Network

มาตราฐานของ Network มี 2 ประเภท

1. OSI มีทั้งหมด 7 Layer กำหนดโดย ISO, De ju re (มาตราฐานมีการตั้งหน่วยงาน หรือองค์กรมากำหนดมาตราฐาน เช่น ISO, ANSI, มอก.)

ข้อเสีย

- Implement ยาก

- ทำงานช้า

2. TCP/IP มี 5 Layer ออกมาเพื่ออธิบายการทำงานของ TCP และ IP เหมาะกับการอธิบายการทำงานของ Internet

   กำหนดโดย De facto (เช่น Window, EBCDIC, IOS, Android)

TCP/IP

1. Physical Link Layer

เพื่อให้การส่ง และรับข้อมูลได้ถูกต้อง ต้องมีการกำหนด Clock (สัญญาณนาฬิกา) และกำหนดขนาดสัญญาณ

Media

- ไร้สาย (คลื่นวิทยุ, ไมโครเวฟ)

- มีสาย (fiber optic)

Header จะมีการใส่ Clock ไปด้วย

Network

2. Data Link Layer

ควบคุมการส่งข้อมูลผ่าน Data Link ให้มีประสิทธิภาพ และถูกต้อง

การตรวจสอบ

- Error Detection ตรวจสอบว่ามี Error หรือไม่

    โดยการติด Parity Bit (Bit ตรวจสอบ) ไปทีข้อมูล โดยวิธีการดูคือดูจาก Bit ทีเป็น 1

1. Even

    Ex. 1 1 0 1 0 1 0 1 0 1 => ต้องเติม 0 เป็น Parity Bit เนืองจากต้องทำให้มี 1 รวมกันเป็นคู่

Before	After
1 1 0 1 0 1 0 1 0 1	1 1 0 1 0 1 0 1 0 1 **0**
1 1 0 1 0 1 0 0 0 1	1 1 0 1 0 1 0 0 0 1 **1**

2. Odd

    Ex. 1 1 0 1 0 1 0 1 0 1 => ต้องเติม 1 เป็น Parity Bit เนืองจากต้องทำให้มี 1 รวมกัน เป็นคี

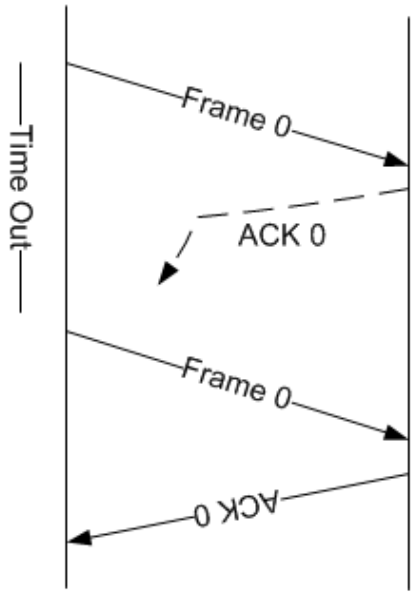
Before	After
1 1 0 1 0 1 0 1 0 1	1 1 0 1 0 1 0 1 0 1 **1**
1 1 0 1 0 1 0 0 0 1	1 1 0 1 0 1 0 0 0 1 **0**

