Internetworking

หัวข้อของข้อสอบ CCNA ในบทนี้มีดังนี้

เทคโนโลยี

- การอธิบายการสื่อสารของ network โดยใช้ตัวอย่างเป็นขั้น ๆ
- การเปรียบเทียบความเหมือนและความแตกต่างของลักษณะหลักของสภาพแวดล้อมของ LAN
- การอธิบายส่วนประกอบของหลักการของ network
- การประเมินกฎสำหรับการควบคุม packet

ขอต้อนรับเข้าสู่ความน่าตื่นตาตื่นใจของโลก network นี่เป็นบทแรกที่จะช่วยให้เข้าใจการทำงานเบื้องต้นของ internetwork โดยเน้นไปที่วิธีการเชื่อมโยงของ network เข้าด้วย routers ต่าง ๆ ของCisco และ switches ก่อนอื่นคุณต้องรู้ก่อนว่าแท้จริงแล้ว network คืออะไร คุณสามารถสร้างการทำงานของ network ได้โดยการเชื่อม LANs หรือ WANs เข้าด้วยกันและเชื่อมต่อ LANs และ WANs ด้วย routers และจัดตั้งหมายเลขของเครือข่ายของ network ด้วยหลักการของ protocol อย่างเช่น IP

ในบทนี้จะกล่าวถึง 4 เรื่องดังต่อไปนี้

- การทำงานเบื้องต้นของ internetwork
- การแบ่งส่วนของ network
- Bridges, switches และ routers ต่าง ๆ จะถูกใช้งานในลักษณะงานของการแบ่งเน็ตเวิร์คอย่างไร
- routers ต่าง ๆ ถูกใช้เพื่อสร้าง internetwork อย่างไร

เรากำลังจะแบ่งแยก โครงสร้างของมาตรฐานที่เรียกว่า Open Systems Interconnection (OSI) และอธิบายแต่ละส่วนให้ผู้อ่านอย่างละเอียด เนื่องจากว่าผู้อ่านต้องนำโครงสร้างสามมิตินี้ไปสร้าง network ของผู้อ่านเองต่อไป โครงสร้าง OSI มีโครงสร้างทั้งหมด 7 ขั้นที่จะสามารถพัฒนา networks ที่แตกต่างกันได้เพื่อการติดต่อเชื่อมโยงที่มีประสิทธิภาพระหว่างระบบที่แตกต่างกัน หนังสือเล่มนี้เป็นศูนย์กลางของข้อมูลต่างๆ ของ CCNA ก็ทำให้เข้าใจโครงสร้างของ OSI อย่างลึกซึ้งอย่างที่ Cisco เล็งเห็น ดังนั้นจึงเป็นเหตุผลว่าทำไมจึงนำโครงสร้างทั้ง 7 ส่วนมาให้ผู้อ่านได้ทำความเข้าใจ

เนื่องจากมีการเฉพาะเจาะจงชนิดของอุปกรณ์มากมายเป็นประเภทต่าง ๆ ที่ใช้อยู่บน layers ต่างๆ ที่แตกต่างกันของโครงสร้างของ OSI มันเป็นส่วนสำคัญที่จะทำความเข้าใจว่าการใช้งานของสายเชื่อมต่อที่แตกต่างกันสามารถใช้งานในการเชื่อมต่อที่ใช้สำหรับ connectors เพื่อสื่อสารกันในระบบ network เราจะใช้หลักความเข้าใจของ Cisco เพื่ออธิบายวิธีการเชื่อมกับไปสู่ routers หรือ switches กับเทคโนโลยี Ethernet LAN หรือแม้กระทั่งการเชื่อมต่อ routers หรือ switches ด้วยการต่อเข้ากับ console

เราจะจบบทนี้ด้วยการอธิบายโครงสร้าง 3 ชั้นของ Cisco ที่ถูกพัฒนาโดย Cisco เพื่อช่วยให้ผู้อ่านได้ออกแบบ นำไปใช้งานได้และแก้ไข internetworks ได้

หลังจากที่อ่านจบบทนี้แล้วจะมีคำถามทบทวน 20 ข้อและ3ข้อเป็นคำถามจากการทดลองทำ ซึ่งคำถามพวกนี้จะช่วยให้ผู้อ่านได้เข้าใจเนื้อหาของบทนี้อย่างตรงตามจุดประสงค์ ดังนั้นอย่าพลาด

Internetworking Basics

ก่อนที่จะมีการลงลึกไปสู่โครงสร้างของ internetworks และการชี้เฉพาะของโครงสร้างความสัมพันธ์ของ OSI ผู้อ่านต้องเข้าใจภาพรวมและค้นหาคำตอบของคำถามหลักที่ว่า “ทำไมถึงสำคัญมากที่จะต้องเรียนรู้เรื่องการทำงานของ internetworks ของ Cisco ”

Networks และ networking ได้เติบโตอย่างทวีคูณมากกว่า 15 ปีที่ผ่านมาอย่างที่ทราบกัน Networksและ networking จะต้องค่อย ๆ ก้าวเข้าเทคโนโลยีของความเร็วแสง ตัวอย่างง่ายๆ เช่น การใช้ข้อมูลร่วมกัน และ printers ให้ดีเท่า ๆกับความความต้องการ อย่างเช่น การใช้ VDOในห้องประชุม หากไม่มีผู้ใดต้องการใช้แหล่งข้อมูลร่วมกันที่อยู่ภายในบริษัทเดียวกัน (สถานการณ์ที่ไม่ปกติที่เพิ่มขึ้น) การเรียกร้องที่ต้องเชื่อมโยงความสัมพันธ์ของข้อมูลต่าง ๆ เข้าด้วยกัน ดังนั้นผู้ใช้สามารถใช้เน็ตเวิร์คร่วมกันได้

ซึ่งมันก็เหมือนกับบางจุดที่ คุณจะต้องแตก networks ก้อนใหญ่ให้เป็นส่วนย่อยเนื่องจากว่าผู้ใช้จะสามารถค่อยซึมซับความเข้าใจ networks ทีละเล็กละน้อยซึ่งก็จะเหมือนกับการที่ networks ค่อย ๆ เติบโตอย่างช้า ๆ ที่จะเข้าสู่การความหนาแน่นของช่องการสื่อสารของ LAN การแตก networks จำนวนที่ใหญ่กว่าให้เป็นจำนวนที่เล็กลงนั้นเรียกว่า networks segmentation และมันจะสำเร็จผลได้โดยใช้ routers, switches และ bridges

สาเหตุที่เป็นไปได้ของความหนาแน่นของช่องทางการสื่อสารของ LAN

- มี host มากเกินไปใน broadcast domain
- broadcast storms (การกระจายข้อมูลที่มากเกินไป)
- Multicasting
- ช่องของ bandwidth มีขนาดต่ำ
- การเพิ่ม hubเข้าไป สำหรับการติดต่อไปยัง
- Traffic จำนวนมากของ ARP หรือ IPX ที่มีจำนวนมาก (IPX เป็น routing protocol ของ Novell เหมือนกับ IP)

routers ต่าง ๆ ถูกใช้เพื่อเชื่อมโยง networks เข้าด้วยกันและเป็นช่องทางของข้อมูลย่อยจาก networks ตัวหนึ่งไปสู่ networks อีกตัวหนึ่ง Ciscoได้กลายเป็นมาตรฐานของ routers เนื่องจาก routers มีคุณภาพสูงเป็นตัวเลือกที่ดีให้เลือก และการบริการที่น่าประทับใจ โดยปกติ routers จะป้องกัน broadcast domain ของอุปกรณ์บน networks ซึ่งจะคอยตรวจจับการส่ง broadcast

การยับยั้ง broadcast นั้นเป็นสิ่งสำคัญเนื่องจากว่าเมื่อ host หรือ server ส่งการกระจายข้อมูล networks ทุกกลไกใน networks จะต้องได้อ่านและดำเนินการการกระจายข้อมูลออกไป (ถ้าไม่เช่นนั้นคุณจะต้องมี routers) เมื่อ interface ของ routers ได้รับการกระจายข้อมูลนี้ มันจะสามารถโต้ตอบด้วยคำตอบง่ายๆด้วยคำพูดที่ว่า Thanks หรือไม่ก็ No Thanks และปฏิเสธการกระจายข้อมูลนั้นได้โดยจะไม่มีการส่งต่อข้อมูลต่อไปให้ networks อีกตัว แม้ว่า routers เหล่านั้นจะเป็นที่รู้จักสำหรับการกระจายโดเมนต่าง ๆ อย่างเป็นปกติ ซึ่งเป็นส่วนสำคัญที่จะจำว่า routers จะทำตัวเป็นกันชนคอยยับยั้งได้อีกด้วย

ข้อดี 2 ประการสำหรับการใช้ routers ใน networks

- โดยปกติแล้ว routers จะไม่ส่งต่อข้อมูล broadcas
- routers สามารถกรอง networks โดยขึ้นอยู่บน layer ที่3 (Network Layer) (ตัวอย่างเช่น IP address)

หน้าที่ 4 ประการของ routers ต่อ networks

- การส่งต่อสับเปลี่ยนข้อมูล
- การกรองข้อมูล
- การติดต่อสื่อสาร internetworks
- การเลือกเส้นทางการส่งข้อมูล

จำไว้ว่า routers ต่าง ๆ เป็นเหมือนกับ switches หลายตัว แต่เรามักจะเรียกว่าเป็น layer 3 switches (ซึ่งเราจะกล่าวเรื่อง layer ในท้ายบทนี้) และจะไม่เหมือนกับโครงสร้าง networks ในขั้นที่ 2 ที่ใช้กรองและส่งต่อ frames, routers (layer 3 switches) นั้น ใช้ Logical addressing และจะมีสิ่งที่เรียกว่า packet switching

routers สามารถกรองข้อมูลโดยใช้ access-list (ซึ่งจะอธิบายในบทที่ 10) และจะมี routers ต่างๆ ที่เชื่อมโยง networks ที่มากกว่าหนึ่งตัวเข้าด้วยกัน และใช้ Logical addressing (IP) ซึ่งเป็นสิ่งที่เรียกว่า internetworks และสิ่งสุดท้าย routers ใช้เส้นทางของ networks หรือแผนที่ของ networks เพื่อเป็นการเลือกเส้นทาง และส่งข้อมูลย่อย ไปยังเน็ตเวิร์คต่าง ๆ ที่อยู่ไกลออกไป

ทางตรงกันข้าม switches ไม่สามารถนำมาสร้าง internetworks ได้ มันถูกใช้เพื่อเพิ่มหน้าที่ต่อ LAN ของinternetworks จุดประสงค์ของ switches นั้นก็เพื่อสร้างการทำงานของ LAN ให้ดีขึ้นหรือเพื่อทำให้มีประสิทธิภาพที่ดีที่สุด หรือทำให้มี Bandwidth เพียงพอสำหรับผู้ใช้ LAN และ switches จะไม่ส่งต่อ

ข้อมูลย่อยไปสู่ networks ตัวอื่น ๆ ดังเช่นที่ routers ทำ มันทำเพียงแค่ switch framesจาก portหนึ่งไปยัง portอื่นๆ ใน switch บน networks ซึ่งมันก็เป็นสิ่งที่ผู้อ่านจะสามารถเข้าใจได้ ว่าอะไรคือ โครงสร้าง อะไรคือ frames และ อะไรคือ packet เราจะบอกคุณตอนท้ายบท

โดยปกติ switch จะยับยั้ง collision domain ซึ่งก็คือการวกกลับของ Ethernet ที่เคยใช้อธิบายบทบาทของ networks ในจุดที่กลไกพิเศษหนึ่งส่งข้อมูลย่อยบน networks ย่อยซึ่งจะบังคับให้กลไกอื่น ๆ บน networks ย่อยเดียวกันส่งจุดสนใจไปที่มันจุดเดียว ในขณะเดียวกันนั้นความแตกต่างของกลไกพยายามที่จะกระจายข้อมูลออกไป ที่นำไปสู่การปะทะกัน ซึ่งจะเป็นหลังจากที่กลไกทั้งสองได้กระจายข้อมูลนั้นอีกครั้งในเวลาเดียวกัน ไม่มีผลอะไรมากนัก เป็นอย่างหนึ่งที่สามารถพบได้ในสภาพแวดล้อมของ hub ที่แต่ละ Host ย่อยจะเชื่อมต่อไปยัง hub ที่จะแสดงให้เห็นถึง collision domain เพียงแค่ domain เดียวใน broadcast domain แต่ในทางตรงกันข้าม ในแต่ละพอร์ตหรือทุก ๆ พอร์ตในการสับเปลี่ยนจะแสดงให้เห็นการชนกันของโดเมนเอง

Note

switch จะสร้างการแบ่งแยก collision domain แต่มันเป็นเพียง single broadcast domain

router สามารถแบ่ง broadcast domain แต่ละ interfaceได้

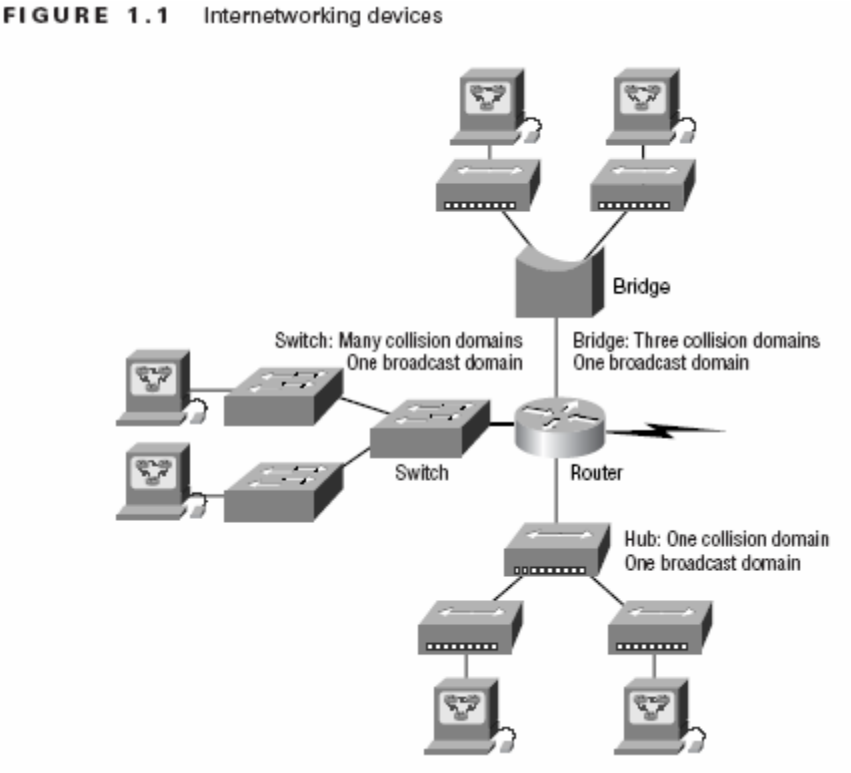
เงื่อนไขของ bridges ถูกแนะนำก่อน router และ hub ดังนั้นมันจึงค่อนข้างที่จะธรรมดาที่คนทั่วไปอ้างถึง bridgeเหมือนกับ switch นั่นก็เป็นเพราะว่า bridgeและ switch ทำหน้าที่พื้นฐานเหมือนกัน นั่นก็คือการยับยั้ง collision domain บน LAN ซึ่งหมายความว่า switch เป็นขั้นต้นของ bridges หลายๆ portรวมกันด้วยสมองกล ซึ่งมีความแตกต่างค่อนข้างมาก switch เตรียมที่จะทำงานทางด้านนี้ไว้แล้ว แต่ต้องเพิ่มการจัดการที่สูงขึ้นทั้งความสามารถและลักษณะ ส่วนใหญ่แล้ว bridges มีเพียง 2 หรือ 4 port และสามารถเพิ่มได้จนถึง 16 port

Note

คุณควรที่ใช้ bridges ใน networks เพื่อลดการชนปะทะหลาย ๆ ครั้งภายใน broadcast domain ต่าง ๆ และเพิ่มจำนวนของ collision domain ใน network ของคุณ การทำเช่นนี้จะเพิ่ม bandwidth ให้เพียงพอกับผู้ใช้ และจำไว้ว่าการใช้ hubใน networks สามารถช่วยเหลือในเรื่องของความหนาแน่นบนEthernet network ของคุณได้ แต่ต้องระมัดระวังเรื่องการออกแบบ networks ไว้เสมอ

รูปโครงสร้างที่ 1.1 แสดงให้เห็นว่า networks จะเป็นอย่างไรเมื่อเข้าไปแทนที่ทั้งหมดของ internetworks จำไว้ว่า routers จะไม่เพียงแต่ทำการยับยั้ง broadcast domain สำหรับ interface ของทุก ๆ LAN แต่ว่ายังป้องกัน ใน networks เพื่อลดการชนปะทะหลาย ๆ ครั้งภายใน broadcast domain ต่าง ๆ และเพิ่มจำนวนของ collision domain อีกด้วย

FIGURE 1.1 Internetworking devices



เมื่อคุณดูที่รูป 1.1 แล้ว คุณสังเกตเห็นว่า routers จะถูกพบที่ส่วนกลาง และนั่นก็จะเชื่อมโยงลักษณะต่าง ๆ ของ networks เข้าด้วยกันหรือไม่ ? เราจะต้องใช้โครงสร้างนี้เนื่องจากการแก้ปัญหาแบบเทคโนโลยีแบบเก่า นั่นคือ bridges และ hub ในบางครั้งเราเพียงใช้แค่ switch หลายๆ ตัว ใน networks ของเราเอง สิ่งต่าง ๆ ก็เปลี่ยนไปได้มาก switch LAN ก็จะเข้าไปอยู่ศูนย์กลางของโลก networks และ routers ก็จะถูกพบว่าเชื่อมโยงเพียง Logical network เข้าด้วยกัน ถ้าเราทำให้การติดตั้งนี้เป็นผลสำเร็จ เราก็จะสามารถสร้างแก่นแท้ของ LANs ได้ และสามารถสร้าง networks จำลอง (VLANs) ซึ่งจะพูดถึงกันในบทที่8 Virtual LANs (VLANs)

ด้านบนสุดของรูปโครงสร้างของ networks 1.1 จะเห็นว่า bridges ถูกใช้เพื่อติดต่อกับ hubและต่อไปยัง routers bridgesจะยับยั้ง collision domain แต่ host ทั้งหมดติดต่อ hubทั้งสองที่ยังคงเข้าสู่ broadcast domainเดียวกัน bridgesสร้างกันชนโดเมนเพียงแค่สองโดเมนเท่านั้น ดังนั้นแต่ละอุปกรณ์จะทำการเชื่อมไปยัง hub ที่เป็นกันชนโดเมนตัวเดียวกันเช่นทุกๆ อุปกรณ์อื่นที่เชื่อมต่อไปยัง hubตัวเดียวกัน เป็นสายเชื่อมโยงที่สนใจ แต่ว่ามันจะดีขึ้นหากว่ามีการชนปะทะเพียงแค่โดเมนเดียวสำหรับ host ทั้งหมด

สังเกตสิ่งอื่น ๆ hub ทั้งสามตัวที่อยู่ด้านล่างถูกเชื่อมโยงไปยัง routers ที่จะสร้างการชนปะทะที่ใหญ่มากและ broadcast domain ที่ใหญ่มาก สิ่งนี้ทำให้ทางเชื่อม networks ดูว่าทำงานได้ดีขึ้น

Note

แม้ว่า Bridge ถูกใช้แบ่ง networks ต่าง ๆ แต่ว่า Bridge จะไม่แยกการกระจายข้อมูลหรือ multicast packet

networks ที่ดีที่สุดเชื่อมเข้ากับ routers คือ LAN switch network ที่ด้านซ้าย ทำไมหรอ? เพราะว่าแต่ละ port บน switch นั้นจะหยุด collision domain แต่มันก็ทำได้ไม่ดีทั้งหมด แต่ว่ากลไกยังเป็นเหมือน broadcast domain คุณจำได้ไหมว่าทำไมถึงเป็นสิ่งที่ไม่ดี เพราะว่ากลไกทั้งหมดต้องรับรู้การกระจายข้อมูล นี่ก็คือเหตุผลว่าทำไม และถ้าการกระจายข้อมูลของคุณใหญ่มาก ผู้ใช้มี bandwidth น้อยและต้องการ broadcastข้อมูลมาก ๆและการทำงานของ network จะช้าและนั่นก็จะเป็นสาเหตุของความอลหม่านของข้อมูล

network ที่ดีที่สุดคือ network ที่สามารถจัดโครงสร้างที่ใช้งานได้ตรงความต้องการ LAN switches กับ routers เข้าไปแทนที่ได้อย่างเหมาะสมใน network นั่นก็จะเป็นการออกแบบ network ที่ดี หนังสือเล่มนี้จะช่วยให้ผู้อ่านได้เข้าใจเรื่อง routers และ switchesได้ ซึ่งอธิบายได้อย่างกระชับ จะค่อยอธิบายทีละตัวอย่างที่สำคัญ ๆ

กลับไปที่ ภาพ 1.1 มี collision domain และ broadcast domain ข้อมูลต่าง ๆ กี่ครั้ง ? คาดว่าคุณน่าจะตอบว่า 9 ครั้งสำหรับ collision domain และ 3 ครั้งสำหรับ broadcast domain เห็นได้ง่ายเพราะว่ามีเพียง routers ที่ยับยั้ง broadcast domain ได้ แต่ว่าการ collision domain 9 ครั้งนั้นดูได้จากทุก hub ของ network คือการ collision domain หนึ่งครั้ง bridges network เท่ากับ 3 การ collision domain บวกกับอีก 5 ครั้งใน switches ของ network (แต่ละครั้งที่เปลี่ยนport)

และตอนนี้คุณก็ได้รู้จักการทำงานของ internetworks และกลไกต่าง ๆ ที่อยู่ใน internetworks ได้เวลานำท่านเข้าสู่โครงสร้างใน internetworks

Real World Scenario

เราควรเปลี่ยน hub ทุกตัวกับ switches หรือไม่

คุณเป็นเจ้าหน้าที่ network ในบริษัทใหญ่ใน San Jose และหัวหน้าของคุณต้องการให้คุณซื้อ switches และไม่แน่ใจเรื่องค่าใช้จ่าย คุณจำเป็นต้องทำมันหรือไม่?

