บทที่ 2
อุปกรณ์เครือข่าย

สายสัญญาณ

ในโลกของการสื่อสารและเครือข่ายคอมพิวเตอร์จะไม่สามารถทำงานได้ หากปราศจากสื่อนำข้อมูล (Transmission Media) ซึ่งทำหน้าที่เป็นตัวกลางในการถ่ายโอนข้อมูลระหว่าง

อุปกรณ์บนเครือข่าย

การที่คอมพิวเตอร์เครื่องหนึ่งจะส่งข้อมูลไปยังอีกเครื่องหนึ่งได้นั้น ต้องมีการเชื่อมต่อกันด้วยสื่อนำสัญญาณประเภทใดประเภทหนึ่งสื่อนำสัญญาณที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ สามารถแบ่งออกได้เป็น 2 ประเภทดังนี้

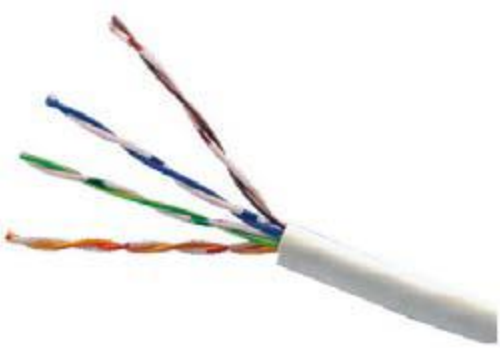
1. สายนำสัญญาณ
   1.1. สายคู่บิดเกลียว (Twisted Pairs)
   1.2. สายโคแอคเชียล (Coaxial Cable)
   1.3. สายใยแก้วนำแสง (Fiber Optics)
2. สื่อไร้สาย (Wireless)

เครือข่ายคอมพิวเตอร์ในปัจจุบันนอกจากสายสัญญาณเป็นสื่อนำข้อมูลแล้ว สื่อไร้สายก็เป็นอีกทางเลือกหนึ่งที่ใช้เชื่อมต่อคอมพิวเตอร์เป็นเครือข่าย เช่น WLAN (Wireless LAN) เป็นเครือข่ายท้องถิ่นที่ใช้อากาศเป็นสื่อนำสัญญาณ

สายคู่บิดเกลียว

เมื่อก่อนเป็นสายสัญญาณที่ใช้ในระบบโทรศัพท์ แต่ปัจจุบันได้กลายเป็นมาตรฐานสายสัญญาณที่เชื่อมต่อในเครือข่ายแบบท้องถิ่น (LAN) สายคู่บิดเกลียวหนึ่งคู่ประกอบด้วยสายทองแดงขนาดเล็ก (Copper) เส้นผ่านศูนย์กลางประมาณ 0.016-0.035 นิ้ว หุ้มด้วยฉนวน (Outer Insulator) แล้วบิดเป็นเกลียวเป็นคู่ โดยสายคู่หนึ่งก็ใช้สำหรับการสื่อสารหนึ่งช่องทางการบิดเป็นเกลียวของสายแต่ละคู่ เพื่อช่วยลดคลื่นแม่เหล็กไฟฟ้าที่รบกวนซึ่งกันและกัน ซึ่งอาจมีจำนวนหลายๆ คู่ที่นำมารวบเข้าด้วยกันและหุ้มด้วยฉนวนภายนอก (Outer Jacket) เช่น สายคู่บิดเกลียวที่ใช้กับเครือข่ายท้องถิ่น (CAT5) ภายในฉนวนห่อหุ้ม

จะมีจำนวนสาย 4 คู่ด้วยกันและหากเป็นสายที่นำไปใช้กับการส่งข้อมูลในระยะทางไกลๆ จำนวนสายภายในอาจมีมากกว่าหนึ่งร้อยคู่

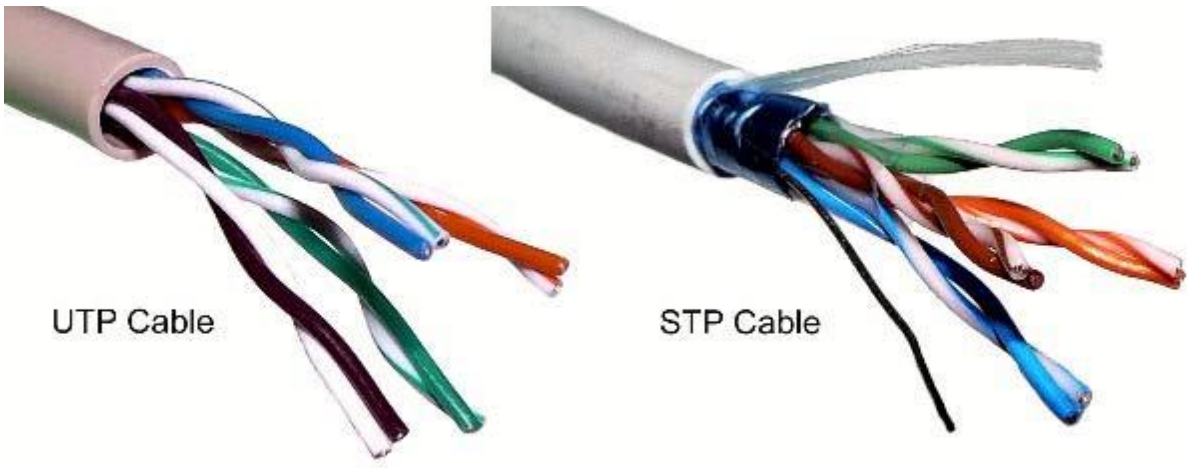


รูปที่ 2.1.1 สายคู่บิดเกลียว Cat-5e รูปที่ 2.1.2 สายคู่บิดเกลียว Cat-5 25 Pairs

ที่มา : www.made-in-china.com, http://img.alibaba.com

สายคู่บิดเกลียวที่มีขายในท้องตลาดมีหลายประเภทด้วยกัน ซึ่งสายสัญญาณอาจจะประกอบด้วยสายคู่บิดเกลียวตั้งแต่หนึ่งคู่ไปจนถึง 600 คู่ในสายขนาดใหญ่ สายคู่บิดเกลียวที่ใช้กับเครือข่าย LAN จะประกอบด้วย 4 คู่ แบ่งออกได้ 2 ประเภทคือ

1. STP (Shielded Twisted Pairs) หรือสายคู่บิดเกลียวชนิดมีชีลด์
2. UTP (Unshielded Twisted Pairs) หรือสายคู่บิดเกลียวชนิดไม่มีชีลด์



รูปที่ 2.1.3 สาย STP และ UTP

ที่มา : www.lanshack.com

Shielded Twist Pair (STP)

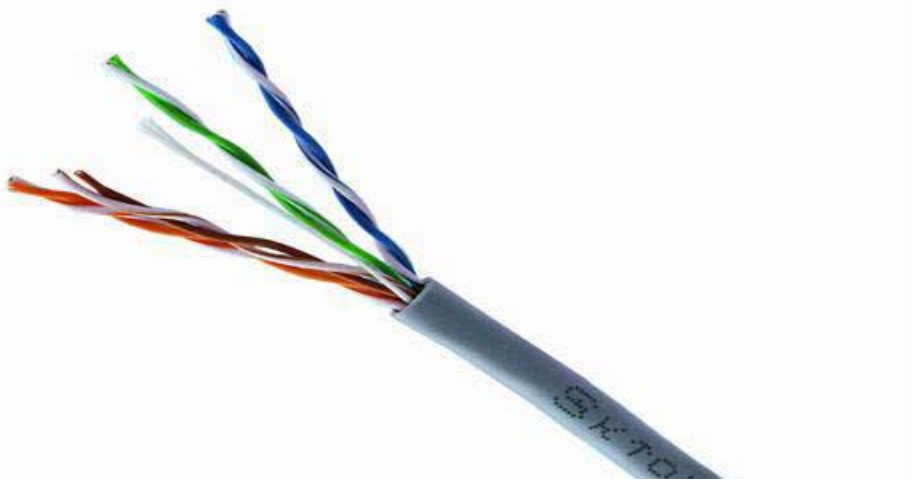
สายคู่บิดเกลียวแบบมีชิลด์ หรือ STP จะมีส่วนที่ป้องกันสัญญาณรบกวนจากภายนอก ซึ่งชั้นป้องกันนี้อาจจะเป็นแผ่นโลหะบางๆ หรือใยโลหะที่ถักเป็นตาข่าย และห่อหุ้มสายคู่บิดเกลียวทั้งหมด จุดประสงค์ของการเพิ่มชั้นห่อหุ้มนี้เพื่อป้องกันสัญญาณรบกวนจากคลื่นแม่เหล็กไฟฟ้าภายนอก เช่น คลื่นวิทยุจากแหล่งต่างๆ ในอากาศ

รูปที่ 2.1.4 โครงสร้างของสาย STP (แบบ SFTP และ FTP)

ที่มา : www.lanshack.com

Unshielded Twist Pair (UTP)

สายคู่บิดเกลียวแบบไม่มีชิลด์ หรือ UTP จะไม่มีส่วนป้องกันสัญญาณรบกวนจากภายนอก เป็นสายที่นิยมเรียกกันสั้นๆ ว่า สาย UTP และเป็นสายที่นิยมใช้งานกันมากที่สุดในระบบเครือข่ายคอมพิวเตอร์ปัจจุบัน การใช้งานสายนี้ความยาวต้องไม่เกิน 100 เมตร



รูปที่ 2.1.5 โครงสร้างของสาย UTP

ที่มา : www.techfest.com, www.global-b2b-network.com

คุณสมบัติพิเศษของสายคู่บิดเกลียว

การใช้สายคู่บิดเกลียวในการรับส่งสัญญาณนั้นจำเป็นต้องใช้สายหนึ่งคู่ในการส่งสัญญาณ และอีกหนึ่งคู่ในการรับสัญญาณ ซึ่งในแต่ละคู่สายจะมีทั้งขั้วบวกและขั้วลบ ในการทำเช่นนี้เป็นเทคนิคอย่างหนึ่งในการรับส่งข้อมูลที่เรียกว่า “Differential Signaling” ซึ่งเทคนิคนี้คิดค้นขึ้นมาเพื่อที่จะกำจัดคลื่นรบกวนที่เกิดกับสัญญาณข้อมูล ที่เกิดขึ้นได้ง่าย และเมื่อเกิดขึ้นกับสายสัญญาณแล้วจะทำให้ข้อมูลยากต่อการอ่านหรือแปลความหมายตัวส่งสัญญาณจะส่งสัญญาณสองสัญญาณ ซึ่งสัญญาณหนึ่งเป็นสัญญาณบวกบนสาย T+ และอีกสัญญาณหนึ่งคือสายสัญญาณลบบนสาย T- เมื่อถึงปลายทางสัญญาณ T- จะถูกกลับรูปร่างของสัญญาณอีกที ซึ่งถ้าไม่มีคลื่นรบกวน สัญญาณ T+ และส่วนกลับของสัญญาณ T- ควรจะมีลักษณะคล้ายๆกัน แต่ถ้ามีคลื่นรบกวน สองสัญญาณนี้จะมีส่วนที่แตกต่างกัน ซึ่งส่วนที่แตกต่างกันนี้เกิดขึ้นจากคลื่นรบกวนนั่นเอง ตามทฤษฎีของคลื่นรบกวนแล้ว คลื่นรบกวนจะเกิดขึ้นกับทั้งสองสัญญาณในขนาดที่เกือบจะเท่ากัน ดังนั้นเมื่อกลับอีกสัญญาณหนึ่ง แล้วบวกทั้งสองสัญญาณเข้าด้วยกัน ส่วนที่เป็นสัญญาณรบกวนก็จะถูกหักล้างกันไป ทำให้ได้เฉพาะสัญญาณที่ต้องการจริงๆ เท่านั้น

มาตรฐานสายสัญญาน

สมาคมอุตสาหกรรมอิเล็กทรอนิกส์ หรือ EIA (Electronics Industries Association) และสมาคมอุตสาหกรรมโทรคมนาคม หรือ TIA (Telecommunication Industries Association) ได้ร่วมกันกำหนดมาตรฐาน EIA/TIA 568 ซึ่งเป็นมาตรฐานที่ใช้ในการผลิตสาย UTP โดยมาตรฐานนี้ ได้แบ่งประเภทของสายออกเป็นหลายประเภทโดยแต่ละประเภทจะเรียกว่า Category N โดย N คือ หมายเลขที่บอกประเภท ส่วนสถาบันมาตรฐานนานาชาติ (International Organization for Standardization) ได้กำหนดมาตรฐานนี้เช่นกัน โดยเรียกสายแต่ละประเภทเป็น Class A-F คุณสมบัติโดยทั่วไปของสายแต่ละประเภทเป็นดังนี้

Category 1/Class A: เป็นสายที่ใช้ได้กับระบบโทรศัพท์อย่างเดียว เหมาะกับการส่งข้อมูลชนิดเสียง

Category 2/Class B: เป็นสายที่รองรับแบนด์วิธได้ถึง 4 MHz และสามารถส่งข้อมูลดิจิตอลได้ถึง 4 Mbps ซึ่งประกอบด้วยสายคู่บิดเกลียว 4 คู่

Category 3/Class C: เป็นสายที่สามารถส่งข้อมูลได้ถึง 16 Mbps และมีสายคู่บิดเกลียว 4 คู่Category 4 : เป็นสายที่สามารถส่งข้อมูลได้ถึง 20 Mbps และมีสายคู่บิดเกลียว 4 คู่

Category 5/Class D: เป็นสายที่สามารถส่งข้อมูลได้ถึง 100 Mbps โดยใช้สาย 2 คู่และสามารถรับส่งข้อมูลได้ถึง 1000 Mbps เมื่อใช้ 4 คู่สายCategory 5 Enhanced (5e): เช่นเดียวกับ Cat5 แต่มีคุณภาพของสายที่ดีกว่า เพื่อรองรับการส่งข้อมูลแบบฟูลดูเพล็กซ์ที่ 1000 Mbps ซึ่งใช้ 4 คู่สาย

Category 6/Class E: รองรับแบนด์วิธได้ถึง 250 MHz

Category 7/Class F: รองรับแบนด์วิธได้ถึง 600 MHz และกำลังอยู่ในระหว่างวิจัย

มาตรฐาน TIA/EIA นั้นได้กำหนดคุณสมบัติต่างๆของสายสัญญาณ UTP ดังนี้

- ความต้านทาน (Impedance) : โดยทั่วไปจะกำหนดไว้ที่ 100 Ohm + 15 %
- ค่าสูญเสียสัญญาณ (Attenuation) : ของสายที่ความยาว 100 เมตร คือ อัตราส่วนระหว่างกำลังสัญญาณที่ส่งต่อกำลังสัญญาณที่วัดได้ที่ปลายสาย มีหน่วยเป็นเดซิเบล (dB)
- NEXT (Near-End Cross Talk) : เป็นค่าของสัญญาณรบกวนของสายคู่ส่งต่อสายคู่รับที่ฝั่งส่งสัญญาณ โดยวัดเป็นเดซิเบลเช่นกัน
- PS-NEXT (Power-Sum NEXT) : เป็นค่าที่คำนวนได้จากสัญญาณรบกวน NEXTของสายอีก 3 คู่ที่มีผลต่อสายคู่ที่วัด ค่านี้จะมีผลเมื่อใช้สายสัญญาณทั้งคู่ในการรับส่งสัญญาณ เช่น กิกะบิตอีเธอร์เน็ต
- FEXT (Far-End Cross Talk) : จะคล้ายกับ NEXT แต่เป็นการวัดค่าสัญญาณรบกวนที่ปลายสาย
- ELFEXT (Equal-Level Far-End Cross Talk) : เป็นค่าที่คำนวณได้จากค่าสูญเสียของสัญญาณ (Attenuation) ลบด้วยค่า FEXT ดังนั้นค่า ELFEXT ยิ่งสูง (มีค่ามาก) แสดงว่าค่าสูญเสียยิ่งสูงด้วย
- PS-ELFEXT (Power-Sum ELFEXT) : เป็นค่าที่คำนวณคล้ายๆกับค่า PS-NEXT คือ เป็นค่าที่คำนวณได้จากการรวม ELFEXT ที่เกิดจากสายสามคู่ที่เหลือ
- Return Loss : เป็นค่าที่วัดได้จากอัตราส่วนระหว่างกำลังสัญญาณที่ส่งไปต่อกำลังสัญญาณที่สะท้อนกลับมายังต้นสาย
- Delay Skew : เนื่องจากสัญญาณเดินทางบนสายสัญญาณแต่ละคู่ด้วยเวลาที่ต่างกันค่าดีเลย์สกิวคือ ค่าแตกต่างระหว่างคู่ที่เร็วที่สุดกับคู่ที่ช้าที่สุด

