.168.2.1 |

NTP Server

203.192.33.2 255.255.255.0 203.192.33.1

Log Server

10.10.10.10 255.255.255.0 10.10.10.1

Router0 configure

Fa0/0 192.168.1.1 255.255.255.0

Fa0/1 192.168.2.1 255.255.255.0

Fa1/0 10.10.10.1 255.255.255.0

Se0/0/0 10.129.1.2 255.255.255.0

Port Rout

203.192.33.0 255.255.255.0 10.129.1.1

NTP setting

R0(config)#ntp server 203.192.33.2

R0(config)#logging 10.10.10.10

R0(config)#logging trap

R0(config)#service timestamps log datetime msec

Router1 configure

Fa0/0 203.192.33.1 255.255.255.0

Se0/0/0 10.129.1.1 255.255.255.0

Port Rout

192.168.1.0 255.255.255.0 10.192.1.2

192.168.2.0 255.255.255.0 10.192.1.2

10.10.10.0 255.255.255.0 10.192.1.2

NTP setting

```

R1(config)#ntp server 203.192.33.2
R1(config)#logging 10.10.10.10
R1(config)#logging trap
R1(config)#service timestamps log datetime msec

```

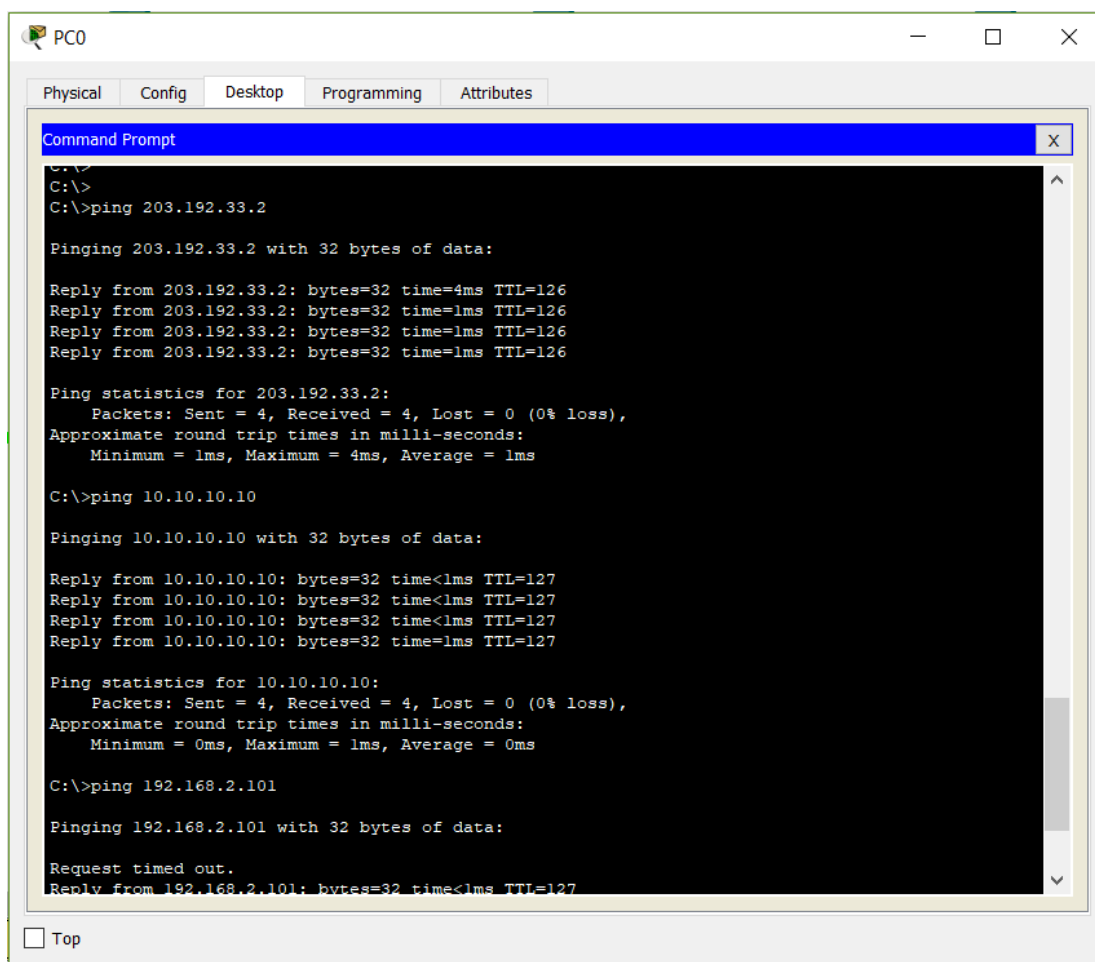
SWitch1 configure

```

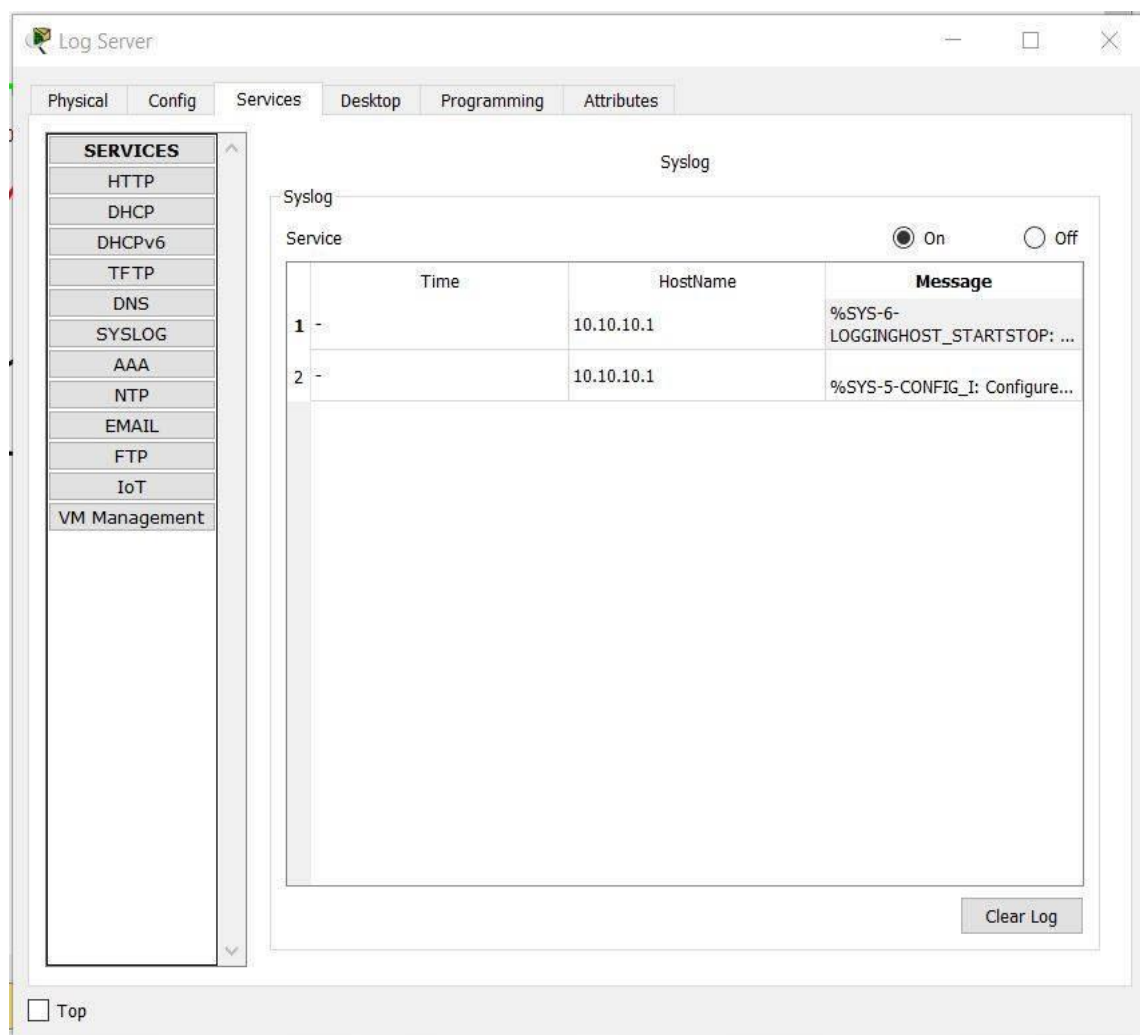
SW1(config)#interface vlan 1
SW1(config-if)#ip address 192.168.2.2    255.255.255.0
SW1(config)#ip default-gateway 192.168.2.1
SW1(config)#logging 10.10.10.10
SW1(config)#logging trap