- ** Parity Bit จะถูกใส่เข้าไปในตอนส่งข้อมูลผ่าน Data Link Layer ที **Trailer**

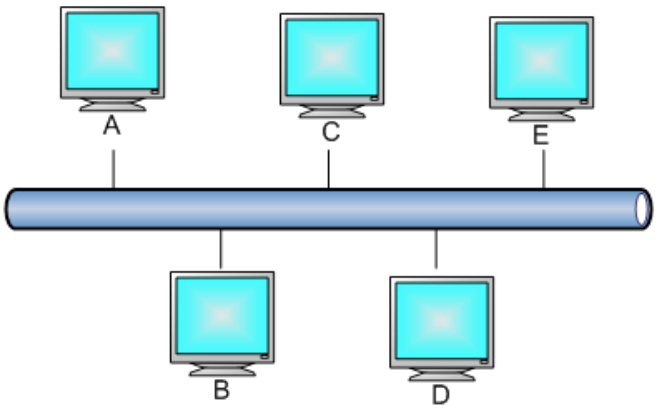
Network

- Error Correction หากเกิด Error ต้องแก้ Error ให้ได้

Flow Control โดยการใส่ Seq.Number เข้าไปใน **Header**



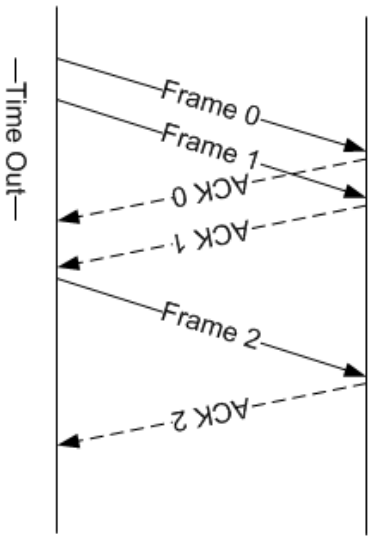
Access Control



หาก A กับ B ส่งข้อมูลพร้อมกันจะเกิดการชนกัน จึงต้องมีการควบคุมการส่งข้อมูล เรียกว่า “Access Control” โดยการส่งข้อมูลในชั้นนี้จะส่ง MAC (Media Access Control 48 bit) เป็น **Header** เขาไปด้วย

การควบคุมการส่งข้อมูลให้มีประสิทธิภาพ

Ex. การส่งข้อมูลผ่านดาวเทียม



ตอนส่งข้อมูลใช้เวลาแค่นิดเดียว แต่ตอนรอ ACK ตอนกลับจะใช้เวลานาน จึงเกิดการสูญเสีย ดังน้นจึงต้องมีการสร้าง Protocol ขึนมาให้ฝั่งส่งทำการส่งข้อมูเลย แต่การควบคุมจะยากกว่า (Full Duplex)

3. Internet Layer

4. Transport Layer

DHCP

หน้าทีหลักๆของ DHCP (Dynamic Host Configuration Protocol)

คือคอยจัดการ แจกจ่ายเลขหมาย IP และ configuration ต่างๆ เช่น Default Router ให้กับลูกข่ายทีมาเชือมต่อกับแม่ข่าย ไม่ให้หมายเลขไอพีของลูกข่ายมีการซ้ำกันอย่างเด็ดขาด อาทิ เครืองคอมพิวเตอร์ตัวหนึงได้ทำการเชือมต่อกับ DHCP Server เครืองเซฟเวอร์ก็จะให้ หมายเลขไอพีกับเครืองคอมพิวเตอร์ทีมาทำการต่อเชือมแบบอัตโนมัติ ซึงไม่ว่าจะมีเครืองคอมพิวเตอร์เชือมต่อมากเท่าไร DHCP Server ก็จะออกเลยหมายไอพีให้คอมพิวเตอร์แต่ละเครืองไม่ซ้ากันทำให้เครือข่ายนัน ไม่เกิดปัญหาในการใช้งาน

Network

DHCP Server มีหลักการในการจ่ายหมายเลขไอพีให้กับลูกข่ายอยู่ 3 วิธีด้วยกันคือ

1. กำหนดด้วยตัวเอง ซึ่งผู้ควบคุมดูแลสามารถทีจะกำหนดไอพีให้กับเครื่องลูกข่ายได้ด้วยตัวเองโดยใช้วิธีเทียบกับหมายเลข MAC
2. แบบอัตโนมัติ DHCP Server จะจ่ายหมายเลขไอพีให้กับเครื่องลูกข่ายแบบอัตโนมัติไม่ซ้ากัน แต่จะออกหมายเลขไอพีตามช่วงของหมายเลขไอพีทีผู้ควบคุมดูแลกำหนดไว้ให้ วิธีนีหมายเลขไอพีจะติดอยู่กับเครื่องลูกข่ายอย่างถาวร เช่นเมือเครื่องลูกข่ายทีเคยได้หมายเขไอพีจากวิธีนีไปแล้วเมือกลับมา เชือมต่อใหม่อีกครัง ก็จะได้หมายเลขไอพีเดิมไปใช้งานนันเอง
3. แบบไดนามิก มีหลักการทำงานเหมือนกับแบบอัตโนมัติแต่แตกต่างอยู่ทีหมายเลขไอพีทีออก ด้วยวิธีไดดามิกจะไม่ถาวร เมือเครื่องลูกข่ายได้หมายเลขไอพีจากวิธีไปแล้ว เมือมีการออกจากระบบแล้วเข้ามาเชือมต่อกับเครือข่ายในภายหลังหมายเลขไอพี ทีได้จะได้เป็นหมายเลขไอพีใหม่เลย