ตารางมาตรฐาน EIA/TIA 568 **และ** ISO/IEC 11801

Category/Class	Cat 5/Class D	Cat 5e	Cat 6/Class E	Cat 7/Class F
Bandwidth	100 MHz	100 MHz	250 MHz	600 MHz
Delay	< 548 ns	< 548 ns	< 548 ns	< 504 ns
Delay Skew	< 50 ns	< 50 ns	< 50 ns	< 20 ns
Attenuation (dB)	24dB@100MHz	24dB@100MHz	36dB@250MHz	54.1dB@600MHz
NEXT (dB)	29.3dB@100MHz	32.3dB@100MHz	33.1dB@250MHz	51.0dB@600MHz
PSNEXT (dB)	N/A	27.1dB@100MHz	30.2dB@250MHz	48dB@600MHz
ELFEXT (dB)	17dB@100MHz	21dB@100MHz	19.2dB@250MHz	Future Study
PSELFEXT (dB)	29.3dB@100MHz	29.3dB@100MHz	39.3dB@250MHz	29.3dB@600MHz
Return Loss (dB)	15-10log(f/20)	17-7log(f/20)	19-10log(f/20)	

ปัญหาหนึ่งของการใช้สายส่งสัญญาณคือ ครอสทอล์ค (Crosstalk) ซึ่งหมายถึงสัญญาณบนสายหนึ่งจะรบกวนสัญญาณบนสายอีกสายหนึ่ง สายคู่บิดเกลียวได้ถูกออกแบบมาเพื่อช่วยลดปัญหานี้ โดยการบิดคู่สายเป็นเกลียวทำให้สัญญาณรบกวนในแต่ละสายหักล้างกัน ถ้าจำนวนเกลียวต่อหน่วยความยาวยิ่งมากเท่าใด จะทำให้ป้องกันครอสทอล์คได้ดีเท่านั้น แต่ข้อเสียคือ จะทำให้ความยาวของสายเพิ่มขึ้น

หัวเชื่อมต่อ RJ-45

สายคู่บิดเกลียวจะใช้หัวเชื่อมต่อแบบ RJ-45 ซึ่งจะมีลักษณะคล้ายกับหัวเชื่อมต่อแบบ RJ-11 ซึ่งเป็นหัวที่ใช้กับสายโทรศัพท์ทั่วๆ ไปข้อแตกต่างระหว่างหัวเชื่อมต่อสองประเภทนี้คือ หัว RJ-45 จะมีขนาดใหญ่กว่าเล็กน้อยและไม่สามารถเสียบเข้ากับปลั๊กโทรศัพท์ได้ และอีกอย่างหัว RJ-45 จะเชื่อมสายคู่บิดเกลียว 4 คู่ ในขณะที่หัว RJ-11 ให้ได้กับสายเพียง 2 คู่เท่านั้น

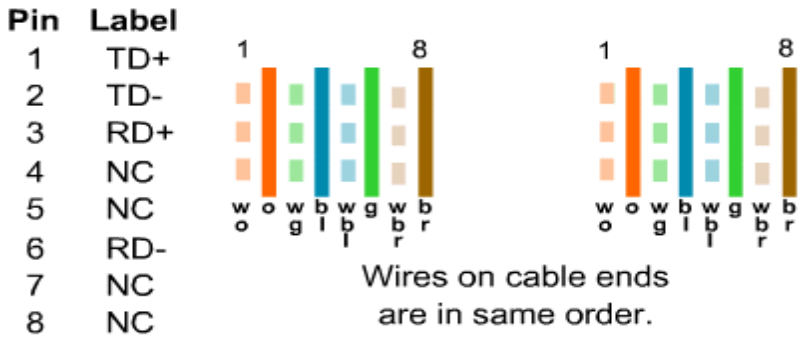
รูปที่ 2.1.6 หัวเชื่อมต่อ RJ-11, RJ-12 และ RJ-45

ที่มา : http://users.utu.fi

มาตรฐานการเข้าหัวสาย UTP

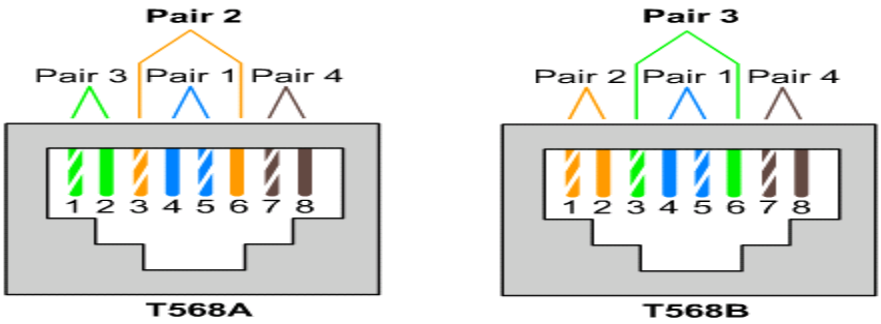
การเข้าหัวสาย UTP นั้นมีอยู่ 2 มาตรฐานที่ได้กำหนดไว้คือ TIA/EIA 568A และ 568B ดังนี้

PIN#	Signal	TIA/EIA 568A	TIA/EIA 568B
1	Transmit+	ขาวเขียว	ขาวส้ม
2	Transmit-	เขียว	ส้ม
3	Receive+	ขาวส้ม	ขาวเขียว
4	N/A	ฟ้า	ฟ้า
5	N/A	ขาวฟ้า	ขาวฟ้า
6	Receive-	ส้ม	ส้ม
7	N/A	ขาวน้ำตาล	ขาวน้ำตาล
8	N/A	น้ำตาล	น้ำตาล



รูปที่ 2.1.7 มาตรฐานการเข้าหัวสาย UTP

ที่มา : http://users.utu.fi



รูปที่ 2.1.8 การเข้าหัว RJ-45 แบบ TIA/EIA 568A และ 568B

ที่มา : http://users.utu.fi

การทดสอบสาย UTP

เมื่อติดตั้งสาย UTP เสร็จแล้ว ขั้นตอนต่อไปคือ การทดสอบสายสัญญาณดังกล่าวให้เป็นไปตามมาตรฐาน ซึ่งเครื่องมือที่ใช้ในการทดสอบสาย UTP จะเรียกว่า เคเบิ้ลแอนาไลเซอร์ (Cable Analyzer)

รูปที่ 2.1.9 Cable Analyzer

ที่มา : www.thailandmultimeter.com

สิ่งที่ทดสอบสายสัญญาณนั้นมีดังต่อไปนี้

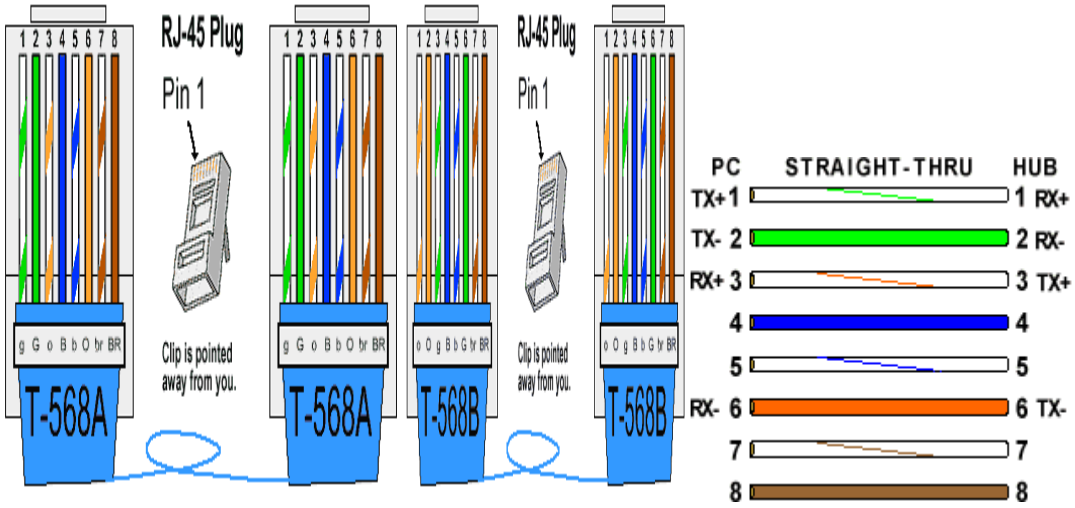
- Wire Map : คือการทดสอบสายสัญญาณว่าติดตั้งถูกต้องหรือไม่ ซึ่งสิ่งที่ต้องทดสอบ คือ
  - ทดสอบการสิ้นสุดที่ปลายสายทั้งสองด้าน
  - ทดสอบความต่อเนื่องของสาย หรือสายขาดระหว่างปลายสายทั้งสองด้าน หรือไม่
  - ทดสอบว่าสายสัญยาณวงจรแต่ละคู่วงจรปิดหรือไม่
  - การทดสอบการครอสโอเวอร์สาย
- ความยาวสาย (Length) : ซึ่งสาย UTP ที่ใช้กับระบบอีเธอร์เน็ตต้องไม่เกิน 100 เมตร
- ค่าคุณสมบัติต่างๆ ของสาย เช่น Delay Skew, Attenuation, NEXT, PSNEXT, ELFEXT เป็นต้น

การใช้งานสาย UTP

การเข้าหัวสาย UTP เพื่อนำสาย UTP ไปใช้งานในระบบเครือข่ายคอมพิวเตอร์นั้นสามารถแบ่งออกได้เป็น 3 ชนิดคือ

1. สาย Straight-Through Cables เป็นสายที่ใช้เชื่อมต่ออุปกรณ์เข้าด้วยกันดังนี้

- สวิทช์ (Switch) กับ เราท์เตอร์(Router)
- สวิทช์ (Switch) กับ คอมพิวเตอร์พีซี (PC) หรือคอมพิวเตอร์เซิร์ฟเวอร์ (Server)
- ฮับ (Hub) กับ คอมพิวเตอร์พีซี (PC) หรือคอมพิวเตอร์เซิร์ฟเวอร์ (Server)

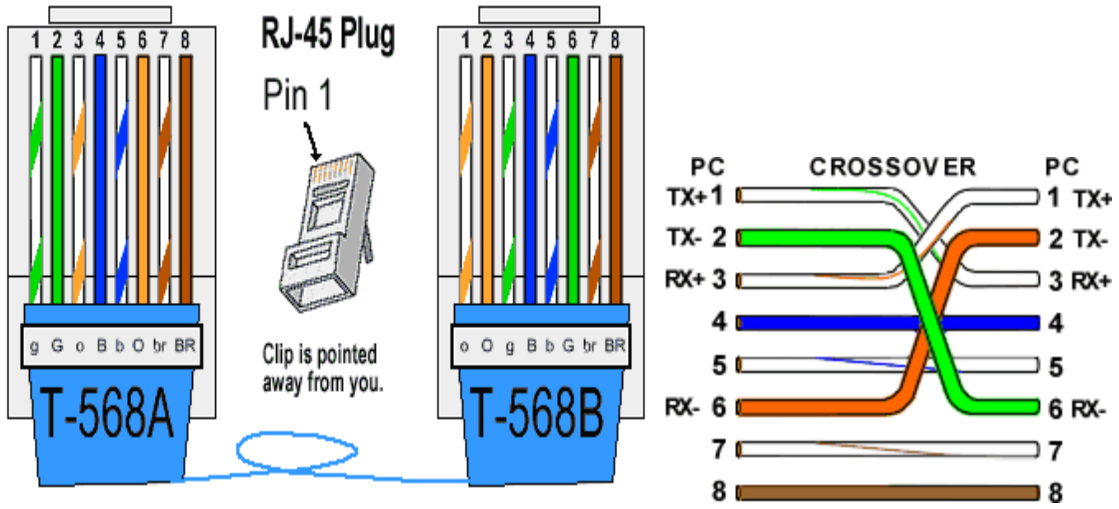


รูปที่ 2.1.10 Straight-Through Ethernet Cable

ที่มา : www.patraswireless.net

2. สาย Crossover Cables เป็นสายที่ใช้เชื่อมต่ออุปกรณ์เข้าด้วยกันดังนี้

- สวิทช์ (Switch) กับ สวิทช์ (Switch)
- สวิทช์ (Switch) กับ ฮับ (Hub)
- ฮับ (Hub) กับ ฮับ (Hub)
- เราท์เตอร์(Router) กับ เราท์เตอร์(Router)
- คอมพิวเตอร์พีซี (PC) กับ คอมพิวเตอร์พีซี (PC)

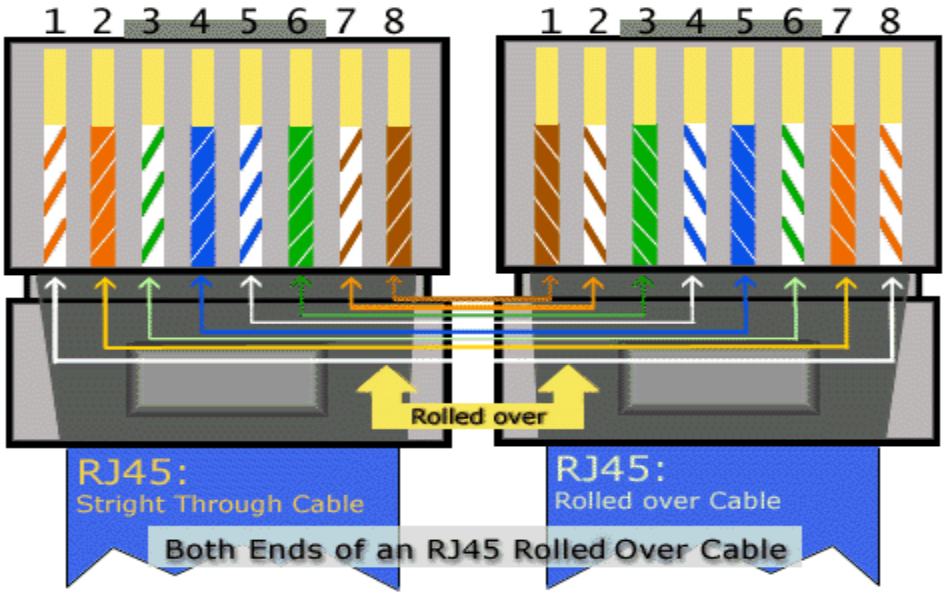


รูปที่ 2.1.11 RJ-45 Crossover Ethernet Cable

ที่มา : www.patraswireless.net

3. สาย Rollover Cable เป็นสายที่ใช้เชื่อมต่ออุปกรณ์เข้าด้วยกันดังนี้

- เราท์เตอร์(Router) กับ คอมพิวเตอร์พีซี (PC)
- สวิทช์ (Managed Switch) กับ คอมพิวเตอร์พีซี (PC)



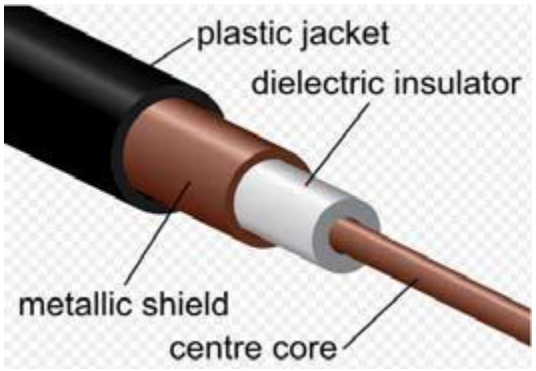
รูปที่ 2.1.12 Rollover Cable

ที่มา : https://secure.cecn.mtu.edu

สายโคแอคเชียล (Coaxial Cable)

เป็นสายสัญญาณประเภทแรกที่ใช้ และเป็นที่นิยมมากในเครือข่ายคอมพิวเตอร์สมัยแรกๆ แต่ในปัจจุบัน เครือข่ายส่วนใหญ่จะใช้สายคู่บิดเกลียวและสายใยแก้วนำแสง ส่วนสายโคแอคเชียลถือได้ว่าเป็นสายที่ล้าสมัยสำหรับเครือข่ายคอมพิวเตอร์ในปัจจุบัน อย่างไรก็ตามยังมีระบบเครือข่ายบางประเภทที่ยังใช้สายประเภทนี้อยู่

สายโคแอคเชียล ส่วนใหญ่จะเรียกสั้นๆ ว่าสายโคแอ็กซ์ (Coax) จะมีตัวนำไฟฟ้าอยู่สองส่วน คำว่า “โคแอ็กซ์” มีความหมายว่า “มีแกนร่วมกัน” ซึ่งชื่อก็บอกความหมายว่าตัวนำทั้งสองตัวมีแกนร่วมกันนั่นเอง โครงสร้างของสายโคแอคเชียล ประกอบด้วยสายทองแดงเป็นแกนกลาง แล้วห่อหุ้มด้วยวัสดุที่เป็นฉนวน ชั้นต่อมาจะเป็นตัวนำไฟฟ้าอีกชั้นหนึ่ง ซึ่งจะเป็นแผ่นโลหะบางๆ หรือ อาจจะเป็นใยโลหะที่ถักเปียหุ้มอีกชั้นหนึ่ง สุดท้ายก็หุ้มด้วยฉนวนและวัสดุป้องกันสายสัญญาณ



