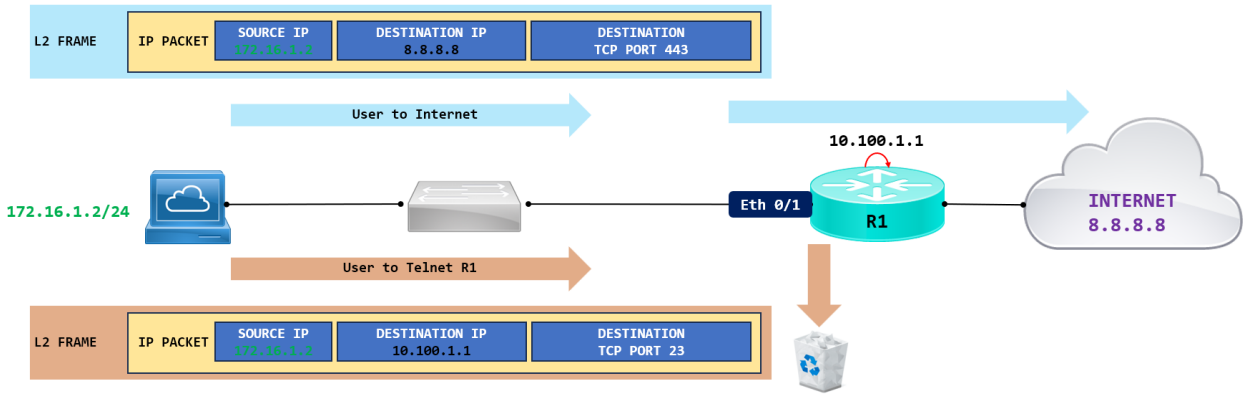
Access Control List ตอนที่ 1

Access Control List หรือ ACL เป็นอีกหนึ่งเครื่องมือที่ช่วยจัดการควบคุมการเข้าถึง Traffic ประเภทต่างๆ ได้ เช่น ต้องการไม่ให้ User ที่อยู่ในเครือข่าย 172.16.1.0/24 สามารถ Telnet หรือ SSH (Secure Shell) เข้าสู่อุปกรณ์เครือข่ายได้ แต่ต้องการให้ใช้งาน Internet ได้ ก็สามารถนำ ACL มาประยุกต์ใช้งานได้



อาจจะมองได้ว่า ACL เป็นการกรอง (Filtering) ก็ได้ ถ้าหากเป็นกลุ่มที่สนใจ หรือ Match เช่น จากตัวอย่างสนใจ User ที่อยู่ในเครือข่าย 172.16.1.0/24 แล้วจะให้ทำอะไรกับกลุ่มนี้บ้าง ถ้าหากเข้าเงื่อนไขที่ไม่อนุญาตก็อาจจะ Drop Packet นั้นทิ้งไป หรือถ้าเข้าเงื่อนไขที่อนุญาตให้ผ่าน ก็สามารถใช้งานได้ จากตัวอย่างด้านบนจะเห็นว่า User ที่มี IP 172.16.1.2 ไม่สามารถ Telnet เข้า Router R1 แต่สามารถใช้งาน Internet ได้

นอกเหนือจากการกรองแล้วเราสามารถใช้ ACL แยกแยะกลุ่ม Traffic ด้วย (Classification) เช่น ถ้าหากเป็นกลุ่มที่สนใจ หรือ Match ก็อาจจะอนุญาตหรือไม่อนุญาตให้ใช้งานระบบ VPN (Virtual Private Network) ได้

การนำ ACL มาประยุกต์งาน เช่น

- การทำ QoS (Quality of Service) หรือคุณภาพการให้บริการ
- นำไปใช้ร่วมกับ Routing Protocol เช่น การทำ Route Map, การ Redistribute ระหว่าง Routing Protocol
- การนำไปใช้ร่วมกับ NAT (Network Address Translation) เพื่อให้ IP Private ภายในองค์กรเปลี่ยนเป็น IP Public ที่กำหนดไว้ได้

ประเภทของ ACL

ACL สามารถแบ่งออกได้เป็นหลักๆ 2 รูปแบบ คือ Standard และ Extended

ACL TYPE	NUMBER / IDENTIFICATION	
NUMBER	STANDARD	1-99 OR 1300-1999
	EXTENDED	100-199 OR 2000-2699
NAMED	STANDARD AND EXTENDED	NAME

Standard ACL

ควบคุมการเข้าถึงโดยที่จะตรวจสอบเฉพาะแค่ Source Address เท่านั้น และไม่สามารถกำหนดเงื่อนไขอย่างอื่นได้เลย เช่น IP ของปลายทาง หมายเลขที่ใช้สำหรับระบุเป็น ACL แบบ Standard มี 2 ช่วง คือ 1-99 และ 1300-1999

