# บทที่ 23

## Lab Extended ACL

นายพรหมาสตร์ นามโคตร ( Mr.Mast ) เรียบเรียง

**Access list แบบ Extended** คือการกรอง packet ที่จะเข้า ออก Routerโดยที่สนใจทุกอย่าง ต้นทางคือ IP Address ใดปลายทางคือ IP Address ใด ไปใช้งานที่ไหน Application ( protocol, port number ) ใด เป็นแบบที่มีความสามารถอนุญาตหรือไม่อนุญาต packet โดยระบุโปรโตคอลและพอร์ตได้ ตัวเลขที่ใช้ในการระบุ Accesslist แบบ Extended นี้คือ 100-199 นั่นเอง

**Lab 1.** ที่ Router R1 ห้าม Network วง 192.168.2.0/24 Telnet เข้ามาที่ IP 10.10.10.1 นอกนั้นอนุญาตทั้งหมด

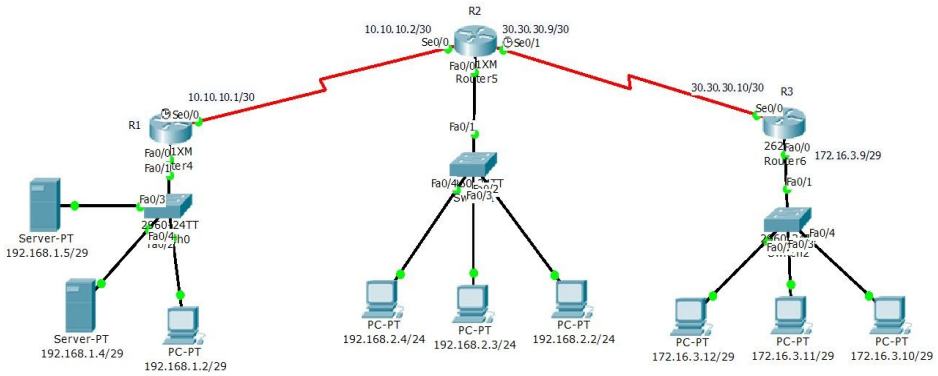
**Lab 2.** ห้าม Network วง 172.16.3.8 / 29 เข้าWebsite 192.168.1.5 อย่างเดียวแต่อนุญาต ให้ใช้ Website อื่นๆ ได้ทุกwebsite (tcp/80,433) อนุญาตให้ใช้ DNS ( tcp,udp /53) , Ftp ( tcp /21) ,Telnet ( tcp /23) Mail ( tcp /25,110,143) และ Ping (icmp) เท่านั้น

**รูปแบบ Config Extended access list (100-199)**

1. Router(config)#access-list (access number) (permit,deny) (protocol tcp,udp,icmp) SA wildcard DA wildcard Eq,Neq,It,gt port number

2. Router(config-if)#ip access-group { number access | name in | out }

**ให้วาดภาพดังนี้**




Config ให้ PC และ Server ทุกเครื่องสามารถติดต่อกันได้

**เฉลย LAB Extended ACL**

**Lab 1.**

การ config มี 2 ขั้นตอน

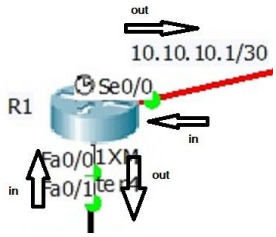
ขั้นตอนที่1 คือการประกาศ ACL จากโจทย์สามารถ config ได้ดังนี้

R1(Config)#access-list 101 deny tcp 192.168.2.0 0.0.0.255 10.10.10.2 0.0.0.0 eq 23

ห้าม network วง 192.168.2.0/24 telnet มาที่IP10.10.10.2

R1(config)# access-list 101 permit ip any any นอกนั้นอนุญาตทุกอย่าง ( ต้องมีบรรทัดนี้ปิดท้ายเพื่ออนุญาตให้เงื่อนไขอื่น ที่ไม่ตรงกับด้านบนสามารถผ่านได้ เนื่องจากจะมีบรรทัดaccess-list 101 deny ip any any ซ่อนอยู่ การจัดเรียงบรรทัดต้องเรียงให้ถูกต้องเพราะACL จะอ่าน config จากบนลงล่าง )