รูปที่ 2.2.1 โครงสร้างของสายโคแอคเชียล

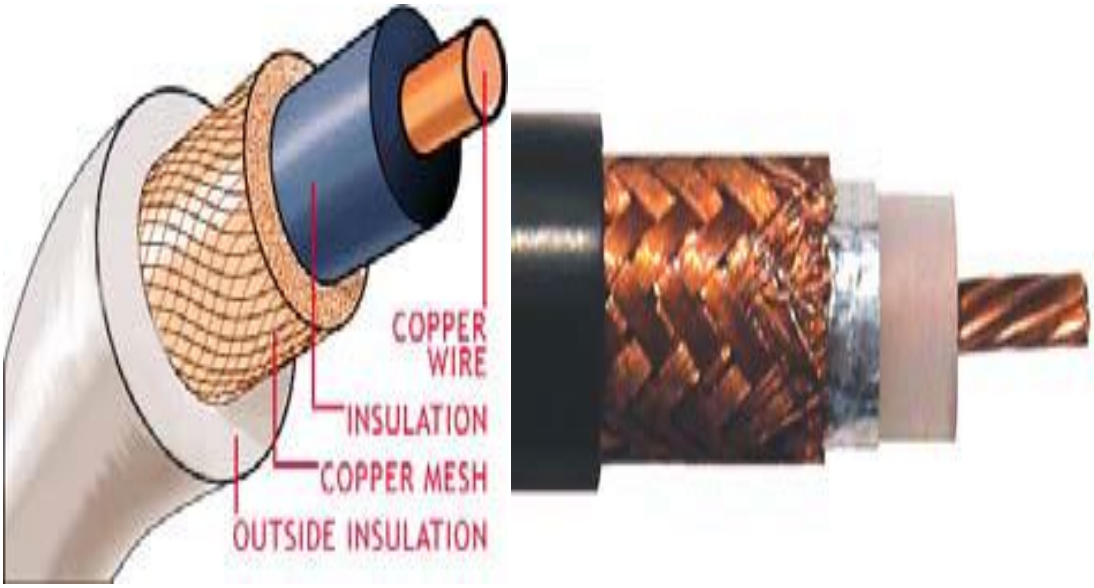
ที่มา : http://commons.wikimedia.org

ส่วนแกนเป็นส่วนที่นำสัญญาณข้อมูล ส่วนชั้นใยข่ายเป็นชั้นที่ใช้ป้องกันสัญญาณรบกวนจากภายนอก และเป็นสายดิน(กราวด์)ในตัว ดังนั้นสองส่วนนี้ต้องไม่เชื่อมต่อกันมิฉะนั้นอาจเกิดไฟช็อตได้

สายโคแอคเชียล (coaxial) เป็นตัวกลางเชื่อมโยงที่มีลักษณะเช่นเดียวกับสายที่ต่อจากเสาอากาศสายโคแอคเชียลที่ใช้ทั่วไปมี 2 ชนิด คือ 50 โอห์มซึ่งใช้ส่งข้อมูลแบบดิจิทัล และชนิด 75โอห์มซึ่งใช้ส่งข้อมูลสัญญาณแอนะล็อก

สายโคแอคเชียลเป็นสายสัญญาณนำข้อมูลไฟฟ้า มีความถี่ในการส่งข้อมูลประมาณ 100MHz ถึง 500 MHz

ส่วนใหญ่สายโคแอคเชียลจะมีลักษณะคล้ายกัน แต่แบ่งออกได้หลายประเภทขึ้นอยู่กับชนิดของเครือข่ายที่ใช้ สายโคแอคเชียลจะถูกแยกเป็นประเภทต่างๆ โดยใช้มาตรา RG (Radio Grade Scale) ซึ่งคำว่า RG ย่อมาจาก Radio Grade ซึ่งมีความหมายว่าท่อนำคลื่น ส่วน /U ที่ต่อท้าย RG จะหมายว่า indicates multiple uses คือสามารถใช้งานได้หลากหลาย สายโคแอคเชียลแบบ RG-58 จะใช้กับเครือข่ายอีเธอร์เน็ตแบบ 10Base2 ซึ่งจะมีค่าความต้านทานที่ 50 โอห์ม



รูปที่ 2.2.2 สายโคแอคเชียล

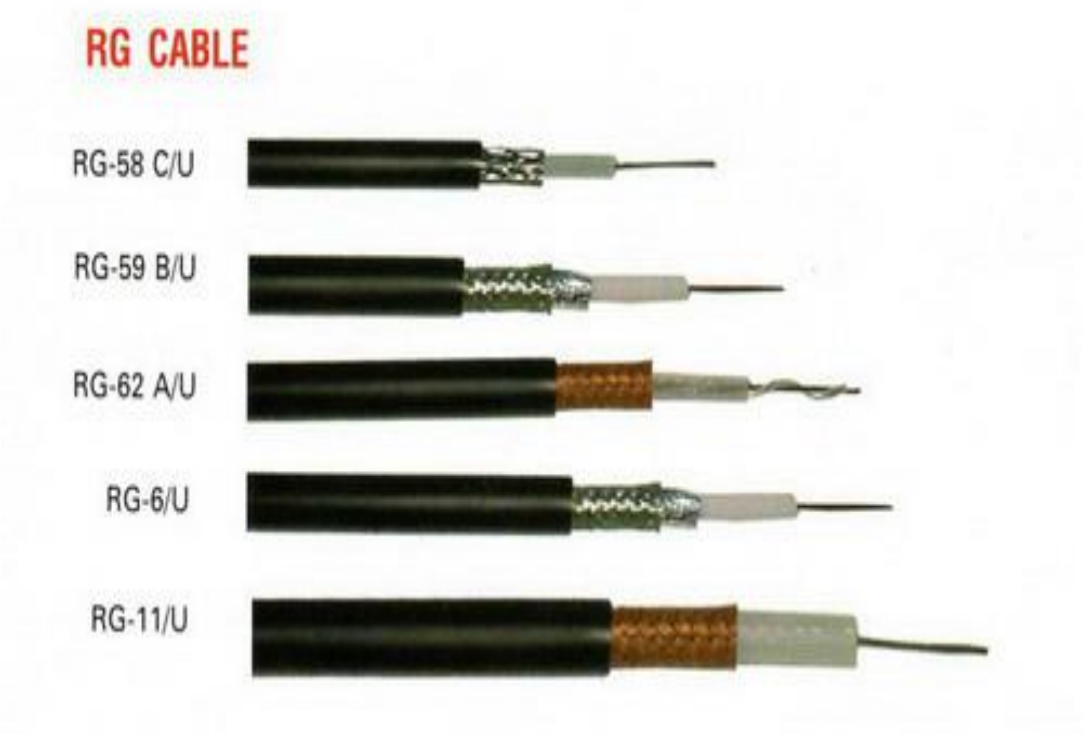
ที่มา : http://searchnetworking.techtarget.com

สาย RG มีด้วยกันหลากหลายรุ่น และแต่ละรุ่นจะมีลักษณะภายนอกคล้ายกัน ซึ่งประกอบไปด้วย 4 ส่วนที่สำคัญดังนี้

- Conductor ตัวนำสัญญาณซึ่งเป็นแกนทองแดง
- Insulator ฉนวนหุ้มตัวนำสัญญาณ
- Shield ทองแดงถักหุ้มตลอดทั้งเส้น เพื่อป้องกันสัญญาณรบกวน
- Jacket ใช้ภายในอาคารจะเป็น PVC, ใช้ภายนอกอาคารจะเป็น PE, ใช้แขวนเสาจะเป็น PE และมี Messenge

มาตรฐานของสาย Coaxial นั้น ถูกกำหนดโดยใช้สัญลักษณ์ RG-# (Radio Guide) มีมาตรฐาน ดังนี้

Type	Impedance	เส้นผ่าศูนย์กลาง	ใช้สำหรับ
RG-6/U	75Ω	0.332" in (8.5mm)	ระบบเคเบิลทีวี หรือจากเสาอากาศโทรทัศน์
RG-6/UQ	75Ω		ที่เป็นสาย RG- 6มีฉนวนหุ้มมากกว่าสาย 6/Uธรรมดา
RG-8/U	50Ω	0.405 in (10.287mm)	Thick Ethernet (10Base5)
RG-9/U	51Ω	0.42 in (10.668 mm)	
RG-11/U	75 Ω	0.405 in(10.287mm)	
RG-58/U	50 or 52 Ω	0.2 in (5 mm)	Thin Ethernet (10base2)
RG-59/U	75 Ω	0.242 in (6.15 mm)	
RG-62/U	92 Ω	0.242 in (6.15 mm)	ARCNET
RG-178/U	50 Ω	0.079 in (2.00 mm)	
RG-179/U	75 Ω	0.094 in (2.38 mm)	



รูปที่ 2.2.3 ประเภทต่างๆ ของ สายโคแอคเชียล

ที่มา : http://www.telepart.net

ประเภทของสายโคแอคเชียล

สายโคแอคเชียลแบ่งออกเป็น 2 ประเภทคือ

1. สายโคแอคเชียลแบบบาง (Thin Coaxial Cable)
2. สายโคแอคเชียลแบบหนา (Thick Coaxial Cable)

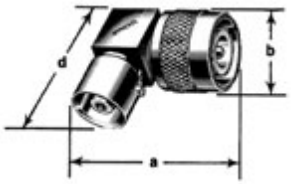
ข้อดี สายโคแอคเชียลจะใช้ใยโลหะถักเป็นชีลด์ (Shield) ทำให้ถูกรบกวนจากแหล่งไฟฟ้าน้อยกว่าสายทองแดงบิดเกลียว

ข้อเสีย สายโคแอคเชียลมีราคาแพงกว่า10-20 เท่าของสายทองแดงคู่บิดเกลียว และยากต่อการใช้งานมากกว่าสายทองแดงคู่บิดเกลียว บางครั้งก็ยังไม่ยืดหยุ่นต่อการใช้งานการส่งผ่านข้อมูล

ขั้วต่อสาย Coaxial แบบต่างๆ

แบบ	Impedance	**ความถี่สูงสุด** RF	Peak Peak	Power	**ราคา**	**รูป**
UHF	50	300 MHz	500 โวลต์	500 วัตต์	ถูก	
BNC	50 หรือ 75	4 GHz	1000 โวลต์	500 วัตต์	ถูก	
TNC	50	10 GHz	1000 โวลต์	1000 วัตต์	ปานกลาง	

ขั้วต่อสาย Coaxial แบบต่างๆ

แบบ	Impedance	**ความถี่สูงสุด** RF	Peak Peak	Power	**ราคา**	**รูป**
N	50 หรือ 75	11 GHz	1000 โวลต์	1000 วัตต์	ปานกลาง	
C	50	11 GHz	1500 โวลต์	-	-	
SMA	50	18 GHz	1000 โวลต์	500 วัตต์	ปานกลาง	
F	75	1 GHz	-	-	ถูก	

สายโคแอคเชียลแบบบาง (Thin Coaxial Cable)

เป็นสายที่มีขนาดเล็ก เส้นผ่านศูนย์กลางประมาณ 0.64 cm. เนื่องจากสายประเภทนี้มีขนาดเล็กและมีความยืดหยุ่นสูงจึงสามารถใช้ได้กับการติดตั้งเครือข่ายเกือบทุกประเภท สายประเภทนี้สามารถนำสัญญาณได้ไกลถึง 185 เมตร ก่อนที่สัญญาณจะเริ่มอ่อนกำลังลง

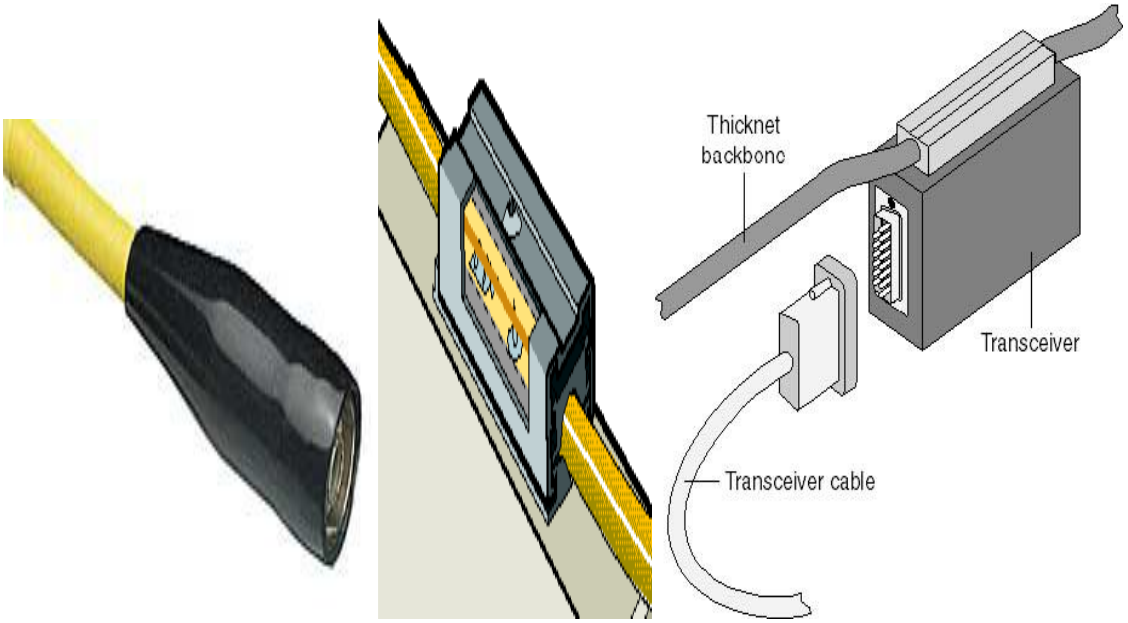
บริษัทผู้ผลิตสายโคแอคเชียลได้ลงความเห็นร่วมกันในการแบ่งประเภทของสายโคแอคเชียลดังแสดงในตาราง สายโคแอคเชียลแบบบางได้ถูกรวมไว้ในสายประเภท RG-58 ซึ่งสายประเภทนี้จะมีความต้านทาน (Impedance) ที่ 50 โอห์ม มีแกนกลางอยู่ 2 ลักษณะคือ แบบที่เป็นสายทองแดงเส้นเดียวและแบบที่เป็นใยโลหะหลายเส้น

รูปที่ 2.2.4 สายโคแอคเชียลแบบบาง

ที่มา : www.amazon.co.uk ,www.hbernstaedt.de

สายโคแอคเชียลแบบหนา (Thick Coaxial Cable)

เป็น สายโคแอคเชียลที่ค่อนข้างแข็ง และใหญ่กว่า สายโคแอคเชียลแบบบาง โดยมีเส้นผ่านศูนย์กลางประมาณ 1.27 cm. สายโคแอคเชียลแบบหนานี้เป็นสายสัญญาณประเภทแรกที่ใช้กับเครือข่ายอีเธอร์เน็ต ส่วนแกนกลางที่เป็นสายทองแดงของ สายโคแอคเชียลแบบหนาจะมีขนาดใหญ่กว่า ดังนั้น สายโคแอคเชียลแบบหนาจึงสามารถนำสัญญาณได้ไกลกว่าแบบบาง โดยสามารถนำสัญญาณได้ไกลถึง 500 เมตร ด้วยความสามารถนี้สายโคแอคเชียลแบบหนาจึงนิยมใช้ในการเชื่อมต่อเส้นทางหลักของข้อมูล หรือ แบ็คโบน (Backbone) ของเครือข่ายสมัยแรกๆ แต่ปัจจุบันได้เลิกใช้ สายโคแอคเชียลแล้ว โดยสายที่นิยมใช้ทำเป็นแบ็คโบนคือ สายใยแก้วนำแสง



รูปที่ 2.2.5 สายโคแอคเชียลแบบหนา

ที่มา: www.homestead.co.uk, www.blackbox.com,

เปรียบเทียบระหว่าง สายโคแอคเชียลแบบบางกับแบบหนา (Thinnet and Thicknet) ตามกฎการนำสัญญาณ สายที่ใหญ่กว่าย่อมนำสัญญาณได้ดีกว่า แต่สายโคแอคเชียลแบบหนา (Thicknet) จะยุ่งยากในการติดตั้งมากกว่า เนื่องจากเป็นสายที่ค่อนข้างแข็ง ในขณะที่สายโคแอคเชียลแบบบาง (Thinnet) มีความยืดหยุ่นที่ดีกว่าทำให้ง่ายต่อการติดตั้งและราคาก็ถูกกว่า ความยืดหยุ่นของสายมีผลต่อการติดตั้งเมื่อเดินสายผ่านท่อขนาดเล็กที่ติดบนฝ้าเพดาน ทำให้เป็นที่นิยมมากกว่า

รูปที่ 2.2.6 การเปรียบเทียบสายโคแอคเชียล

ที่มา : http://technet.microsoft.com

หัวเชื่อมต่อ

สายโคแอคเชียลแบบบางและแบบหนา (Thinnet and Thicknet) จะใช้หัวเชื่อมต่อชนิดเดียวกัน ที่เรียกว่าหัวต่อ BNC ซึ่งใช้ในการเชื่อมต่อระหว่างสายสัญญาณและเน็ตเวิร์คการ์ด หัวเชื่อมต่อแบบ BNC นี้มีหลายแบบ ดังนี้

1. หัวเชื่อมสาย BNC (BNC Cable Connector) เป็นหัวที่เชื่อมเข้ากับปลายสายโคแอคเชียล
2. หัวเชื่อมสายรูปตัว T (BNC T-Connector) เป็นหัวที่ใช้เชื่อมต่อระหว่างสายสัญญาณกับเน็ตเวิร์คการ์ด
3. หัวเชื่อมสาย Barrel (BNC Barrel Connector) เป็นหัวที่ใช้ในการเชื่อมต่อสายสัญญาณเพื่อให้สายมีขนาดความยาวมากขึ้น
4. ตัวสิ้นสุดสัญญาณ (BNC Terminator) เป็นหัวที่ใช้ในการสิ้นสุดสัญญาณ