```

ไฟล์ที่ configuring สมบูรณ์ ถ้าถูกต้องตามโจทย์ที่อาจารย์ให้มา สามารถ Ping ไปยัง NTP server และ Log server ได้ และสามารถ Ping ไป PC 3 ถึง PC 5 ที่อยู่ใน net work เดียวกันได้



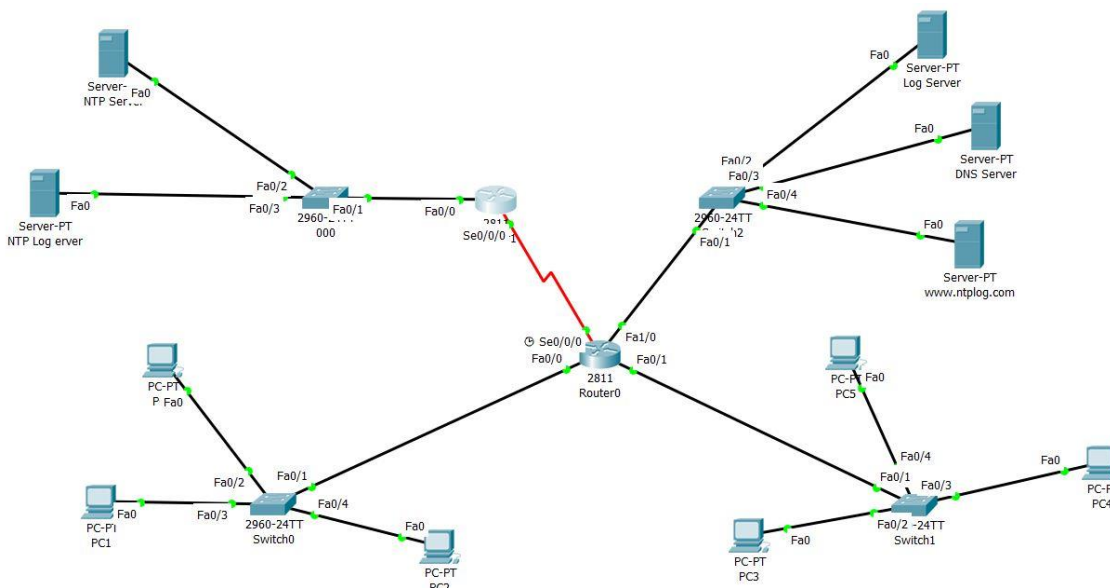
รูปภาพ ไฟล์ที่ configuring สมบูรณ์ สามารถ ping ไปหา NTP-server log และ pc
ที่อยู่ใน net work เดียวกันได้จากโจทย์ที่กำหนดให้



รูปภาพ การแสดงผลบน log server

เพิ่มเติมต่อจากโจทย์

อุปกรณ์ : เพิ่ม NTP log server 1 เครื่อง , Log server 1 เครื่อง , DNS server 1 เครื่อง , Server www.ntplog.com 1 เครื่อง , Switch 1 เครื่อง , สายนำสัญญาณชนิดตรง(Straight Through)



รูปภาพ แบบจำลองเครือข่ายตามรูปผังงานการเชื่อมต่อเครือข่ายด้วยอุปกรณ์ที่เพิ่มเติม

PC0-PC5 configure

| PC | IP Address | Subnet Mask | Gateway | DNS Server |
|----|---------------|---------------|-------------|-------------|
| 0 | 192.168.1.101 | 255.255.255.0 | 192.168.1.1 | 10.10.10.11 |
| 1 | 192.168.1.102 | 255.255.255.0 | 192.168.1.1 | 10.10.10.11 |
| 2 | 192.168.1.103 | 255.255.255.0 | 192.168.1.1 | 10.10.10.11 |
| 3 | 192.168.2.101 | 255.255.255.0 | 192.168.2.1 | 10.10.10.11 |
| 4 | 192.168.2.102 | 255.255.255.0 | 192.168.2.1 | 10.10.10.11 |
| 5 | 192.168.2.103 | 255.255.255.0 | 192.168.2.1 | 10.10.10.11 |