ถ้าหากว่าคุณต้องการ เนื่องจากว่า switches สามารถเพิ่มหน้าที่มากมายต่อ network ที่ hubไม่สามารถทำได้ แต่ว่าส่วนใหญ่แล้วเรามักมีปัญหาเรื่องเงิน hubยังคงสามารถสร้าง network ที่ดีได้ ถ้าหากว่าคุณออกแบบ network และทำให้สามารถทำงานได้อย่างเหมาะสม

มาพูดถึงผู้ใช้งาน 40 ท่านต่อ hub 4 ตัว หนึ่ง hub ต่อ 10 ผู้ใช้งาน จุดนี้ hub ทั้งหมดต้องเชื่อมต่อเข้าด้วยกัน ดังนั้นคุณจะมี collision domain ที่ใหญ่มากและ broadcast domain ที่ใหญ่มากเช่นกัน ถ้าหากว่าคุณสามารถมี switches เข้าเพียงหนึ่งตัวและต่อเข้าไปแต่ละ hub เข้าไปใน switches portให้เหมือนกับ

switches ใน server ซึ่งคุณจะมี collision domain 4 domain และ broadcast domain 1 domain แต่ว่าจะติดอยู่ก็ตรงเรื่องของราคา switches network ของคุณนั้นจะดีกว่าที่เคยเป็นดังนั้นทำไปเถอะ เพิ่ม switches เข้าไป ไม่มีอะไรที่คุณต้องเสีย

Internetworking Models

เมื่อ network ตัวแรกเกิดขึ้นมา คอมพิวเตอร์ก็จะติดต่อสื่อสารได้กับเพียงคอมพิวเตอร์ที่เป็นคอมพิวเตอร์ที่อยู่ในฝ่ายผลิต ตัวอย่างเช่น บริษัทดำเนินการตามแบบของ DEC net หรือตามแบบของ IBM อย่างใดอย่างหนึ่งเท่านั้น ในช่วงปลายปี 1970 โครงสร้างความสัมพันธ์ Open System Interconnection (OSI) ถูกสร้างโดยองค์กรนานาชาติสำหรับมาตรฐาน (ISO) เพื่อหยุดอุปสรรคนี้

โครงสร้าง OSI นี้เป็นพื้นฐานที่มีความสำคัญที่ช่วยผู้ให้บริการสร้างกลไกการทำงาน network ที่หลากหลายและ softwareในรูปแบบของ protocol ดังนั้นผู้ให้บริการ networks ต่างๆ ก็จะทำงานด้วยกันได้ ถึงแม้ว่าจะไม่ได้สมบูรณ์แบบนักแต่ว่าก็ถือได้ว่าเป็นการทำงานที่ยอดเยี่ยมทีเดียว

โครงสร้างของ OSI เป็นขั้นพื้นฐานของสถาปัตยกรรมโครงสร้าง network ซึ่งใช้อธิบายว่าข้อมูลดิบและข้อมูล network ติดต่อสื่อสารจากการใช้งานในคอมพิวเตอร์ไปสู่การสื่อสาร network สู่การใช้งานของคอมพิวเตอร์อีกตัวหนึ่ง โครงสร้างความสัมพันธ์ OSI จะอ้างอิงการกระจายตัวออกเป็นส่วนๆ ตาม โครงสร้าง layer

The Layered Approach

โครงสร้างความสัมพันธ์เป็นขอบข่ายของร่างแผนว่าควรจะเข้าไปแทนที่ มันจะสร้าง Addresses ของความต้องการกระบวนการสำหรับการสื่อสารที่มีประสิทธิผลและแบ่งกระบวนการในการจัดกลุ่มแบบอย่างเป็นรูปแบบที่ถูกเรียกว่า layer เมื่อระบบการติดต่อสื่อสารถูกออกแบบในลักษณะนี้มันถูกเรียกว่า layer architecture

ลองคิดตามตัวอย่างดังนี้

คุณและเพื่อนบางคนต้องการเริ่มก่อตั้งบริษัท หนึ่งในสิ่งแรก ๆ คุณจะต้องนั่งและคิดว่างานอะไรที่ต้องทำ และใครจะเป็นผู้ใช้งาน และจะต้องทำตามคำสั่งอะไรบ้าง และผู้ใช้งานจะต้องติดต่อกันอย่างไร คุณ

จะต้องจัดกลุ่มงานต่าง ๆ อย่างละเอียดในส่วนต่าง ๆ และต้องคุยกันถึงในส่วนของคำสั่ง และสรุปส่วนต่าง ๆ และการจัดการส่วนต่าง ๆ แต่ละส่วนนั้นก็จะมีความเป็นเอกภาพอยู่ซึ่งจะทำให้ผู้ใช้งานยุ่งและต้องการเน้นไปที่หน้าที่ของตัวมันเอง

ใน scenario นั้นเราจะใช้ส่วนต่าง ๆ เพื่อเป็นการเปรียบเปรยกับ layer ในระบบการสื่อสาร สำหรับสิ่งต่าง ๆ เหล่านี้ก็จะดำเนินการอย่างเรียบง่าย ผู้ใช้งานในส่วนต่างๆก็จะต้องเชื่อในและวางใจในส่วนต่างเมื่อต้องทำงานตามหน้าที่ของมัน ซึ่งจะมีหน้าที่ของพวกมันเองอย่างมีเอกภาพที่เหมาะสม ในระหว่างการประชุมก็ควรจะมีการจดโน้ต เพื่อจดจำกระบวนการทั้งหมดเพื่อความสะดวกภายหลังจาการร่วมกันวางแผนเกี่ยวกับมาตรฐานของการจัดการที่ต้องรองรับแผนงานทางธุรกิจที่วางไว้หรือความสัมพันธ์ของโครงสร้าง

เมื่อถึงเวลาเริ่มธุรกิจ หัวหน้าส่วนต่าง ๆ ก็จะมีการป้องกันส่วนต่าง ๆ ของแผนการที่สัมพันธ์กันกับส่วนนั้น ๆ ของมันเอง ที่มีความจำเป็นอย่างยิ่งว่าจะพัฒนาวิธีการปฏิบัติเพื่อให้เป็นผลที่สำเร็จตามคำสั่งที่ได้รับมอบหมาย วิธีการปฏิบัติเหล่านี้ หรือ protocol จะต้องเรียบเรียงเข้าสู่มาตรฐานการจัดการการทำคู่มือและติดตามอย่างใกล้ชิด แต่ละวิธีการที่หลากหลายในคู่มือจะรวบรวมเหตุผลที่แตกต่างกันและมีหลายความสำคัญและหลายความสำเร็จ ถ้าคุณมีหุ้นส่วนหรือหาเพื่อนร่วมงานมันอาจจะเป็นการเปรียบเทียบธุรกิจของมันเอง อย่าง protocol แบบแผนทางธุรกิจของมันเอง ที่เหมาะสมกับคุณ (หรืออย่างน้อยก็เข้ากันได้กับมัน)

ผู้พัฒนา software สามารถใช้ความสัมพันธ์ของโครงสร้างเพื่อเข้าใจการสื่อสารของกระบวนการทำงานของคอมพิวเตอร์และเห็นสิ่งที่เป็นหน้าที่ ที่จำเป็นที่จะให้เป็นผลสำเร็จในแต่ละ layer ถ้าพวกเขาพัฒนา protocol layer ที่แน่นอน พวกเขาจำเป็นต้องเกี่ยวข้องกับหน้าที่เฉพาะของ layer ไม่ใช่ที่ layer อื่น ๆ สำหรับอีก layer และprotocolจะจัดการหน้าที่อื่น ๆ เทคนิคสำหรับความคิดนี้ก็คือการทำให้ตาบอดกระบวนการสื่อสารนั้นจะสัมพันธ์กันเป็นสะท้อนกลับหรือจับกลุ่มกันในเฉพาะ layer

Advantages of Reference Models

โครงสร้าง OSI เป็นลำดับขั้นตอน ทั้งข้อดีและประโยชน์สามารถที่จะประยุกต์ใช้ได้กับทุกโครงสร้าง layer จุดประสงค์หลักของโครงสร้างใด ๆ ก็ตามโดยเฉพาะโครงสร้างของOSI จะต้องยินยอมให้ผู้สร้าง network เข้าไปจัดการในความหลากหลาย

สรุปข้อดีของการใช้โครงสร้าง OSI layer แต่ว่าไม่ได้มีข้อจำกัด ตามที่กล่าวไว้ในที่นี้

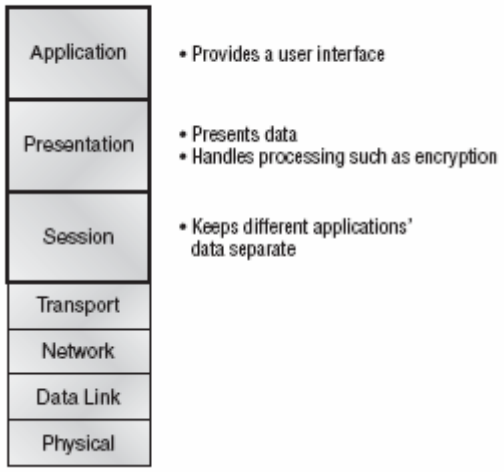
1. มันจะแบ่งการสื่อสารของ network ออกเป็นกลุ่มย่อย ๆ และเป็นส่วนประกอบที่ง่ายๆ ดังนั้นจะช่วยเสริมในการพัฒนา การออกแบบและการแก้ปัญหา

2. มันจะยินยอมให้มีการพัฒนาที่หลากหลายตลอดไปจนสร้างมาตรฐานของส่วนประกอบของ network
3. มันจะช่วยสนับสนุนมาตรฐานของอุตสาหกรรมโดยกำหนดสิ่งที่เป็นหน้าที่ของโครงสร้างในแต่ละ layer
4. มันยินยอมให้ประเภทต่างๆ ของ network ฮาร์ดแวร์ และ ซอฟท์แวร์ ทำการสื่อสารกัน
5. มันจะสร้างโอกาสใน layer หนึ่งจากผลกระทบที่ได้รับจาก layer อื่น ๆ ดังนั้นจึงไม่ทำให้การพัฒนาหยุดยั้ง

The OSI Reference Model

หน้าที่ที่สำคัญที่สุดของการแบ่งหน้าที่เฉพาะของ OSI คือการช่วยการแปลงข้อมูลระหว่าง Host ที่ต่างชนิดกันกับความหมาย ตัวอย่างเช่น สามารถทำให้เราสามารถแปลงข้อมูลระหว่าง Unix host กับ Pc หรือ Mac

FIGURE 1.2 The upper layers



OSI ไม่ได้เป็นโครงสร้างที่เป็นรูปเป็นร่างไปตลอด ในทางตรงกันข้ามมันเป็นตัวชี้นำว่าผู้พัฒนาการใช้สามารถใช้เพื่อสร้าง และก่อให้เกิดการใช้ที่ทำให้เกิดผลสำเร็จบน network มันสามารถแบ่งโครงสร้างของงานสำหรับการสร้างหรือมาตรฐานการทำ network ให้เป็นผลสำเร็จ หลักการต่าง ๆ และแผนการทำงานของ internetworks

OSI มีโครงสร้างทั้งหมด 7 ชั้นแบ่งเป็น 2 กลุ่มใหญ่ 3 layer ด้านบน ว่าด้วยเรื่องวิธีการภายในตำแหน่งสุดท้ายที่จะติดต่อสื่อสารกันเองและต่อผู้ใช้ แต่สำหรับ 4 layer ด้านล่างนั้น ว่าด้วยเรื่องของการส่งต่อข้อมูลจากตอนท้ายไปยังตอนท้าย รูป 1.2 แสดงให้เห็นถึง 3 layer ด้านบนกับหน้าที่ของ layer และรูป 1.3แสดงให้เห็น 4 layer ด้านล่างและหน้าที่ของมันเอง

เมื่อคุณได้ดูรูป 1.2 แล้ว เข้าใจว่าการติดต่อสื่อสารของผู้ใช้กับคอมพิวเตอร์ที่ Application layerและ layer ในชั้นที่สูงขั้นไป มีหน้าที่ที่ติดต่อสื่อสารระหว่าง host กันเอง จำไว้ว่าไม่มี layer ที่สูงกว่าอันไหนรู้เกี่ยวกับการทำงานของ network หรือ network Addresses นั่นก็จะเป็นหน้าที่ของ 4 layer ด้านล่าง

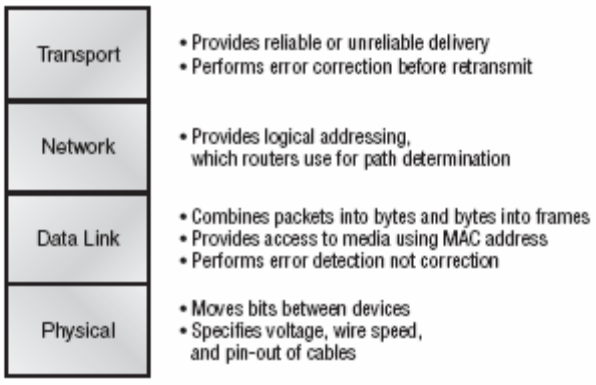
ในรูป 1.3 คุณจะเห็นว่ามี 4 layer ด้านล่างที่ทำให้เข้าใจเรื่องการส่งต่อข้อมูลผ่านทั้งรูปร่างของการติดต่อหรือ ผ่าน switch กับ routers layer ด้านล่างนี้จะยุติการสร้างซ้ำการไหลของข้อมูลจากการส่งต่อข้อมูลจาก hostไปสู่ปลายทางประโยชน์ของhost

สรุปหลักการ network ที่จัดการใน 7 ชั้นของ layer

- สถานที่จัดการ network
- Web และ Application servers
- Gateways (ที่ไม่ใช้ default gateways)
- Network hosts

OSI คือสิ่งที่มีค่อนข้างมากใน Emily Post ของโลก Network Protocal อย่างธรรมดา ก็ดังเช่นที่คุณ Postได้เขียนไว้ในหนังสือที่ได้ตั้งมาตรฐานหรือที่เรียกว่า Protocal สำหรับสังคมของมนุษย์ที่มีการกระทำต่างเกิดขึ้นต่อกัน OSI ได้พัฒนาโครงสร้างความสัมพันธ์ของ OSI ดังที่เคยมีมาก่อนและนำไปสู่การเปิด Network Protocal กำหนดคุณสมบัติที่ดีของโครงสร้างการสื่อสารที่มันยังมีอยู่จนทุกวันนี้ ที่เป็นที่นิยมของการเปรียบเทียบสำหรับกลุ่มของ Protocal

FIGURE 1.3 The lower layers

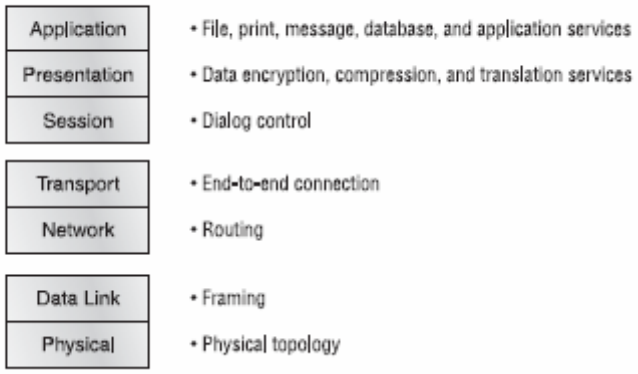


โครงสร้างของ OSI Model มี 7 layer ดังนี้

1. Application layer (layer 7)
2. Presentation layer (layer 6)
3. Session layer (layer 5)
4. Transport layer (layer 4)
5. Network layer (layer 3)
6. Data link layer (layer 2)
7. Physical layer (layer 1)

รูป 1.4 แสดงให้เห็นถึงหน้าที่ของแต่ละ layer ของโครงสร้าง OSI ด้วยการแนะนำนี้จะทำให้คุณผู้อ่านได้ลงลึกไปในรายละเอียดแต่ละหน้าที่ของ layer

FIGURE 1.4 Layer functions



Application Layer

Application layer ของโครงสร้าง OSI ทำให้เห็นจุดที่ผู้ใช้งานสื่อสารโดยตรงกับคอมพิวเตอร์ layer นี้เข้ามาเพียงเพื่อเล่นเมื่อมีการเข้าสู่ network อย่างชัดเจนและจะเป็นสิ่งจำเป็นอย่างเร็ว ตัวอย่างในกรณีของ internet Explorer (IE) คุณควรจะเอาส่วนประกอบต่าง ๆ ของ network ออกจากระบบ ตัวอย่างเช่น TPC/IP NIC card และอื่น ๆ คุณควรที่จะใช้ IE ที่จะดูเนื้อหา HTML ท้องถิ่น ซึ่งไม่เป็นปัญหา แต่สิ่งต่าง ๆ เหล่านี้ก็จะไม่เป็นระเบียบ ถ้าหากคุณพยายามที่จะทำบางสิ่งบางอย่างเหมือนการเข้าไปดูเนื้อหาของ HTML ซึ่งจะต้องซ่อมแซมการใช้ HTTP หรือ ยก file ด้วย FTP นั่นก็เป็นเพราะว่า IE จะโต้ตอบต่อการเรียกร้องอย่างเช่นความพยายามที่เข้าสู่ Application layer และสิ่งที่จะเกิดขึ้นก็คือการติดต่อระหว่างการใช้งานโปรแกรมจริงซึ่งไม่ได้เป็นทั้งหมดของรูปแบบของ layer และlayer ด้านล่างที่ถัดมาก็หาวิธีสำหรับการใช้เพื่อส่งข้อมูลลงไปตลอดกลุ่มของ protocol

ในอีกทางหนึ่งก็คือจะไม่มี IE ที่อยู่กับ Application layer ไปตลอด มันติดต่อกับ Application layer protocol เมื่อมันจำเป็นต้องติดต่อกับแหล่งข้อมูลระยะไกล

Application layer มีหน้าที่ชี้และสร้างการสื่อสารกับคู่หูอย่างตั้งใจอีกด้วย และตัดสินใจว่ามีแหล่งข้อมูลที่เพียงพอสำหรับการติดต่อสื่อสารนั้นอยู่หรือไม่

งานนี้เป็นงานที่สำคัญก็เพราะว่าการทำงานของคอมพิวเตอร์บางครั้งต้องการข้อมูลมากกว่าที่เห็นบนหน้าจอ บ่อยครั้งที่ Application layer รวมส่วนประกอบการสื่อสารเข้าด้วยกันจากการใช้งานใน network มากกว่าหนึ่ง ตัวอย่างที่สำคัญที่สุดก็คือการเปลี่ยนแปลงข้อมูลและ e-mail ได้ดีพอๆกับการควบคุมได้ในระยะไกล มีการจัดการ network การทำงานของลูกค้าหรือ server และพื้นที่ของข้อมูล การใช้ networkจำนวนมากทำให้มีการบริการสำหรับการสื่อสารบนกลุ่มของnetwork แต่สำหรับทำงานของnetworkในปัจจุบันและอนาคตความจำเป็น เป็นสิ่งที่ทำให้ต้องพัฒนาอย่างเร็วเพื่อนำไปสู่จุดที่เกินขอบเขตหลักการของ Physical networking ทุกวันนี้การแลกเปลี่ยนข้อตกลงและข้อมูลระหว่างองค์กรทำให้กว้างขึ้นเพื่อต้องการวิธีการการทำงานของnetwork ดังตัวอย่างด้านล่าง

World Wide Web (WWW) การเชื่อมโยง server ที่ไม่สามารถนับได้ (ซึ่งจำนวนได้เพิ่มขึ้นตามวันเวลาที่ผ่านไป) แสดงให้เห็นถึงโครงสร้างที่หลากหลาย ส่วนใหญ่ก็คือ multimedia และสามารถที่จะรวบรวมรูปต่าง ๆ เนื้อหา วีดีโอ และเสียง (และราวกับว่าแรงกดดันจะเก็บระยะเพิ่มขึ้น websites ที่ปีน slicker และที่เป็น snappier จำไว้ว่า the snazzier มันต้องการทรัพยากรของเรามาก) Netscape Navigator และ IE นั้นเป็นสิ่งที่ทำให้เปิดดูและเข้าสู่ websites ได้ง่าย

E-mail gateways มีประโยชน์หลายอย่างสามารถใช้ Simple Mail Transfer Protocal (SMTP) หรือ มาตรฐาน X.400 เพื่อใช้ส่งข้อความระหว่าง e-mail

Electronic data Interchange (EDI) การประกอบส่วนต่าง ๆ ของมาตรฐานพิเศษและกระบวนการของการทำงานอย่างต่อเนื่องเช่นการทำบัญชี การขนส่งหรือการรับส่ง และการสั่งและการสร้างขึ้นมาใหม่ของแนวทางการประกอบธุรกิจ

กระดานข่าวที่น่าสนใจเป็นพิเศษ รวมถึงห้อง chatใน internet ต่าง ๆ ที่ผู้คนสามารถพบปะติดต่อสื่อสารกันได้โดยการส่ง post ข้อความหรือการคุยกันสด ๆ พวกเขาสามารถแบ่งปัน software domainสาธารณะได้

ประโยชน์ต่าง ๆ ที่รวบรวมการใช้งานดังเช่น Gopher กับ WAIS ซึ่งใช้งานได้ดีพอ ๆ กับ search engines อย่าง google กับ yahoo ที่ช่วยให้ผู้ใช้งานต่าง ๆ สามารถหาที่มาและข้อมูลต่าง ๆ ตามที่พวกเขาต้องการได้บน internet

การบริการด้านการจัดการเรื่องการเงิน เป้าหมายของกลุ่มการเงิน การบริการนี้ได้รวบรวมและขายข้อมูลสำหรับการลงทุน การตลาด อัตราการแลกเปลี่ยน และข้อมูลที่น่าเชื่อถือให้กับสมาชิก

The Presentation Layer

Presentation layer ได้ชื่อมาจากหน้าที่หลักของมันเอง มันแสดงข้อมูลต่อ Application layer และมีหน้าต่อการแปลงข้อมูลและการสร้างรูปแบบการติดต่อ

layer นี้สำคัญต่อการแปลและหารหัสและหน้าที่ของการสับเปลี่ยนหน้าที่ การประสบความสำเร็จสำหรับเทคนิคการเปลี่ยนแปลงข้อมูลคือต้องมีการปรับข้อมูลให้เป็นรูปแบบมาตรฐานสำหรับการเปลี่ยนแปลง คอมพิวเตอร์ต่าง ๆ เป็นโครงสร้างที่ได้รับการจดลิขสิทธิ์สำหรับการจัดเก็บข้อมูลและการเปลี่ยนข้อมูลกลับไปสู่รูปแบบเดิมเพื่อการอ่าน (ตัวอย่างเช่น EBCDIC เป็น AIC II) โดยการเตรียมบริการการแปล Presentation นั้นทำให้แน่ใจว่าการแปลงข้อมูลจาก Application layer ของระบบหนึ่งสามารถอ่านได้ด้วยการใช้ Application layer อีกอันหนึ่ง

OSI มีมาตรฐาน protocol ที่ให้คำจำกัดความว่าข้อมูลที่ได้มาตรฐานนั้นจะจัดเก็บได้อย่างไร ผลที่ได้ก็จะเหมือนกับการบีบข้อมูล ลดความดันข้อมูล การเข้ารหัสและการถอดรหัสนั้นเกี่ยวเนื่องกับlayerนี้ มาตรฐานของ Presentation layer เกี่ยวเนื่องอยู่ในการจัดการ multimedia ด้วยการดูแลนี้ขึ้นตรงกับ graphic และ visual image Presentation

PICT คือรูปแบบของรูปภาพที่ถูกจัดเก็บโดยใช้โปรแกรมของ Macintosh สำหรับการเปลี่ยน QuickDraw graphics

TIFF คือ รูปแบบของการจับรูปภาพของการจัดเก็บไฟล์ ซึ่งก็คือรูปแบบของภาพที่เป็นมาตรฐานสำหรับเงื่อนไขที่สูง รูปแผนที่เล็ก ๆ

JPEG มาตรฐานของรูปที่ทำให้เราได้สนุกไปกับ Joint Photographic Expert Group เป็นมาตรฐานของภาพและเสียง

MIDI คือการสื่อสารเพลงที่เป็นระบบดิจิตอล บางครั้งเรียกว่า Musical Instrument Device Interface ใช้สำหรับเพลงที่เป็นดิจิตอล

MPEG เป็นมาตรฐานที่ได้รับความนิยมของ Moving Picture Expert Group สำหรับการเพิ่มแรงบีบและเข้ารหัสของภาพวีดีโอที่ใช้สำหรับ CDs มันจะมีการจัดเก็บด้วยอัตราที่น้อยจนไปถึง 1.5 Mbps