(BNC Connector) BNC T-Connector BNC Barrel Connector BNC Terminator

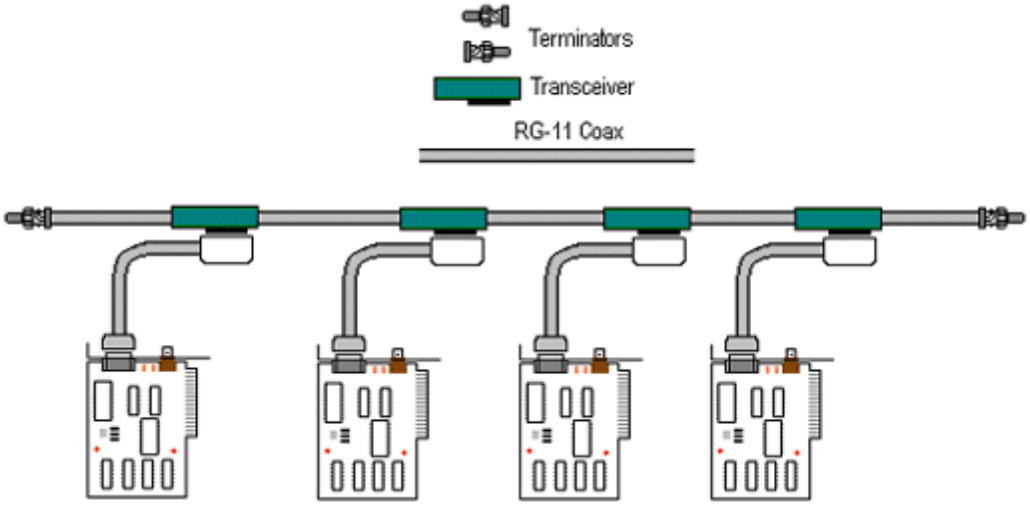
รูปที่ 2.2.7 หัวเชื่อมต่อสายโคแอคเชียลแบบต่างๆ

ที่มา : http://www.traderscity.com, https://hongkong01.rs-online.com

มาตราฐาน 10BASE

เป็นมาตรฐานซึ่งกำหนดขึ้นโดยองค์กร IEEE ใช้เป็นสายสื่อสารมาตรฐานในการสื่อสารข้อมูลด้วยโปรโตคอล CSMA/CD (หรือ IEEE 802.3) ซึ่งยังแบ่งออกเป็น

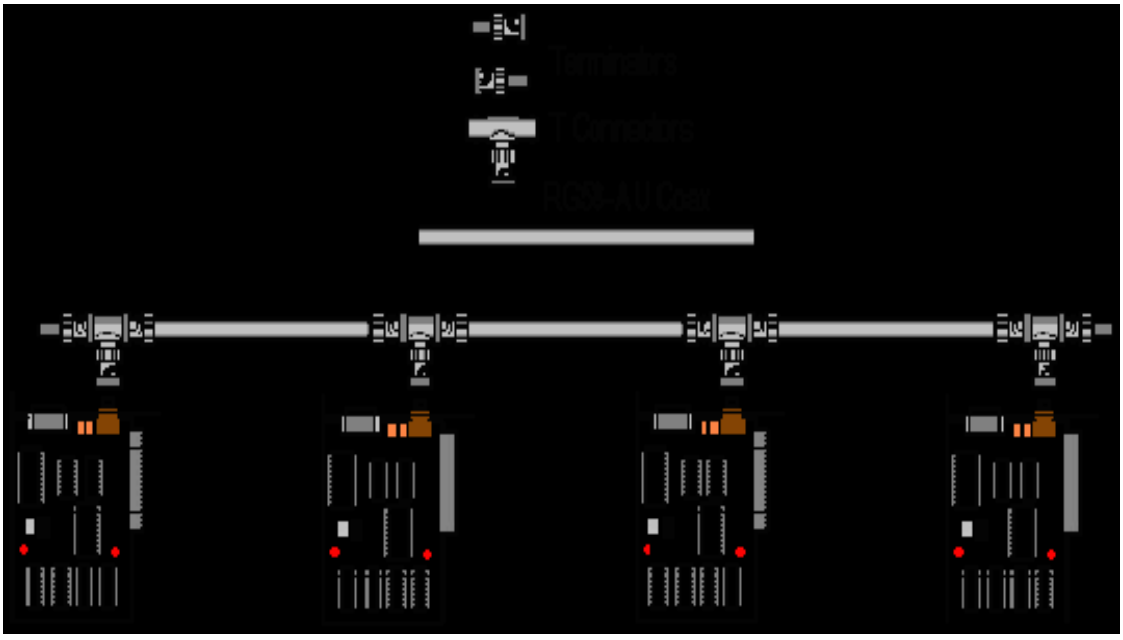
1. มาตรฐาน 10BASE5 หรือมาตรฐาน Original 802.3 Standard เป็นสายโคแอคเชียลมาตรฐานของเครือข่าย LAN ที่มีแบบการส่งสัญญาณข้อมูลแบบเบสแบนด์ สามารถส่งข้อมูลได้ด้วยอัตราเร็ว 10 Mbpsความยาวสูงสุดของสายสื่อสารใน 1 ช่วง (Segment) จากปลายสุดด้านหนึ่งของสายถึงปลายสุดอีกด้านหนึ่งของสายเท่ากับ 500 เมตร โดยสามารถมีแทป (Tap) ต่อเข้าระหว่างสาย 1 ช่วงได้สูงสุดเท่ากับ 100 แทป ระยะทางของการสื่อสารจะสามารถเพิ่มขึ้นได้อีกถ้ารีพีตเตอร์โดยจำกัดไว้ว่าสามารถใช้รีพีตเตอร์ได้มากที่สุด 4 เครื่องต่อ 1 เส้นทางระหว่าง 2 สเตชั่น ซึ่งทำให้สามารถเพิ่มระยะทางการสื่อสารของเครือข่าย LAN ไปได้ไกลถึง 2.5 กม.



รูปที่ 2.2.8 การเชื่อมต่อตามมาตรฐาน 10Base5

ที่มา : http://cptd.chandra.ac.th

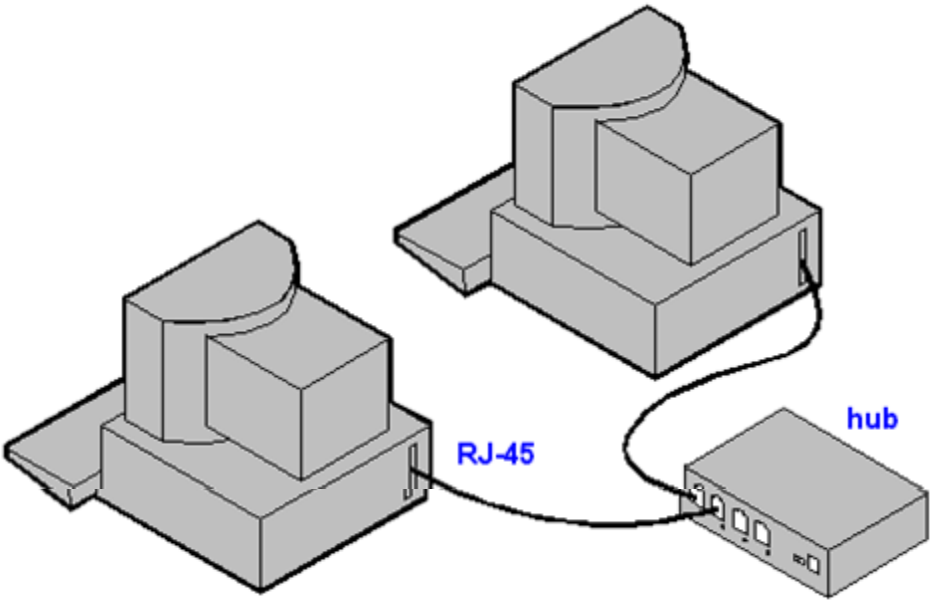
2. มาตรฐาน 10BASE2 หรือสาย Cheapernet เป็นสายโคแอคเชียลที่มีขนาดเล็กกว่าสาย10 BASE5 แต่มีอัตราส่งข้อมูลเท่ากัน ทำให้ราคาของสาย 10 BASE2 ถูกกว่า แต่การที่ขนาด ของสายเล็กลงก็ทำให้ระยะทางการเชื่อมต่อสเตชั่นเข้ากับสายเคเบิลสั้นลงด้วย คือสามารถมีแทปใน1 ช่วงสายได้สูงสุด 30 แทปและมีระยะทางการสื่อสารได้ไกลสุดเท่ากับ 185 เมตร



รูปที่ 2.2.9 การเชื่อมต่อตามมาตรฐาน 10Base2

ที่มา : http://cptd.chandra.ac.th

3. มาตรฐาน 10BASE-T เป็นสายเกลียวคู่แบบไม่มีชีลด์ซึ่งใช้กับเครือข่าย LAN แบบ Passive STAR เช่นกัน แต่มีอัตราเร็วในการส่งข้อมูลสูงถึง 10 เมกะบิตต่อวินาที

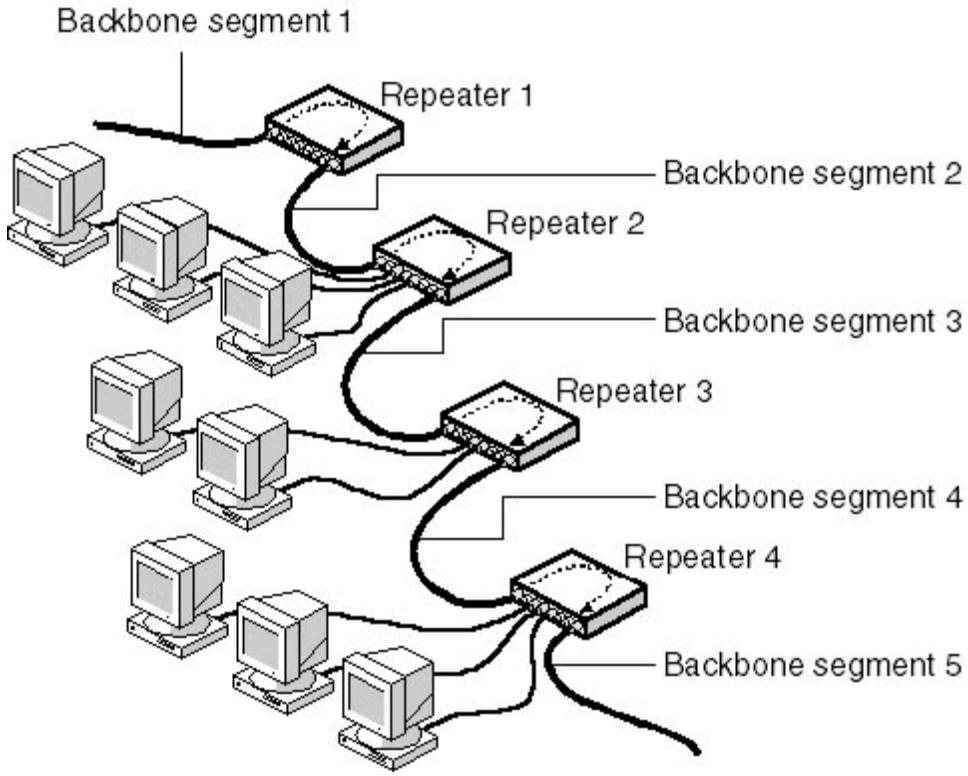


รูปที่ 2.2.10 การเชื่อมต่อตามมาตรฐาน 10Base-T

ที่มา : http://dictionary.zdnet.com

4. มาตรฐาน 10Broad36 หรือสาย Broadband เป็นสายโคแอคเชียลแบบบรอดแบนด์ซึ่งสามารถรับส่งสัญญาณได้หลายช่องสัญญาณในสายเส้นเดียวกัน วิธีการโดยการแบ่งแถบความถี่ที่กว้างออกเป็นช่องความถี่ย่อยๆ แล้วแต่ละช่องสามารถรับส่งข้อมูลได้โดยไม่ขึ้นต่อกัน ตัวอย่างการรับส่งข้อมูลแบบบอรดแบนด์เช่น เคเบิลทีวี โดยสัญญาณทีวีแต่ละช่องจะส่งไปบนสายเคเบิลเดียวกัน การเปลี่ยนช่องทีวีก็คือการปรับช่องความถี่ให้รับสัญญาณของช่องทีวีที่ต้องการนั่นเอง
5. มาตรฐาน 10Broad36 ถูกออกแบบเพื่อสำหรับการเชื่อมต่อที่ต้องการระยะทางมากกว่าแบนด์วิธเลข 36 หมายถึง 3,600 เมตร แต่การใช้งานจริงๆ นั้นมีน้อยมาก เนื่องจากส่วนใหญ่จะนิยมใช้สายไฟเบอร์ออฟติกสำหรับการเชื่อมต่อในระยะไกลการเลือกสาย Coaxial ให้เหมาะกับการใช้งานและให้ได้ประสิทธิภาพสูง มีหลักที่ต้องคำนึงถึงดังนี้
   - ค่าความต้านทานไฟฟ้ากระแสสลับ (Impedance) มีหน่วยวัดเป็น Ohms. โดยทั่วไปจะมีอยู่ด้วยกัน 2 ค่าคือ 50 Ohms. (ใช้กับระบบ LAN ซึ่งในปัจจุบันไม่เป็นที่นิยม
   - เนื่องจากใช้สาย UTP แทน) และ 75 Ohms. (ใช้กับระบบรักษาความปลอดภัย, ระบบกล้องโทรทัศน์วงจรปิด, ระบบเคเบิ้ลทีวี, ทีวีรวม และระบบดาวเทียม)

- ค่าการลดทอนสัญญาณ มีหน่วยวัดเป็น dB ซึ่งค่าที่ได้ยิ่งน้อยเท่าไหร่ การนำสัญญาณของสายเส้นนั้นยิ่งมีประสิทธิภาพสูง
- Shield ส่วนมากจะวัดออกมาเป็น % (เปอร์เซ็นต์) ยิ่งมาก ยิ่งดี เพราะจะได้ช่วยป้องกันสัญญาณรบกวนจากภายนอกได้อย่างมีประสิทธิภาพ
- ควรเลือก Jacket ให้เหมาะสมกับงานที่จะใช้ติดตั้งกฎ 54321



รูปที่ 2.2.11 การเชื่อมต่อตามกฎ 54321

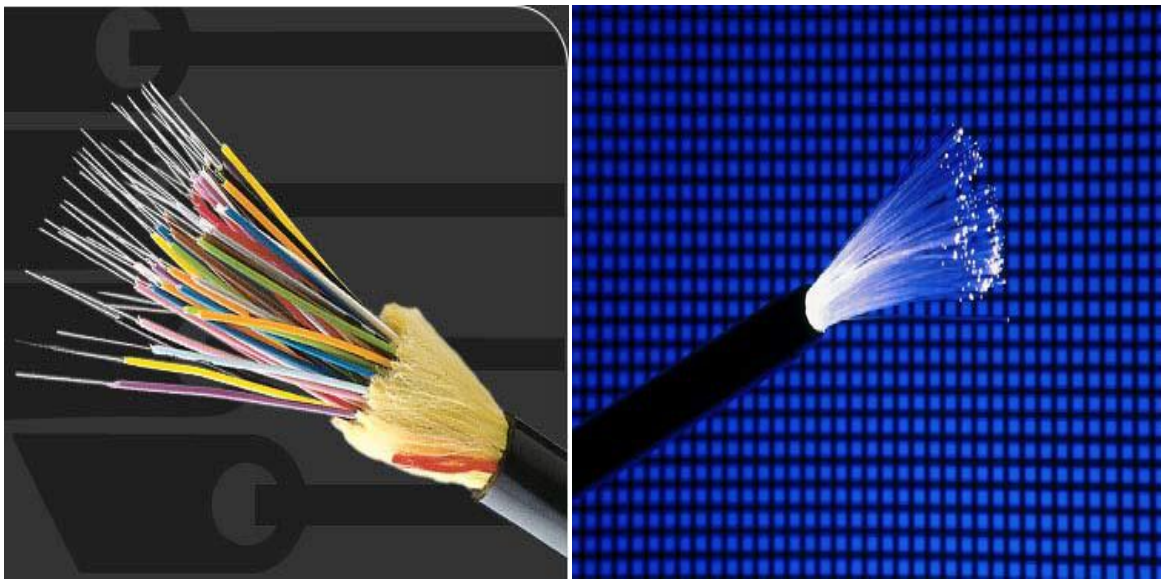
ที่มา : www.microsoft.com

ในระบบ Network ในอดีตนั้นยังไม่มีอุปกรณ์ประเภท Bridge และ Switch เพื่อที่จะนำมาใช้ในการเชื่อมโยง Segment ระหว่างกัน สมัยนั้นมีเพียงอุปกรณ์ประเภท shared-access Ethernet ซึ่งนั้นก็คือ Ethernet ประเภทหนึ่งที่ใช้อุปกรณ์ Repeater หรือ Hub ในการเชื่อมโยงSegment ระหว่างกัน โดยในการใช้ Repeater หรือ Hub ในการเชื่อมโยงนั้นจะมีข้อจำกัดในการเชื่อมโยง Segment และข้อจำกัดของจำนวน Repeater หรือ Hub ที่จะนำมาใช้ในการเชื่อมโยง ซึ่งได้มีกฎ “54321” ขึ้นมาซึ่งกฎของ “54321” นั้นก็คือ จะถูกนำไปใช้ในการเชื่อมต่อใน สองลักษณะดังนี้