Extended ACL

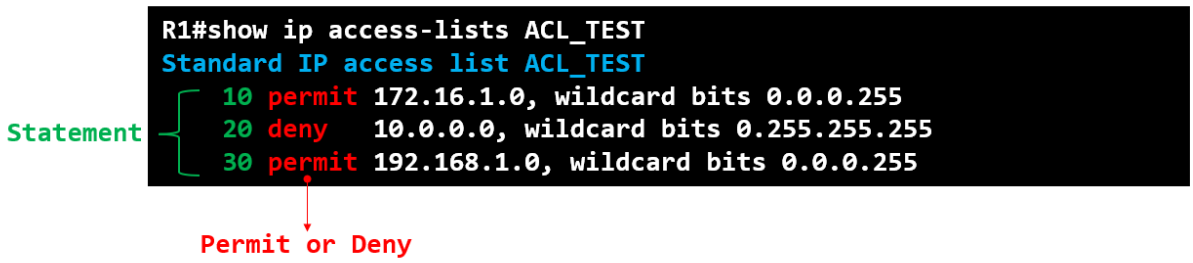
มีความยืดหยุ่นกว่าแบบ Standard โดยที่สามารถระบุได้ทั้ง IP ทั้งต้นทางและปลายทางที่ต้องการได้ อีกทั้งยังระบุ Protocol อย่างเช่น TCP/UDP ICMP OSPF เป็นต้น รวมถึงหมายเลข TCP/UDP Port Number ยกตัวอย่างเช่น ถ้าไม่ต้องการให้ใช้งาน Telnet เข้าอุปกรณ์ ก็จะทำการ Block TCP Port 23 กับกลุ่ม IP ที่ไม่อนุญาตให้ใช้งาน หมายเลขที่ใช้สำหรับระบุเป็น ACL แบบ Extended มี 2 ช่วงเช่นกัน คือ 100-199 และ 2000-2699

Name ACL

นอกเหนือจากใช้หมายเลขในการแบ่งแยกประเภทของ ACL แล้ว เรายังสามารถเขียน ACL ในอีกรูปแบบหนึ่งคือ Name Access List ซึ่งใช้ชื่อแทนการใช้ตัวเลขเพื่อแบ่งแยกว่า ACL เบอร์ไหนเป็น ACL แบบ Standard หรือ Extended ทำให้จดจำได้ง่ายกว่าการใช้ตัวเลข

```
R1#show ip access-lists ACL_TEST --> [NAME ACL]
Standard IP access list ACL_TEST
    10 permit 172.16.1.0, wildcard bits 0.0.0.255
    20 deny   10.0.0.0, wildcard bits 0.255.255.255
    30 permit 192.168.1.0, wildcard bits 0.0.0.255
```

ACL Operation



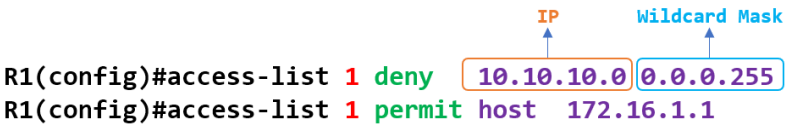
จากรูปด้านบนเป็นส่วนประกอบของ ACL แบบ Name ACL แบบ Standard โดยใช้ชื่อ ACL_TEST โดยใน 1 ALC อาจจะมีหลาย Statement ก็ได้ ในตัวอย่างมี 3 Statement คือ 10, 20 และ 30 ซึ่งแต่ละ Statement ก็จะมีเงื่อนไขแตกต่างกัน เช่น Statement ที่ 10 Permit คือ อนุญาตให้ IP 172.16.1.0/24 ผ่านได้ ใน Statement ที่ 20 Deny ไม่อนุญาตให้ IP 10.0.0.0/8 ผ่านได้ และการพิจารณาเงื่อนไขของ ACL ก็จะทำจากบนลงล่างเสมอ ถ้าหากมี Packet ที่เข้าเงื่อนไขใน Statement ที่ 10 แล้ว จะไม่นำ Packet นั้นมาพิจารณากับ Statement ที่เหลืออยู่ในบรรทัดด้านล่างอีกต่อไป แต่ถ้าหากไม่เข้าเงื่อนไขของ Statement ใดๆ เลย ก็จะไม่อนุญาตให้ Packet นั้นผ่านได้ เพราะโดย Default ของ ACL จะเป็น “implicit deny” ซึ่งจะไม่แสดงอยู่ใน Configuration ของ Router