NTP Server

203.192.33.2 255.255.255.0 203.192.33.1

NTP Log Server 203.192.33.3 255.255.255.0 203.192.33.1

Log Server

10.10.10.10 255.255.255.0 10.10.10.1

DNS Server

10.10.10.11 255.255.255.0 10.10.10.1

www.ntplog.com Server

10.10.10.12 255.255.255.0 10.10.10.1

Router0 configure

Fa0/0 192.168.1.1 255.255.255.0

Fa0/1 192.168.2.1 255.255.255.0

Fa1/0 10.10.10.1 255.255.255.0

Se0/0/0 10.129.1.2 255.255.255.0

Port Rout

203.192.33.0 255.255.255.0 10.129.1.1

---Rount0 NTP setting---

R0(config)#ntp server 203.192.33.2

R0(config)#ntp update-calendar

R0(config)#logging 10.10.10.10

R0(config)#logging trap

R0(config)#service timestamps log datetime msec

Router1 configure

Fa0/0 203.192.33.1 255.255.255.0

Se0/0/0 10.129.1.1 255.255.255.0

Port Rout

192.168.1.0 255.255.255.0 10.192.1.2

192.168.2.0 255.255.255.0 10.192.1.2

10.10.10.0 255.255.255.0 10.192.1.2

---Rount1 NTP setting---

R1(config)#ntp server 203.192.33.2

R0(config)#ntp update-calendar

R1(config)#logging 203.192.33.3

R1(config)#logging trap

R1(config)#service timestamps log datetime msec

SWitch1 configure

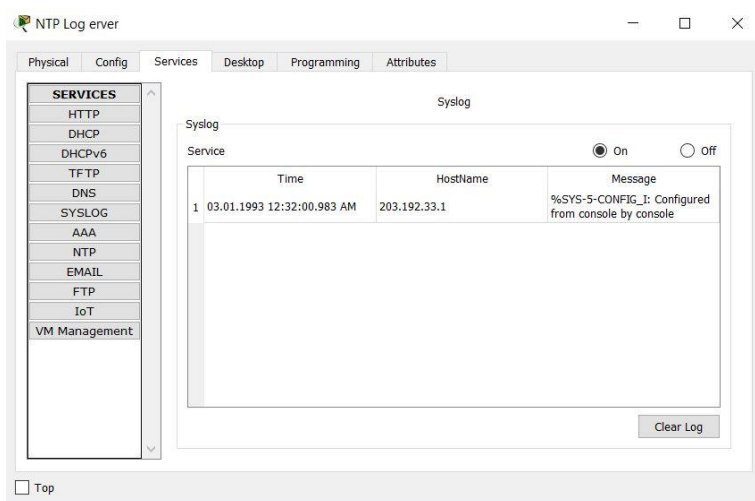
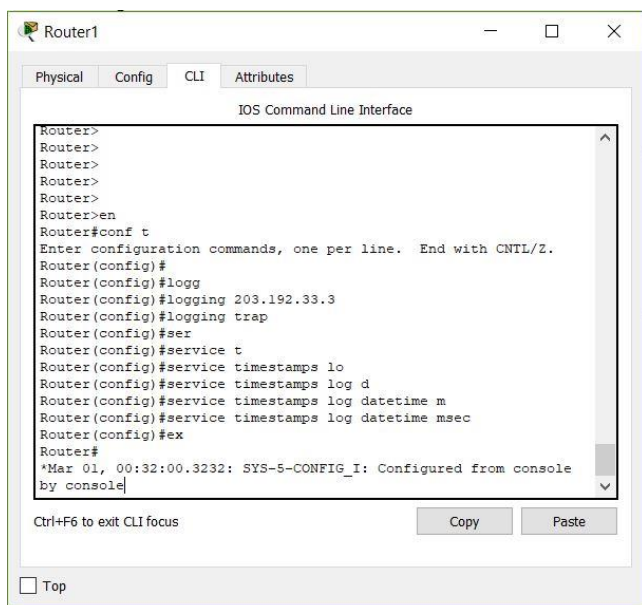
SW1(config)#interface vlan 1