ลักษณะแรก ในกรณีที่ต้องการเชื่อมโยง Segment ระหว่างกันโดยใช้ Repeater หรือ Hub นั้นจะสามารถเชื่อมโยง Segment ได้สูงสุดเพียง 5 Segment และสามารถใช้อุปกรณ์ Repeater หรือ Hub ได้สูงสุดเพียง 4 ตัว

ลักษณะที่สอง ในกรณีที่ต้องการเชื่อมโยง Segment โดยใช้ Repeater หรือ Hub เชื่อมโยงระหว่างกันในลักษณะ End-to-End ผ่านอุปกรณ์ที่ชื่อ IRL (เป็นสาย Fiber Optic ชนิดหนึ่ง) จำนวน2 คู่ โดยที่สามารถเชื่อมโยง Segment ได้สูงสุดเพียง 3 Segmentจาก 2 ลักษณะถ้ามารวมกันก็จะกลายเป็น 54321 (1 คือ ทั้งหมดที่กล่าวมาอยู่ใน collisiondomains เดียวกัน)

สายใยแก้วนำแสง (Fiber Optic)



รูปที่ 2.3.1สายใยแก้วนำแสง

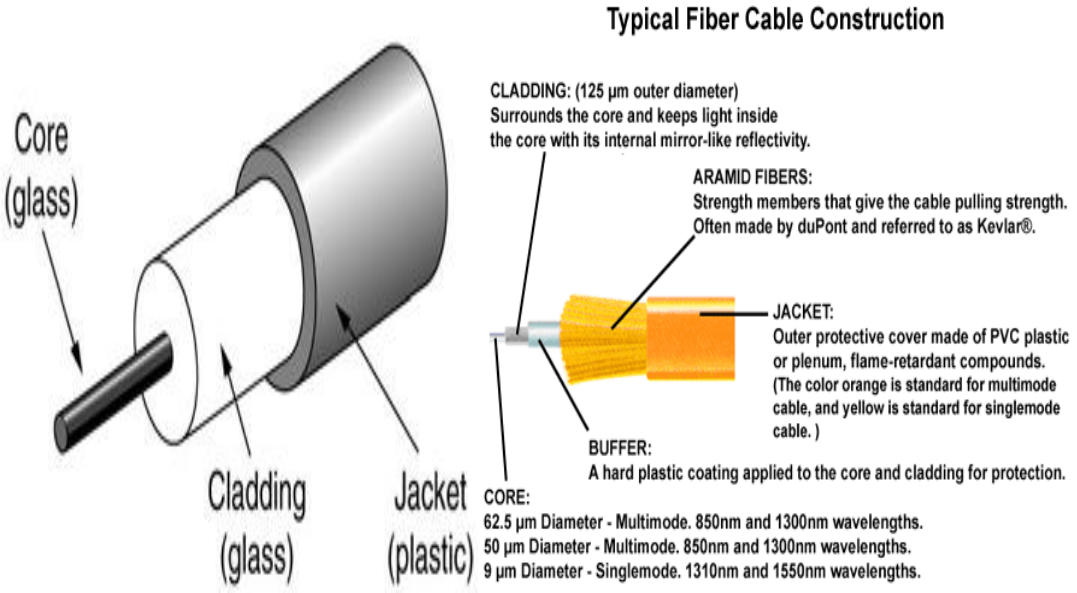
ที่มา : http://www.fiberopticspros.net

สายสัญญาณที่ใช้กับเครือข่ายคอมพิวเตอร์ในปัจจุบันมี 2 ประเภท โดยแบ่งตามชนิดของตัวนำที่ใช้ ประเภทแรกคือ แบบที่ใช้โลหะเป็นตัวนำสัญญาณ (Conductive Metal) เช่น สายคู่บิดเกลียว (Twist Pairs) และสายโคแอ๊กซ์ (Coaxial Cable) ซึ่งปัญหาของสายที่มีตัวนำเป็นโลหะนั้นก็คือสัญญาณที่วิ่งอยู่ภายในสายนั้นอาจจะถูกรบกวนได้โดยคลื่นแม่เหล็กไฟฟ้าแหล่งต่างๆ เช่น มอเตอร์ไฟฟ้า เครื่องใช้ไฟฟ้าต่างๆ ที่ผลิตสนามแม่เหล็ก หรือแม้กระทั่งปรากฏการณ์ธรรมชาติ เช่น ฟ้าผ่าเป็นต้น และการเดินสายเป็นระยะทางไกลมากๆ เช่นระหว่างประเทศจะมีการสูญเสียของสัญญาณเกิดขึ้น จึงต้องใช้อุปกรณ์สำหรับทวนสัญญาณติดเป็นจำนวนมาก เพราะฉนั้นจึงมีการคิดค้นและพัฒนาสายสัญญาณแบบใหม่ ซึ่งใช้ตัวนำ

ซึ่งไม่ได้เป็นโลหะขึ้นมาก็คือ สายใยแก้วนำแสง (Fiber Optic) ซึ่งใช้สัญญาณแสงในการส่งแทนสัญญาณไฟฟ้า ทำให้การส่งสัญญาณไม่ถูกรบกวนจากสนามแม่เหล็กไฟฟ้าต่างๆ ทั้งยังคงทนต่อสภาพแวดล้อมอีกด้วย และตัวกลางที่ใช้สำหรับการส่งสัญญาณแสงก็คือ ใยแก้วซึ่งมีขนาดเล็กและบางทำให้ประหยัดพื้นที่ไปได้มาก สามารถส่งสัญญาณไปได้ไกลโดยมีการสูญเสียของสัญญาณน้อย ทั้งยังให้อัตราข้อมูล (Band Width) ที่สูงกว่าสายแบบโลหะหลายเท่าตัว

โครงสร้างของเส้นใยแก้วนำแสง

ส่วนประกอบของใยแก้วนำแสงประกอบด้วยส่วนสำคัญคือ ส่วนที่เป็นแกน (Core) ซึ่งจะอยู่ตรงกลางหรือชั้นในแล้วหุ้มด้วยส่วนห่อหุ้ม (Cladding) แล้วถูกหุ้มด้วยส่วนป้องกัน (Coating) อีกชั้นหนึ่งโดยที่แต่ละส่วนนั้นทำด้วยวัสดุที่มีค่าดัชนีการหักเหของแสงต่างกัน ทั้งนี้ก็เพราะต้องคำนึงถึงหลักการหักเหและแสงสะท้อนกลับหมดของแสง ส่วนที่เหลือก็จะเป็นส่วนที่ช่วยในการติดตั้งสายสัญญาณได้ง่ายขึ้น เช่น Strengthening Fiber ก็เป็นส่วนที่ป้องกันไม่ให้สายไฟเบอร์ขาดเมื่อมีการดึงสายในตอนที่ติดตั้งสายสัญญาณ



รูปที่ 2.3.2โครงสร้างของสายใยแก้วนำแสง

ที่มา : http://lib.store.yahoo.net

แกน (Core)

เป็นส่วนตรงกลางของเส้นใยแก้วนำแสง และเป็นส่วนนำแสง โดยดัชนีหักเหของแสงส่วนนี้ต้องมากกว่าส่วนของแคลด (Clad) ลำแสงที่ผ่านไปในแกนจะถูกขังหรือเคลื่อนที่ไปตามแกนของเส้นใยแก้วนำแสงด้วยกระบวนการสะท้อนกลับหมดภายใน

ส่วนห่อหุ้ม (Cladding)

เป็นส่วนที่ห่อหุ้มส่วนของแกนเอาไว้ โดยส่วนนี้จะมีดัชนีหักเหน้อยกว่าส่วนของแกนเพื่อให้แสงที่เดินทางภายในแกน สะท้อนอยู่ภายในแกนตามกฎของการสะท้อนด้วยการสะท้อนกลับหมด โดยใช้หลักของมุมวิกฤติ

ส่วนป้องกัน (Coating/Buffer)

เป็นชั้นที่ต่อจากแคลด เป็นที่กันแสงจากภายนอกเข้าเส้นใยแก้วนำแสงและยังใช้ประโยชน์เมื่อมีการเชื่อมต่อเส้นใยแก้วนำแสง โครงสร้างอาจจะประกอบไปด้วยชั้นของพลาสติกหลายๆ ชั้น นอกจากนั้นส่วนป้องกันยังทำหน้าเป็นตัวป้องกันจากแรงกระทำภายนอกอีกด้วยตัวอย่างของค่าดัชนีหักเห เช่น แกนมีค่าดัชนีหักเหประมาณ 1.48 ส่วนของแคลดและส่วนป้องกันซึ่งทำหน้าที่ป้องกันแสงจากแกนออกไปภายนอกและป้องกันแสงภายนอกรบกวน จะมีค่าดัชนีหักเหเป็น 1.46 1.52 ตามลำดับ

คลื่นแสงและไฟเบอร์ออฟติค

สายไฟเบอร์ออฟติคทำจากใยแก้วขนาดเล็กซึ่งประกอบด้วย2 ส่วนหลักคือ แกนหรือคอร์ (Core) และถูกห่อหุ้มด้วยแคลดดิ้ง (Cladding) แสงที่เป็นตัวนำสัญญาณจะถูกส่งเข้าไปในคอร์เนื่องจากส่วนคอร์และแคลดดิ้งมีค่าดัชนักเหไม่เท่ากัน ทำให้แสงกระทบผิวของแคลดดิ้งแล้วสะท้อนกลับหมด (Total Reflection) ให้แสงเดินทางเฉพาะส่วนที่เป็นคอร์ไปจนถึงปลายทาง การเดินทางของแสงเป็นไปตามกฎการส่งสัญญาณของแสง(Principle of the transmission) ซึ่งสรุปคร่าวๆ ดังนี้

- ลำแสงจะส่องเข้าใยแก้วด้วยมุมเล็กๆ (θ)
- ความสามารถของใยแก้วในการรับแสงจะถูกจำกัดโดยค่า NA (Numerical Aperture)

ซึ่งคำนวณได้จาก

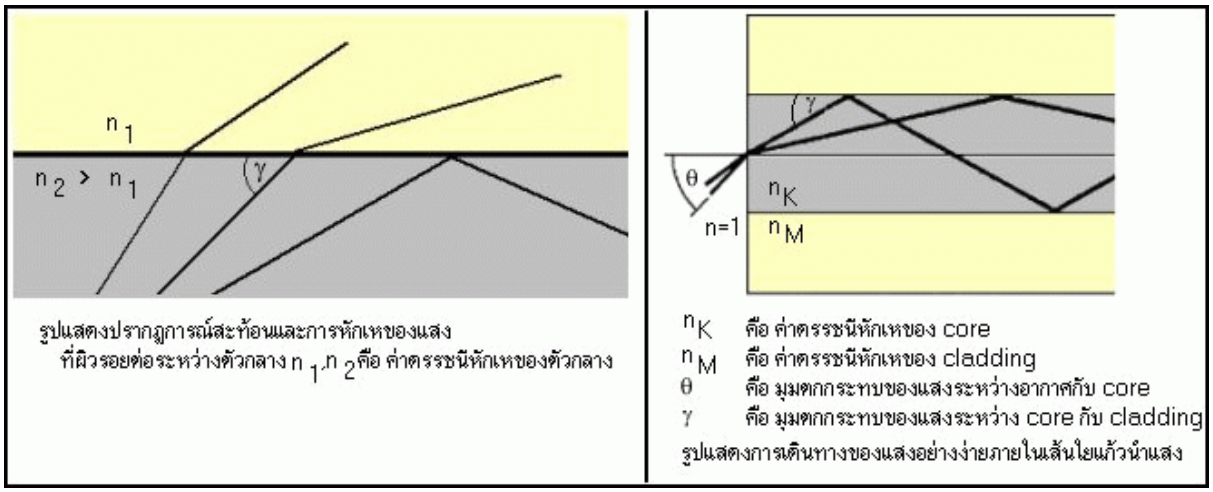
NA=SINθ = $\sqrt{}$n2K – n2M

θ =SIN-1 = $\sqrt{}$n2K – n2M

โดย θ : มุมกว้างสุดที่รับแสงได้

nK : ดัชนีหักเหของแสงของคอร์ (Core Reflection Index)

nM : ดัชนีหักเหของแสงของแคลดดิ้ง (Cladding Reflection Index)



รูปที่ 2.3.3 การเดินทางของลำแสง

ที่มา : http://www.geocities.com/u440604/net13.htm

Light propagation

ลำแสงที่ส่งเข้าไปในใยแก้วจะเกิด 2 กรณีขึ้นอยู่กับมุมตกกระทบ (γ) กล่าวคือ

1. ถ้ามุมของแสง > θ ลำแสงหักเหออกจากคอร์ ทำให้แสงเดินทางไม่ถึงปลายเส้นเหตุการณ์นี้เรียกว่าการหักเห(Refraction)
2. ถ้ามุมของแสง < θ ลำแสงจะสะท้อนผิวของแคลดดิ้งกลับเข้ามายังส่วนคอร์ ทำให้แสงเดินทางไปยังปลายทางได้ เหตุการณ์นี้เรียกว่าการสะท้อนกลับ (Reflection)ความเร็วของแสง (Velocity)ความเร็วของแสงที่เดินทางในใยแก้วนั้นจะถูกกำหนดโดยค่าดัชนีหักเห (RefractiveIndex) ของคอร์(Core) ใยแก้วค่าดัชนีหักเหแสง (n) เป็นค่าที่ไม่มีหน่วยและเป็นอัตราส่วนระหว่างความเร็วของแสงในสูญญากาศต่อความเร็วของแสงในวัตถุนั้น

n= c/v

โดย n : ค่าดัชนีหักเหแสงของวัตถุ (Refraction Index)

c : ความเร็วแสงในสูญญากาศ (3x108 เมตร)

v : ความเร็วแสงวัตถุ

โดยทั่วไปค่าของ n จะอยู่ที่ประมาณ 1.45 – 1.55

แสงที่ถูกส่องเข้าไปในใยแก้วด้วยมุมตกกระทบที่ต่างกันจะไม่เดินทางแนวเดียวกัน แสงที่ส่องตรงไปยังศูนย์กลางของใยแก้ว จะเดินทางเกือบจะเป็นเส้นตรง ส่วนแสงที่ส่องด้วยมุมตกกระทบที่ใหญ่ หรือส่องไปยังเปลือกนอกของคอร์ (Core) จะเดินทางตามแนวยาวกว่าจากต้นสายไปปลายสาย ดังนั้นจึงเดินทางค่อนข้างช้า แนวที่แสงเดินทางในใยแก้วจะเรียกว่า “ โหมด (Mode)” เมื่อแสงเดินทางในไฟเบอร์จะเกิดการสูญเสียพลังงาน