ประโยชน์ของ DHCP มีอะไรบ้าง

ประโยชน์ของ DHCP นันจะช่วยในเรืองระบบการจัดการเครือข่ายเป็นส่วนสำคัญ โดยมีการบริหารและจัดการระบบหมายเลขไอพีทีไม่ซ้ากันไม่ว่าจะมีเครืองลูก ข่ายมากขนาดไหนก็ตาม เพราะถ้าไม่มี DHCP เข้ามาช่วยในเรืองนี การจัดแจงและจ่ายหมายเลขไอพีจะเป็นเรืองยากถ้าเครือข่ายนันเป็นเครือข่าย ทีมีขนาดใหญ่ DHCP เป็นโพรโทคอลทีนิยมใช้ในโครงข่ายอินเตอร์เน็ต และโครงข่ายขนาดใหญ่ทีมีลูกข่ายเข้ามาทำการเชือมต่อกับ Server อยู่ตลอดเวลา และ DHCP ยังช่วยให้ไม่ต้องเสียเวลาในการกำหนดค่าต่างๆ ให้กับเครืองลูกข่าย เพราะว่า DHCP จะทำการการตังค่าระบบ เครือข่ายแบบอัตโนมัตินันเอง

NAT (Network Address Translation)

แบ่งเป็น 2 ประเภท

1. Static NAT

Static NAT เป็นการแปล ไอพีแอดเดรส ชนิดกำหนดค่า แอดเดรส ตายตัว จากเครือข่ายภายใน ไปยังเครือข่ายภายนอก ส่วน แอดเดรส ภายนอกจะไม่มีการเปลียนแปลง ดังนัน ความสัมพันธ์ระหว่าง ไอพีแอดเดรส ของ เครือข่ายภายนอกและภายในจะเป็นแบบแน่นอนตายตัว

2. Dynamic NAT

Network

เป็นแบบตรงกันข้าม ทีมีการนำเอา ไอพีแอดเดรส จาก กลุ่มของ ไอพีแอดเดรส ทีแชร์หรือร่วมใช้งานกัน หรือทีเรียกว่า แอดเดรส Pool มาทำการแปล จาก แอดเดรส Pool ภายใน ให้เป็น Address Pool สำหรับเครือข่ายภายนอก หรือในทางกลับกัน รูปแบบนีจะต้องได้รับการจัด Configure โดยผู้ดูแลระบบเครือข่าย แต่หลังจากทีจัด Configure เป็นทีเรียบร้อยแล้ว Routerทีสนับสนุน NAT จะเป็นผู้จ่าย ไอพีแอดเดรส ให้กับคอมพิวเตอร์อย่างเหมาะสม และเพือให้เกิดความรวดเร็วในการทำงาน ผู้บริหารจัดการเครือข่ายจะต้อง ทำการ Map ระยะของ ไอพีแอดเดรส หากเป็นไปได้ (ลักษณะนี คล้ายๆกับการทำงานของ DHCP Server ทีไม่ได้กำหนดเครือง PC แต่ละเครืองให้มี ไอพีแอดเดรส ทีตายตัว โดยผู้จัดการเครือข่าย จะกำหนด แอดเดรส ขึนมาจำนวนหนึง เป็นระยะหรือช่วงของ แอดเดรส เช่น 192.80.20.15 - 192.80.20.50 เป็นต้น ดังนันใครทีเข้ามาทีเครือข่ายก่อน ก็จะได้รับแจก แอดเดรส ไปใช้งานก่อน โดยเครืองคอมพิวเตอร์ จะไม่ได้รับ IP ทีซ้ากัน ข้อแตกต่างกันระหว่าง NAT กับ DHCP Server ตรงที ไอพีแอดเดรสของ NAT เป็น ไอพีแอดเดรส ทีได้รับการจดทะเบียนแล้ว เพือแจกให้กับเครืองคอมพิวเตอร์ทีเข้าๆออกบนเครือข่าย ไปยังภายนอก