Quick Time สำหรับการใช้โปรแกรม Macintosh ที่ใช้กับงานเสียงแบบ audio และวีดีโอ

RTF Rich Text Format คือการจัดเก็บไฟล์ที่สามารถทำให้คุณเปลี่ยน word processors ที่แตกต่างกันแม้ว่าอยู่ในระบบการจัดการที่แตกต่างกัน

Session layer

Session layer เป็นมีหน้าที่สำหรับการจัดตั้ง และจัดการและแยกการศึกษาระหว่างทั้งหมดกับ Presentation layer ใน layer นี้เตรียมการควบคุมการสนทนาระหว่างอุปกรณ์หรือnode ที่มีปัญหา มันรวบรวมการสื่อสารระหว่าง ระบบและส่งให้กับการสร้างข้อมูลของการสื่อสารโดยจะนำเสนอ 3 รูปแบบที่แตกต่างกันคือ Simplex, Half duplex และ Full duplex ผลลัพธ์ของพื้นฐานของ Session layer จะเก็บความแตกต่างของ application ของข้อมูลที่แตกต่างกันจากข้อมูลของ application อื่นๆ

ด้านล่างนี้เป็นบางตัวอย่างของ Session layer protocols และ interfaces (ตามCisco)

Network File System (NFS) ถูกพัฒนาโดย Sun Microsystems และใช้กับ TCP/IP และ Unix คอมพิวเตอร์ที่ทำงานเพื่ออนุญาตให้เครื่องลูกข่ายเข้าแหล่งข้อมูลต่าง ๆ ได้ในระยะไกล

Structure Query Language (SQL) พัฒนาโดย IBM ที่ทำให้ผู้ใช้งานและวิธีการใช้งานขึ้นสำหรับการกำหนดข้อมูลที่ต้องการได้ทั้งในพื้นที่ท้องถิ่นหรือระยะไกล

Remote Procedure Call (RPC) อุปกรณ์ที่เครื่อง client / server ติดต่อกันโดยตรง โดยจะใช้สำหรับสภาพแวดล้อมที่ให้การบริการ วิธีการของมันก็คือการสร้างเครื่อง client หรือแสดงออกบน server

X Window ถูกใช้อย่างกว้างขวางเป็น terminals ที่ฉลาดสำหรับการติดต่อเพื่อ remote กับคอมพิวเตอร์Unix อนุญาตให้พวกมันเข้าสู่การจัดการทำตัวเองเป็นตัวตรวจสอบที่อยู่บนพื้นที่เดียวกัน

AppleTalk Session Protocol (ASP) client / server ที่เป็นทั้งการสร้างและการดูแลรักษา sessions ระหว่างเครื่อง AppleTalk กับเครื่อง server

Digital Network Architecture Session Control Protocol (DNA SCP) เป็น DECnet Session layer Protocol

The Transport layer

Transport Layer segmentsกับ การประกอบข้อมูลขึ้นใหม่ภายใน traffice ของข้อมูล การบริการถูกตั้งใน Transport layer ทั้งในส่วนของ segment และการประกอบข้อมูลขึ้นใหม่จาก layer ชั้นที่สูงกว่าและรวมเป็นอันเดียวกันใน layer บน traffice ของข้อมูล Transport Layer เตรียมการในเรื่องend-to-end ของการบริการการส่งต่อข้อมูล และสามารถที่จะสร้างการเชื่อมต่ออย่างเหมาะสมระหว่าง host ที่ทำการส่งกับปลายทางของ host บน internetwork

บางทีผู้อ่านบางท่านอาจจะคุ้นเคยกับ TCP กับ UDP แล้ว (แต่ว่าถ้าไม่รู้จักก็ไม่ต้องกังวลเพราะว่าจะมีอยู่ในบทที่ 2 internet protocol) ถ้าคุณรู้จักทั้งการทำงานบน Transport layer และ TCP ที่มีการบริการ

อย่างมีประสิทธิภาพ แต่ว่ากับ UDP ไม่เป็น สิ่งนี้หมายความว่าการพัฒนาประโยชน์มีมากกว่าหนึ่งทางเลือก เพราะว่ามีตัวเลือก 2 protocol เมื่อทำงานกับ TCP/UDP protocol

Transport layer มีหน้าที่เตรียมกลไกสำหรับการใช้ที่มากมายเป็นทวีคูณที่ layer ที่สูงขึ้น การสร้าง sessions และแตก circuit ออก ซึ่งมันยังซ่อนรายละเอียดของข้อมูลที่ขึ้นอยู่กับ network จาก layer ที่สูงกว่าโดยการเตรียมการแปลงข้อมูลที่เข้าใจง่าย

Note

การทำงานของ network ที่วางใจได้สามารถใช้ใน Transport layer ซึ่งหมายความว่า ความรู้ ความต่อเนื่อง และการควบคุมไหลลื่น ก็จะถูกใช้ด้วย

Transport layer สามารถใช้ได้เมื่อปราศจากการติดต่อสื่อสารหรือการปรับการติดต่อสื่อสาร แต่อย่างไรก็ตาม Cisco เป็นส่วนที่เกี่ยวข้องกับคุณในเรื่องความเข้าใจส่วนของปรับการติดต่อสื่อสารของ Transport layer ตามส่วนต่าง ๆ จะเตรียมการปรับการติดต่อการสื่อสาร (อย่างมีประสิทธิภาพ) แบบคร่าว ๆ ของTransport layer

The Flow Control

ความมั่นคงของข้อมูลทำให้มั่นใจที่ Transport layer โดยดูแล flow control และอนุญาตให้ผู้ใช้ได้เรียกร้องการส่งต่อข้อมูลอย่างมีประสิทธิภาพระหว่างระบบ Flow control สามารถป้องกันการส่ง hostที่ด้านหนึ่งของการติดต่อสื่อสารจากการไหลที่มากเกินไปของ buffers ต่อการรับhost ซึ่งเป็นเหตุการณ์ที่เกิดขึ้นได้ในระหว่างข้อมูลหาย การแปลงข้อมูลที่มีประสิทธิภาพถูกใช้เมื่อการปรับการติดต่อสื่อสารเมื่อมี sessionsการสื่อสารระหว่างระบบ และ protocol ก็ทำให้มั่นใจว่าการทำตามนี้จะเป็นผล

- การส่งส่วนย่อยถูกยอมรับให้กลับมาสู่ผู้ส่งตลอดระยะเวลาการรับ
- ส่วนย่อยใด หากไม่ได้รับการยอมรับจะมีการส่งซ้ำเกิดขึ้น
- ส่วนย่อยจะส่งกลับมาอย่างเป็นลำดับภายในคำสั่งอย่างเหมาะสมตามระยะเวลาที่มาถึงจุดหมายปลายทาง
- สามารถจัดการการไหลข้อมูลเป็นการดูแลตามคำสั่งเพื่อหลีกเลี่ยงความหนาแน่น หรือการที่มีการโหลดข้อมูลมากเกินไป หรือว่าจะเป็นการสูญหายของข้อมูล

Connection-Oriented Communication (การปรับการติดต่อสื่อสารในการสื่อสาร)

ในการปรับการสื่อสารที่มีประสิทธิภาพ หลักการก็มีอยู่ว่าต้องส่งต่อการจัดการปรับการสื่อสารในการสื่อสารกับหลักการอ้อม ๆ โดยสร้าง sessions หลักการของการส่งต่อจะสร้าง sessions

การปรับการสื่อสารกับระบบที่เข้ากันที่เรียกว่า Call set up หรือ three-way handshake และเมื่อข้อมูลได้รับการแปลงจนสำเร็จแล้วการยุติการติดต่อก็จะเข้าแทนที่เพื่อที่จะแบ่ง virtual circuit อก

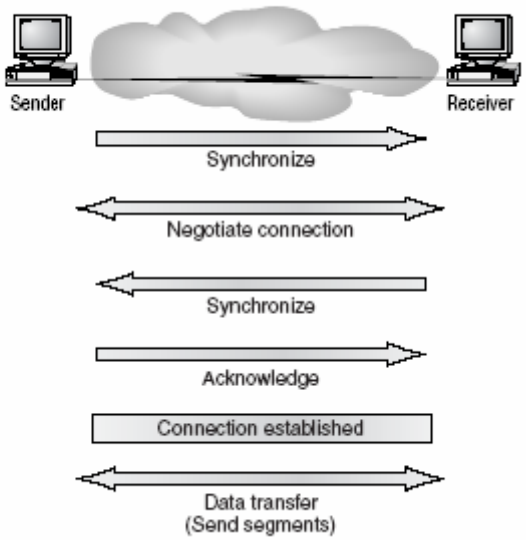
รูปที่ 1.5 ทำให้เห็น session ที่มีประสิทธิภาพเข้าแทนที่ระหว่างระบบการรับและการส่ง ดูที่ภาพนั่นคุณจะเห็นทั้งการใช้โปรแกรม host ซึ่งเริ่มต้นโดยแจ้งการจัดระบบการจัดการเดียวที่เป็นการติดต่อเกี่ยวกับการทำให้รู้จักระบบการจัดการสองอันติดต่อโดยการยืนยันการส่งข้อความข้าม network ที่การเปลี่ยนแปลงนั้นถูกพิสูจน์และทั้งคู่นั้นพร้อมที่จะถูกแทนที่ หลังจากความต้องการนี้การแทนที่ได้เกิดขึ้นพร้อมกัน การติดต่อจะเป็นการสร้างที่สมบูรณ์และจะเริ่มการแปลงข้อมูล

ในขณะที่การแปลงข้อมูลเกิดขึ้นระหว่าง hosts กลไกทั้งสองก็ทำการตรวจสอบซึ่งกันและกัน ซึ่งก็จะติดต่อสื่อสาร protocol software เดียวกันเพื่อที่จะทำให้แน่ใจว่าทั้งสองทำงานได้ดีและได้รับข้อมูลครบถ้วนเหมาะสม

นี่ก็จะเป็นการสรุป session ของการปรับการสื่อสารที่เรียกว่า three-way handshake ตามรูป 1.5

- ส่วนที่ได้รับการยอมรับแรกเป็นการยอมรับที่ถูกต้องการสำหรับการเกิดขึ้นในเวลาเดียวกัน
- ส่วนย่อยที่ 2 และ 3 ยอมรับการร้องขอและสร้าง connection parameters ตามกฎ ที่เกิดขั้นระหว่าง host ตามลำดับของผู้รับที่เป็นทั้งการร้องขอที่เกิดขั้นที่พร้อมกันดังนั้นการติดต่อทั้งสองผ่านก็จะเกิดขึ้นด้วย
- ส่วนย่อยสุดท้ายนั้นเป็นการยอมรับด้วย มันทำให้รู้ว่าจุดสิ้นสุดของ host นั้นมีการยอมรับการการตกลงเรื่องการสื่อสารและนั่นก็เป็นการสร้างการสื่อสารที่แท้จริง การแปลงข้อมูลสามารถเกิดขึ้นได้ตอนนี้

FIGURE 1.5 Establishing a connection-oriented session



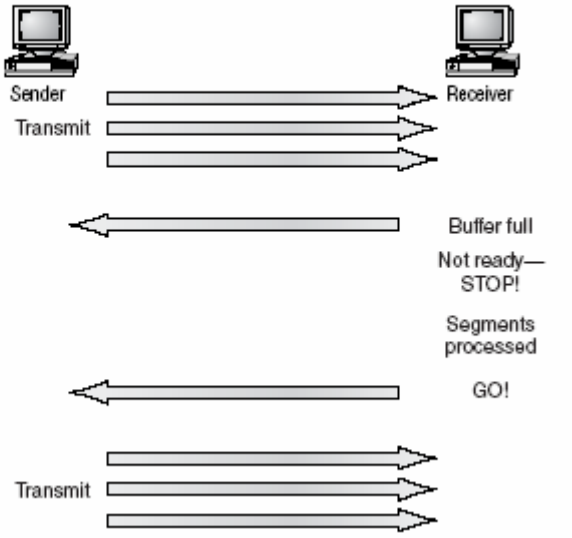
เสียงค่อนข้างธรรมดา และสิ่งต่าง ๆ ไปได้ราบรื่น บางครั้งในระหว่างการแปลงข้อมูลความหนาแน่นสามารถเกิดขึ้นได้เนื่องจากว่า คอมพิวเตอร์ความเร็วสูงทำให้เกิดการเดินทางของข้อมูลที่เร็วกว่าการจัดการแปลงข้อมูลด้วย network ส่วนต่าง ๆ ของคอมพิวเตอร์จะส่งไดอะแกรมที่เหมือนจริงไปยัง gateway เดี่ยวหรือปลายทางที่สามารถซ่อมแซมสิ่งต่าง ๆ ได้อย่างดี ในกรณีล่าสุด gateway หรือปลายทางสามารถกลายเป็นที่ทำให้แออัดแม้ว่าไม่มีแหล่งข้อมูลเลยสักที่ ที่สามารถเป็นสาเหตุของปัญหา ในกรณีอื่นปัญหาส่วนใหญ่เกี่ยวกับการความหนาแน่นในการส่งข้อมูลแบบคอขวด นั่นก็คือการส่งข้อมูลจำนวนมากในความสามารถที่จำกัด ไม่ใช่แค่เพียงรถเท่านั้นที่มีปัญหาการจราจรคับคั่งบน freeway

เมื่อเครื่องได้รับข้อมูลที่ท่วมท้นอย่างรวดเร็วตอนกำลังทำงาน มันก็จะเก็บเข้าไปสู่ความจำในส่วนที่เรียกว่า Buffer การ buffer นี้เป็นเพียงแค่การแก้ปัญหาถ้าหากว่าข้อมูลนั้นมีการแตกออกเล็กน้อย แต่ว่าถ้าไม่เป็นเช่นนั้น การไหลบ่ามาของข้อมูลมีมาอย่างต่อเนื่อง การใช้หน่วยความจำนั้นจะถูกใช้จนหมด การรับข้อมูลที่ท่วมท้นอย่างเต็มที่มันก็จะมากเกินไปและมันจะมีการทำซ้ำเกิดขึ้นโดยจะปฏิเสธการรับเพิ่มข้อมูลใด ๆ อีก

แต่ว่าไม่ต้องกังวลกับส่วนนี้มาก เนื่องจากหน้าที่ของการแปลงข้อมูลระบบต่าง ๆ ของการควบคุมการท่วม network สามารถทำงานได้ค่อนข้างดี แทนที่จะมีการทิ้งที่มาของข้อมูลและปล่อยให้ข้อมูลหายไปเฉย ๆ การแปลงข้อมูลสามารถส่งคำว่า “ not ready” ไปยังผู้ส่งได้ หรือยังแหล่งที่มาของการท่วมท้นของข้อมูลได้ (ดังที่แสดงให้เห็นในรูป 1.6) กลไกการทำงานของเครื่องนี้ก็เหมือนกับ stoplight สัญลักษณ์ที่ส่งไปบอกเพื่อหยุดการส่งถ่ายข้อมูลเพื่อเข้าครอบคลุมอีกเครื่องหนึ่ง หลังจากที่ผู้รับอีกเครื่องหนึ่งดำเนินการส่วนต่าง ๆ ให้พร้อมในหน่วยความจำ นั่นก็คือการ buffer มันก็จะส่งคำว่า “ready” ออกไปเพื่อแปลงตัวชี้นำเมื่อเครื่องรอการส่งต่อข้อมูลส่วนที่เหลือก็จะได้รับคำนี้ “go” เพื่อบอกว่ามันกำลังทำการส่งข้อมูลอยู่

ในขั้นพื้นฐานแล้วการแปลงการปรับการสื่อสารที่มีประสิทธิภาพ ข้อมูลที่ส่งออกไปยัง host ที่รอรับนั้นจะต้องเป็นลำดับที่เรียงต่อกันไปอย่างตอนแปลงข้อมูล มีการส่งข้อมูลพลาดถ้าคำสั่งถูกฝ่าฝืน ถ้าข้อมูลส่วนย่อยหายไป หรือซ้ำซ้อน เสียหายระหว่างทาง ความผิดพลาดถูกส่งไป ปัญหานี้ถูกแก้ได้โดยมี host ที่ยอมรับแต่ละอันได้และทุก ๆ ข้อมูลย่อยได้

FIGURE 1.6 Transmitting segments with flow control



Note

การแปลงข้อมูลที่ไม่มีการสื่อสารก็จะอยู่บทที่ 2

การบริการพิจารณาการปรับการสื่อสารถ้ามันมีลักษณะดังนี้

- วงจรแนวดิ่งถูกตั้งขึ้น (ตัวอย่าง three-way handshake)
- ใช้ตามลำดับ
- ใช้การยอมรับ
- ใช้การควบคุมการไหล

Note

การควบคุมการไหลคือ buffering, windowing และการหลีกเลี่ยงการหนาแน่น

Windowing

จำนวนข้อมูลในครั้งหนึ่งที่เกิดขึ้นอย่างรวดเร็วและมีประสิทธิภาพและคุณก็สามารถจินตนาการได้มันควรจะช้าถ้าหากว่ากลไกการส่งข้อมูลต้องคอยการตอบรับภายหลังจากการส่งข้อมูลย่อยแต่ละครั้ง แต่เนื่องจากมีเวลาภายหลังการส่งข้อมูลย่อยและก่อนที่จะเสร็จกระบวนการและมีการยอมรับจากกลไกการรับข้อมูล ผู้ส่งใช้การแตกออกเหมือนกับโอกาสการส่งข้อมูลที่มากขึ้น จำนวนของข้อมูล (นับเป็นไบต์) ที่เหมือนการแปลงถูกยอมรับการส่งโดยปราศจากการรับการยอมรับ ซึ่งมันเรียกว่า Window

Note

Window เคยถูกใช้ควบคุมจำนวนสำคัญ การไม่ยอมรับข้อมูล

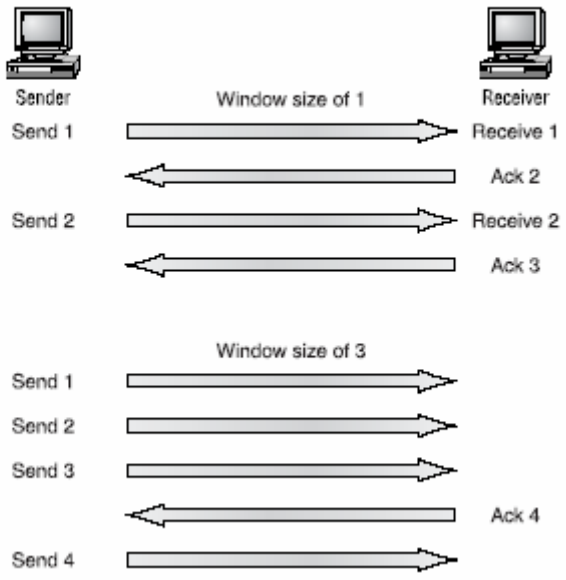
ดังนั้นขนาดของ window ควบคุมจำนวนข้อมูลที่มีการแปลงจากจุดจบหนึ่งไปสู่จุดอื่น ในขณะที่บาง protocol มีการบอกจำนวนข้อมูลโดยการสังเกตจำนวนข้อมูลที่ถูกแบ่งเป็นส่วน ๆ หรือการวัด TCP/IP โดยการนับจำนวนของไบต์

ดังที่เห็นในรูป 1.7 มีขนาด windows 2 ขนาด อันหนึ่งจัดไปที่ 1 และอีกอันจัดไปที่ 3 เมื่อคุณสร้างโครงสร้างขนาดของwindow ที่ 1แล้ว เครื่องส่งจะคอยการยอมรับสำหรับส่วนย่อยแต่ละข้อมูล มันส่งข้อมูลก่อนการส่งข้อมูลอีกส่วนหนึ่ง ถ้าคุณสร้างขนาดของ window ที่ 3 มันจะยอมให้มีการแปลงข้อมูลย่อย 3 ส่วนก่อนการยอมรับจะตอบรับ ในตัวอย่างพิเศษ ทั้งกลไกการส่งและการรับอยู่ที่สถานที่ทำงาน ในความเป็นจริงแล้วตัวอย่างนี้จะหาได้อยาก เพราะว่าส่วนใหญ่แล้วการยอมรับและการแบ่งข้อมูลเป็นส่วน ๆ จะเกิดปนกันเหมือนกับการท่องไปบน neywork และผ่านไปบน router

Note

ถ้าTCP session ถูกset up กับ window ขนาด 2 ไบต์ และระหว่างการเปลี่ยนขนาด window เปลี่ยนจาก 2ไบต์ เป็น 3 ไบต์ การส่ง host ต้องแปลงให้เป็น 3 ไบต์ก่อนการยอมรับแทนของเดิมที่เป็น 2 ไบต์ที่สร้างวงจร

FIGURE 1.7 Windowing



Acknowledgements

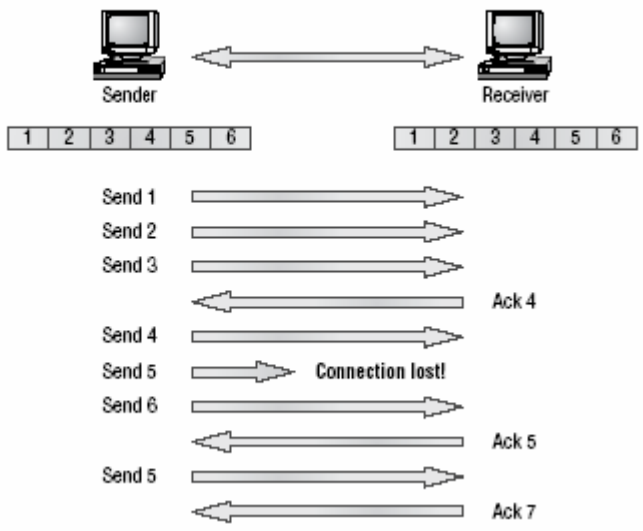
การส่งข้อมูลที่น่าเชื่อถือทำให้มั่นใจในกลุ่มของข้อมูลที่ส่งจากเครื่องหนึ่งไปสู่อีกเครื่องหนึ่งโดยเชื่อมโยงข้อมูลอย่างเต็มตามหน้าที่ มันเป็นสิ่งที่รับประกันได้ว่าข้อมูลจะไม่ซ้ำซ้อนหรือสูญหาย นี่ก็เป็นสิ่งสำเร็จที่เรียกว่า Positive acknowledgement with retransmission ซึ่งเป็นเทคนิคที่ต้องการกลไกการสื่อสารกับแหล่งการส่งข้อมูลส่งข้อความที่ผ่านการยอมรับกลับมาสู่ผู้ส่งเมื่อกลไกนั้นได้รับข้อมูล ผู้ส่งข้อมูลแต่ละหน่วยจะส่งและคอยการตอบรับก่อนการส่งหน่วยต่อไป เมื่อมีการส่งข้อมูลหน่วยหนึ่ง กลไกการส่งต่อจะเริ่ม เครื่องจับเวลาและการส่งซ้ำ ถ้ามันหมดเวลาก่อนการตอบรับ ก็จะถูกส่งกลับจากการสิ้นสุดการรับ

ในรูป 1.8 กลไกการส่งจะส่งจากหน่วยที่ 1 ไป 2 และต่อไปที่ 3 จุดที่จะยอมรับข้อมูลก็จะเป็นที่หน่วยที่ 4 เมื่อได้รับการตอบรับ ผู้ส่งก็จะส่งต่อไปที่ 4,5 และส่งต่อไปที่ 6 ถ้าหน่วยที่ 5 ไม่ทำงานไปจนถึงที่สุด จุดที่ตอบรับนั้นก็ยอมรับว่าเหตุการณ์ที่เกิดขึ้นกับการเรียกร้องนั้นจะต้องส่งใหม่อีกครั้ง กลไกการส่งก็จะส่งข้อมูลที่หายไปอีกครั้งและรอการตอบรับที่มันจะต้องรับคำสั่งเพื่อส่งต่อการส่งไปที่หน่วยที่ 7