SW1(config-if)#ip address 192.168.2.2 255.255.255.0

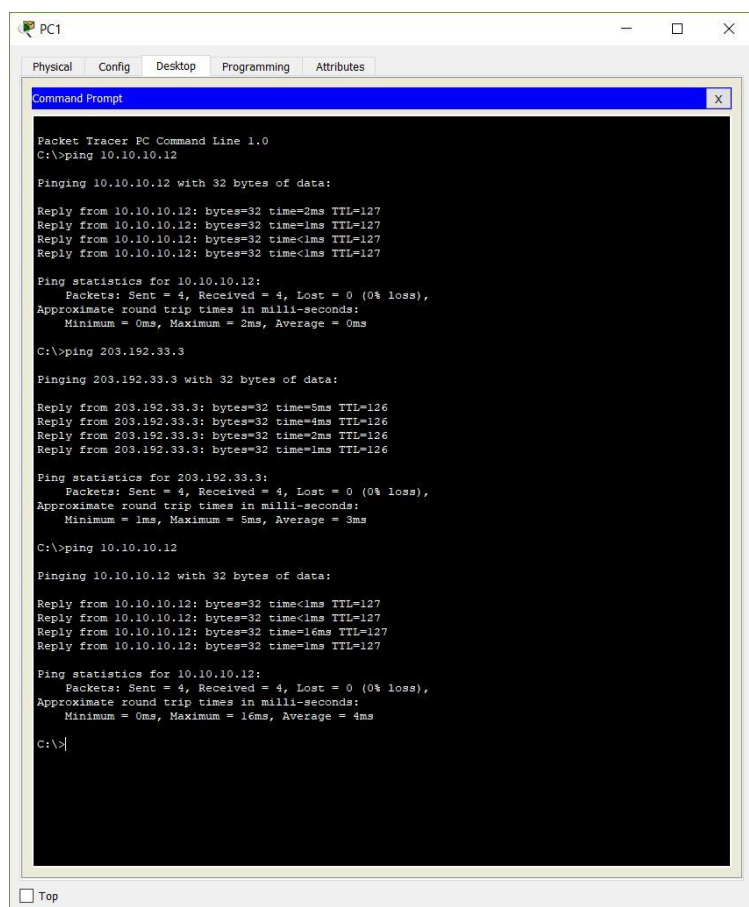
SW1(config)#ip default-gateway 192.168.2.1

SW1(config)#logging 10.10.10.10

SW1(config)#logging trap



รูปภาพ การ configure บน Router1 เพื่อส่ง logging message ไปยัง NTP Log Server



The screenshot shows a Packet Tracer PC Command Line window for PC1. The window has tabs for Physical, Config, Desktop, Programming, and Attributes. The Command Prompt is open, displaying the results of three ping commands. The first command is 'ping 10.10.10.12', which shows four successful replies with 0% loss. The second command is 'ping 203.192.33.3', which also shows four successful replies with 0% loss. The third command is 'ping 10.10.10.12' again, showing four successful replies with 0% loss. The window has a 'Top' button at the bottom left.

```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 10.10.10.12

Pinging 10.10.10.12 with 32 bytes of data:

Reply from 10.10.10.12: bytes=32 time=2ms TTL=127
Reply from 10.10.10.12: bytes=32 time=1ms TTL=127
Reply from 10.10.10.12: bytes=32 time<1ms TTL=127
Reply from 10.10.10.12: bytes=32 time<1ms TTL=127

Ping statistics for 10.10.10.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>ping 203.192.33.3

Pinging 203.192.33.3 with 32 bytes of data:

Reply from 203.192.33.3: bytes=32 time=5ms TTL=126
Reply from 203.192.33.3: bytes=32 time=4ms TTL=126
Reply from 203.192.33.3: bytes=32 time=2ms TTL=126
Reply from 203.192.33.3: bytes=32 time=1ms TTL=126

Ping statistics for 203.192.33.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 5ms, Average = 3ms

C:\>ping 10.10.10.12

Pinging 10.10.10.12 with 32 bytes of data:

Reply from 10.10.10.12: bytes=32 time<1ms TTL=127
Reply from 10.10.10.12: bytes=32 time<1ms TTL=127
Reply from 10.10.10.12: bytes=32 time=16ms TTL=127
Reply from 10.10.10.12: bytes=32 time=1ms TTL=127

Ping statistics for 10.10.10.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 16ms, Average = 4ms

C:\>
```

รูปภาพ การ ping ไปยัง NTP Log Server , DNS Server และ www.ntplog.com

อ้างอิง

<https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbngxudW50YXd1dHJtMmt8Z3g6MjZhZTliZmZmOWZhOGUyOQ>

<https://saixiii.com/what-is-ntp/>

<http://angсила.cs.buu.ac.th/~57660132/files/591/887370/887370-59-Week-09.pdf>

<https://www.bloggang.com/mainblog.php?id=likecisco&month=13-09-2014&group=3&gblog=21>

<http://googleapps.gict.co.th/email-hosting/google-apps/bangkok/service-logfile/TH>

<https://www.youtube.com/watch?v=DtFU-43mkZU>