หน้าทีของ NAT

แปลงจาก Private IP (IP ทีใช้ในองค์กร ex. 192.168.10.1) ไปเป็น Public IP ทีภายนอกรู้จัก

Network

ข้อดี

1. เพื่อเพิม IP Address ให้สามารถมี Address ใช้งานได้มากขึน
2. Security เพิมมากขึนเนืองจากเป็น IP Address ภายใน ภายนอกจะไม่รู้ทำให้เข้าถึงได้ยาก

ข้อเสีย

เส้นทางการสือสารกับโลกภายนอก อย่าง เช่น อินเทอร์เนต จะต้องเกิด ช่วงหน่วงเวลา หรือทีเรียกว่า Delay เนืองจากทุกๆ แอดเดรส ภายในเครือข่ายขององค์กร จะต้องได้รับการแปลงให้เป็น ไอพีแอดเดรส อย่างถูกต้องเสียก่อน หากมีการติดต่อกับอินเทอร์เนต ทีเดียวพร้อมๆกัน หลายๆเครือง ก็อาจเกิดปัญหาติดขัดได้ แม้จะไม่มากนักก็ตาม

** 1 Public Address จะมีได้ ~ 60 K Address โดยจะขึนอยู่กับ OS เช่น Window ได้ ~ 4000 Address

DNS

แบ่งเป็น 2 ประเภท

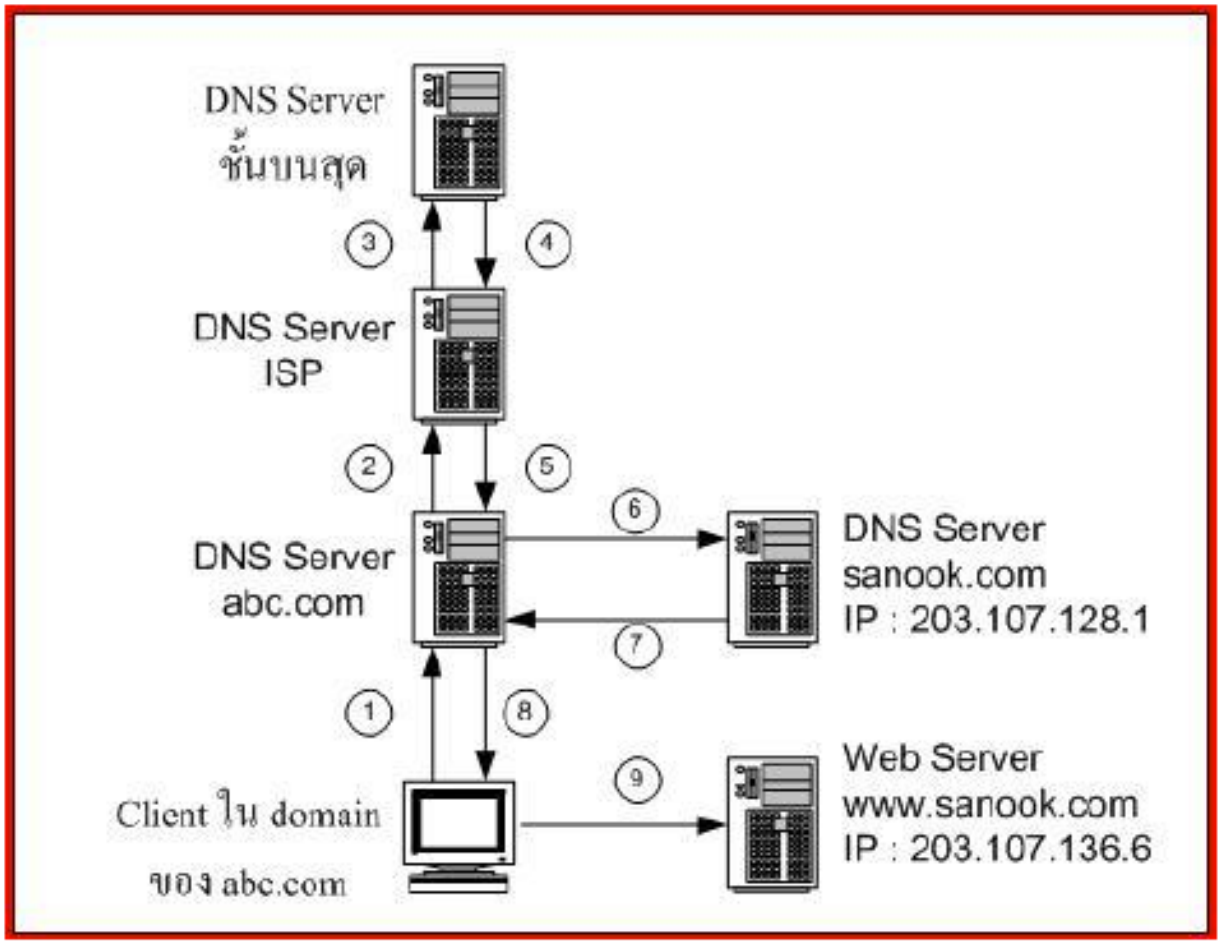
1. Generic (.com ,.org)