The Network Layer

Network Layer (หรือที่เรียกว่า layer 3) จัดการเรื่อง Address หรือกำหนดที่อยู่ของการทำงานบน network ตัดสินใจว่าทางใดเป็นทางที่ดีที่สุดที่จะใช้ย้ายข้อมูลซึ่งหมายความว่า network Layer ต้องมีการขนส่งข้อมูลระหว่างการใช้งานที่เข้าไปไม่ผูกติดกับพื้นที่ router (หลักการlayer 3) เป็นการชี้เฉพาะ layer ของ network เตรียมการบริการ network ภายใน internetwork

FIGURE 1.8 Transport layer reliable delivery



มันเกิดขึ้นดังนี้ ขั้นแรกเมื่อข้อมูลที่ถูกแบ่งเป็นส่วนย่อยได้รับบนการติดต่อของ router ปลายทางของ IP addressก็จะถูกตรวจ ถ้าข้อมูลที่ถูกแบ่งไม่ได้ถูกกำหนดจุดสำหรับ router ที่เฉพาะอัน มันก็จะค้นหาจุดหมายปลายทางของ network address ที่ตารางของ router หากว่า router ออกจากการติดต่อสื่อสารข้อมูลที่แบ่งเป็นส่วน ๆ ก็จะถูกส่งไปที่การติดต่อเพื่อที่จะถูกสร้างและส่งออกไปที่พื้นที่ของ network ถ้า router ไม่สามารถหาทางเข้าสำหรับปลายทางของข้อมูล network ในตารางเส้นทาง router ก็ปล่อยข้อมูลนั้น

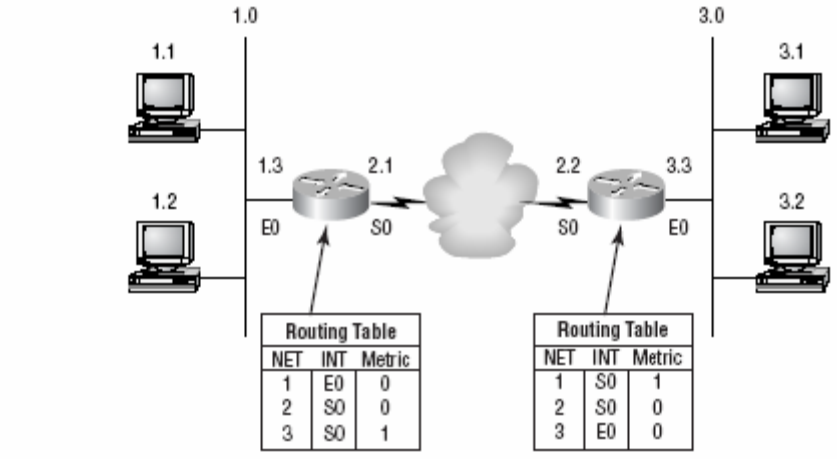
ข้อมูลที่ถูกแบ่ง 2 ประเภทที่ถูกใช้ใน network layer นั่นก็คือ ข้อมูลและเส้นทางล่าสุดData packets จะถูกใช้ขนส่งข้อมูลของผู้ใช้งานไปสู่ internetwork protocol ถูกใช้สนับสนุนช่องทางของข้อมูลที่เรียกว่า router protocols ตัวอย่างเช่น IP กับ IPX คุณจะได้เรียนรู้เกี่ยวกับ IP address ในบทที่ 2 และบทที่ 3 (IP Subnetting and Variable Length Subnet Masks (VLSMs)

Router update packets ใช้ update routers ข้างเคียงที่เกี่ยวกับการเชื่อมต่อกับ network ไปสู่ router ทั้งหมดภายใน internetwork protocol ที่ส่งข้อมูลที่แบ่งเป็นส่วน ๆ นั้นเรียกว่า routing protocol ตัวอย่างก็คือ RIP, EIGRP และ OSPF ข้อมูลของเส้นทางล่าสุดเคยช่วยสร้างและซ่อมแซมเส้นทางตารางที่แต่ละ routers

ในรูปที่ 1.9 จะให้ตัวอย่างของ Routing table ส่วน routing table ใช้ใน routers ได้รวมข้อมูลดังด้านล่างนี้

Network address Protocol-specific network address routers ต้องซ่อมแซม routing table สำหรับ routing protocol เดียว เพราะว่าแต่ละ routing protocol จะเก็บแนวทางของ network กับการตั้ง address ที่ต่างกัน ซึ่งก็เหมือนกับป้ายถนนที่ต่างภาษาพูดกันโดยที่อยู่ที่อาศัยก็อยู่บนถนนเดียวกัน ดังนั้นถ้าจะมีวิถีของชาวอเมริกา สเปน และฝรั่งเศส บนถนนที่ชื่อว่า CAT สัญลักษณ์ที่อ่าน ก็เป็น CAT/GATO/CHAT

FIGURE 1.9 Routing table used in a router

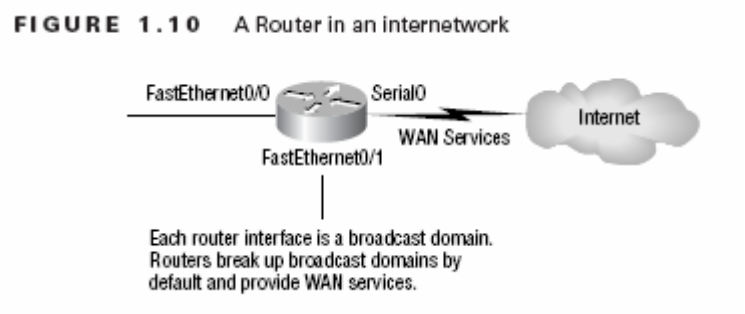


Interface ทางออกของข้อมูลจะถูส่งออกไปเมื่อปลายทางได้กำหนดข้อมูลของการติดต่อไปยัง Interface แล้ว

Metric ระยะทางที่ไปถึง network ที่อยู่ไกล routing protocol ที่แตกต่างกันใช้เป็นวิธีการที่แตกต่างกันของการคำนวณระยะทาง ตอนนี้ก็จะพูดถึง routing protocol ที่อยู่ในบทที่ 5 routing protocol บางตัวใช้บางสิ่งที่เรียกว่า hop count (ข้อมูลของจำนวน routers ส่งผ่านไปตลอดเส้นทาง network) ในขณะที่ส่วนอื่นใช้ bandwidth delay of the line หรือแม้การทำเครื่องหมายตอนนับ (1/18ต่อวินาที)

ดังที่ได้กล่าวไว้ข้างต้น router แตกการกระจายของโดเมนที่ไม่เป็นรูปแบบ การส่งข้อมูลจะไม่ส่งต่อไปยัง routers ยังจำได้ไหมว่าทำไมถึงเป็นสิ่งดีที่ routers ต่างๆ ยังคงแตกการชนปะทะของโดเมน แต่ว่าก็สามารถใช้ใน layer 2 (Data Link Layer) switches เนื่องจากว่าการติดต่อแต่ละครั้งใน routerได้แสดงการแยกของ network มันต้องกำหนดลักษณะพิเศษของ network และแต่ละhostบน network จะต้องเชื่อมต่อกับ router ที่เป็น router หมายเลขเดียวกัน รูปที่ 1.10 แสดงให้เห็นถึงว่า router ทำอย่างไรใน internetwork

FIGURE 1.10 A Router in an internetwork



นี่เป็นจุดประสงค์บางอย่างที่เกี่ยวกับ router ที่ควรจะจดจำ

- router จะไม่ส่งการกระจายใด ๆ หรือmulticast packet
- router ใช้ Logical address ใน network layer เป็นตัวนำไปสู่การตัดสินใจของ hop router ตัวต่อไปเพื่อที่จะส่ง ข้อมูลที่แบ่งเป็นส่วน ๆ ไปให้
- router สามารถใช้ access lists ที่สร้างโดย administrator ที่จะควบคุมความปลอดภัยบนลักษณะต่าง ๆ ของข้อมูลที่แบ่งเป็นส่วน ๆ ที่ยินยอมให้เข้าออกในการสื่อสาร
- router สามารถเตรียม layer 2 ที่นำไปสู่หน้าที่ถ้าจำเป็นและสร้างเส้นทางที่เหมือจริงตลอดการติดต่อสื่อสารเดียวกัน
- หลักการของ layer 3 (router ในกรณีนี้) สามารถทำให้เกิดการสื่อสารระหว่าง LANs จริง (VLANs)
- router สามารถทำให้เกิดการบริการที่มีคุณภาพ (QoS) สำหรับประเภทพิเศษต่าง ๆ ของการเดินทางของ network

Note

Switching กับ VLANs มีอยู่ในบทที่ 7 (layer 2 switching) และ บทที่ 8

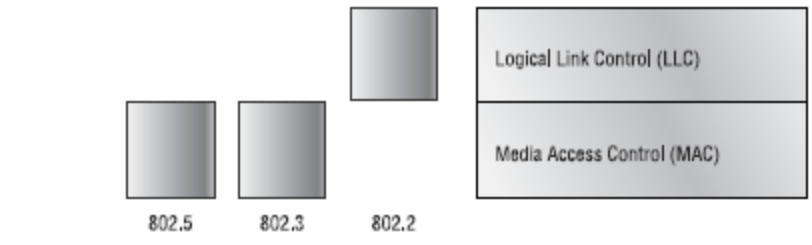
The Data Link Layer

Data Link Layer ทำให้เกิดการส่งข้อมูลที่เป็นรูปร่างและจัดการกับการแจ้งเตือนว่า Error, network topology, และ การควบคุมการไหล นี่หมายความว่า data link layer สามารถทำให้มั่นใจว่าข้อความจะถูกส่งไปยังที่ที่เหมาะสมบน LAN ที่ใช้ hardware address และแปลงข้อความจาก network layer ภายในบิตสำหรับ Physical Layer เพื่อส่งต่อ

Data link layer จัดเก็บข้อความเป็นส่วน ๆ แต่ละส่วนเรียกว่า data frame และเพิ่มการแก้ไขตามคำสั่งของ header ที่มีจุดสิ้นจุดของ hardware และที่มาของ address สิ่งนี้ได้เพิ่มข้อมูลที่สร้างรูปแบบจากลักษณะของ capsule ที่ห้อมล้อมข้อความเดิมในจำนวนมากวิธีการเดียวกันที่กลไกต่างๆหรือหลักการชี้นำและเครื่องมือต่าง ๆ ที่ติดกับหน่วยวัดของดวงจันทร์ที่โครงการ Apollo ได้กำหนดไว้ ชิ้นต่าง ๆ ของอุปกรณ์เหล่านี้เป็นประโยชน์เพียงระหว่างตำแหน่งที่ของระยะที่แน่นอนกับหน่วยวัดที่ถูกเอาออกและถูกปฏิเสธเมื่อระยะที่ถูกกำหนดนั้นสมบูรณ์ การเดินทางของข้อมูลไปยัง network นั้นก็เหมือนกัน

รูป 1.11 นั้นแสดงให้เห็นData Link Layer กับ Ethernet และIEEE ที่เฉพาะเจาะจง เมื่อคุณตรวจสอบจะสังเกตเห็นว่ามาตรฐานของ IEEE 802.2 ถูกใช้เพื่อเชื่อมและเพิ่มบทบาทต่อมาตรฐาน IEEE ตัวอื่น

FIGURE 1.11 Data Link layer



มันเป็นสิ่งสำคัญที่จะต้องเข้าใจว่า router ที่ทำงานกับ Network Laye rจะไม่สนใจตำแหน่งเฉพาะของ host ทั้งหมดทั้งปวง routerจะไม่เกี่ยวข้องเพียงตำแหน่งของ network และเป็นวิธีที่ดีที่สุดที่จะเข้าถึง

network ซึ่งรวมทั้ง network ที่อยู่ไกล ๆ ด้วย routerเป็นสิ่งที่มีอยู่ตลอดเมื่อเข้าไปยัง network มันเป็นสิ่งที่ดีที่ Data Link Layer มีหน้าที่ชี้ภาพรวมแต่ละหลักการที่อยู่ในพื้นที่ของ network

สำหรับ host ที่ส่งข้อมูลเป็นส่วนๆ ไปยัง host ต่าง ๆ ที่เป็นส่วนตัว บน local network ที่ดีพอ ๆ กับการส่งข้อมูลระหว่าง router ที่ Data Link Layer ใช้ hardware addressing แต่ละครั้งที่ข้อมูลที่เป็นส่วน ๆ ถูกส่งระหว่าง router มันจะประกอบกับการควบคุมข้อมูลที่ Data Link Layer แต่ข้อมูลนั้นจะถูกถอดออกที่ router ที่ใช้รับและมีเพียงข้อมูลเดิมที่แบ่งเป็นส่วน ๆ ก็จะถูกเอาออกโดยไม่มีการเปลี่ยนแปลงใด ๆ ทั้งหมด การกำหนดข้อมูลที่แบ่งเป็นส่วน ๆ นั้นจะมีต่อไปแต่ละ hop จนกระทั่งมีการส่งข้อมูลนั้นครั้งสุดท้ายไปยัง host ที่ใช้รับอย่างถูกต้อง มันค่อนข้างที่สำคัญที่จะเข้าใจว่าตัว packet ไม่ทางเลือก router ได้ มันได้แต่ถูกห่อหุ้มด้วยประเภทของความต้องการควบคุมข้อมูลเพื่อที่จะถูกส่งต่อไปอย่างเหมาะสมกับสื่อชนิดต่าง ๆ ที่แตกต่างกัน

IEEE Ethernet มี layer ย่อย ๆ อีกสอง layer

Media Access Control (Mac) 802.3 บอกถึงวิธีการที่ packet จะเข้าไปแทนที่ การแย่งการเข้า network คือ “first come/ first served” (มาก่อนได้ก่อน) การเข้าไปที่ทุกคนสามารถใช้ bandwidth เดียวกันได้ ตามชื่อของมัน Physical addressing กำหนดไว้ที่ Media Access Control ซึ่งดีพอๆ กับ Logical topologies Logical topology คือ เป็นวิธีการของสัญลักษณ์ที่ส่งไปยัง physical topology

Line discipline, การแจ้ง error (not correction) , คำสั่งการส่งของระบบ และทางเลือก flow control ที่สามารถถูกใช้ใน layer ย่อยนี้ได้

Logical Link Control (LLC) 802.2 มีหน้าที่ชี้เฉพาะ Network Layer protocols และห่อหุ้มพวกนั้นไว้ LLC header บอก Data Link layer ถึงสิ่งที่ต้องทำต่อ packet ของโครงสร้างหนึ่งที่ได้รับ มันทำงานดังนี้ host จะรับโครงสร้างและมองใน LLC header เพื่อที่จะหาที่ที่ packet ถูกกำหนดเอาไว้ หรือที่จะพูดว่า IP protocol ที่ Network layer LLC สามารถที่จะทำเกิด flow control และ การเรียงตามลำดับของ control bits.

Switches และ bridges ที่พูดตอนต้น ๆ ของบท ทั้งการทำงานของ Data Link layer และ filter Network ที่ใช้ hardware(MAC) address เราจะค้นหาสิ่งเหล่านี้ในsection ด้านล่างนี้

Switches and Bridges at Data Link layer

Layer 2 switching ประกอบไปด้วย hardware-based bridge เนื่องจากว่ามันใช้ hardware พิเศษที่เรียกว่า application-specific integrated circuit (ASIC) ส่วน ASICs สามารถที่จะ run up เข้าสู่ gigabit speedsด้วยอัตรา latency ที่ต่ำ

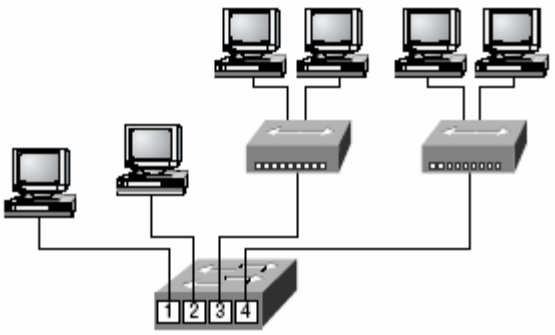
Note

Latency คือ การนับระยะเวลาตั้งแต่ frame เข้าสู่ portไปจนถึงออกจาก port

Bridges กับ switches อ่านแต่ละ frame เหมือนกับว่ามันผ่านไปที่ network วิธีการใช้ layer 2 ใส่แหล่ง hardware address ใน filter table และเก็บ รอยของจับ frame ที่ได้รับ ข้อมูลนี้ (เข้าไปใน filter table ของ bridges หรือ switch) ช่วยให้เครื่องได้เลือกตำแหน่งของกลไกการส่งที่พิเศษ

รูป 1.12 แสดง Switch ใน internetwork

FIGURE 1.12 A switch in an internetwork



Each segment has its own collision domain.
All segments are in the same broadcast domain.

ในธุรกิจอสังหาริมทรัพย์นั้นทั้งหมดเกี่ยวกับที่ตั้ง ทำเล ซึ่งมันก็เหมือนกับ หลักการของ layer 2 กับ layer 3 ดังนั้นทั้งคู่จะต้องสามารถตกลงกับ network ได้ มันเป็นสิ่งที่ต้องจำให้ได้ว่าที่ตั้งทำเลนั้นเกี่ยวข้องกับส่วนต่าง ๆ ของมัน โดยเบื้องต้นแล้ว กลไกที่ layer 3 (ตัวอย่างเช่น router) จำเป็นต้องหาที่ตั้งของ network เฉพาะที่ ในทางตรงกันข้ามกลไกของ layer 2 (switch and bridges) จำเป็นต้องหาที่ตั้งของกลไกพิเศษในตอนท้าย ดังนั้น network พวกนั้นต้องมี router เหมือนกับอุปกรณ์เฉพาะตัว ที่ต้องเป็น switches กับ bridges และ routing table ที่เป็น แผนที่ network สำหรับ router ก็เหมือนกับ filter table ที่เป็นแผนที่เฉพาะเจาะจงว่าจะต้องใช้งานกับ switches กับ bridges

หลังจากที่ filter table ถูกสร้างขึ้นในกลไก layer 2 มันจะเป็นเพียงการส่ง frame ต่อไปยัง segment ที่ที่ปลายทาง hardware address ที่ถูกกำหนดไว้ ถ้าปลายทางนั้นอยู่บนframe หรือ segment เดียวกัน Layer 2 จะบล็อก frame จากการไปสู่ segment อื่น ๆ ถ้าปลายทางนั้นอยู่บน segment ที่ต่างกัน frame สามารถส่งไปสู่ segment นั้นได้ สิ่งนี้เรียกว่า transparent bridging

เมื่อ interface ของ switch ได้รับ frame กับปลายทางของ hardware address ที่ไม่ได้ถูกพบในกลไกของ filter table มันจะส่ง frame ไปยัง segment ทั้งหมดที่เชื่อมต่อไว้ ถ้าเป็นกลไกที่ไม่รู้จักมันก็จะตอบเป็น mystery frame ในการส่งครั้งนี้ Switch จะ update filter table ความสัมพันธ์กับที่ตั้งของกลไก

นั้น แต่ในกรณีของปลายทาง address ของการส่ง frame เป็นการกระจาย address Switch จะส่งการกระจายทั้งหมดสู่ segment ที่เชื่อมต่อเอาไว้ทุกอันอย่างไม่เป็นรูปแบบ

ทุกกลไกที่ได้กระจายนั้นถูกส่งต่อไปยังการกระจายโดเมนเดียวกันที่ถูกพิจารณาไว้ ซึ่งอาจเกิดปัญหาได้คือ กลไกของ Layer 2 จะเพิ่ม broadcast storm ของ layer 2 ที่ทำให้เกิดการกระตุก และวิธีเดียวที่จะหยุด broadcast storm จากการเพิ่มภายใน internetwork ต้องเป็นกลไก layer 3 หรือที่เรียกว่า router

ข้อดีของการใช้ Switch แทน hubsใน internetwork คือ Switch port แต่ละตัวเป็นกันชนป้องกันการปะทะของโดเมนกันเองอย่างแน่นอน (ในทางตรงกันข้าม hubsสร้างการชนปะทะของโดเมนครั้งใหญ่) แต่ว่ามีการป้องกันกับ switch แต่ว่าคุณยังคงไม่สามารถยับยั้ง broadcast domaims ของข้อมูลได้ และทั้ง switches และ bridgesก็ไม่สามารถทำได้เช่นเดียวกัน Switchจะส่งต่อไปในรูปแบบธรรมดาสู่ broadcast ทั้งหมดแทน

ข้อดีของอีกข้อของLAN switching เหนืออุปกรณ์ตรงกลางของ hubs คือกลไกบน segment ทุกตัวเสียบเข้าไปใน switch ที่สามารถลอกเลียนแบบการส่งต่อได้ อย่างน้อยที่สุดนานเท่านานที่ LAN switching จะทำได้ มีเพียง host ตัวเดียวบนแต่ละ port และ hub ที่ไม่ได้เสียบไปใน Switch port ก็อย่างที่คุณเดา hubยอมให้หนึ่งกลไกต่อ network segment ทำการติดต่อสื่อสารได้ในเวลานั้น

แต่ละ network Segment ที่เชื่อมต่อไปยัง switch ที่ต้องมีประเภทที่เป็นของกลไกเดียวกัน สิ่งนี้มีความหมายกับคุณและฉันคือว่า คุณสามารถเชื่อมต่อ Ethernet hub ภายใน switch port และสามารถติดต่อ Ethernet hosts ใน hub ได้หลายเท่า แต่ว่าไม่สามารถผสม Token Ring hosts กับ กลุ่มEthernet ได้ใน segment เดียวกัน การผสม hosts เรียกว่า media translation และ Cisco พูดว่า คุณจะต้องมี router อยู่รอบ ถ้าหากคุณจำเป็นต้องมีการบริการนี้ แม้ว่าฉันจะพบว่าสิ่งนี้ไม่เป็นจริงในความเป็นจริง แต่จำไว้ว่าเรากำลังศึกษาข้อสอบของ CCNA อยู่นะ ถูกไหม

The Physical Layer

มาถึงตอนท้ายแล้ว เราพบว่า physical layer ทำสองสิ่ง คือจะส่ง bits และรับ bits Bitsจะมาเพียงค่า 1 หรือ 0 หรือว่าเป็นการนับแบบรหัสมอส Physical layer เชื่อมโยงโดยตรงกับประเภทต่าง ๆ ของการติดต่อสื่อสารอย่างเป็นจริง การสื่อสารที่ต่างชนิดกันแสดงค่าของ bits เหล่านี้ในวิธีที่แตกต่างกัน บางครั้งอาจใช้ audio tone ในขณะที่ส่วนอื่น ๆ ใช้ state transitions เปลี่ยนจากโวลต์ที่สูงเป็นต่ำและ ต่ำไปเป็นสูง protocol พิเศษถูกใช้สำหรับการสื่อสารแต่ละประเภทเพื่ออธิบายรูปแบบ bit ที่เหมาะสมที่ถูกใช้งาน วิธีที่

ข้อมูลถูกใส่รหัสในการส่งสัญญาณการสื่อสาร และคุณภาพที่หลากหลายของพื้นผิวของรูปร่างอุปกรณ์การสื่อสาร