ACL Configuration

การตั้งค่าการใช้งานของ ACL จะมีรูปแบบของคำสั่งหรือ Command Line ดังนี้

- Standard ACL ใช้หมายเลข 1-99 และ 1300-1999 เพื่อเป็นการกำหนดเป็น Standard ACL สำหรับ Standard ACL มีรูปแบบคำสั่งตามที่ได้แสดงด้านล่าง

```
R1(config)#access-list [1-99 or 1300-1999] [permit/deny] [Source-IP]
```



ในตัวอย่างคำสั่งของ ACL แบบ Standard จะเลือกระบุได้เฉพาะ Source IP เท่านั้น โดยสามารถระบุ Source IP เป็นกลุ่มที่สนใจได้ โดยใช้ Wildcard Mask เข้ามาเกี่ยวข้อง หรือระบุเฉพาะ IP ที่สนใจก็ได้ จากตัวอย่างคำสั่งด้านบนจะหมายความว่า ACL Standard หมายเลข 1

- ไม่อนุญาตให้ Packet ต้นทางที่มี Source IP ในช่วง 10.10.10.0-255 ผ่านได้ (เพราะ Wildcard Mask มีค่าเป็น 0.0.0.255)

- อนุญาตให้ Packet ที่มี Source IP 172.16.1.1 เท่านั้นผ่านได้

- Extended ACL ได้ใช้หมายเลข 100-199 และ 2000-2699 เพื่อเป็นการระบุว่าเป็นการใช้งาน Extended ACL สำหรับ Extended ACL มีรูปแบบคำสั่งตามที่ได้แสดงด้านล่าง

```
R1(config)#access-list [100-199 or 2000-2699] [permit/deny] [Protocol] [Source-IP] [Source Port Number] [Destination IP] [Destination Port]
R1(config)#access-list 100 deny tcp 10.10.10.0 0.0.0.255 host 192.168.1.1 eq 23
```

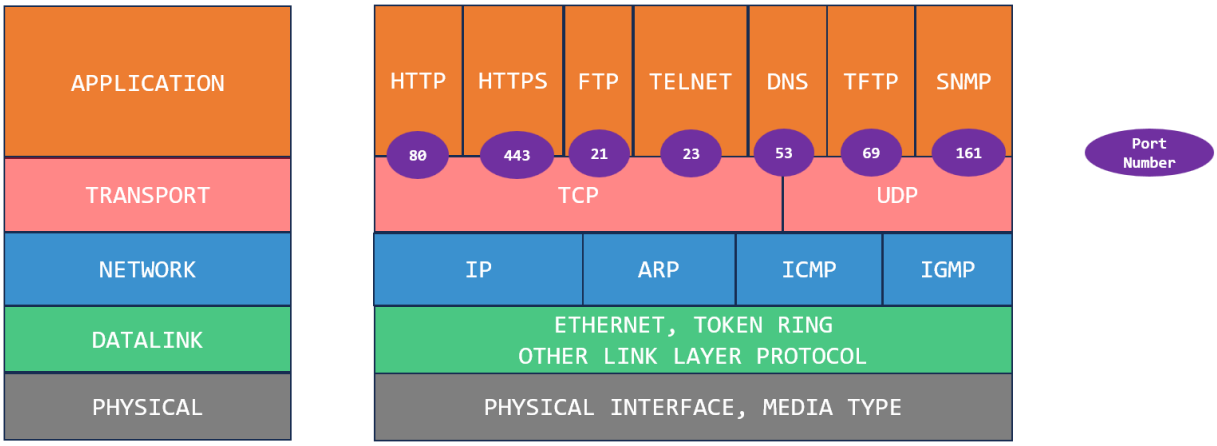
จากตัวอย่างคำสั่ง ACL แบบ Extended ด้านบน สามารถแปลความได้ว่า ACL Extended หมายเลข 100

- ไม่อนุญาตให้ IP ต้นทางที่อยู่ในกลุ่ม 10.10.10.0-255 ไปยัง IP 192.168.1.1 ด้วยการ Telnet ได้

จะเห็นได้ว่า Extended ACL จะมีความยืดหยุ่นมากขึ้นโดยที่สามารถเลือก Protocol ได้ เช่น OSPF, EIGRP, ARP, ICMP รวมไปถึง TCP/UDP ในรูปด้านล่างจะแสดง Protocol ที่สามารถเลือกใช้งานได้

```
R1(config)#access-list 100 deny ?
  <0-255>       An IP protocol number
  ahp           Authentication Header Protocol
  eigrp         Cisco's EIGRP routing protocol
  esp           Encapsulation Security Payload
  gre           Cisco's GRE tunneling
  icmp          Internet Control Message Protocol
  igmp          Internet Gateway Message Protocol
  ip            Any Internet Protocol
  ipinip        IP in IP tunneling
  nos           KA9Q NOS compatible IP over IP tunneling
  object-group  Service object group
  ospf          OSPF routing protocol
  pcp           Payload Compression Protocol
  pim           Protocol Independent Multicast
  sctp          Stream Control Transmission Protocol
  tcp           Transmission Control Protocol
  udp           User Datagram Protocol
```