ขั้นตอนที่2 คือการ enable ACL ที่ interface ให้ดูที่ Source IP ว่าวิ่งเข้าRouter หรือ วิ่งออกจากRouter โดย packet ที่เข้าRouter จะเป็น in และ packet ที่ออกจาก Router จะเป็น out




จากโจทย์ IP ที่สนใจ คือ IP วง **192.168.2.0/24** อยู่ทางขวามือของRouter R1 ดังนั้นถ้าทำการon ACL ที่ interface s0/0 จะเป็น in เพราะ packet วิ่งเข้าRouter R1

R1(config)#interface s0/0

R1(config-if)#ip access-group 1 in

เมื่อ show config ดู จะต้องเป็นดังนี้

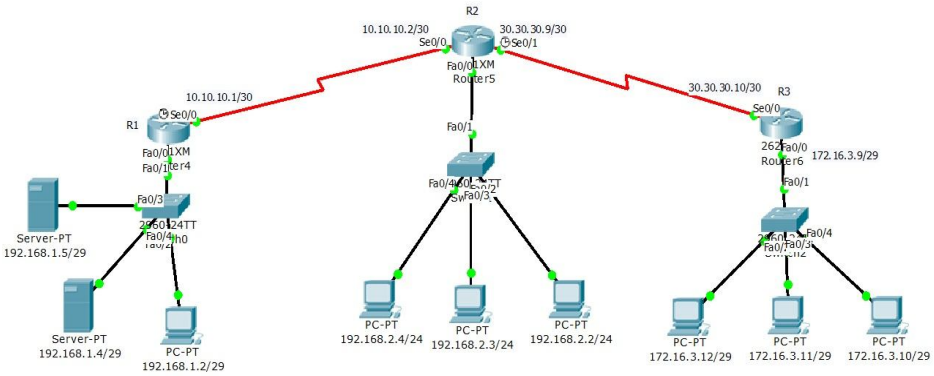
R1#show running-config

interface Serial0/0

ip access-group 1 in

**Lab 2.**

จากโจทย์ ควรConfig ที่ Router R3 ดังนี้




## ขั้นตอนการสร้างกฎต่างๆตามโจทย์

R3(config)# access-list 101 deny tcp 172.16.3.8 0.0.0.7 host 192.168.1.5 eq 80

R3(config)# access-list 101 permit tcp 172.16.3.8 0.0.0.7 any eq 80

R3(config)# access-list 101 permit tcp 172.16.3.8 0.0.0.7 any eq 443

R3(config)# access-list 101 permit tcp 172.16.3.8 0.0.0.7 any eq 53

R3(config)# access-list 101 permit udp 172.16.3.8 0.0.0.7 any eq 53

R3(config)# access-list 101 permit tcp 172.16.3.8 0.0.0.7 any eq 21

R3(config)# access-list 101 permit tcp 172.16.3.8 0.0.0.7 any eq 23

R3(config)# access-list 101 permit tcp 172.16.3.8 0.0.0.7 any eq 25

R3(config)# access-list 101 permit tcp  172.16.3.8  0.0.0.7  any  eq 110

R3(config)# access-list 101 permit tcp  172.16.3.8  0.0.0.7  any  eq 143

R3(config)# access-list 101 permit icmp 172.16.3.8 0.0.0.7 any

ขั้นตอนที่2 คือการ enable ACL ที่ interface ให้ดูที่ Source IP ว่าวิ่งเข้าRouter หรือ วิ่งออกจาก Router โดย packet ที่เข้า Router จะเป็น in และ packet ที่ออกจาก Router จะเป็น out

**ขั้นตอนการ enable ACL ที่ interface**

R3(config)#interface Serial0/0

R3(config-if)#ip access-group 101 **out**

ลองดูนะครับเป็นตัวอย่างในการอนุญาตให้ใช้งานแค่บางอย่างเท่านั้น

หวังว่าบทความนี้คงจะก่อให้เกิดประโยชน์ไม่มากก็น้อยสำหรับผู้ที่ทำงานอยู่กับอุปกรณ์Cisco นะครับ

**สนับสนุนโดย** http://www.jodoi.com