Physical layer ระบุเรื่อง กระแสไฟ กลไก วิธีการปฏิบัติ การต้องการหน้าที่ปฏิบัติสำหรับการปฏิบัติ ซ่อมแซม และการลด physical link ระหว่างระบบ และ layer นี้จะอยู่ในที่ที่ระบุการเชื่อมต่อไว้ระหว่าง data terminal equipment (DTE) กับ data communication equipment (DCE) บริษัทโทรศัพท์เก่า ๆ บางบริษัทยังคงใช้ การโทรแบบ DCE data อุปกรณ์ circuit-terminating
DCE จะอยู่ในที่ที่สามารถให้บริการได้เสมอ ในขณะที่ DTE จะติดอยู่กับกลไก การบริการของDTE ส่วนใหญ่ต้องเข้า modem หรือ channel service unit/data service unit (CSU/DSU)

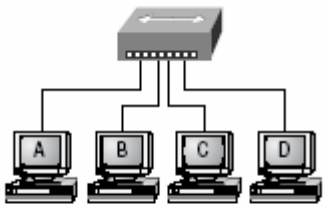
ตัวเชื่อมของ Physical layer และ physical topology ที่แตกต่างกัน ที่ระบุโดย OSI ที่เหมือนกับเป็นมาตรฐานที่ยินยอมให้แยกระบบเพื่อการสื่อสาร CCNA สนใจเพียงแค่มาตรฐานของ IEEE Ethernet

Hubs at The Physical Layer

Hub เป็นตัวทำซ้ำ multiple-port อย่างแท้จริง Repeater ได้รับสัญญาณแบบดิจิตอลและขยายความถี่ซ้ำหรือทำให้เกิดสัญญาณใหม่ และเมื่อส่งต่อสัญญาณดิจิตอลออกไป portทุกตัวที่ทำงานโดยปราศจากการค้นหาข้อมูลใด ๆ hub ที่ทำงานก็ทำหน้าที่เหมือนกัน สัญญาณดิจิตอลใด ๆ จาก segment บน port ของ hub ที่เกิดใหม่หรือขยายความถี่ซ้ำและส่งออกไปยัง port ทุกตัวบน hub สิ่งนี้มันหมายความว่ากลไกทุกตัวเสียบเข้าไปที่ hub ที่อยู่ในการชนปะทะโดเมนเดียวกันที่ดีพอ ๆ กันกับการกระจายโดเมนเดียวกัน รูป 1.13 แสดง hub ใน network

Hub ก็เหมือนกับตัวทำซ้ำไม่ได้ตรวจสอบการเดินทางเหมือนกับตอนที่มันเข้าแล้วก็ตอนที่มันส่งต่อข้อมูลออกไปยัง ports ตัวอื่น ๆ ของ physical media กลไกทุกตัวเชื่อมต่อไปยัง hub หรือ hubs หลาย ๆ ตัว ที่ต้องได้ยินถ้ากลไกได้รับการส่งต่อ Physical Star Network ที่ hub เป็นศูนย์กลางและขยาย cable ต่าง ๆ ไปยังทุกทิศทุกทางจากตัวมัน ที่เป็นประเภทของ topology ที่ hub สร้างขึ้น การออกแบบอย่างแท้จริงแล้วทำโดยการสุ่ม star ในขณะที่ Ethernet network ดำเนินการ logical bus topology ที่หมายความว่าสัญญาณต้องวิ่งจากจุดปลายหนึ่งไปสู่อีกจุดปลายหนึ่งของ network

FIGURE 1.13 A hub in a network



All devices in the same collision domain
All devices in the same broadcast domain
Devices share the same bandwidth

Ethernet Networking

Ethernet คือการเชื่อมต่อการสื่อสารที่เข้าโดยวิธีการยอมให้ host ทุกตัวบน network แบ่ง bandwidth เดียวกันของการเชื่อมโยงกัน Ethernet เป็นที่นิยมเนื่องจากมันสามารถอ่านสเกล ซึ่งหมายความว่ามันสามารถเปรียบเทียบอย่างง่าย ๆกับการรวมตัวเทคโนโลยีใหม่อย่างเช่น Fast Ethernet และ Gigabit Ethernet ภายในพื้นฐานของ network ที่ยังคงอยู่ มันเป็นการง่ายอย่างความสัมพันธ์ต่อการทำให้เกิดผลในที่แรกและกับมัน การแก้ปัญหาอย่างตรงไปตรงมาที่สมเหตุสมผล Ethernet ใช้ทั้ง Data Link และ Physical Layer พิเศษ และในบทนี้จะข้อมูล Data Link และ Physical Layer ที่จำเป็นต่อการดำเนินการให้เป็นผลการแก้ปัญหาและการซ่อมแซม Ethernet network

การทำงานของ Ethernet ใช้ Carrier Sense Multiple with Collision Detection (CSMA/CD) protocol ที่ช่วยกลไกต่าง ๆ ที่ใช้ bandwidth ร่วมกันโดยที่ไม่มีกลไก 2 ตัวที่ส่งข้อมูลในเวลาเดียวกันบน network กลาง CSMA/CD ถูกสร้างเพื่อเอาชนะปัญหาของการชนปะทะเหล่านั้นที่เกิดขึ้นเมื่อ packet ต่าง ๆ เสมือนว่าถูกส่งต่อจากการขยายตลอดทั้ง network

ดังนั้น CSMA/CD protocol ทำงานดังนี้ เมื่อ host ต้องการแปลงข้อมูลไปทั้งหมดของ network มันเป็นการตรวจสอบครั้งแรกกับการแสดงของสัญญาณดิจิตอลในการสื่อสาร ถ้าทั้งหมดนี้มันไม่มีอะไรเกิดขึ้น (ไม่มีการแปลงข้อมูลของ host) Host ก็จะทำการแปลงข้อมูลด้วยตัวมันเอง แต่ว่าจะไม่หยุดที่ตรงนั้น การแปลงของ host ควบคุมการสื่อสารอย่างต่อเนื่องเพื่อทำให้แน่ใจว่าจะไม่มี host ตัวอื่นเริ่มการแปลงข้อมูล ถ้า host ค้นหาสัญญาณตัวอื่นบนการสื่อสาร มันจะส่งการกระจายสัญญาณเข้าไปแทรกซึ่งเป็นสาเหตุให้จุดบน segment หยุดการส่งข้อมูล (คิดว่าสัญญาณไม่ว่าง) จุดต่าง ๆ จะตอบรับการเข้าแทรกของสัญญาณโดยการรอก่อนที่จะพยายามส่งต่อสัญญาณอีกครั้ง การกำหนดการหลีกเลี่ยง algorithms เมื่อมีการปะทะกันของฐานต่าง ๆ ที่สามารถส่งต่อได้อีกครั้ง ถ้าการชนปะทะยังคงเกิดขึ้นได้หลังจากการพยายาม 15 ครั้ง จุดต่าง ๆ ก็จะพยายามส่งต่อแล้วเวลาก็จะหมดไป ค่อนข้างจะเรียบร้อย

เมื่อมีการชนปะทะเกิดขึ้นบน Ethernet

- การเข้าแทรกของสัญญาณบอกให้ทราบว่ากลไกต่าง ๆ ที่ชนปะทะได้เกิดขึ้น
- การชนปะทะสัมพันธ์กับการสุ่มการหลีกเลี่ยง algorithms
- แต่ละหลักการของ Ethernet segment หยุดการส่งต่อสำหรับช่วงเวลาสั้นจนกระทั่งหมดเวลา

ผลกระทบของการมี CSMA/CD network ที่มีการสนับสนุนการชนปะทะอย่างหนัก

- การล่าช้า
- Low thoughput
- การบีบอัด

Note

Backoff on 802.2 network คือความล่าช้าการส่งข้อมูลซ้ำที่ถูกให้ทำตามเมื่อมีการชนปะทะเกิดขึ้น เมื่อการชนปะทะเกิดขึ้น host ก็จะเริ่มต้นการส่งใหม่ภายหลังเวลาที่กำหนดการล่าช้าหมดลง

ในsection ต่าง ๆ ก็จะพูดถึงรายละเอียดของ Ethernet ทั้ง Data Link layer (layer 2) และ Physical Layer (layer 1)

Half – and full – Duplex Ethernet

Half Duplex Ethernet คือ การระบุลงใน Ethernet ดั้งเดิม 802.2 Cisco พูดว่า ใช้สายไฟเพียงหนึ่งคู่กับสัญญาณดิจิตอลที่วิ่งอยู่ both directions on the wire อย่างแน่นอนการชี้เฉพาะของ IEEE อธิบายกระบวนการของ half-duplex ในบางสิ่งที่อย่างแตกต่างกัน แต่สิ่งที่ Cisco พูดถึงเกี่ยวกับความรู้สึกทั่วไปของสิ่งที่เกิดขึ้นที่นี่กับ Ethernet

มันใช้ CSMA/CD protocol เพื่อช่วยป้องกันการชนปะทะและยอมให้มีการส่งต่อถ้ามีการเกิดการปะทะเกิดขึ้น ถ้า hub ถูกติดกับ switch ถ้าต้องจัดการในส่วนของ half-duplex เพราะตอนท้ายของสถานีต้องสามารถสืบหาการชนปะทะได้ Half-duplex Ethernet ตัวอย่าง 10 BaseT มีผลเพียงประมาณ 30 หรือ 40 เปอร์เซ็นต์ อย่างที่ Cisco เข้าใจ 10 BaseT network จำนวนใหญ่จะให้คุณอย่างปกติก็เพียง 3-4 Mbps เป็นอย่างมากสุด

แต่ว่า Full-duplex Ethernet ใช้สายไฟสองคู่แทนหนึ่งคู่แบบ half-duplex Ethernet และ full duplex ใช้การเชื่อมต่อจากจุดไปหาจุด ระหว่างตัวส่งของกลไกการส่งและตัวรับของกลไกการรับ สิ่งนี้มันหมายความว่ากับตัวการแปลง full-duplex data คุณจะได้รับข้อมูลที่เร็วขึ้นย้ายการเปรียบเทียบไปยัง half-duplex และเนื่องจากการส่งข้อมูลถูกส่งบนชุดของสายไฟที่แตกต่างกันมากกว่าได้รับข้อมูล ไม่มีการชนปะทะกันจะเกิดขึ้น

เหตุผลที่คุณจะไม่ต้องกังวลเรื่องการชนปะทะก็เพราะว่าตอนนี้มันเหมือนกับ freeway กับช่องทางที่เพิ่มอย่างทวีคูณแทนที่จะเป็นช่องทางเดียวที่ทำให้เกิดขึ้นโดย half-duplex Full-duplex Ethernet ถูกคาดว่าจะเสนอให้มีผล 100 เปอร์เซ็นต์ in both directions ตัวอย่างเช่น คุณสามารถได้รับ 20 Mbps กับ 10 Mbps Ethernet ที่ running full-duplex หรือ 200 Mbps สำหรับ Fast Ethernet แต่ว่าอัตรานี้เป็นบางสิ่งที่ทำให้รู้ว่าเหมือนกับรวบรวมอัตราที่เปลี่ยนดังเช่นที่คุณคาดว่าจะได้รับผล 100 เปอร์เซ็นต์ ไม่มีการรับรองว่า ในการทำงานของ internetwork เหมือนกับการมีชีวิต

Note

Full duplex Ethernet ต้องการการเชื่อมต่อจากจุดไปสู่จุดเมื่อมีเพียงสองจุดที่ถูกแสดง คุณต้องrun full-duplex กับ กลไกใด ๆ ที่ยอมรับ hub

Full-duplex Ethernet สามารถใช้ได้ใน 3 สถานการณ์ดังนี้

- การเชื่อมต่อจาก Switch ไปสู่ host
- การเชื่อมต่อจาก Switch ไปหา Switch
- การเชื่อมต่อจาก host ไปหา host โดย cable เป็นสะพาน

ถ้ามันเป็นเรื่องความสามารถของความเร็ว เมื่อ full-duplex Ethernet port ถูกเปิด switch เป็นลำดับแรกที่ติดต่อไปยังจุดจบที่ระยะไกลแล้วต่อรองกับจุดจบอื่นของ Fast Ethernet Link นี่ถูกเรียกว่า auto-detect mechanism ส่วน mechanism เป็นการชี้ขาดบนประสิทธิภาพของการแลกเปลี่ยนที่ได้ตรวจสอบซึ่งถ้าสามารถ run ได้ที่ 10 หรือ 100 Mbps แล้วการตรวจสอบถ้าสามารถ run full duplex ได้ แต่ถ้าไม่สามารถ run full duplex ได้มันจะ run half duplex แทน

Note

จำไว้ว่าถ้า half duplex Ethernet มีการแบ่งการชนปะทะโดเมนและทำให้จำนวนข้อมูลในครั้งหนึ่งมีประสิทธิภาพที่ต่ำกว่า Full duplex Ethernet ดังเช่นตัวอย่างมีการชนปะทะของโดเมนอย่างเฉพาะตัวและจำนวนข้อมูลในครั้งนั้นก็จะมีประสิทธิภาพที่สูงกว่า

Ethernet at The Data Link Layer

Ethernet at the Data Link Layer มีหน้าที่สำหรับ address Ethernet โดยทั่วไปแล้วอ้างถึง hardware addressing หรือ Mac addressing Ethernet มีหน้าที่ต่อ framing packet ด้วยซึ่งได้รับจาก Network Layer และการเตรียมที่จะส่งต่อไปบน local network และส่งไปเชื่อมต่อยังการสื่อสารของ Ethernet

มี 4 ประเภทที่แตกต่างกันของ Ethernet frame ที่หาได้

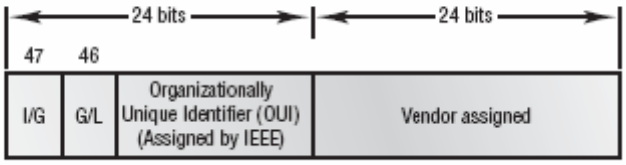
- Ethernet_II
- IEEE802.3
- IEEE802.2
- SNAP

จะขอข้าม 4 ประการด้านบนของ Ethernet frame ใน section ที่กำลังจะกล่าวถึง

Ethernet Addressing

เราจะเข้าสู่การทำงานของ Ethernet addressing มันใช้ Media Access Control (MAC) Address burned เข้าสู่แต่ละEthernet Network Interface Card (NIC)และ ทุกNIC MACหรือ hardware address เป็น 48-bit (6 byte) address ที่ถูกเขียนใน hexadecimal format
รูปที่ 1.14 แสดง 48-bit MAC address และ วิธีการแบ่ง bit ทำอย่างไร

FIGURE 1.14 Ethernet addressing using MAC addresses



Organizationally unique identifier (OUI) ถูกกำหนดโดย IEEE ต่อองค์กร ซึ่งถูกเขียนให้เป็น 24 bit หรือ 3 ไบต์ ในมุมกลับ องค์กรได้กำหนดที่อยู่ของ administer ทั่วโลก (24 บิต หรือ 3ไบต์)ที่รวบรวม (เป็นเพียงสมมติและไม่รับรองดังที่กล่าวมาแล้ว) แต่ละ adapter และ ทุก adapter ที่พวกเขาได้ผลิต ดูรูปอย่างละเอียด high-order bit เป็นบิตส่วนเดียวหรือบิตเป็นกลุ่ม (I/G) เมื่อมันมีค่าเป็น 0 เราสามารถเข้าใจได้ว่ามันเป็น address ของ MAC และมันจะแสดงตัวอย่างดีส่วนของ MAC header เมื่อมันมีค่าเป็น 1 เราก็เข้าใจได้ว่า address แสดงให้เห็นทั้ง การกระจายและ multicast ใน Ethernet หรือการกระจายหรือ functional address ใน TR และ FDDI (ใครรู้จัก FDDI บ้าง?) bit ถัดไปคือ G/L bit (หรือที่รู้จักกันว่า U/L ซึ่งU หมายถึง Universal) เมื่อตั้งค่าให้เป็น 0 bit ตัวนี้แสดงที่อยู่ของ administered ทั่วโลก(ตามอย่างของ IEEE) เมื่อบิตเป็น 1 มันก็แสดงให้เห็นถึงการปกครองท้องถิ่นและ administered address (เหมือนใน DECnet) คำสั่งที่ต่ำ 24 bit ของ Ethernet address แสดงถึง address ท้องถิ่น หรือการเข้ารหัสของโรงงาน โดยทั่วไปแล้วส่วนนี้จะเริ่มใน 24 0s สำหรับทำการ์ดแรกและทำตามคำสั่งต่อ ๆ ไปจนกระทั่งถึง 24 1sสำหรับการทำการ์ดสุดท้าย(16,777,216th) คุณจะพบว่าผู้ผลิตส่วนมากจะใช้ส่วนที่เหมือนกันเหล่านี้ 6 hex digits เหมือนกับ 6 ตัวสุดท้ายของserial number เหล่านั้นที่การ์ดเดียวกัน

Note

MAC addressesเป็นส่วนหนึ่งของ IPX/SPX configuration ของ host หรือจะเป็นก็ต่อเมื่อ IPX/SPXยังคงใช้อยู่อย่างแน่นอน

Ethernet Frame

Data Link layer มีหน้าที่ทำให้เกิดการรวมกันของ bits ใน bytes และ bytes ใน frame Frame ถูกใช้ใน data link layer เพื่อนำ Packet ห่อเข้าในแคปซูล ออกจาก Network Layer สำหรับการส่งต่อบน ตัวอย่างการเข้าของการสื่อสาร มี 3 ตัวอย่างของวิธีการเข้าการสื่อสาร คือ การแข่งขัน (Ethernet), การส่งผ่าน (ทำให้เป็น Ring and FDDI) และ polling (IBM mainframe and 100-VG anyLAN)

หน้าที่ของ Ethernet stations ต้องผ่าน data frame ระหว่างการใช้กลุ่มของ bit อื่น ๆ อย่างเช่น รูปแบบของ MAC frame สิ่งนี้จะทำให้เกิดการป้องการการเกิด error จาก cyclic redundancy check (CRC) แต่จำไว้ว่า การป้องกันการเกิด error นี้ ไม่ใช่ error ที่ถูกต้อง 802.3 frame และ Ethernet frame จะแสดงให้เห็นในรูป1.15

Note

การห่อแคปซูลของ frame ภายในประเภทที่ต่างกันของ frame ถูกเรียกว่า tunneling

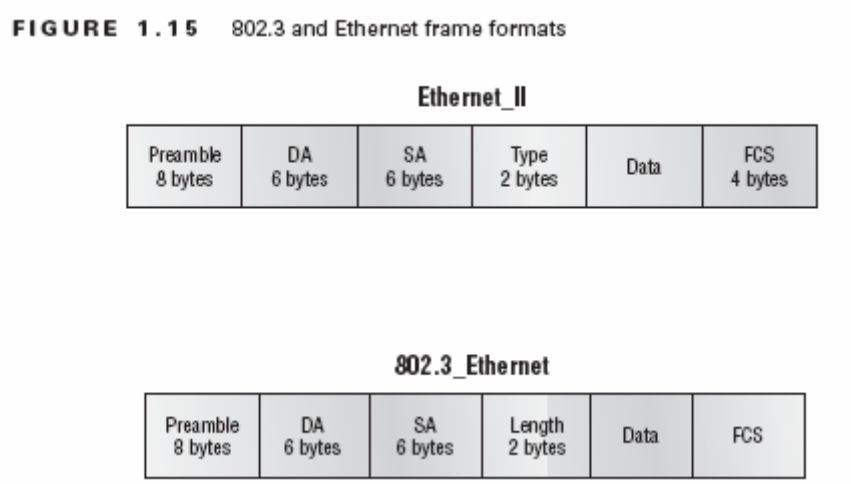
ตามรายละเอียดของสาขาที่แตกต่างกันของ 802.3 กับ Ethernet frame type

ทางเลือกรูปแบบ 1,0 ทำให้เกิด 5 MHz clock ที่จุดเริ่มของแต่ละ packet ที่ยอมให้มีการรับอุปกรณ์ที่จะ lock การมาของ bit stream

Start Frame Delimiter (SFD) /Synch บทนำมี 7 octets (กลอน 8) และ SFD มี 1 octet (synch)

SFD คือ 10101011 ที่คู่สุดท้ายเป็น 1 เพื่อให้ผู้รับได้เข้ามาสู่ทางเลือกรูปแบบ 1,0 บางทีมีที่ตรงกลาง และค้นหาจุดเริ่มต้นของข้อมูล

FIGURE 1.15 802.3 and Ethernet frame formats



Destination Address (DA) การใช้การส่งที่จำนวน 48-bit อย่างน้อยต้องเป็นบิตที่สำคัญ (LSB) ลำดับแรก DA ถูกใช้โดยการรับหน้าที่ต่าง ๆ เพื่อการตัดสินใจว่า Packet ที่เข้ามาถูกกำหนดที่อยู่ให้เป็นจุด

เฉพาะหรือไม่ destination address สามารถเป็น addressเดี่ยวได้ หรือ กระจายก็ได้ หรือจะเป็น multicast MAC address ก็ได้ จำไว้ว่าการกระจายทั้งหมดที่เป็น 1(หรือ Fs ใน hex)และถูกส่งไปยังอุปกรณ์ทั้งหมด แต่ว่า multicast ถูกส่งเพียง ส่วนย่อยที่คล้ายกันของจุดบน network

Note

Hex ก็คือ คำย่อของ hexadecimal ที่ถูกระบบนับจำนวนที่ใช้ จำนวนตัวอักษร 6 ตัวแรก(จาก A ถึง F) เพื่อขยายจำนวนที่มากกว่า 10 digits ในระบบของ decimal Hexadecimal มีทั้งหมด 16 digits

Source Address (SA) SAเป็น MAC address 48-bit ที่ใช้ระบุการส่งอุปกรณ์และใช้ LSB ก่อน รูปแบบ Broadcastและ Multicast address ผิดกฎภายใต้หลักของ SA

Length or Type 802.3 ใช้ ลักษณะของ Length แต่ Ethernet ใช้ลักษณะของ Type เพื่อใช้ระบุ Network layer protocol 802.3 ไม่สามารถระบุ layer ของ protocol ขั้นที่สูงกว่าได้และต้องถูกใช้กับคุณสมบัติของ LAN-IPX **ตัวอย่างเช่น**

ข้อมูล นี่เป็น packet ที่ถูกส่งลงไปสู่ Data Link layer จาก Network Layer ขนาดของมันมีหลากหลาย จาก 64 ถึง 1500 ไบต์

Frame Check Sequence (FCS) FCS เป็นหมวดหนึ่งตอนปลายของ Frame ที่ถูกใช้เก็บ CRC

หยุดตรงนี้พักหนึ่งเถอะ แล้วค้นหา frame ต่าง ๆ ที่จับอยู่บนการวิเคราะห์ Ether peek Network ที่น่าเชื่อถือ คุณสามารถเห็นได้ว่า frame ข้างล่างนี้ มีแค่ 3 ส่วน คือ destination source และ type (ถูกแสดงเหมือนกับ Protocol Type ในการวิเคราะห์นี้)

```
Destination:   00:60:f5:00:1f:27
Source:        00:60:f5:00:1f:2c
Protocol Type: 08-00 IP
```

นี่เป็น Ethernet_II frame สังเกตว่า หน่วยของตัวอย่างคือ IP หรือ 08-00 in hexadecimal Frame ถัดมามี field ต่างๆ ที่เหมือนกัน ดังนั้นมันจำเป็นที่ต้องเป็น Ethernet_II frame ด้วย

```
Destination:   ff:ff:ff:ff:ff:ff Ethernet Broadcast
Source:        02:07:01:22:de:a4
Protocol Type: 81-37 NetWare
```