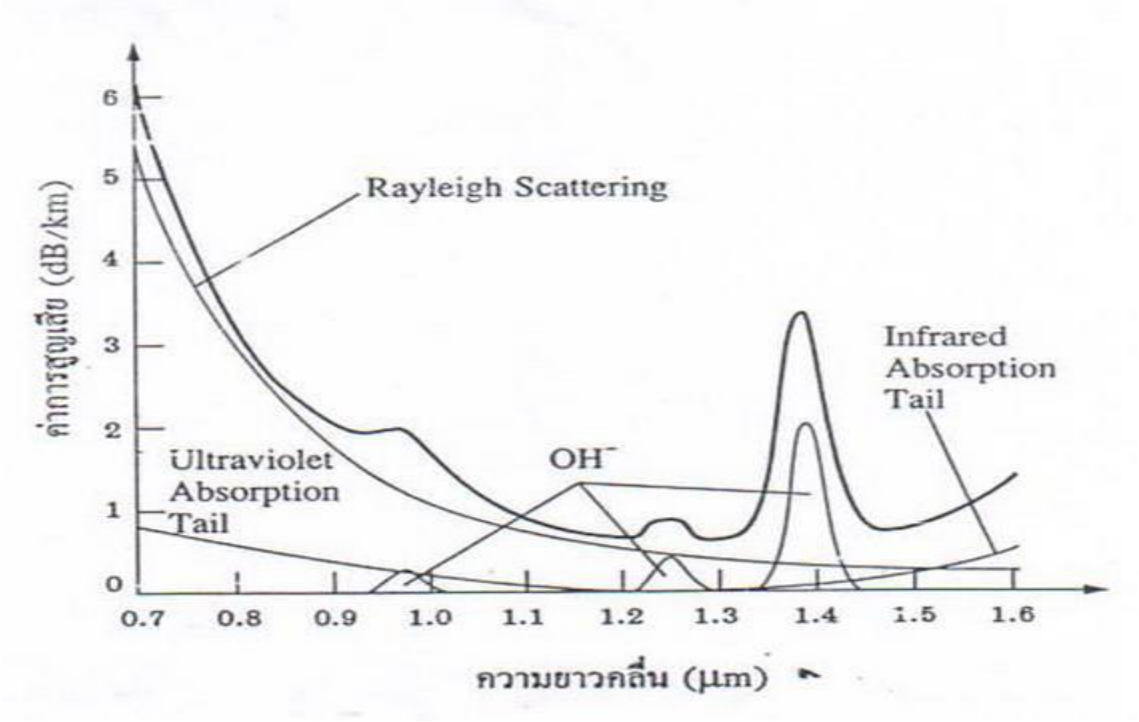
Attenuation

การสูญเสียพลังงาน (Attenuation) ของแสงในสายไฟเบอร์เกิดจากหลายสาเหตุ ดังนี้

- Light Absorbtion : การดูดกลืนแสงหมายถึง การที่แสงเปลี่ยนพลังงานไปเป็นพลังงานความร้อน การดูดกลืนนี้จะขึ้นอยู่กับคุณสมบัติของสายไฟเบอร์ ซึ่งแบ่งออกได้จาก 2 สาเหตุ คือ อินทรินสิก (Intrinsic) คือ เกิดจากเนื้อสารที่ใช้ทำสายไฟเบอร์ และ เอ็กส์ทรินสิก (Extrinsic) ซึ่งเกิดจากความไม่บริสุทธ์ของสายไฟเบอร์ เช่น มีโมเลกุล OH ซึ่งจะมีผลมากที่ความยาวคลื่นแสงประมาณ 1,240 nm. และ 1,390 nm.การสูญเสียที่เกิดขึ้นจากเอ็กส์ทรินสิก (Extrinsic)จะมีค่าน้อยมากสำหรับสายไฟเบอร์ที่ใช้ในปัจจุบัน
- Raylight Scrattering : การแตกกระจายของแสงก็มีผลต่อการสูญเสียพลังงานของแสงเช่นกัน การแตกกระจายของแสงเกิดจากการที่โปรตรอนของแสงวิ่งชนโมเลกุลของสายไฟเบอร์ทำให้แสงแตกกระจายไปทุกทิศทาง ซึ่งบางส่วนอาจจะเดินทางออกนอกคอร์ของสายไฟเบอร์หรือมีบางส่วนที่สะท้อนกลับ
- Bending Loss : เกิดจากการที่สายไฟเบอร์โค้งงอจะทำให้แสงบางส่วนหลุดออกจากส่วนคอร์ของใยแก้ว ตัวอย่างเช่น สายแบบซิงเกิลโหมดอาจโค้งงอได้โดยรัศมีไม่เกิน 10 cm. ถ้าการโค้งงอ

มากกว่านี้การสูญเสียสัญญาณจะเพิ่มขึ้นเป็นค่าทวีคูณ รัศมีการโค้งงอของสายไฟเบอร์จะขึ้นอยู่กับการออกแบบสายไฟเบอร์และความยาวคลื่นแสงที่ใช้

ค่าสูญเสียสัญญาณ (Attenuation) สำหรับความยาวคลื่นแสงที่ใช้จะคำนวณได้จากอัตราส่วนระหว่างกำลังของสัญญาณแสงที่ส่องเข้าใยแก้วกับกำลังของสัญญาณแสงที่ได้รับที่ปลายสาย ซึ่งค่านี้จะแสดงในหน่วยเดซิเบล (Decibel หรือ dB) การวัดค่าสูญเสียนั้นจะต้องรวมเราค่าสูญเสียจากทุกๆ สาเหตุเข้าด้วยกัน



รูปที่ 2.3.4 แสดงความลดทอนของแสงตามความยาวคลื่นแสง

ที่มา : http://www.kingsolder.com

จากกราฟข้างบนที่แสดงความสัมพันธ์ระหว่างค่าสูญเสียสัญญาณกับความยาวคลื่นแสงที่ใช้ ดังนั้นระบบการสื่อสารโทรคมนาคมจะใช้แสงที่มีความยาวคลื่นที่ให้ค่าสูญเสียต่ำดังแสดงในกราฟข้างบนซึ่งจะมีช่วงความยาวคลื่นคือ

- 820 – 880 nm (Short Haul)
- 1,285 – 1,330 nm (Medium Haul)
- 1.525 – 1,570 nm (Long Haul)

อีกสาเหตุหนึ่งที่มีผลต่อการส่งสัญญาณคือ การแยกกระจาย (Dispersion) ซึ่งจะมีผลทำให้แบนด์วิธของช่องสัญญาณลดลง การแยกกระจายจะมีหลายประเภท ประเภทหลักๆ มีดังนี้

- Model Dispersion : เมื่อแสงที่มีความยาวคลื่นสั้นถูกส่องเข้าไปในใยแก้ว พลังงานของแสงจะไม่ถูกส่งไปถึงสายทั้งหมด เนื่องจากแสงที่ส่องเข้าไปจะเดินทางในใยแก้วหลายแนว หรือหลายโหมด ซึ่งแสงแต่ละโหมดจะแบ่งพลังงานกันบางโหมดอาจเดินทางโดยใช้เวลามากกว่าโหมดอื่น ทำให้พลังงานของแสงที่ปลายสายลดลง
- Chromatic Dispersion : แสงที่ส่องเข้าไปในสายจะประกอบด้วยสเปกตรัมเล็กๆ ของความยาวคลื่นแสง ด้วยเหตุนี้แสงจึงเดินทางด้วยความเร็วที่ต่างกัน เนื่องจากความเร็ว ของแสงขึ้นอยู่กับดัชนีหักเห ความยาวคลื่นก็เช่นกันการแบ่งประเภทของสายไฟเบอร์นั้นจะใช้โมเดลดิสเปอร์ชั่นเป็นเกณฑ์คือ สายไฟเบอร์ประเภทที่โมเดลดิสเปอร์ชั่นมีผล (มัลติโหมด) และสายไฟเบอร์ประเภทที่ไม่แสดงโมเดลดิสเปอร์ชั่น (ซิงเกิลโหมด)
- สายไฟเบอร์แบบมัลติโหมดจะมีขนาดคอร์ใหญ่กว่ามาก (ประมาณ 50-100ไมครอน) ซึ่งอนุญาตให้แสงหลายโหมดผ่านได้
- สายไฟเบอร์แบบซิงเกิลโหมดมีขนาดประมาณ 5-10 ไมครอนอนุญาตให้แสงโหมดเดียว (1,310 nm หรือ 1,550 nm) ผ่านได้เท่านั้นซึ่งทำให้การแตกกระจายของสัญญาณลดลงได้มาก

ประเภทของใยแก้วนำแสง

ภายในใยแก้วนำแสงนั้น จำนวนลำแสงที่เดินทางหรือเกิดขึ้นจะเป็นตัวบอกโหมดของแสงที่เดินทางภายในเส้นใยแก้วนำแสงนั้น กล่าวคือ ถ้ามีแนวลำแสงอยู่แนวเดียวเรียกว่า เส้นใยแก้วนำแสงโหมดเดียว (Singlemode Fiber) แต่ถ้าภายในเส้นใยแก้วนำแสงนั้นมีแนวลำแสงอยู่จำนวนหลายลำแสง เรียกว่า “เส้นใยแก้วนำแสงหลายโหมด (Multimode Fiber)” นอกจากการแบ่งชนิดใยแก้วนำแสงตามลักษณะของโหมดแล้ว ก็ยังมีวิธีอื่นที่แบ่งโดยวัสดุที่ทำ เช่น เส้นใยที่ทำจากแก้วพลาสติก หรือโพลิเมอร์

Multimode Fiber Optic (MMF)

สายไฟเบอร์แบบมัลติโหมด (Multimode Fiber Optic หรือ MMF) เป็นสายไฟเบอร์ที่นิยมใช้งานในระบบแลน (LAN) มากที่สุด โครงสร้างภายในของเส้นใยแก้วนำแสง จะประกอบด้วย แกนและแคลด ดังได้กล่าวมาแล้วข้างต้น สำหรับเส้นใยแก้วนำแสงแบบหลายโหมดประเภทที่นิยมกันมากที่สุดมีขนาดเส้นผ่าน

ศูนย์กลางของแกนที่ 62.5 ไมครอน (1 Micron = 10-6 m = mm) และส่วนที่เป็นแคลดมีเส้นผ่านศูนย์กลาง 125 ไมครอน ซึ่งส่วนใหญ่จะเรียกสายไฟเบอร์ประเภทนี้สั้นๆ เป็น 62.5/125 MMF ส่วนสายไฟเบอร์ขนาดอื่นที่นิยมรองลงมาคือ 50/125 MMF

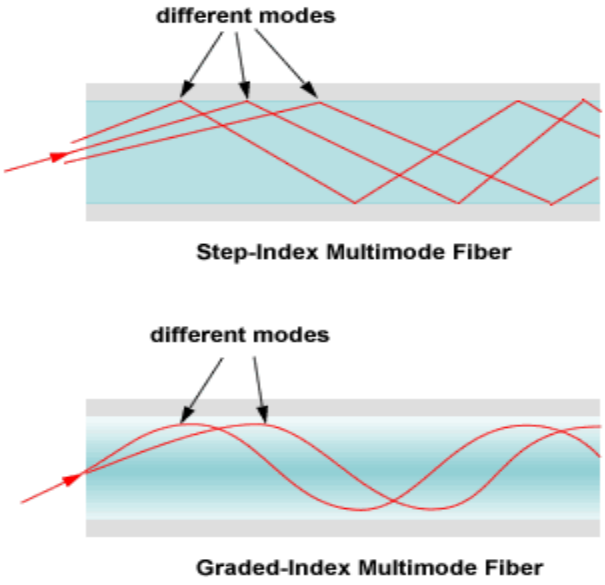
รูปที่ 2.3.5 สายไฟเบอร์แบบมัลติโหมด

ที่มา : http://www.cablesdirect.com

ขนาดของแกนของสายมัลติโหมดจะมีขนาดใหญ่กว่าสายแบบซิงเกิลโหมด สายไฟเบอร์แบบมัลติโหมดนี้ยังแบ่งย่อยได้อีกตามลักษณะของดัชนีหักเหของส่วนที่แกนและแคลด เช่น ใยแก้วนำแสงชนิดดัชนีขั้นบันได (Step Index) และดัชนีรูปมน (Graded Index) เป็นต้นเนื่องจากขนาดเส้นผ่านศูนย์กลางของแกนของเส้นใยแก้วนำแสงหลายโหมดนั้นมีขนาดใหญ่ดังนั้นแสงที่ตกกระทบที่ปลายส่งของเส้นใยแก้วนำแสงมีมุมตกกระทบที่ต่างกันหลายค่า จากหลักการสะท้อนกลับหมดของแสงที่เกิดขึ้นภายในส่วนของแกนที่ทำให้มีแนวลำแสงที่เกิดขึ้นหลายแนว ซึ่งแนวการเดินทางของแสงจะนิยมเรียกว่า โหมด ดังนั้นคำว่า “มัลติโหมด (Multimode)” จึงหมายถึงสายใยแก้วที่อนุญาติให้แสงเดินทางผ่านหลายแนวนั่นเอง

เนื่องจากมุมตกกระทบของโหมดแสงบนผิวระหว่างแกนและแคลดนั้นไม่เท่ากัน ทำให้ระยะทางการเดินทางของแสงแต่ละโหมดจากต้นสายไปยังปลายสายไม่เท่ากัน ซึ่งเหตุกาณ์นี้จะเรียกว่าการแตกกระจาย

ของโหมดแสง (Model Dispertion) ซึ่งเหตุการณ์นี้จะมีผลกระทบต่อประสิทธิภาพในการรับสัญญาณที่ปลายสาย ด้วยเหตุนี้จึงมีการพัฒนาใยแก้วนำแสงแบบดัชนีรูปมน (Graded Index) ขึ้นมาเพื่อแก้ปัญหานี้ สายไฟเบอร์แบบ Graded Index ของแสงในส่วนแกนนี้มีค่าเปลี่ยนแปลงตามระยะทางจากจุดศูนย์กลาง ทำให้ระยะเดินทางของแสงแต่ละโหมดมีค่าใกล้เคียงกันมากขึ้น

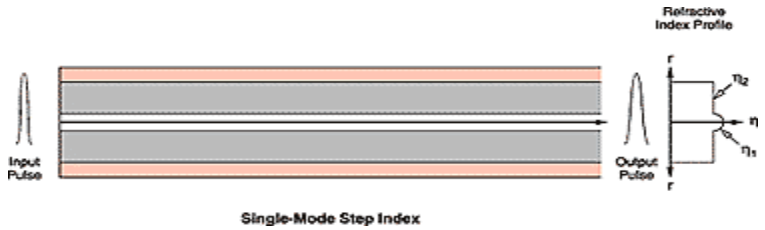


รูปที่ 2.3.6 สายมัลติโหมดประเภทต่างๆ

ที่มา : http://www.fiberoptics4sale.com

Singlemode Fiber Optic (SMF)

ไฟเบอร์ออฟติกแบบซิงเกิลโหมด (Single Mode Fiber Optic หรือ SMF) มีเส้นใยแก้วส่วนแกนขนาดเล็กกว่าสายแบบมัลติโหมด โดยจะมีขนาดเส้นผ่านศูนย์กลางของแกนประมาณ 8-10 ไมครอน และส่วนที่เป็นแคลดประมาณ 125 ไมครอน สายแบบนี้จะอนุญาตให้แสงเดินทางเพียงแนวเดียว ซึ่งเป็นที่มาของคำว่า ซิงเกิลโหมด (Single Mode)



รูปที่ 2.3.7 สายไฟเบอร์แบบซิงเกิลโหมด

ที่มา : http://www.bloggang.com

ข้อดีของเส้นใยแก้วนำแสงชนิดโหมดเดียวคือ แสงจะไม่เกิดการแตกกระจาย (Model Dispersion) ซึ่งเกิดขึ้นกับเส้นใยแสงชนิดหลายโหมด ดังนั้นจึงทำให้การรับสัญญาณที่ปลายสายดีกว่า ทำให้ส่งสัญญาณได้ไกลกว่า

การเชื่อมต่อสายไฟเบอร์

การส่งสัญญาณแสงไปในสายใยแก้วนำแสงจะต้องทำการแปลงสัญญาณไฟฟ้าจากอุปกรณ์กำเนิดสัญญาณให้เป็นสัญญาณแสงก่อนจึงจะสามารถส่งสัญญาณผ่านไปในใยแก้วนำแสง ได้ ระบบสื่อสารใยแก้วนำแสงโดยทั่วไปจะต้องมีการเชื่อมต่อในส่วนของใยแก้วนำแสงเสมอ โดยการเชื่อมต่อสายใยแก้วนำแสงนั้นอาจมีการคลาดเคลื่อน ซึ่งทำให้เกิดการสูญเสียสัญญาณได้ จากลักษณะต่างๆ ของใยแก้วเช่น จากการที่ตำแหน่งของแกนวางไม่ตรงกัน หรือการมีระยะห่างระหว่างแกนเป็นต้น จึงได้มีการคิดค้นวิธีการคิดค้นต่างๆ ที่นำมาใช้เชื่อมต่อเส้นใยแก้วนำแสงเพื่อให้มีการสูญเสียน้อยที่สุด

การเชื่อมต่อใยแก้วนำแสงมีหลายวิธีซึ่งการที่จะเลือกใช้วิธีใดก็แล้วแต่ความเหมาะสมกับงานต่างๆ ที่ต้องการติดตั้งในระบบสื่อสาร หรือเครือข่ายสื่อสารดังรายละเอียดต่อไปนี้

การเชื่อมต่อเชิงกล (Mechanical Splice)

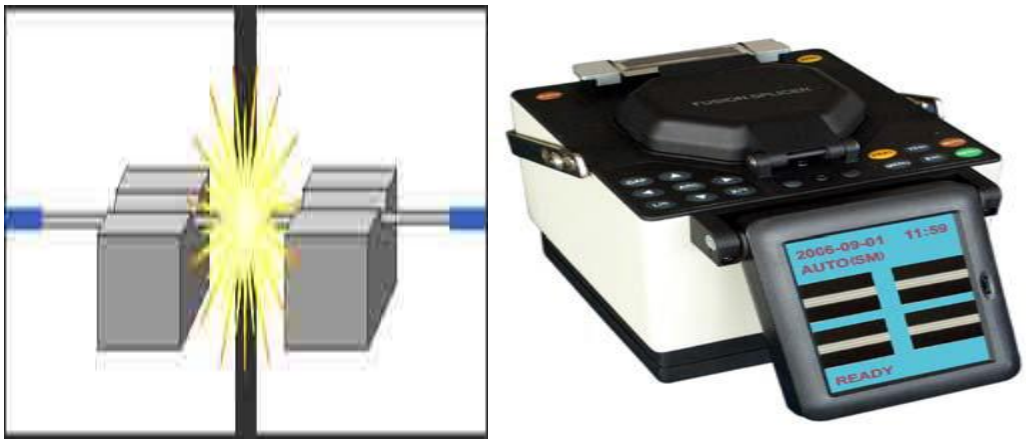
หลักการทั่วๆ ไปของการเชื่อมต่อเชิงกลก็คือ การวางเส้นใยแก้วนำแสงให้อยู่ในแนวแกนเดียวกัน โดยใช้อุปกรณ์ที่เหมาะสม และพยายามทำให้ปลายทั้งสองของเส้นใยแก้วนำแสงอยู่ชิดกันมากที่สุด ซึ่งการออกแบบอุปกรณ์ต่างๆ ในการเชื่อมต่อนี้จะช่วยลดการสูญเสียแสงเนื่องจากการติดตั้งจากการเบี่ยงเบนในแนวต่างๆลง ตัวอย่างเช่น การที่จะส่งผ่านสัญญาณแสงจากเส้นใยแก้วเส้นหนึ่งไปยังอีกเส้นหนึ่งให้มีการสูญเสียน้อยที่สุด ตรงรอยต่อระหว่างเส้นใยแก้วทั้งสองอาจมีการใช้เจลเชื่อมต่อด้วย (Index Matching Gel) เป็นของเหลวใสที่มีค่าดัชนีหักเหใกล้เคียงกับค่าดัชนีหักเหของเส้นใยแก้วนำแสง การเชื่อมต่อวิธีนี้อาจทำให้เกิดการสูญเสียสัญญาณอยู่ในช่วง 0.1-0.5 dB