2. Countries (.th, .jp)

มีหน้าที ในการแปลงค่า Domain Name เป็นค่า IP Addresss

Network

วิธีการทำงาน



สมมติว่ามีเครื่อง Client เครื่องหนึ่งใน บริษัทของ abc.com ต้องการจะเข้าไปดู ข้อมูลใน Website ที www.sanook.com ขั้นตอนที่เกิดขึ้น ระหว่างผู้ใช้ทำการพิมพ์ http://www.sanook.comแล้วกด Enter จนถึงได้เห็นข้อมูล Website ที ต้องการปรากฏขึ้นนั้น กลไกจะเป็นดังนี เครื่อง Clientจะส่งคำสั่งขอข้อมูล หมายเลข IP Address ของ www.sanook.comไปที DNS Server ที่ดูแลโซนของ Client นีซึ่งก็คือ abc.com

(ขั้นตอน ที 1) สมมติว่า DNS Server นีไม่มีข้อมูลมันจะทำการส่งคำสั่งขอข้อมูลต่อไปยัง DNS Server ของ ISP

(ขั้นตอนที 2) เครื่อง DNS Server ของ ISP ได้รับคำสั่งแล้วทำการค้นหาข้อมูล IP Address ที่ต้องการแต่สมมติว่าไม่พบข้อมูลมันจึงทำการส่งคำสั่งขอข้อมูลไปยัง DNS Server ระดับสูงขึ้นไปอีก

(ขั้นตอนที 3) DNS Server ระดับบนสุดได้รับการร้องขอก็จะทำการหาข้อมูลให้ แต่ก็ยังไม่สามารถจะตอบค่า IP Address กลับมาให้ได้เพราะไม่มีข้อมูล แต่รู้ว่า DNS Server ของ www.sanook.comอยู่ที IP อะไร จึงให้ข้อมูล IP

Address 203.107.128.1 กลับมายัง DNS Server ของ ISP

(ขันตอนที 4) และส่งผ่านต่อมายัง DNS Server ของ abc.com

(ขันตอนที 5) DNS ของ abc.com จึงถามหา IP Address ไปที DNS ของ Sanook.com

(ขันตอนที 6) แล้วได้คำตอบ กลับมาว่า IP ของ www.sanook.com นีคือ 203.107.136.6

(ขันตอนที 7) จากนัน DNS abc.com ก็บอกไปยังเครือง Client ว่า IP เป็นอะไรข้างต้น

(ขันตอนที 8) ถึงขันตอนนี Client จะรู้แล้วว่า www.sanook.com นันมี IP Address เท่ากับ203.107.136.6 มันจึงร้องขอข้อมูลไปยัง IP Address นี

(ขันตอนที 9) แล้วก็ได้เห็นข้อมูลดังปรากฏในจอ จากขันตอนทีกล่าวมาทังหมดจะเห็นว่ามีการทำงานทีซับซ้อนเพือให้การใช้งานของเราง่ายขึนและนีก็ คือบทบาทของ Domain Name System ทีได้กล่าวมาแล้ว

** เมือได้ข้อมูลในรอบแรกแล้ว DNS Server ทีร้องขอ และเครือง Client จะจับเก็บลงในแคชเพือใช้ในการเรียกในครังต่อไป