ฉันสรุปส่วนนี้ดังนั้นคุณจะเห็นว่า frame สามารถมีได้มากกว่า IP มันสามารถมี IPX หรือ 8-31h. คุณสังเกตเห็นไหมว่า frame นี้ถูกกระจายออก คุณสามารถบอกได้เพราะว่า destination hardware address คือ 1 ทั้งหมด ในการจับคู่ หรือ เป็น Fs ทั้งหมด ใน hexadecimal

ตอนนี้มาให้ความสนใจเป็นพิเศษกับหน่วยของ Length ในframe ถัดไป สิ่งนี้ต้องเป็น 802.3 frame

```
Flags:          0x80 802.3
Status:         0x00
Packet Length: 64
Timestamp:      12:45:45.192000 06/26/1998
Destination:    ff:ff:ff:ff:ff:ff Ethernet Broadcast
Source:         08:00:11:07:57:28
Length:         34
```

ปัญหากับ frame นี้ คือ คุณจะรู้ได้อย่างไรว่า protocol ไหนที่ packet นี้กำลังจะถูกส่งไปยัง Network Layer มันไม่ได้ถูกระบุไว้ใน frame ดังนั้นมันต้องเป็น IPX ทำไมนะหรอ ก็เพราะว่าเมื่อ เนื้อหาถูกสร้างขึ้น ตัวอย่าง 802.3 frame (ก่อน IEEE จะทำและเรียกมันว่า 802.3 Raw) Novell is pretty much the only LAN server out there. ดังนั้น Novell จึงอ้างได้ว่าถ้าคุณกำลังให้ LAN ดำเนินการ มันจะต้องเป็น IPX มันไม่ได้รวมหน่วยข้อมูล Network Layer Protocol เข้าไปใน 802.3 frame

802.2 and SNAP

ตั้งแต่ 802.2 Ethernet frame ไม่สามารถระบุตัวมันเองได้ที่ upper-layer protocol มันเห็นได้ชัดว่าต้องมีตัวช่วย

IEEE กำหนด802.2 LLC เป็นพิเศษเพื่อที่จะทำให้เกิดหน้าที่นี้และอื่น ๆ รูปที่ 1.13 แสดงให้เห็นตัวอย่าง IEEE 802.3 กับ LLC (802.2) และ Subnetwork Access Protocol (SNAP) frame

รูป 1.16 แสดงให้เห็นข้อมูลของ LLC header ที่ถูกเพิ่มเข้าไปใน data portionของ frame ตอนนี้เรามาดูกันที่ 802.2 frame กับ คัดบางส่วนของ SNAP จากการวิเคราะห์ของเรา

802.2 Frame

ตามนี้คือ 802.2 frame ที่ถูกคัดออกมาจากการวิเคราะห์ของ protocol

```
Flags:          0x80 802.3
Status:         0x02 Truncated
Packet Length:64
Slice Length: 51
Timestamp:      12:42:00.592000 03/26/1998
Destination:    ff:ff:ff:ff:ff:ff Ethernet Broadcast
Source:         00:80:c7:a8:f0:3d
LLC Length:     37
Dest. SAP:      0xe0 NetWare
Source SAP:     0xe0 NetWare Individual LLC
  SublayerManagement Function
Command:        0x03 Unnumbered Information
```

คุณสามารถสังเกตเห็นได้ว่าframe แรกมี Lengthe field ดังนั้นมันเหมาะที่จะเป็น 802.3 ถูกไหม อาจจะ ลองมองอีกครั้ง มันมี DSAP และ SSAP ด้วย ดังนั้นมันจึงไม่ได้เป็น 802.3 frame (จำไว้ว่า 802.2 frame คือ 802.3 frame กับข้อมูลของ LLC ในส่วนของข้อมูลของ header ดังนั้นเรารู้แล้วว่า อะไรคือ upper-layerของ protocol

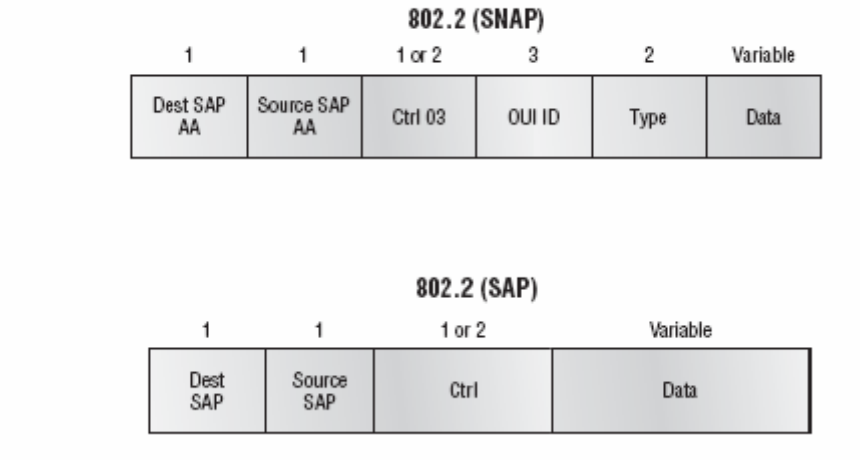
SNAP Frame

SNAP frame มี Protocol field เป็นของตัวเองที่ชี้เฉพาะ upper-layer protocol นี่เป็นวิธีจริงที่ยอมให้ Ethernet_II Ether-Type field ถูกใช้ใน 802.3 frame แม้ว่าแนวทางของ network ข้างล่างนี้แสดงให้เห็น protocol field มันเป็นตัวอย่างของ Ethernet อย่างแท้จริง (Ether-Type field)

```
Flags:          0x80 802.3
Status:         0x00
Packet Length:78
Timestamp:      09:32:48.264000 01/04/2000
802.3 Header
Destination:    09:00:07:FF:FF:FF AT Ph 2 Broadcast
Source:         00:00:86:10:C1:6F
LLC Length:     60
802.2 Logical Link Control (LLC) Header
Dest. SAP:      0xAA SNAP
Source SAP:     0xAA SNAP
Command:        0x03 Unnumbered Information
Protocol:       0x080007809B AppleTalk
```

คุณสามารถชี้เฉพาะ SNAP ได้เพราะ DSAP และ SSAP field เป็น AA เสมอ และ Command field เป็น 3 เสมอ ตัวอย่าง frame นี้ถูกสร้างขึ้น protocol บางตัวทำงานได้ดีใน 802.3 Ethernet frame ที่ไม่มี Ether-Type field การยอมให้ protocol ที่มีสิทธิสร้างโดยหลักการของผู้พัฒนาที่ถูกใช้ใน LLC frame IEEE กำหนดรูปแบบของ SNAPที่ใช้คัดเลือกรหัสเดียวกันเหมือน Ethernet_II
มาจนกระทั่งถึงปี 1997 SNAP frame ก็ล้าสมัยในการตลาด แต่อย่างไรก็ตาม 802.11 ไร้สาย LAN พิเศษตัวใหม่ใช้ Ethernet SNAP field เพื่อระบุ Network Layer Protocol Cisco ยังคงใช้ SNAP frame กับ protocol ที่มีกรรมสิทธิ์ Cisco Discovery Protocol(CDP) บางอย่างจะไปพูดในบทที่ 9 การจัดการ Cisco internetwork

FIGURE 1.16 802.2 and SNAP



Ethernet At Physical Layer

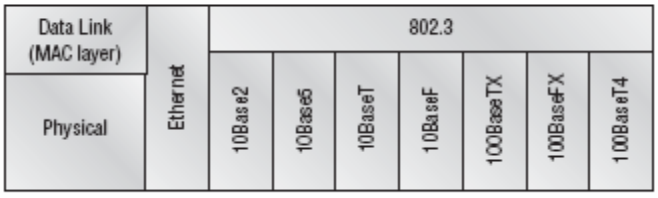
Ethernet เป็นการกระทำที่เกิดผลเป็นลำดับแรกของกลุ่มที่เรียกว่า DIX (Digital, Intel, and Xerox) พวกเขาสร้างและทำให้เกิด Ethernet LAN พิเศษรายแรก ที่ IEEE ใช้สร้าง IEEE802.3 Committee ที่เป็น 10 Mbps network ที่ รันอยู่ใน coax และในที่สุด การสลับคู่ และ fiber physical media

IEEE เผยแผ่ 802.3 Committee ให้เป็น 2 กลุ่มใหม่ที่รู้จักในชื่อ 802.3u (Fast Ethernet) และ 802.3ab(Gigabit Ethernet on category 5) และลำดับสุดท้าย 802.3ae (10 Gbps over fiber and coax)

รูป 1.17 แสดง IEEE 802.3 และ Original Ethernet Physical Layer Specifications

เมื่อออกแบบ LAN มันสำคัญที่จะต้องเข้าใจประเภทที่แตกต่างกันของEthernet media ที่จะหาให้คุณได้ แน่นอนมันเป็นเรื่องใหญ่ที่จะ run Gigabit Ethernet บนแต่ละ desktop และ10 Gbps ของระหว่าง switch และแม้ว่านี่จะเกิดขึ้นเพียงหนึ่งวันและพิสูจน์มูลค่าของ network นั้น วันนี้จะเป็นวันที่ค่อนข้างแตกต่าง แต่ว่าคุณจะต้องผสมและจับคู่ประเภทที่แตกต่างของวิธีต่าง ๆ ของEthernet media ที่หาได้โดยทั่วไป คุณสามารถติดตามด้วยการแก้ปัญหาของ network ที่มี cost-effective ที่ทำงานอย่างดีเยี่ยม

FIGURE 1.17 Ethernet Physical layer specifications



EIA/TIA (Electronic Industries Association and A newer Telecommunications Industry Alliance) เป็นมาตรฐานของตัวที่สร้าง Physical Layer Specification สำหรับ Ethernet EIA/TIA ชี้เฉพาะว่า Ethernet ใช้ registered jack (RJ) connector กับ 4, 5 wiring อย่างต่อเนื่องบน unshielded twisted-pair (UTP) cabling (RJ-45) แต่อย่างไรก็ตาม อุตสาหกรรมจะขยับขยายไปสู่การที่จะเรียกสิ่งนี้ว่า “ตัวเชื่อม 8-pin modular”

ตัวอย่าง Ethernet cable ที่ถูกระบุโดย EIA/TIA ของตัวลดขนาดไฟฟ้าเดิม ๆ ที่กำหนดการหายของสัญญาณเหมือนกับการเดินทางบนความยาวของ cable และถูกวัดในหน่วยความถี่ของเสียง (dB) cabling ถูกใช้ในการรวมและhome market จะถูกวัดใน categories cable ที่มีคุณสมบัติสูงจะมีอัตราของลำดับขั้นที่สูงและการลดขนาดของไฟฟ้าจะต่ำ ตัวอย่างเช่น category 5 ดีกว่า category 3 เพราะว่า category 5 มีสายไฟที่บิดเป็นเกลียวมีมากกว่าต่อฟุต และดังนั้นจึงมี crosstalk น้อย
Crosstalk คือการไม่ต้องการติดต่อสัญญาณจากคู่ที่เป็นด้านเดียวกันในcable

Near End Crosstalk (NEXT) เป็นการวัด crosstalk ที่ปลายทางของการส่งของcable Far End Crosstalk (FEXT) ถูกวัดที่จุดปลายที่ไกลออกไปที่สัญญาณถูกเชื่อมใน cable Power Sum (PSNEXT)การคำนวณคณิตศาสตร์ขั้นพื้นฐานที่เหมือนกับว่าคู่ทั้งสี่กำลังถูกกระตุ้นพลังงานในเวลาเดียวกัน การคำนวณต่าง ๆ ของ(PSNEXT) ถูกทำให้แน่ใจว่าจะไม่มีความต้องการแสดง crosstalk ที่ดังเกินไปเมื่อทุกคู่ทำงานเหมือนจริง PSNEXT เป็นตัวอย่างที่ถูกใช้ใน Gigabit Ethernet ที่มากกว่า 10 BaseT หรือ 100 BaseT

นี่คือมาตรฐานของ IEEE 802.3 ดั้งเดิม

10 Base2 10 Mbps, baseband technology, ความยาวขึ้นไปถึง185 เมตร และสามารถสนับสนุนให้เป็นถึง 30 สถานีการทำงานบน segment เดียว การใช้ Physical กับ Logical bus กับ ตัวเชื่อม AUI เลข 10 หมายถึง 10Mbps Base หมายถึง baseband technology และเลข 2 หมายถึง เกือบ 200 เมตร

10 Base2 Ethernet cards ใช้ BNC (British Naval Connector, Bayonet Neill Concelman, หรือ Bayonet Nut Connector) และ T-connector เพื่อเชื่อมต่อกับ network

10Base5 10 Mbps baseband technology, ความยาวมีไปถึง 500เมตร รู้จักกันในชื่อ thicknet ใช้ physical และ logical busด้วยการเชื่อมต่อแบบ AUI สามารถทำได้ถึง 2500 เมตร ถ้าใช้กับตัวขยาย (repeater) รองรับผู้ใช้งานได้ 1024 เครื่องในแต่ละ segments

10BaseT 10 Mbps เป็นประเภท UTP 3 สาย ที่ไม่เหมือนกับ 10 Base2 และ 10 Base5 network แต่ละอันจะต่อเข้ากับ hubหรือ switch คุณสามารถใช้สายประเภทนี้ได้ถ้าคุณมีแค่ host เพียงหนึ่งตัวต่อ segments หรือเพียงหนึ่งตัวหรือเพียงหนึ่งสาย โดยใช้ตัวต่อ RJ-45 (ตัวต่อที่มี 8 ขา) ด้วยการต่อแบบสตาร์และแบบบัส

“Base” ในความหมายของ network หมายถึง “baseband” ซึ่งเป็นวิธีการส่งสัญญาณสื่อสารข้อมูลในระบบ network

ในแต่ละมาตราฐาน 802.3 จะทำการกำหนด Attachment Unit Interface (AUI) ที่เป็นข้อกำหนดการอนุญาตส่งถ่ายข้อมูลหนึ่งบิตต่อครั้ง (one-bit-at-a-time) ไปยัง physical layer จาก data link layer ที่อนุญาต MAC ที่ไม่เปลี่ยนแปลงแต่สามารถบอกรายละเอียดให้ทาง physical layer เข้าใจและรองรับเทคโนโลยีใหม่ได้ แรกเริ่มของอุปกรณ์ของ AUI เป็นตัวเชื่อมต่อแบบ 15 pin ใช้เป็นตัวรับส่งสัญญาณ (ส่งสัญญาณ/รับสัญญาณ) โดยใช้ตัวเปลี่ยนจาก 15 pin เป็นสายตีเกลียว (twisted-pair)

สิ่งหนึ่งอุปกรณ์ของ AUI ไม่สามารถรองรับ Ethernet 100Mbs เพราะการรวบรวมของความถี่ ดังนั้น 10BaseT จึงต้องการอุปกรณ์ชนิดใหม่ 802.3 จึงกำหนดมาตรฐานแบบใหม่คือ Media Independent Interface (MII) ซึ่งรองรับการสื่อสารแบบ 100Mbs MII ใช้การ nibble หมายถึงหารกำหนดให้ใช้ 4 บิต Gigabit internet ใช้การเชื่อมต่อแบบ Gigabit Media Independent Interface (GMII) ส่งต่อข้อมูลทีละ 8 บิต

802.3u (Fast Ethernet) ซึ่งเข้ากันกับ 802.3 Ethernet เพราะว่าใช้รูปแบบลักษณะเฉพาะทางกายภาพเหมือนกัน Fast Ethernet และ Ethernet ใช้ข้อจำกัดการส่งข้อมูล Maximum Transfer Unit (MTU) เหมือนกัน, ใช้กลไกของ MAC เหมือนกัน และรักษารูปแบบของโครงสร้างซึ่งใช้เป็นแบบ 10BaseT Ethernet ปกติแล้ว Fast Ethernet จะถูกจัดให้อยู่ในรูปแบบของ IEE 802.3 นอกจากนั้นมันรองรับความเร็วที่เพิ่มขึ้นเพียง 10 ครั้ง นั่นก็คือ 10BaseT

นี่คือการขยายความของมาตรฐาน IEE Ethernet 802.3

100BaseTX (IEEE 802.3u) EIA/TIA ประเภท 5, 6 หรือ 7 UTP 2 สายตีเกลียว ใช้ได้กับหนึ่งเครื่องต่อหนึ่งส่วน รองรับความยาว 100 เมตร ใช้ตัวต่อ RJ-45 ด้วย physical star topology และ logical bus

100Base FX (IEEE 802.3u) ใช้สายไฟเบอร์ 62.5/125 ไมครอน multimode ด้วย topology จุดต่อจุด (point to point) รองรับความยาว 142 เมตร สามารถใช้ได้กับตัวต่อแบบ ST หรือ SC ซึ่งคือตัวเชื่อมต่อระหว่าง interface

1000BaseCX (IEEE 802.3z) สายทองแดงคู่ตีเกลียว เรียกว่า twinax (เหมือนกันกับสาย coaxial) รองรับความยาวเพียง 25 เมตร

1000BaseT (IEEE 802.3ab) Category 5 เป็นสายแบบ UTP 4 เส้น รองรับความยาว 100 เมตร

1000BaseSX (IEEE 802.3z) MMF ใช้เส้นผ่านศูนย์กลาง 62.5 และ 50 ไมครอน ใช้ laser 850 นาโนเมตร ใช้งานได้ในความยาว 220 เมตร ด้วย 62.5 ไมครอน และ 550 เมตรด้วย 50 ไมครอน

1000BaseLX (IEEE 802.3z) Single mode fiber ซึ่งใช้เส้นผ่านศูนย์กลาง 9 ไมครอน และ laser1300 นาโนเมตร สามารถใช้งานได้ถึง 3 กิโลเมตร ถึง 10 กิโลเมตร

100VG-AnyLAN คือสายคู่ตีเกลียวเทคโนโลยีเป็นมาตรฐานแรกของแลน 100Mbps ตั้งแต่ที่ขัดแย้งกันกับเทคนิคของการส่งสัญญาณของ Ethernet (ใช้ข้อกำหนดในการถามสิทธิในการเข้าถึง) ไม่เป็นที่นิยม และในตอนนี้ก็สูญหายไปแล้ว

Ethernet Cabling

สาย Ethernet เป็นสิ่งสำคัญที่ต้องอธิบาย โดยเฉพาะถ้าคุณวางแผนที่จะทำการทดสอบ CCNA ชนิดของสาย Ethernet ที่มีอยู่คือ

- Straight-through cable
- Crossover cable
- Rolled cable

เราจะมาดูรายละเอียดในแต่ละชนิด

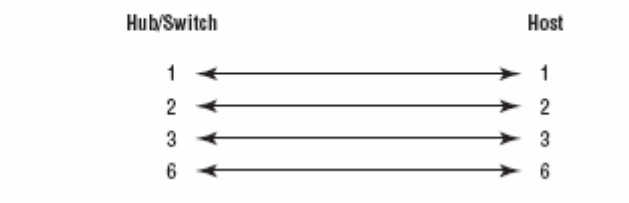
Straight-Through Cable

สาย straight-through จะถูกใช้ในการต่อกับ

- Host ไปยัง switch หรือ hub
- Router ไปยัง switch หรือ hub

สาย 4 เส้นจะถูกใช้ในสาย straight-through ใช้ต่อกับอุปกรณ์ Ethernet มันเกี่ยวข้องกันโดยปกติที่จะสร้างชนิดนี้ รูปที่ 1.18 แสดงสาย 4 เส้นที่ถูกใช้ในสาย Ethernet straight-through

FIGURE 1.18 Straight-through Ethernet cable



สังเกตว่า มีเพียง pinที่ 1, 2, 3 และ 6 ที่ถูกใช้ การเชื่อมโยง จาก 1 ถึง 1 จาก 2 ถึง 2 จาก 3 ถึง 3 จาก 6 ถึง 6 you'll be up และ การทำงาน network ก็จะหมดเวลา แต่อย่างไรก็ตาม จำไว้ว่า สิ่งนี้จะเป็นเพียงสาย Ethernet อย่างเดียวและจะไม่ทำงานกับ Voice, Token Ring, ISDN, etc.