รูปที่ 2.3.8 การเชื่อมต่อเชิงกล

ที่มา : http://webserv.kmitl.ac.th

การเชื่อมต่อด้วยวิธีหลอมรวม

การเชื่อมต่อด้วยวิธีหลอมรวม เป็นวิธีการเชื่อมต่อเส้นใยแก้วนำแสงสองเส้นด้วยการให้ความร้อนปลายเส้นใยแก้ว จากนั้นปลายเส้นใยแก้วก็จะถูกดันมาเชื่อมต่อกัน การเชื่อมต่อในลักษณะนี้เป็นการเชื่อมต่อแบบถาวร เส้นใยแก้วนำแสงที่เชื่อมต่อกันแล้วดูเสมือนว่าเป็นเส้นเดียวกัน การสูญเสียที่เกิดจากการเชื่อมต่อด้วยวิธีนี้มีค่าอยู่ระหว่าง 0.01-0.2 dB ในขั้นตอนของการเชื่อมต่อนั้น ความร้อนที่ทำให้ปลายเส้นใยแก้วนำแสงอ่อนตัวนั้นมาจากประกายไฟที่เกิดจากการอาร์กระหว่างขั้วอิเล็กโทรดในการหลอมรวม



รูปที่ 2.3.9 เครื่อง Fusion Splice

ที่มา : http://www.timbercon.com

สำหรับการเชื่อมต่อแบบหลอมรวมแบบเดิมนั้น การปรับตำแหน่งการวางตัวของเส้นใยแก้วนำแสง 2 เส้น อาศัยวิธีการปรับฐานรองด้วยการสังเกตผ่านกล้องขยาย แต่ในปัจจุบันมีการใช้วิธีการปรับทางแสงมาช่วยในการจัดวางดังกล่าว ทั้งนี้เพื่อให้การดำเนินการเป็นไปอย่างอัตโนมัติวิธีการนี้มีชื่อว่า “แอลไอดี (Light Injection and Detection, LID)” โดยอาศัยหลักการตรวจวัดปริมาณแสงที่ได้จากเส้นใยแก้วนำแสงเส้นที่สองซึ่งส่งผ่านมาจากเส้นใยแก้วเส้นที่หนึ่ง ถ้าพบว่าการวางตัวของเส้นใยแก้วทั้งสองอยู่ในตำแหน่งที่เหมาะสม ปริมาณแสงที่ตรวจวัดได้จะให้ค่ามากที่สุด พร้อมที่จะทำการหลอมรวม แสงที่ใช้ในการตรวจสอบมาจากการส่งผ่านแสงของแอลอีดี เข้าไปในบริเวณที่เส้นใยแก้วถูกทำให้โค้ง โดยท่อทรงกระบอกซึ่งมีรัศมีเล็ก (ประมาณ 2-3 มิลลิเมตร)และการตรวจวัดแสงก็อาศัยอุปกรณ์รับแสง ซึ่งวางชิดกับบริเวณที่ถูกทำให้โค้งของเส้นใยแก้วนำแสง วิธีการตรวจวัดแสงดังกล่าว อาศัยคุณสมบัติของใยแก้วนำแสงเกี่ยวกับการโค้งงอของเส้นใยแก้วที่ทำให้เกิดการสูญเสียขึ้น

หัวเชื่อมต่อ (Connector)

นอกจากการเชื่อต่อเส้นใยแก้วนำแสงเข้าด้วยกันด้วยวิธีการหลอมรวมดังกล่าวมาแล้วการเชื่อมต่อเส้นใยแก้วนำแสงยังสามารถทำได้โดยใช้หัวเชื่อมต่ออีกด้วย การเชื่อมต่อเส้นใยแก้วนำแสงด้วยหัวเชื่อมต่อทำให้ผู้ใช้มีความสะดวก สามารถถอดเปลี่ยนได้ตามความจำเป็น ในปัจจุบันมีการผลิตหัวเชื่อมต่อสำหรับเส้นใยแก้วนำแสงออกมาหลายแบบ ซึ่งการเลือกใช้แบบใดก็ขึ้นอยู่กับสภาพการใช้งานเป็นหลัก โดยทั่วไปแล้วหัวเชื่อมต่อได้ถูกออกแบบมาเพื่อช่วยให้ปลายเส้นใยแก้วนำแสงอยู่ใกล้กันมากที่สุดเท่าที่จะทำได้ นอกจากนี้หัวเชื่อมต่อยังต้องมีคุณสมบัติอื่นๆ อีก เช่นแข็งแรงทนทาน เมื่อใช้งานทำให้เกิดการสูญเสียของแสงต่ำและมีราคาถูก เป็นต้น

หัวเชื่อมต่อแบบ ST

หัวเชื่อมต่อแบบ ST นี้ได้รับการออกแบบโดยบริษัท AT&T ซึ่งเป็นหัวเชื่อมต่อที่นิยมมากที่สุดสำหรับสายไฟเบอร์แบบมัลติโหมด

รูปที่ 2.3.10 หัวเชื่อมต่อแบบ ST

ที่มา : http://www.timbercon.com

หัวเชื่อมต่อแบบ FC/PC

หัวเชื่อมต่อแบบ FC/PC จะมีลักษณะคล้ายๆ กับหัวเชื่อมต่อแบบ ST และเป็นหัวเชื่อมต่อที่เคยเป็นที่นิยมใช้กับสายซิงเกิลโหมดมาก

รูปที่ 2.3.11 หัวเชื่อมต่อแบบ FC/PC

ที่มา : http://www.bloggang.com

หัวเชื่อมต่อแบบ SC

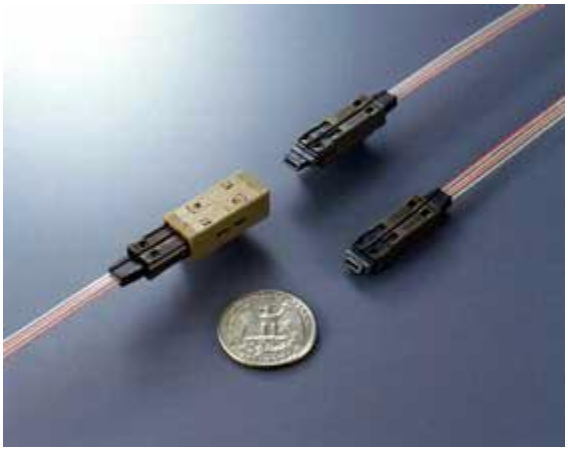
เป็นหัวเชื่อมต่อที่กำลังเป็นที่นิยมใช้กับสายไฟเบอร์ในปัจจุบัน

รูปที่ 2.3.12 หัวเชื่อมต่อแบบ SC

ที่มา : http://www.bloggang.com

หัวเชื่อมต่อแบบ SMF (Small Form Factor)

เนื่องจากหัวเชื่อมต่อที่กล่าวมาข้างต้นเป็นหัวเชื่อมต่อที่มีขนาดใหญ่ทำให้เปลืองพื้นที่บนอุปกรณ์เครือข่าย เช่น สวิตซ์ ดังนั้นจึงได้มีการออกแบบหัวเชื่อมต่อใหม่ที่มีขนาดเล็ก เช่น หัวเชื่อมต่อแบบ MT-RJ ออกแบบโดยบริษัท AMP ซึ่งปัจจุบันเปลี่ยนชื่อเป็น Tyco เป็นหัวเชื่อมต่อประเภท Small Form Factor ที่ออกแบบให้มีขนาดเล็กและใช้งานได้ง่าย



รูปที่ 2.3.13 หัวเชื่อมต่อแบบ SMF

ที่มา : http://jae-connector.com

การทดสอบสายไฟเบอร์

เมื่อติดตั้งสายไฟเบอร์เสร็จเรียบร้อยแล้วก่อนที่จะใช้งานสายไฟเบอร์นั้นจำเป็นที่ต้องทำการทดสอบด้านต่างๆ มีดังนี้

- การทดสอบด้านเมคานิก
- การทดสอบด้านกายภาพ
- การทดสอบเกี่ยวกับคุณสมบัติของสาย
- การทดสอบเกี่ยวกับการรับส่งสัญญาณ

สำหรับการทดสอบ 3 ประเภทแรก จะทดสอบแค่ครั้งเดียว เพราะค่าพารามิเตอร์มีการปลี่ยนแปลงน้อยมากในระหว่างการใช้งาน ก่อนที่จะมีการใช้สายไฟเบอร์นั้นต้องมีการตรวจวัดค่าสมบัติต่างๆ ของสายไฟก่อน

การทดสอบการรับส่งข้อมูล

การทดสอบหลักๆ ของสายไฟเบอร์ที่ติดตั้งแล้ว เพื่อให้แน่ใจว่าสายไฟเบอร์สามารถรับส่งข้อมูลได้ตามต้องการมีดังนี้

- การทดสอบการสูญเสียของสัญญาณของลิงค์ (End-To-End Optical Link Loss)
- อัตราการสูญเสียต่อหน่วยความยาว (Attenuation)

- การสูญเสียเนื่องจากการเชื่อมต่อแบบต่างๆ (Splice, Connectors)
- ความยาวของสายไฟเบอร์

การทดสอบแบบอื่นๆ เช่น แบนวิธ หรือการสูญเสียเนื่องจากการแตกกระจายของแสง (Modal Dispersion) การสูญเสียเนื่องจากการสะท้อนกลับของแสง

ค่าการสูญเสียของสัญญาณแสง (Optical Loss Budget)

ค่าการสูญเสียของสัญญาณแสงที่เดินทางผ่านสายไฟเบอร์ออฟติกนั้นจะมีข้อจำกัดอยู่เพื่อให้การรับส่งข้อมูลเป็นไปได้อย่างถูกต้อง ซึ่งค่านี้จะขึ้นอยู่กับหลายอย่าง เช่น กำลังแสงที่ใช้ส่งความสามารถในการรับสัญญาณของตัวรับสัญญาณ การเชื่อมต่อสายสัญญาณ ไม่ว่าจะเป็นการSplice หรือการใช้หัวเชื่อมต่อ เพื่อให้สามารถคำนวณค่าสูญเสียของสายสัญญาณได้ ต่อไปนี้เป็นค่าการสูญเสียที่นิยมใช้ในการคำนวณ

- 0.2 dB/km สำหรับสายซิงเกิลโหมดที่ความยาวคลื่น 1,550 nm
- 0.35 dB/km สำหรับสายซิงเกิลโหมดที่ความยาวคลื่น 1,310 nm
- 1.0 dB/km สำหรับสายมัลติโหมดที่ความยาวคลื่น 1,300 nm
- 3.0 dB/km สำหรับสายมัลติโหมดที่ความยาวคลื่น 850 nm
- 0.05 dB สำหรับการสไปลซ์แบบหลอมละลาย (Fusion Splice)
- 0.1 dB สำหรับการสไปลซ์เชิงกล (Mechanical Splice)
- 0.2-0.5 dB สำหรับการเชื่อมต่อโดยใช้หัวเชื่อมต่อ (Connector)
- 3.5 dB สำหรับการใช้ตัวแยกสัญญาณจาก 1 ไป 2 (Splitter)

หลังจากที่ทราบค่าโดยประมาณของการสูญเสียอันเนื่องมาจากสาเหตุต่างๆ แล้ว ค่าสูญเสียของสัญญาณแสงของลิงค์ก็สามารถคำนวณได้

การสูญเสียของสัญญาณแสงในสาย Fiber Optic

การสูญเสียของสัญญาณแสงในสาย Fiber Optic เป็นส่วนสำคัญที่ทำให้เกิดความผิดพลาดของข้อมูลข่าวสาร ทำให้การเชื่อมต่อสื่อสารด้วยระยะทางไม่เป็นไปตามที่คาดหวัง (ปกติสาย Fiber Optic สามารถเชื่อมต่อได้ด้วยระยะทางที่ยาวเกินกว่า 1-2 กิโลเมตร ทั้งนี้ขึ้นอยู่กับว่าใช้สาย Fiber Optic แบบใด

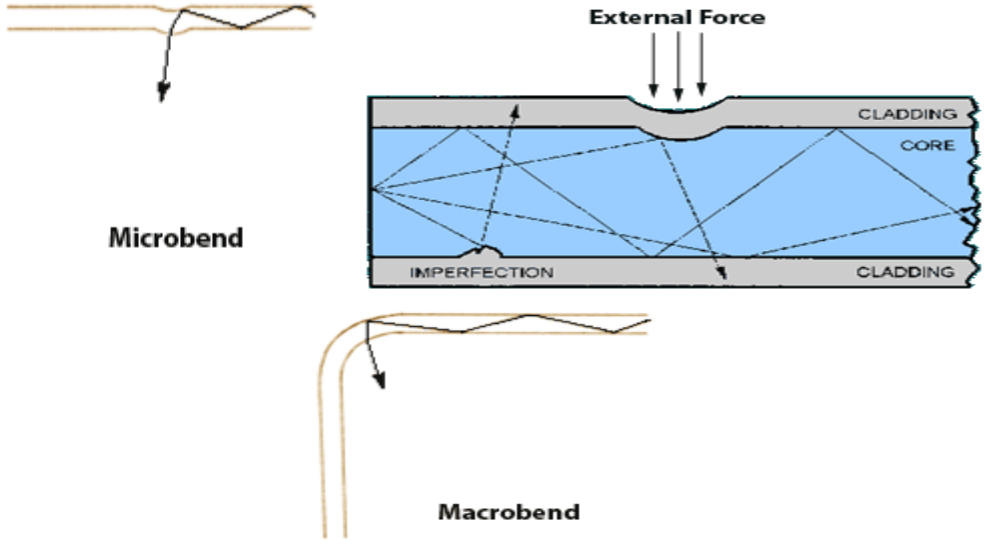
(แบบ Multimode หรือ Single Mode) รวมทั้งยังขึ้นอยู่กับโปรโตคอลของเครือข่าย อย่างไรก็ดี ปัจจัยหลักคือการสูญเสียของสัญญาณแสงในสาย ข้อเท็จจริงที่เกี่ยวกับการทำให้ เกิดการสูญเสียของกำลังแสงในสาย มีหลายประการดังนี้

ความสูญเสีย Power ของ Fiber Optic ขึ้นอยู่กับ ความยาวคลื่นที่ใช้ ความยาวคลื่นยิ่งมากเท่าใด อัตราการสูญเสียของแสง จะน้อยลง เช่น การสูญเสียกำลังแสง บนความยาวคลื่น 1300 nm ได้แก่ การเอาสาย Fiber Optic ที่มีขนาดต่างๆ มาเชื่อมต่อกัน ทำให้เกิดการสูญเสียกำลังแสงได้

- Intrinsic
- Loss Inherent to Fiber
- การสูญเสียที่เกิดจากการผลิต Fiber
- Freshnel Reflection
- Bending Loss

Bending Loss

เกิดจากปัญหาการโค้งงอของสาย เกินค่ารัศมีความโค้งงอของสายตามปกติ (Minimum Bend Radius)



รูปที่ 2.3.14 Bending Loss

ที่มา : http://www.timbercon.com

Bending Loss ยังสามารถเกิดขึ้นได้จากการองค์ประกอบย่อยๆ ดังนี้

- ความโค้งที่มีความแหลมบริเวณแกนของสาย
- ความไม่สมบูรณ์ของ Buffer และ Jacket โดยมีความคลาดเคลื่อนของการวางตำแหน่งระหว่างกันที่ห่างประมาณ 2-3 มิลลิเมตร
- การติดตั้งสายไม่ถูกวิธีหรือไม่เรียบร้อย ปัจจัยต่างๆ เหล่านี้ เรียกว่า Micro Bending สามารถเกิดขึ้นได้เมื่อความยาวของสายเพิ่มมากขึ้น

การสูญเสียเนื่องจากการเข้าหัว Connector และทำ Splice ไม่ดี

Splice Loss สามารถเกิดขึ้น ณ ที่ใดก็ได้ที่มีการตัดต่อและเชื่อมสายเข้าด้วยกัน โดยประกอบด้วย การ Loss 2 แบบ ได้แก่ Mechanical Loss และ Fusion Splicing Loss

Mechanical Loss จะมีอัตราสูงที่สุด เมื่อเทียบกับ Fusion Splicing โดยมีอัตราการ Loss ตั้งแต่ 0.2 ไปจนถึง 1.0 dB ขึ้นไป