สำหรับ Protocol TCP/UDP ทำงานอยู่บน Transport Layer จะมีหมายเลข Port ที่คอยกำกับไว้เพื่อรองรับ Application ที่ต้องการใช้งาน ดังเช่นรูปด้านล่าง



- Name ACL จะเป็นการตั้งชื่อของ ACL แทนที่จะใช้หมายเลขเพื่อระบุว่าเป็น ACL ประเภทใด ซึ่งสามารถจดจำได้ง่ายกว่า รูปแบบคำสั่งแสดงในตัวอย่างด้านล่าง

```
R1(config)#ip access-list [Standard ACL or Extended ACL] [Name]
R1(config-std-nacl)#[Sequence Number] [Permit/Deny] [Source-IP]
```

```
R1(config)#ip access-list standard ACL_STD
R1(config-std-nacl)#10 deny 10.10.10.0 0.0.0.255
```

เห็นได้ว่า Configuration ของ ACL แบบ Name จะค่อนข้างดูเป็นระเบียบและดูได้ง่ายกว่าแบบ Number

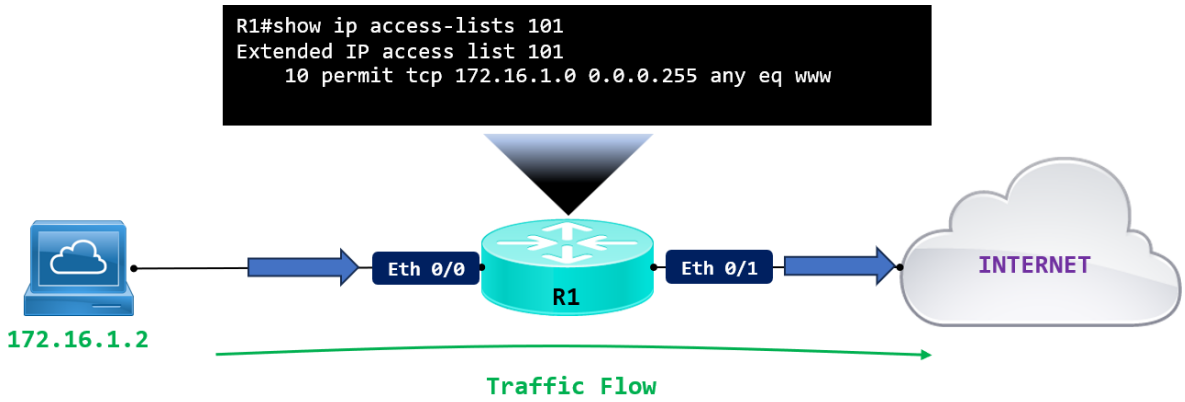
```
R1#show running-config
ip access-list standard ACL_NAME
 permit 10.10.10.0 0.0.0.255

R1#show ip access-lists ACL_NAME
Standard IP access list ACL_NAME
    10 permit 10.10.10.0, wildcard bits 0.0.0.255
```

การ Apply บน Interface

การนำ ACL ไปใช้งานบน Interface จะพิจารณาตามทิศทางเข้า-ออกของ Packet ตัวอย่างตามรูปที่ได้แสดงด้านล่าง ถ้าหาก User ต้องการใช้งาน Internet ทิศทางของการส่งข้อมูล IP Packet จะออกจากเครื่อง User แล้วเข้า Interface Eth0/0 หรือ Inbound และออกที่ Interface Eth0/1 หรือ Outbound เพื่อไปยัง Internet

ถ้าหากได้มีการสร้าง ACL เพื่อที่จะให้ผู้ใช้งานที่อยู่ใน Network 172.16.1.0/24 สามารถออก Internet ได้ จะเห็นได้ว่าสามารถนำ ACL นี้ไปใช้ได้ 2 จุด คือ Interface Eth0/0 โดยระบุทิศทางเป็น Inbound หรือที่ Interface Eth0/1 ก็ได้ โดยระบุทิศทางเป็น Outbound



หลังจากทำการสร้าง ACL แล้ว ในลำดับถัดไปจะต้องนำ ACL ไปผูกกับ Interface เพื่อควบคุมหรือ Filter Traffic ที่เราต้องการ สำหรับคำสั่งที่นำ ACL ไปใช้บน Interface จะมีรูปแบบของคำสั่งตามที่ได้ในรูปแสดงด้านล่าง และการ Config ภายใต้ Interface

```
R1(config-if)#ip access-group [ACL] [in/out]
```