Crossover cable

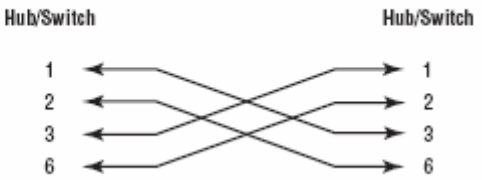
สาย Crossover สามารถใช้เพื่อติดต่อ

- switch ไปหา switch
- hub ไปหา hub
- host ไปหา host
- Hub ไปสู่ switch
- Router ตรงไปยัง host

สายทั้ง 4 ที่เหมือนกันถูกใช้ในสายนี้เหมือนกับในสายของ straight-through เราเพียงแค่เชื่อมต่อ pin ที่ต่างกันเข้าด้วยกัน รูป 1.19 แสดงวิธีที่ สายสี่เส้นถูกใช้ใน สาย crossover Ethernet

สังเกตว่าการแทนที่ของการเชื่อมโยง จาก 1 ถึง 1 และอื่น ๆ ที่นี่เราเชื่อมต่อ pin ต่าง ๆ จาก 1 ไปหา 3 และ 2 ไปหา 6 บนแต่ละด้านของสาย

FIGURE 1.19 Crossover Ethernet cable



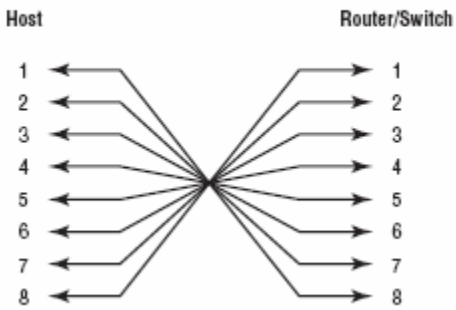
Rolled cable

แม้ว่า rolled cable ไม่ได้ถูกใช้เชื่อมต่อกับการเชื่อมต่อ Ethernet เข้าด้วยกัน คุณสามารถใช้สาย rolled Ethernet เพื่อเชื่อมต่อ host ไปยังแผงควบคุมหมายเลขทางการสื่อสารของ router

ถ้าคุณมี Cisco router หรือ switch คุณจะใช้สายนี้เพื่อเชื่อมโยง PC ของคุณที่ทำ HyperTerminal ไปยัง Cisco hardware สายแปดสายที่ถูกใช้ในสาย cable นี้จะเชื่อมต่อกับอุปกรณ์หมายเลข แม้ว่าจะไม่ครบทั้ง 8 สาย ที่ใช้ส่งข้อมูล เหมือนใน Ethernet networking

รูป 1.20 แสดงให้เห็น สาย 8 เส้นที่ถูกใช้ใน rolled cable

FIGURE 1.20 Rolled Ethernet cable



สิ่งเหล่านี้เป็นความเหมาะสมของการสร้างสาย cable ที่ง่ายที่สุดเนื่องจากว่าคุณสามารถตัดออกบนด้านหนึ่งของสาย straight-through และ ย้อนกลับมาที่จุดสุดท้าย

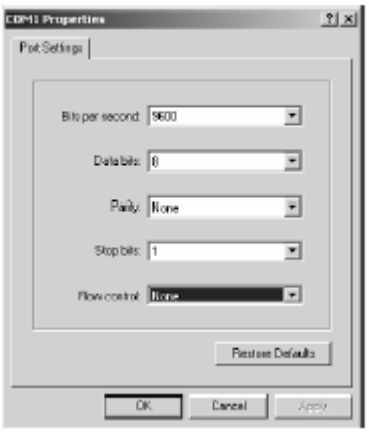
และเมื่อคุณมีสาย cable ที่ถูกต้องที่เชื่อมต่อจาก PC ของคุณ ไปยัง Cisco router หรือ switch คุณสามารถเริ่ม HyperTerminal เพื่อสร้างแผงควบคุมการเชื่อมโยงและโครงสร้างกลไก ชุดของโครงสร้างก็มีดังนี้

1. เปิด HyperTerminal และ ใส่ชื่อสำหรับการเชื่อมต่อ มันไม่ได้อยู่ตรงที่ชื่อที่คุณตั้ง แต่ฉันใช้ cisco เสมอแล้วก็ click OK

2. เลือกพอร์ตของการสื่อสาร ทั้ง COM 1 หรือ COM2 อันไหนก็ได้ที่ถูกเปิดบน PC ของคุณ

3. ตอนนี้ให้ตั้งค่าที่ port setting ค่าที่ผิดปกติ (2400 bps และ ไม่มี hardware ควบคุมการไหล)อาจจะไม่ทำงาน คุ๖จะต้องตั้งค่าที่ port setting ดังที่แสดงให้เห็นในรูป 1.21

FIGURE 1.21 Port settings for a rolled cable connection



สังเกตว่า ค่าของ bit ในตอนที่ ตั้งค่า 9600 และflow control ถูกตั้งค่าให้เป็น none ณ จุดนี้ คุณสามารถ click OK และกด Enter และคุณควรจะเชื่อม port อุปกรณ์การควบคุมของCisco ของคุณ

Wireless Networking (การทำงานของ Network ไร้สาย)

ทุกวันนี้ไม่มีหนังสือที่จะสมบูรณ์ได้โดยปราศจากการพูดถึงการทำงานของ wireless networking นั่นก็เพราะว่าเมื่อ 2 ปีที่ผ่านมา มันไม่ใช่เรื่องธรรมดาที่จะพบคนทั่วไปใช้เทคโนโลยี ในปี 1996 คนส่วนใหญ่ไม่ค่อยมี e-mail address แน่นอนแต่ว่าบางคนมี ซึ่งในตอนนี้ทุกคนมีและเป็นสิ่งที่เกิดขึ้นเหมือนกันในโลกไร้สาย นั่นก็เพราะว่าการทำงานของ wireless networking เป็นทางที่สะดวกสบายอย่างมาก ฉันพนันได้ว่ามีบางคนที่อ่านหนังสือนี้อยู่มี wireless networking ที่บ้าน ฉันก็เป็นคนหนึ่งที่มี ด้วยเหตุผลดังนี้ ตอนนี้ฉันกำลังกล่าวถึงประเภทต่าง ๆ ของ wireless networking ความเร็วของมันและการกำหนดระยะทาง รูปที่ 1.22 แสดงบางประเภทของ wireless networking ที่ใช้ในปัจจุบัน

มาพูดถึงประเภทที่หลากหลายเหล่านี้ของ wireless networking และความเร็วรวมทั้งระยะทางของแต่ละอย่าง

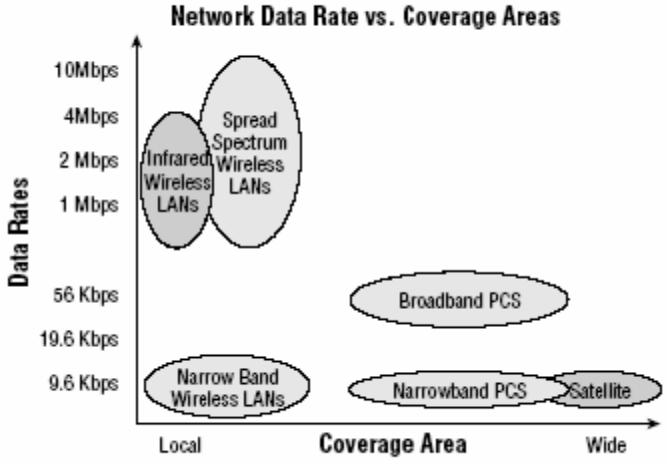
Narrowband Wireless LANs Narrowband radio เป็นเหมือนกับชื่อของมัน มันเป็นสัญญานของคลื่นความถี่วิทยุที่แคบพอ ๆ กับที่มันจะเป็นไปได้ในขณะที่มันยังคงสามารถส่งข้อมูลผ่านไปได้ตลอด ปัญหาของการแทรก คือ การหลีกเลี่ยงโดยความแตกต่างของผู้ใช้โดยตรงบนความแตกต่างของช่องความถี่

ความยาวที่คุณได้รับเป็นความเหมาะสม แต่ว่าความเร็วที่จะมีได้ในทุกวันนี้ไม่เพียงพอสำหรับการใช้งานร่วมกันของผู้ใช้งาน รวมกับคุณต้องมีอุปกรณ์ที่มีประสิทธิภาพรองรับการทำงานได้ดีพอ ๆ กับการซื้อใบอนุญาต FCC ที่จะทำความถี่ทีแต่ละ site

Personal Communication Services (PCS) PCS รวมทุกสาขาของmobile หรือ portable และการบริการเสริมการสื่อสารสำหรับส่วนตัวและธุรกิจ Federal Communication commission (FCC) กำหนด PCS อย่างคร่าว ๆ เหมือนการเคลื่อนที่ และอุปกรณ์ที่ระบุการสื่อสารสำหรับทั้งส่วนตัวและธุรกิจที่สามารถทำร่วมกันในชนิดต่าง ๆ ของการแข่งขัน network Narrowbandหรือ broadband PCS คือสิ่งที่ถูกใช้ในทุกวันนี้

Narrowband PCS ชื่อก็บอกเป็นนัยแล้วว่าลักษณะบางอย่างของ narrowband PCS ต้องการการบริการขนาดเล็กกว่าของ spectrum มากกว่าที่ broadband PCS ต้องการ ด้วยการอนุญาตของ narrowband PCS คุณจะสามารถเข้าสู่การใช้งานได้ ตัวอย่างเช่น two-way paging และหรือ text-based messaging ลองคิดดูว่าคนทั่วไปใช้ PDAs กับ keyboard ภายนอก หรือ อื่น ๆ เช่นการรับและการส่ง wireless e-mail ซึ่งมันอธิบายถึงความสามารถที่จะทำได้โดยใช้สัญญาณไมโครเวฟ ด้วย narrowband PCS คุณสามารถที่จะใช้งาน service ที่ดีได้โดยใช้ตัววัดสัญญาณ wireless ซึ่งก็คือการ monitoring mobileหรือการใช้อุปกรณ์รีโมทเสริม แบบ remotely monitoring จะเป็นตัวช่วยเพิ่มความสามารถของความเข้มสัญญาณของระบบ ที่รู้จักอย่างทั่วไป การอ่านค่าที่สามารถวัดได้จะเป็นไปโดยอัตโนมัติเป็นผลที่ดีที่ถูกนำมาใช้กับเทคโนโลยีนี้

FIGURE 1.22 Wireless Networks



Broadband PCS Broadband Personal Communications Service (PCS) ถูกใช้กับในหลายระบบwireless ทั้ง mobile และfixed radio Mobile broadband เป็นชุดที่รวมทั้ง voice และลักษณะการส่งข้อมูล 2 ทาง สามารถที่จะเจอได้อย่างปกติโดยอย่างเช่น ส่งที่เล็ก, เคลื่อนที่ได้, ทำได้หลายอย่าง ตัวอย่างเช่น กล้องดิจิตอล โทรศัพท์มือถือ ในอุตสาหกรรม services นี้จะถูกพูดถึงว่าเป็นเรื่องธรรมดาของการบริการโทรศัพท์เคลื่อนที่ และการให้บริการข้อมูลเคลื่อนที่ แหล่งของการบริการเหล่านี้รวมอยู่ในองค์กรเดียวกันที่ให้บริการทางด้าน broadband PCS spectrum เช่น AT&T Wireless, Verizon, Sprint PCS และอื่น ๆ

Satellite การให้บริการระบบ Satellite คุณจะได้รับบริการที่ความเร็วที่น่าพอใจ ความเร็วจะอยู่ที่ 1 Mbps และเพิ่มโดยการโหลดให้เป็น 2 Mpbs แต่ว่ามีการทำให้เสียเวลาโดยการรบกวนเมื่อมีการเชื่อมต่อ ดังนั้นการทำงานจึงไม่ดีนักเมื่อคุณต้องเจอกับการกระจายของการสื่อสาร ข่าวดีก็คือว่าความเร็วนั้นจะเพิ่มขึ้น แต่ถึงกระนั้น ก็ไม่สามารถทำให้มันสมบูรณ์ได้กับสิ่งที่คุณได้รับด้วย LANs ไร้สาย แนวโน้มการใช้ satellite-based network เป็นการควบคุมพื้นที่ทางภูมิศาสตร์ที่ใหญ่

Infrared Wireless LANs ที่นี่เรามีทางตรงกันข้ามอยู่ค่อนข้างมาก เทคโนโลยีนี้ทำงานจริงได้อย่างดีที่ควบคุมในเวลาสั้น การกระจายทางสื่อสารในส่วนของ Personal Area Network (PAN) และความเร็วก็เพิ่มขึ้นด้วย แต่ว่าอัตราที่เป็นไปได้ยังคงเป็นจำนวนที่สั้นมาก โดยทั่วไปแล้วใช้สำหรับการแปลง laptop ไปหา laptop และ laptop ไปสู่ PDA อัตราความเร็วอย่างทั่ว ๆ ไป จาก 115 Kbps เป็น 4 Mbps แต่ว่าอัตราพิเศษเรียกว่า Very Fast Infrared (VFIR) พูดว่าเราสามารถเพิ่มความเร็วไปถึง 16 Mbps ได้ในอนาคต แล้วเราจะได้เห็นมัน

Spread Spectrum Wireless LANs ตัวอย่าง wireless LANs (WLANs) ใช้ spread spectrum มันเป็นเทคนิคคลื่นความถี่วิทยุที่เป็นวงกว้างที่ทางทหารนำมาใช้ในความเป็นจริงและการรักษาความปลอดภัย (ที่ยังโต้แย้งได้) WLAN ที่ได้รับความนิยมใช้ในปัจจุบันคือ 802.11 b ที่ทำงานขั้นไปถึง 11 Mbps แต่ว่าตัวใหม่ 802.11 สามารถชนกระทบถึงประมาณ 22 Mbps (ตามที่คาดไว้ 54 Mbps) และเพิ่มได้อีกขึ้นอยู่กับใครเป็นทำอุปกรณ์นั้น บวกกับ802.11 a ตัวใหม่อยู่ในอัตรา 5 Ghz และทำให้ bandwidth ประมาณ 50 Mbps และสามารถเพิ่มได้มากถึง 100 Mbps ในอนาคตอันใกล้ แต่ว่าระยะทางยังคงน้อยกว่าที่คุณรับด้วย 802.11 b/g ใช้ในที่ร่มและ 802.11 a ในระยะที่สั้นกว่าที่ตลาดกลางแจ้งเมื่อ bandwidth ที่เพิ่มขึ้นเป็นความต้องการ แต่ว่าตลาดยังคงเป็นคนอายุน้อยและเป็นคนที่ทราบว่าในอนาคตกำลังติดตามสำหรับสิ่งเหล่านี้เพิ่มขึ้นและการมาของ WLANs

Note

802.11 WLANs มี bandwidth ทั้งหมดไปจนถึง 11 Mbps และพิจารณาว่า “Wi-Fi” (Wireless Fidelity)

Data Encapsulation

เมื่อ Host ส่งข้อมูลข้าม network ไปยังอุปกรณ์อีกตัวหนึ่ง ข้อมูลจะตรงไปสู่ encapsulation ซึ่งเป็นการห่อหุ้มด้วยข้อมูลของ protocol ที่แต่ละ layer ของโครงสร้าง OSI ซึ่งการสื่อสารของ layer นั้นๆจะต่อเข้ากับตัว layer ที่เหมือนกันของฝั่งอุปกรณ์ด้านรับ

การสื่อสารและการเปลี่ยนข้อมูลในแต่ละ layer ใช้ Protocol Data Units (PDUs) การยึดถือการควบคุมข้อมูลที่ผูกมัดต่อข้อมูลที่แต่ละ layer ของโครงสร้าง พวกเขาผูกมัดข้อมูลต่อheader ในส่วนหน้าของข้อมูล field แต่ว่าสามารถอยู่ในตัว trailer หรือตอนปลาย ของมัน

แต่ละ PDU เป็นการผูกติดข้อมูลโดยการ encapsulating มันที่แต่ละ layer ของโครงสร้าง OSI และแต่ละอันมีชื่อเฉพาะที่ขึ้นอยู่กับข้อมูลที่ทำให้เกิดในแต่ละ header ข้อมูล PDU นี้ถูกอ่านเท่านั้นโดย layer ที่เข้ากันบนกลไกการยอมรับ ภายหลังจากการอ่าน มันจะถอนออก และ ข้อมูลจะถูกส่งต่อไปยัง layer ถัดไป

รูป 1.23 แสดง PDUs และวิธีการควบคุมข้อมูลในแต่ละ layer ภาพนี้แสดงให้เห็นการแปลงข้อมูลของ user ใน layer บนเพื่อการสื่อสารบนระบบ network. ข้อมูลที่ถูกแปลงจะถูกส่งไปยัง transport layer ซึ่งจะมีการ set up virtual circuit ไปยังอุปกรณ์ตัวรับเพื่อทำการจัดส่ง package หลังจากนั้นข้อมูลจะถูกแบ่งออกเป็นข้อมูลย่อย และมีการสร้าง Transport layer header และเก็บไว้ที่ส่วน header ของ data field ณ จุดนี้เราจะเรียก ข้อมูลย่อยเหล่านี้ว่า Segment. Segment แต่ละอันจะมีการจัดเรียงลำดับ ดังนั้นข้อมูลย่อยเหล่านี้จะสามารถนำกลับมาเรียงรวมกันใหม่ได้อย่างถูกต้องเหมือนข้อมูลต้นฉบับที่จัดส่ง

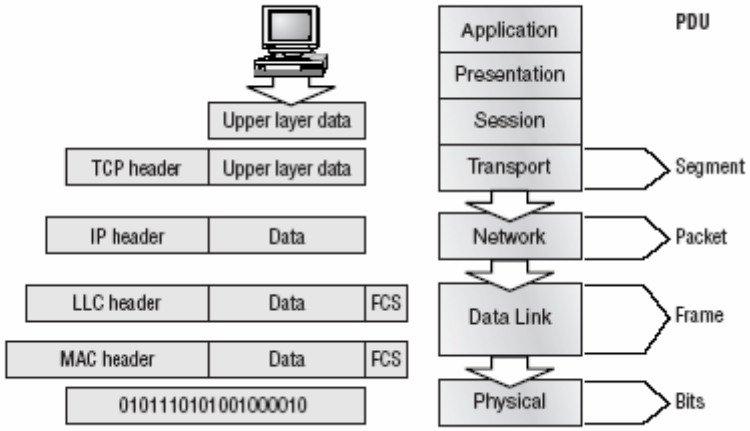
Segment จะถูกส่งต่อมายัง Network layer เพื่อจัดการเกี่ยวกับ Network address และเส้นทางการส่งข้อมูล (routing) ข้ามระบบเครือข่าย Logical address เช่น IP มีไว้เพื่อช่วยให้มีการส่ง Segment ไปยัง Network ปลายทางได้อย่างถูกต้อง Network layer protocol จะทำการเพิ่ม control header เข้าไปใน Segment ที่ได้รับมาจาก Network layer ข้อมูลเหล่านี้จะถูกเรียกว่า Package หรือ datagram

Transport และ Network layer จะทำงานร่วมกันเพื่อสร้างชุดของข้อมูลขึ้นมาใหม่บน เครื่องฝ่ายรับ (Receiving host) แต่ไม่มีส่วนเกี่ยวข้องในการจัดส่ง PDU ภายในเครือข่ายเดียวกัน (local network) ซึ่งเป็นทางเดียวที่จะส่งข้อมูลไปที่ router หรือ host

Data Link layer มีหน้าที่นำ packet จาก network layer และแทนที่ packet บน network medium (มีสาย หรือ ไร้สาย) Data Link layer ห่อแต่ละ packet ใน frame และ header ของ frame ก็จะนำไปสู่ hardware address ของแหล่งที่มาและ จุดหมายปลายทางของ host ถ้ากลไกของจุดหมายปลายทางอยู่บน network เดียว แล้ว frame ถูกส่งไปที่ router เพื่อที่จะกำหนดเส้นทางผ่านไปยัง

Internetwork ในเมื่อ รับจุดหมายปลายทางของ network frame ใหม่ถูกใช้เพื่อรับ packet ที่จุดหมายปลายทางของ host

FIGURE 1.23 Data encapsulation



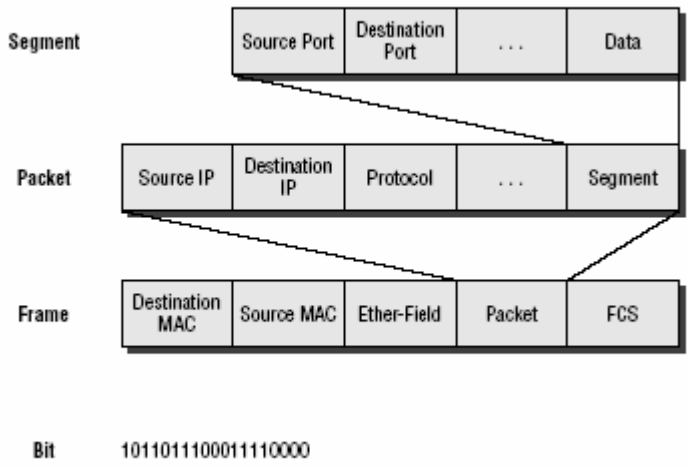
การใส่ frame นี้บน network มันต้องเป็นอันแรกที่ถูกใส่ในสัญญาณดิจิตอล ตั้งแต่ frame เป็นกลุ่มของตัวเลข 1 และ 0 แท้จริงแล้ว Physical layer มีหน้าที่ใส่รหัส ดิจิตอลเหล่านี้ในสัญญาณดิจิตอล ที่ถูกอ่านโดยกลไกต่าง ๆ บน local network เดียวกัน การได้รับกลไกจะทำให้สอดคล้องกันบนสัญญาณดิจิตอล และถอนออก (ถอดรหัส) 1 และ 0 ออกจากสัญญาณดิจิตอล ในจุดนี้กลไกต่าง ๆสร้าง frame ต่าง ๆ ที่ทำให้ CRC ทำงาน และตรวจสอบคำตอบที่ติดกับคำตอบในเขตของ FCS ของ frame มันจับคู่กัน packet ถูกดึงจาก frame และสิ่งที่ถูกทิ้งของframe ที่ถูกปฏิเสธ กระบวนการนี้ถูกเรียกว่า de-encapsulation ส่วน packet ถูกส่งไปที่ network layer ที่ address ถูกตรวจสอบ ถ้า address ตรงกัน segment ถูกดึงจาก packet และสิ่งที่ถูกทิ้งไว้ของpacket ก็คือการปฏิเสธ Segment ถูกทำให้เกิดที่ Transport layer ที่มีการสร้าง data stream ซ้ำและยอมรับการส่งต่อสถานีที่ได้รับในแต่ละชิ้น แล้วความสุขก็ส่งมอบ data stream ไปที่ตำแหน่งของ upper-layer

กลไกของการเปลี่ยนแปลง วิธีที่ข้อมูลถูก วิธีการทำงานดังนี้Data encapsulation

1. ผู้ใช้ข้อมูลถูกเปลี่ยนไปสู่ ข้อมูลสำหรับการเปลี่ยนบน network
2. ข้อมูลที่เปลี่ยน segment และ กาเชื่อมต่ออย่างแท้จริง ถูกจัดตั้งระหว่างการส่งและรับ host
3. Segment ถูกทำให้เปลี่ยน packet หรือ datagram และ logical address ถูกแทนที่ใน header ดั้งนั้น แต่ละ packet สามารถกำหนดเส้นทางไปสู่ internetwork
4. packet หรือ diagram ถูกทำให้เปลี่ยน frame สำหรับการส่งต่อหรือบน local network Hardware (Ethernet) address ถูกใช้เพื่อชี้ความเป็นหนึ่งเดียวของ host บนส่วนของ local network

5. frame ถูกทำให้เปลี่ยน bits และการใส่รหัสดิจิตอล และ นับเวลาเรื่องตารางถูกใช้ การอธิบายนี้ใน รายละเอียดที่มากกว่าการใช้ layer addressing ซึ่งจะใช้ รูป 1.24

FIGURE 1.24 PDU and layer addressing



จำไว้ว่า data stream เป็นการส่งจาก upper layer ลงไปสู่ Transport layer เราจะไม่สนใจว่า data stream มาจากใคร เนื่องจากว่าสิ่งนั้นเป็นปัญหาของโปรแกรมเมอร์ งานของช่างเทคนิคที่ต้องสร้าง data stream ใหม่ที่เชื่อถือได้ และส่งมันไปยัง upper layer บนกลไกการรับ

ก่อนที่เราจะพูดคุยกันไปกันไกลที่รูป 1.24 เรามาพูดคุยกันเรื่อง port ของตัวเลขต่าง ๆ และทำให้แน่ใจว่าเราเข้าใจ การ Transport layer ใช้ port หมายเลขต่าง ๆ ที่จะกำหนดทั้ง virtual circuit และกระบวนการการทำงานของ upper layer ดังที่เห็นจากรูป 1.25

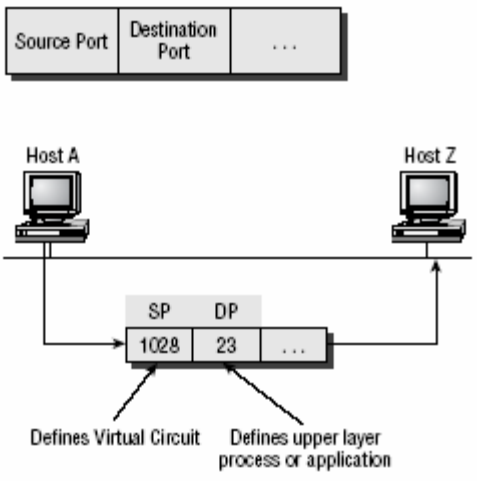
Transport layer นำ data stream ที่ทำการแบ่ง segment ต่าง ๆ ออก และสร้างความน่าเชื่อถือของ session โดยสร้าง virtual circuit แล้วเรียงลำดับ (หมายเลข) แต่ละ segment และใช้ยินยอม และ flow control ถ้าคุณใช้ TCP virtual circuit เป็นการกำหนดโดยแหล่งที่มาของหมายเลข port จำไว้ว่า host ทำให้การเริ่มนี้เกิดขึ้นที่ port หมายเลย 1024 (0 ตลอดไปจนถึง 1023 ที่จองไว้สำหรับหมายเลข port ที่รู้จักกันเป็นอย่างดี) จุดหมายปลายทางของหมายเลข port กำหนดกระบวนการการใช้ upper layer ที่ data stream ถูกส่งต่อเมื่อ data stream มีการสร้างซ้ำอย่างน่าเชื่อถือบนตัวรับ host

ตอนนี้เราเข้าใจหมายเลข port แล้ว และวิธีที่หมายเลข port ถูกใช้ที่ Transport layer กลับไปดูที่รูป 1.24 เมื่อข้อมูล Transport layer header ถูกเพิ่มในชิ้นของข้อมูล มันกลายเป็น segment และถูกส่งลงไปยัง network layer ไปด้วยกันกับปลายทางของ IP address (จุดหมายปลายทางของ IP address ถูกส่งลงไปจาก upper layers ไปสู่ Transport layer ด้วย data stream และจะถูกค้นพบผ่านชื่อของวิธีการแก้ปัญหาที่ upper layers DNS อย่างเหมาะสม)

Network layer เพิ่ม header และเพิ่ม addressที่เหมาะสม (IP addresses) ที่ด้านหน้าของแต่ละ segment Packet มี protocol field อธิบายว่ามันมาจาก (ทั้ง UDP หรือ TCP) หรือว่าคุณสามารถคิดเกี่ยวกับมันได้ว่า "ใครเป็นเจ้าของ segment " สิ่งนี้ปล่อย network layer ส่ง segment ไปสู่ protocol ที่ถูกต้องที่ Transport layer เมื่อ packet ไปถึงการรับ host Network Layer มีหน้าที่สำหรับการค้นหาจุดหมายปลายทางของ hardware address จะสืบค้นที่ๆ packet ควรถูกส่งบน Local Network ทำสิ่งนี้โดยการใช้ Address Resolution Protocok (ARP) ซึ่งจะพูดในบทที่ 2 IP ที่ network layer ค้นหาที่จุดหมายปลายทาง ถ้ามันยอมหมุนค้นหาจุดหมายปลายทาง IP address แล subnet mask ถ้ามันย้อนออกจากความต้องการของ local network hardware address ของ local host ที่ถูกขอร้องโดย ความต้องการของARP packet เป็นการถูกกำหนดสำหรับ host เดียว IP จะต้องค้นหา IP address ของ gateway router) ที่ผิดปกติแทน

Packet ทำตามด้วยกันกับปลายทางของ hardware address ของทั้ง local host หรือ default gateway ถูกส่งต่อให้ Data Link layer สำหรับ Data Link layer จะเพิ่ม header ไปที่ด้านหน้าของ packet และทั้งหมดจะถูกเรียกว่า frame (พวกเราเรียกว่า frame ก็เพราะว่ามันเป็นการรวม header กับ trailer เข้าไปกับ packet ซึ่งจะทำให้เกิดข้อมูลที่เจาะจงไว้เหมือนกัน หรือ frame อันหนึ่ง) ไม่ว่าจะเป็นอัตราใดๆ มันถูกแสดงที่รูป 1.24 Frame ใช้ Ether-Type field เพื่ออธิบายที่มาที่ไปของ protocol ใน network layer การตรวจสอบวงจรของการทำงาน (CRC) ถูกรันบน frame และที่ได้จาก CRC ก็จะถูกแทนที่ใน Frame Check Sequence (ลำดับของการตรวจสอบ frame) ที่พบอยู่ในส่วนท้ายของ frame

FIGURE 1.25 Port numbers at the Transport layer



ขณะนี้ frame ได้ถูกสร้างเรียบร้อยแล้วและถูกส่งไปยัง physical layer ด้วยหนึ่ง bit ต่อครั้ง ซึ่งเป็นการใช้กฎของ bit timing ที่เข้ารหัสข้อมูลในสัญญาณ ดิจิตอล อุปกรณ์ทั้งหมดในเครือข่าย network จะทำการ synchronize ด้วย clock และการ เลือกจำนวนว่ามีค่าเป็น 1 หรือ 0 จากสัญญาณดิจิตอล และการสร้าง frame หลังจากที่ frame ได้สร้างใหม่แล้ว CRC จะทำการตรวจสอบซึ่งจะทำให้แน่ใจว่า frame นั้นใช้งานได้ ถ้าทุกอย่างดีพร้อมแล้ว host ก็จะตรวจสอบ address ปลายทางเพื่อจะหา frame ที่จะถูกส่งให้มัน

ถ้ากระบวนทั้งหลายเหล่านี้ทำให้คุณงง ไม่ต้องแปลกใจ เราจะไปพูดอีกทีว่าการ encapsulation ของข้อมูล และการสื่อสารใน internetwork ในบทที่ 5

The Cisco Three-Layer Hierarchical Model

ส่วนใหญ่ช่วงแรก ๆ เราไม่เข้าใจการจัดลำดับชั้นของโครงสร้าง แต่ว่าก็มีบางคนที่คิดว่ามันเหมือนกับการลำดับชั้นของญาติพี่น้อง ความไม่สัมพันธ์กันของลำดับขั้นที่พบในช่วงแรก เราไม่มีประสบการณ์ในแง่มุมใด ๆ ของชีวิต มันเป็นลำดับขั้นที่ช่วยให้เราเข้าใจว่าที่เราเป็นเจ้าของหรือวิธีการทำให้ของนั้นเหมาะสมต่อกัน และอะไรคือหน้าที่ จะไปที่ไหน มันจะนำไปสู่คำสั่งและความสามารถของความเข้าใจ ที่มีต่อโครงรวม ตัวอย่างเช่น ถ้าคุณต้องการเลื่อนขั้น ลำดับขั้นจะชี้ให้คุณเห็นว่าคุณต้องขอร้องจากหัวหน้าของคุณไม่ใช่จากผู้ใต้บังคับบัญชาของคุณ ซึ่งเขาก็เป็นคนที่มีบทบาทที่จะยอมรับหรือปฏิเสธความต้องการของคุณ ดังนั้นโดยทั่วไปแล้ว การเข้าใจการจัดลำดับขั้นช่วยให้เรามองเห็นว่าเราควรจะไปหาสิ่งที่เราต้องการได้อย่างเหมาะสม

การจัดลำดับมีข้อดีหลายอย่างในการออกแบบ network ที่อยู่รอบ ๆ ตัวคุณ เมื่อใช้อย่างเหมาะสมมันจะทำให้ network มีความสามารถในการคิดได้มากขึ้น มันช่วยให้เรากำหนดพื้นที่ว่าเป็นพื้นที่ไหนที่ควรจะแสดงหน้าที่อย่างชัดเจน นอกจากนั้นคุณสามารถใช้เครื่องมือเหมือนกับ access list ลำดับที่แน่นอนในลำดับชั้นของ network และหลีกเลี่ยง access list ในลำดับชั้นที่ผิด

มาดูกันว่า network ใหญ่สามารถถูกทำให้ซับซ้อนได้อย่างมากด้วย multiple protocol ที่ให้รายละเอียดขององค์ประกอบ (configuration) และเทคโนโลยีที่หลากหลาย การจัดลำดับชั้นช่วยให้เราสามารถสรุปการรวบรวมที่ซับซ้อนของรายละเอียดของโครงสร้างความเข้าใจ ดังนั้น configuraiton เฉพาะทำให้มีความต้องการ โครงสร้างที่ชี้เฉพาะการปฏิบัติที่เหมาะสมเพื่อที่จะเข้าร่วมในนั้น

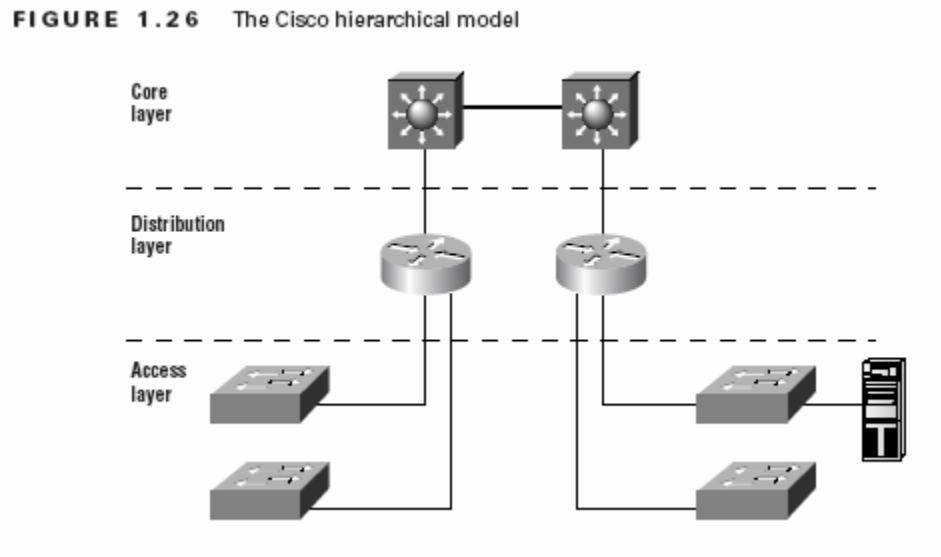
โครงสร้างการจัดลำดับชั้นของ Cisco ช่วยให้คุณออกแบบ ทำให้สำเร็จ และซ่อมแซม scalable ความเชื่อถือได้ ผลกระทบของการจัดลำชั้นของ internetwork Cisco กำหนดลำดับชั้นอยู่ 3ชั้น ดังที่จะได้เห็นในรูป 1.26 แต่ละชั้นจะมีหน้าที่เฉพาะดังนี้

- The core layre : Backbone
- The distribution layer : Routing
- The access layer : Switching

แต่ละ layer มีหน้าที่พิเศษ แต่อย่างไรก็ตามจำไว้ว่า ทั้ง 3 layer เป็น logical และไม่จำเป็นต่อกลไกของ physical มาดูกันที่ โครงสร้างของ OSI ที่เป็นลำดับขั้นที่เป็น logical อีกอันหนึ่ง Layer ทั้ง 7 ชั้นที่อธิบายหน้าที่แต่ว่าไม่จำเป็นต่อ protocol ถูกหรือไม่ บางครั้ง protocol มีโครงสร้างที่มากกว่าหนึ่ง layer ของโครงสร้าง OSI และบางครั้ง multiple protocol สื่อสารภายใน layer เดียว ในทางเดียวกันเมื่อเราสร้าง Physical ที่ทำงานได้ของลำดับชั้นของnetwork เราจะมีกลไกมากมายใน layer เดียว หรือเราจะมีกลไกการแสดงหน้าที่เดี่ยวที่ layer 2 ตัว การกำหนดของ layer เป็น logical ไม่ใช่เป็น physical

เรามาดูแต่ละ layer กันอย่างใกล้ชิดเถอะ

FIGURE 1.26 The Cisco hierarchical model



The Core Layer

ตามตัวอักษรแล้วก็ คือ ส่วนในสุดของ network ที่จุดบนสุดของการจัดลำดับ core layer มีหน้าที่ขนส่งการสื่อสารขนาดใหญ่ที่ทั้งน่าเชื่อถือและรวดเร็ว จุดประสงค์หลักของ core layer ของ network ก็คือ การ switch การสื่อสารด้วยความเร็วที่สามารถเป็นไปได้ การขนส่งการสื่อสารข้ามส่วนในสุดเป็นเรื่องธรรมดาของผู้ใช้ส่วนใหญ่ แต่อย่างไรก็ตามจำไว้ว่าผู้ใช้ข้อมูลดำเนินการที่จะกระจาย layer ที่ส่งความต้องการไปยังส่วนในสุดหากว่าต้องการ

ถ้าหากว่ามีความผิดพลาดเกิดขึ้นในส่วนในสุดทุกๆ ผู้ใช้ที่ใช้คนเดียวสามารถได้รับผลกระทบได้ ดังนั้นความต้านทานความผิดพลาดที่จุด layer นี้ คือ ผลที่เกิดขึ้น ส่วนในสุดเป็นเหมือนการพบการ

สื่อสารที่มีปริมาณมาก ดังนั้นความเร็วและศักยภาพเป็นตัวขับดันความเกี่ยวพันที่นี่ การให้หน้าที่ของส่วนในสุด คือ การออกแบบพิเศษบางอัน เราเริ่มต้นด้วยบางสิ่งที่ไม่อยากทำกันเถอะ

- อย่าทำการใด ๆ ที่ทำให้การสื่อสารช้าลง ซึ่งรวมถึงการใช้ access list การสื่อสารระหว่าง ระบบเครือข่ายจำลอง(VLANs) และ การfilter packet

- อย่า support การเข้าทำงานเป็นกลุ่มที่นี่

- หลีกเลี่ยงการกระจาย core (ตัวอย่างเช่น การเพิ่มเราเตอร์) เมื่อ internetwork โตขึ้น ถ้าการแสดงกลายมาเป็นผลที่เกิดขึ้นใน core ที่ให้สิทธิพิเศษในการ upgrades การขยายที่มากขึ้น

ตอนนี้มีสองสามสิ่งที่เราต้องการให้ทำเมื่อตอนออกแบบ core ซึ่งมีดังนี้

- ออกแบบcore เพื่อความน่าเชื่อถือที่สูง พิจารณาเทคโนโลยีการเชื่อมข้อมูลที่ทำให้ง่ายขึ้น ทั้งความเร็วและการมีมากเกินไปของการเชื่อมโยง ตัวอย่างเช่น FDDI, Fast Ethernet (ด้วยการเชื่อมที่มากมายเหลือเฟือ) หรือแม้กระทั่ง ATM

- ออกแบบด้วยความเร็วอย่างตั้งใจ core ควรจะมีศักยภาพนิดหน่อย

- เลือกการสื่อสาร protocol ด้วยเวลาการบรรจบกันที่ต่ำ ความเร็วและการมีเหลือเฟือของการสื่อสารการเชื่อมโยงข้อมูลจะไม่มีตัวช่วยถ้าพื้นผิวการสื่อสารสั้น

The Distribution Layer

Distribution layer คือ บางครั้งมีการอ้างถึงการทำงานเหมือน workgroup layer และเป็นจุดการสื่อสารระหว่างการเข้า layer และ core หน้าที่เบื้องต้นของการกระจาย layer ที่ทำให้เกิดการสื่อสาร การ filter และการเข้า WAN และตัดสินใจเรื่อง packet ที่สามารถเข้าไปสู่ core ถ้าต้องการ

ส่วนการกระจาย layer ต้องตัดสินใจเรื่องวิธีความเร็วในการเรียกใช้ network service ที่ถูกจัดการ ตัวอย่างเช่น การเรียกไฟล์ถูกส่งต่อไปยัง server หลังจากที่การกระจาย layer ตัดสินใจเลือกทางที่ดีที่สุด ส่งต่อความต้องการไปยัง core layer ถ้าหาว่าต้องการ แล้ว core layer จะส่งต่อไปยังความต้องการการบริการที่ถูกต้องโดยเร็ว

การกระจาย layer จะเป็นนโยบายสำเร็จสำเร็จ network ที่นี่คุณจะสามารถฝึกคิดอย่างเหมาะสมในการจัดการกำหนด network การกระทำทั้งหลายเหล่านี้ทั่วไปควรจะทำที่การกระจาย layer ซึ่งมีดังนี้

- router

- อุปกรณ์ประมวลผล ตัวอย่างเช่น access list, packet filter และ การเรียงลำดับ

- อุปกรณ์รักษาความปลอดภัยและหลักการของ network ร่วมด้วย address translation และ firewalls
- การกระจายซ้ำระหว่างการสื่อสาร protocol รวมทั้งการสื่อสารที่คงที่
- การสื่อสารระหว่าง VLANs และการใช้การสนับสนุนการทำงานกลุ่มอื่น ๆ
- การกำหนดของการกระจายและ multicast domain

สิ่งที่จะหลีกเลี่ยงที่การกระจาย layer ถูกจำกัดสำหรับหน้าที่เหล่านี้ที่เป็นของเฉพาะตัวสำหรับอย่างหนึ่งของ layer อื่น ๆ

The Access Layer

Access Layer ควบคุมผู้ใช้และการทำงานเป็นกลุ่มที่เข้าไปในแหล่งของ internetwork การ access layer คือ การพูดถึงเหมือนกับ desktop layer ในบางครั้ง ที่มาของnetwork ผู้ใช้ส่วนใหญ่ต้องการจะถูกหาเฉพาะที่ การกระจาย layer จัดการการสื่อสารสำหรับการใช้งานเดี่ยว ตามที่บางหน้าที่อยู่ใน access layer

- การดำเนินการเข้าการควบคุมและการสร้างหลักการ
- การสร้างการแยกการชนปะทะของโดเมน(segmentation)
- การเชื่อมต่อการทำงานเป็นกลุ่มภายในการกระจาย layer

เทคโนโลยีอย่างเช่น DDR และ Ethernet switching คือ ความถี่ที่ถูกพบใน access layer การสื่อสารที่คงที่ (แทนการสื่อสารที่ไม่คงที่ของ protocol) ถูกพบได้ที่นี่เช่นเดียวกัน

ดังที่ได้เขียนไว้ มีการแบ่งลำดับออกเป็น 3 ชั้นไม่ได้บอกเป็นนัยว่ามี router ที่แยกออก 3 ตัว ซึ่งมันสามารถมีแค่ 2-3 ตัวหรือว่ามากกว่านั้น จำไว้ว่านี่คือ วิธีการที่จัดลำดับ

Summary

ฉันรู้ว่านี่มันเหมือนกับว่าเป็นอีกหนึ่งบทที่จะไม่จบ แต่ว่ามันจบแล้ว และคุณทำมันได้ ตอนนี้คุณได้มีข้อมูลของการสร้าง คุณพร้อมที่จะสร้างมันได้ในระยะเวลาหนึ่ง และมันจะเป็นการดีที่ได้รับประกาศนียบัตรด้วยตัวคุณเอง

บทนี้เริ่มด้วยการพูดคุยเรื่องโครงสร้างของ OSI ที่มี 7 ชั้น ที่ช่วยในวิธีการพัฒนาการออกแบบที่สามารถ run บนตัวอย่างอื่นๆ ของระบบหรือnetwork แต่ละ layer มีหน้าที่พิเศษของมันเองและเลือกหน้าที่ภายในโครงสร้างที่ทำให้มั่นใจว่าแข็งแรง หรือมีผลของการสื่อสารเกิดขึ้น ฉันทำให้คุณทราบรายละเอียดของแต่ละ layer และพูดถึงแนวคิดของ Cisco ที่เกี่ยวกับโครงสร้างของ OSI

และแต่ละ layer ในโครงสร้างของ OSI มีความแตกต่างที่พิเศษของประเภทต่าง ๆ ของหลักการ ฉันบรรยายความแตกต่างของกลไก สาย cable และการเชื่อมต่อที่ใช้แต่ละ layerจำไว้ว่า hub เป็น กลไกของ physical layer และส่งสัญญาณดิจิตอลซ้ำไปยังทุก segment ที่ยอมรับสัญญาณที่มันได้รับมา switch segment ของ network ใช้ hardware address และกระจายการชนปะทะโดเมนต่าง ๆ router กระจายการกระจายโดเมน (และการชนปะทะโดเมน) และใช้การ address เป็น logic เพื่อส่ง packet โดย internetwork

สุดท้าย บทนี้ว่าด้วยเรื่องของโครงสร้างลำดับชั้น 3 ชั้นของCisco ฉันอธิบายรายละเอียดของ 3 layer และวิธีช่วยออกแบบและทำให้สำเร็จของแต่ละ layer ของ Cisco internetwork เรากำลังจะพูดเรื่อง IP addressing ในบทถัดไป

Exam Essentials

จำเรื่องสาเหตุของความเป็นไปได้ของการหนาแน่นของการสื่อสารของ LAN host ที่มากเกินไปในการกระจายโดเมน broadcast storms multicasting และ bandwidth ต่ำ ที่เป็นสาเหตุทั้งหมดของการเกิดความหนาแน่นของการสื่อสารของ LAN

ความเข้าใจที่แตกต่างระหว่าง collision domain และ broadcast domain. Collision domainคือระยะเวลาของ Ethernet ที่ถูกใช้อธิบายการรวบรวมของกลไกของ network ในกลไกที่เป็นพิเศษที่ส่ง packet บนส่วนต่าง ๆ ของ network การพบกันของทุก ๆ กลไกบน segment เดียวกันที่ให้ความสนใจการกระจายโดเมน คือ ที่ซึ่งชุดของกลไกทั้งหมดบน segment ของ network ได้ยินการกระจายทั้งหมดที่ส่งบนsegment นั้น

ความเข้าใจระหว่าง hub , bridge , switch และ router. Hub สร้างการชนปะทะเดียวและการกระจายเดียว. Bridge กระจายการชนปะทะของโดเมนต่าง ๆ แต่สร้างการกระจายโดเมนใหญ่ ๆ อันหนึ่ง พวกมันใช้ hardware address เพื่อ filter network. Switch เป็น bridge ที่มี port เป็นทวีคูณกับความฉลาดที่มากกว่า พวกมันกระจายการชนปะทะแต่ว่าสร้างการกระจายโดเมนใหญ่อันหนึ่งด้วย default switch ใช้

hardware address เพื่อ filter network . Router กระจายการกระจายโดเมน (และการชนปะทะโดเมน) และใช้ address เป็น logic เพื่อ filter network

จำเรื่องความแตกต่างระหว่าง connection-oriented (การปรับการสื่อสาร) และ connectionless (การไร้การสื่อสาร) ในการทำงานของ network การปรับการสื่อสารใช้การยอมรับและการควบคุม flow เพื่อสร้าง session ที่น่าเชื่อถือ ยิ่งไปกว่านั้นการปรับการสื่อสารถูกใช้มากกว่าการไร้การสื่อสาร ในการทำงานของ network การไร้การสื่อสารของการทำงานถูกใช้ส่งข้อมูลโดยไม่ยอมรับหรือการควบคุม flow นี่เป็นการคิดที่ไม่น่าเชื่อถือ

จำ layer ของ OSI คุณต้องจำว่าโครงสร้างของ OSI มี 7 ชั้นและแต่ละ layer มีหน้าของมันเอง Application, Presentation และ Session layer เป็น layer ชั้นสูงกว่าและมีหน้าที่สำหรับการสื่อสารจากผู้ใช้ติดต่อกับกลไกการใช้งาน (application) Transport layer ทำให้เกิด การแบ่งส่วนย่อย ๆ (segmentation) การเรียงลำดับ (sequencing) และ virtual circuit (วงจรที่ใช้งาน) network layer ทำให้เกิดการสร้าง address ของ network ที่เป็น logic และการสื่อสารโดย internetwork Data Link layer ทำให้เกิดโครงสร้างและการวางแผนของข้อมูลบน network ขนาดกลาง Physical layer มีหน้าที่สำหรับการนำ 1 และ 0 และใส่รหัสตัวเลข 1กับ 0 ในสัญญาณดิจิตอลสำหรับการส่งบน network

จำเรื่องประเภทต่าง ๆ ของ Ethernet cabling และเมื่อคุณจะใช้มัน สายเคเบิล 3 ประเภทที่สามารถสร้างจากสายเคเบิลของEthernet คือ straight-through (เพื่อการเชื่อมต่อของ PC หรือ router ของEthernet ที่ติดต่อไปยัง hubหรือ switch) การข้าม (การเชื่อมต่อ hub ไปยัง hub หรือ hub ไปยัง switch หรือจาก switch ไปหา switch หรือ จาก PC ไปยัง PC) และการม้วน (สำหรับแผงควบคุมการสื่อสารจาก PC ไปยัง router หรือ switch)

การเข้าใจวิธีการเชื่อมต่อสายเคเบิลของแผงควบคุมจาก PC ไปยัง router และการเริ่ม Hypet Terminal การม้วนสายเคเบิลและการเชื่อมต่อมันจาก COM port ของ host ไปยัง แผงควบคุม port ของ router การเริ่มHyper Terminal และการติดตั้ง BPS ให้เป็น 9600 และควบคุม flow จนกระทั่งเป็น none

จำเรื่อง โครงสร้าง 3 ชั้นของ Cisco ทั้ง 3 layers ในการจัดลำดับของ Cisco เป็นcore, distribution(การกระจาย) และ access layers