Fusion Splice Loss มีอัตราการ Loss ต่ำสุด โดยมีอัตราการ Loss ต่ำกว่า 0.1 dB และอัตราการ Loss ที่ต่ำกว่า 0.05 เป็นเรื่องที่เป็นไปได้ หากใช้เครื่องมือและอุปกรณ์ Splice ที่มีคุณภาพดี นอกจากนี้ยังมี Factor อื่นๆ ที่ทำให้เกิดการ Loss ของ Connector ดังนี้

- ปัญหาสกปรก หรือ Contamination บน Connector (ปัญหาที่เกิดบ่อยที่สุด)
- การติดตั้ง Connector ที่ไม่ถูกต้องไม่เรียบร้อย
- การชำรุดเสียหายที่เกิดขึ้นบนพื้นผิวของ Connector
- Poor Scribe (Cleave)
- Mismatched Fiber Cores
- Misaligned Fiber Cores
- Index of Reflection Mismatch

Loss Inherent to Fiber การสูญเสียใน Fiber ที่ไม่สามารถจะขจัดไปได้ ในระหว่างกระบวนการผลิต มีสาเหตุเกิดจาก Impurities ในกระจก รวมทั้งการดูดซึมของแสงในระดับของโมเลกุล การสูญเสียของแสง

ขึ้นอยู่กับ ความหนาแน่นเชิงแสง ส่วนประกอบของ Fiber Opticรวมทั้งโครงสร้างทางโมเลกุลของ Fiber ซึ่งเรียกว่า Rayleigh Scattering เมื่อแสงมากระทบกับส่วนประกอบดังกล่าว ก็จะเกิดการ กระจายตัวของแสงไปยังทิศทางต่างๆ ขึ้น

การสูญเสียที่เกิดจากการแตกหักของพื้นผิว

เนื่องจากว่าสาย Fiber Optic มีส่วนที่ทำมาจาก Silica และกระจก ดังนั้น การโค้งงอสายมากเกินไปมีส่วนทำให้เกิดการแตกหัก รวมทั้งการติดตั้งที่ขาดระมัดระวังก็มีส่วนทำให้เกิดการแตกหักได้เช่นกัน

OTDR

OTDR (Optical Time Domain Reflectometer) คือเครื่องมือที่ใช้ทดสอบคุณสมบัติของสายไฟเบอร์ จุดประสงค์ของเครื่องมือนี้ก็เพื่อตรวจวัดและค้นหาเหตุการณ์ต่างๆ ที่เกิดขึ้นบนสายไฟเบอร์ เช่น ความยาวของสาย ตำแหน่งที่มีการเชื่อมต่อ (Splice) หรือหัวเชื่อมต่อ (Connector) และอัตราการสูญเสีย ของสัญญาณ (Attenuator) ข้อดีของ OTDR ก็คือ เราสามารถใช้ทดสอบสายไฟเบอร์จากปลายข้างเดียวเท่านั้น OTDR จะแสดงผลเป็นกราฟที่แสดงการสูญเสียของสัญญาณในระหว่างการส่งข้อมูล ดังนั้น OTDR จึงเป็นเครื่องวัดที่นิยมมากที่สุดสำหรับทดสอบสายไฟเบอร์

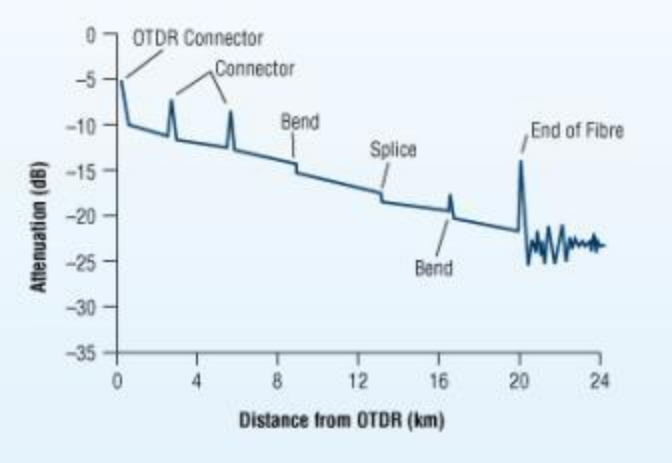
รูปที่ 2.3.15 OTDR

ที่มา : http://www.bpcomms.co.uk

OTDR สามารถตรวจวัดคุณสมบัติของสายไฟเบอร์ได้หลายประเภท ซึ่งสิ่งที่ OTDRรายงานให้ทราบนั้น จะเรียกว่าเหตุการณ์ (Event) ซึ่งจะมีอยู่ 2 ประเภทคือ

- เหตุการณ์ที่มีการสะท้อนกลับของแสง (Reflective Event) คือเหตุการณ์ที่ค่าสะท้อนกลับของแสงมีการเปลี่ยนแปลงในสายไฟเบอร์ซึ่งอาจเกิดได้เนื่องจากสายแตกหัก การเชื่อมต่อสายไม่ว่าจะเป็นแบบใช้หัวเชื่อมต่อ การสไปลซ์แบบแมคานิก หรือสุดปลายสาย การเชื่อมต่อแบบใช้หัวเชื่อมต่อจะสูญเสียสัญญาณประมาณ 0.5 dB และการสไปลซ์แบบแมคานิก จะสูญเสียสัญญาณประมาณ 0.2 dB
- เหตุการณ์ที่ไม่มีการสะท้อนกลับของแสง (Non-Reflective Event) เป็นเหตุการณ์ที่แสงจะไม่สะท้อนกลับ เช่น การสไปลซ์แบบหลอมละลาย (Fusion Splice) เป็นต้น

การแสดงผลของ OTDR โดยทั่วไปจะมีลักษณะดังแสดงในรูป เหตุการณ์ต่างๆ จะแสดงผลบนกราฟที่ไม่เหมือนกัน กราฟจะอธิบายลักษณะของสายไฟเบอร์ที่กำลังทดสอบอยู่ทำให้เราสามารถนับจำนวนครั้งและตำแหน่งที่มีการเชื่อมต่อ สไปลซ์หัวเชื่อมต่อได้ ซึ่งจะช่วยในการค้นหาจุดเสียของสาย จุดที่สายขาดหรือจุดที่มีการเชื่อมต่อไม่ดี เป็นต้น



รูปที่ 2.3.16 กราฟที่แสดงโดย OTDR

ที่มา : http://www.bpcomms.co.uk

OTDR เป็นเครื่องมือตรวจวัดสายไฟเบอร์ที่สำคัญและมีประโยชน์มากสำหรับการติดตั้งเครือข่ายที่ใช้สายไฟเบอร์ออฟติก ผู้ใช้เครื่องมือนี้ควรที่จะมีความรู้ทั่วไปเกี่ยวกับแสง ซึ่งก่อนที่จะใช้งานควรจะศึกษาคู่มือการใช้งานให้ดีก่อน

ข้อดีของระบบสายใยแก้วนำแสง เหนือกว่าระบบสายทองแดงดังนี้

1. ความสามารถในการรับส่งข้อมูลข่าวสารเส้นใยแก้วนำแสงที่เป็นแท่งแก้วขนาดเล็ก มีการโค้งงอได้ ขนาดเส้นผ่าศูนย์กลางที่ใช้กันมากคือ 62.5/125 ไมโครเมตร เส้นใยแก้วนำแสงขนาดนี้เป็นสายที่นำมาใช้ภายในอาคารทั่วไป เมื่อใช้กับคลื่นแสงความยาวคลื่น 850 นาโนเมตร จะส่งสัญญาณได้มากกว่า 160 เมกะเฮิรตซ์ ที่ความยาว 1 กิโลเมตร และถ้าใช้ความยาวคลื่น 1,300 นาโนเมตร จะส่งสัญญาณได้กว่า 500 นาโนเมตร ที่ความยาว 1 กิโลเมตร และถ้าลดความยาวลงเหลือ 100 เมตร จะใช้กับความถี่ของสัญญาณมากกว่า 1 กิกะเฮิรตซ์ได้ ดังนั้นจึงดีกว่าสายยูทีพีแบบ Cat5e ที่ใช้กับสัญญาณได้ 100 เมกะเฮิรตซ์ หรือสายยูทีพีแบบ Cat6 ที่ใช้กับสัญญาณได้ 1000 เมกะเฮิรตซ์
2. กำลังสูญเสียต่ำ เส้นใยแก้วนำแสงมีคุณสมบัติในเชิงการให้แสงวิ่งผ่านได้ การบั่นทอนแสงมีค่าค่อนข้างต่ำ ตามมาตรฐานของเส้นใยแก้วนำแสง การใช้เส้นสัญญาณนำแสงนี้ใช้ได้ยาวถึง 2,000 เมตร หากระยะทางเกินกว่า 2,000 เมตร ต้องใช้รีพีตเตอร์ทุกๆ 2,000 เมตร การสูญเสียในเรื่องสัญญาณจึงต่ำกว่าสายตัวนำทองแดงมาก ที่สายตัวนำทองแดงมีข้อกำหนดระยะทางเพียง 100 เมตร
3. หากพิจารณาในแง่ความถี่ที่ใช้ผลตอบสนองทางความถี่มีผลต่อกำลังสูญเสียโดยเฉพาะ ในลวดตัวนำทองแดง เมื่อใช้เป็นสายสัญญาณ คุณสมบัติของสายตัวนำทองแดงจะ เปลี่ยนแปลงเมื่อใช้ความถี่ต่างกัน โดยเฉพาะเมื่อใช้ความถี่ของสัญญาณที่ส่งในตัวนำทองแดงสูงขึ้น อัตราการสูญเสียก็จะมากตามแต่กรณีของเส้นใยแก้วนำแสงเราใช้สัญญาณ รับส่งข้อมูล จึงไม่มีผลกับกำลังสูญเสียทางแสงคลื่นแม่เหล็กไฟฟ้าไม่สามารถรบกวนได้ปัญหาที่สำคัญของสายสัญญาณแบบทองแดงคือการเหนี่ยวนำโดยคลื่นแม่เหล็กไฟฟ้าปัญหานี้มีมาก ตั้งแต่เรื่องการรบกวนระหว่างตัวนำหรือเรียกว่าครอสทอร์ค
4. แมตช์พอดีทางอิมพีแดนซ์ ทำให้มีคลื่นสะท้อนกลับ การรบกวนจากปัจจัยภายนอกที่เรียกว่า EMI ปัญหาเหล่านี้สร้างให้ผู้ใช้ต้องหมั่นดูแล แต่สำหรับเส้นใยแก้วนำแสงแล้วปัญหาเรื่องเหล่านี้จะไม่มี เพราะแสงเป็นพลังงานที่มีพลังงานเฉพาะและไม่ถูกรบกวนโดยคลื่นแม่เหล็กไฟฟ้า การเดินทางในเส้นแก้วก็ปราศจาก การรบกวนของแสงจากภายนอก
5. น้ำหนักเบาเส้นใยแก้วนำแสงมีน้ำหนักเบากว่าเส้นลวดตัวนำทองแดง น้ำหนักของเส้นใยแก้วนำแสงขนาด 2 แกนที่ใช้ทั่วไปมีน้ำหนักเพียงประมาณ 20 ถึง 50 เปอร์เซ็นต์ของสายยูทีพี แบบ Cat5e

6. ขนาดเล็กเส้นใยแก้วนำแสงมีขนาดทางภาคตัดขวางแล้วเล็กกว่าลวดทองแดงมาก ขนาดของเส้นใยแก้วนำแสงเมื่อรวมวัสดุหุ้มแล้วมีขนาดเล็กกว่าสายยูทีพี โดยขนาดของสายใยแก้วนี้ใช้ พื้นที่ประมาณ 15 เปอร์เซ็นต์ของเส้นลวดยูทีพีแบบ Cat5e
7. มีความปลอดภัยในเรื่องข้อมูลสูงกว่าการใช้เส้นใยแก้วนำแสงมีลักษณะใช้แสงเดินทางในข่าย จึงยากที่จะทำการแท็ปหรือทำการดักฟังข้อมูล
8. มีความปลอดภัยต่อชีวิตและทรัพย์สินการที่เส้นใยแก้วนำแสงเป็นฉนวนทั้งหมดจึงไม่นำกระแสไฟฟ้า การลัดวงจรการเกิดอันตรายจากกระแสไฟฟ้าจึงไม่เกิดขึ้น

เน็ตเวิร์คการ์ด

รูปที่ 2.4.1 เน็ตเวิร์คการ์ด

ที่มา : http://www.waycomputer.com/images_product/20090718015501b112043.jpg

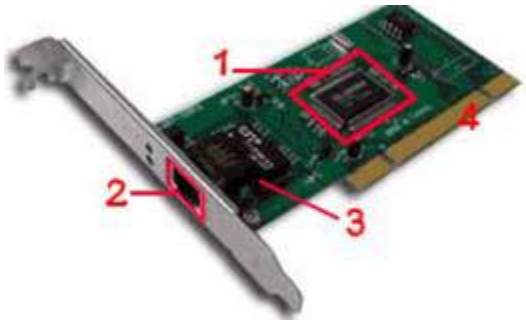
เน็ตเวิร์คการ์ดเป็นจุดเชื่อมต่อระหว่างคอมพิวเตอร์และระบบเครือข่าย ส่วนใหญ่จะเรียกว่า NIC (Network Interface Card) หรือบางทีก็เรียกว่า “แลนการ์ด (LAN Card)” อุปกรณ์นี้จะทำหน้าที่แปลงข้อมูลเป็นสัญญาณที่สามารถส่งไปตามสายสัญญาณหรือสื่อแบบอื่นได้ ปัจจุบันนี้มีแลนการ์ดหลายประเภท ซึ่งถูกออกแบบให้ใช้กับเครือข่ายประเภทต่างๆ เช่น อีเธอร์เน็ตการ์ด (Ethernet Card) โทเคนริงการ์ด (Token Ring Card) ไวร์เลสแลนการ์ด (Wireless Lan card) เป็นต้นการ์ดแต่ละประเภทอาจใช้ได้กับสายสัญญาณบางชนิดเท่านั้น หรืออาจจะใช้ได้กับสายสัญญาณหลายชนิด

เน็ตเวิร์คการ์ดจะติดตั้งกับคอมพิวเตอร์โดยเสียบเข้ากับช่องบนเมนบอร์ดของคอมพิวเตอร์ ส่วนมากคอมพิวเตอร์ที่ผลิตในปัจจุบันจะมีเฉพาะช่องเสียบ PCI ซึ่งใช้บัสขนาด 32บิต

อัตราข้อมูลที่สามารถส่งผ่านมีหลายระดับเช่น 10 Mbps 100 Mbps และ 1,000 Mbps หรือที่เรียกสั้นๆ ว่า “กิกะบิตแลน (Gigabit LAN)” บางการ์ดอาจทำงานได้ที่ความเร็วเดียว ส่วนบางการ์ดสามารถทำงานได้หลายระดับความเร็ว เช่น การ์ดที่ระบุว่าเป็นแบบ 10/100 หมายความว่าการ์ดนี้ใช้ได้กับเครือข่ายที่มีความเร็วทั้ง 10 Mbps และ 100 Mbps การเลือกอัตราข้อมูลจะขึ้นอยู่กับอุปกรณ์ฮับ หรือสวิตช์ที่คอมพิวเตอร์เชื่อมต่อ อย่างไรก็ตามการเลือกชนิดของการ์ดยังขึ้นอยู่กับงบประมาณและประเภทของเครือข่าย การเลือกควรเผื่อไว้สำหรับการขยายและการอัพเกรดเครือข่ายในอนาคตด้วย

ส่วนประกอบของการ์ดแลน

การ์ดแลนจะประกอบไปด้วยส่วนต่างๆ ที่ทำหน้าที่ควบคุมการรับ/ส่งข้อมูลระหว่างเครื่องคอมพิวเตอร์ภายในเครือข่าย ซึ่งการ์ดและจะไม่สามารถทำงานได้หากขาดส่วน ประกอบดังนี้



รูปที่ 2.4.2 ส่วนประกอบต่างๆ ของเน็ตเวิร์คการ์ด

ที่มา : http://itg.nrct.go.th

1. ชิปควบคุม (Controller Chip) ใช้สำหรับควบคุมการทำงานและการรับ/ส่งข้อมูลของการ์ดแลน ซึ่งการ์ดแลนทุกตัวจะต้องมีชิปตัวนี้ และความเร็วในการรับ/ส่งข้อมูลของการ์ดแลนก็จะขึ้นอยู่กับยี่ห้อและรุ่นของชิปตัวนี้เช่นกัน ชิปควบคุมรุ่นใหม่สามารถรับ/ส่งข้อมูลได้ทำความเร็วสูงถึง 1,000 Mbps หรือ 1 Gbps
2. หัวต่อ RJ-45 ใช้ต่อเข้ากับสายแลนแบบ UTP (Unshielded Twisted Pair) และแบบ STP (Shielded Twisted Pair) ซึ่งทั้งสองแบบจะต่างกันตรงที่สายแบบ STP จะมีชีลด์ป้องกันสัญญาณรบกวนทำให้การรับ/ส่งข้อมูลทำได้อย่างมีประสิทธิภาพ ในขณะที่ UTP จะไม่มีชีลด์

3. บู๊ตรอม (Boot ROM) เป็นอุปกรณ์เสริมสำหรับการ์ดแลน ซึ่งการ์ดแลนส่วนมากจะมีซ็อกเก็ตว่างๆ ไว้สำหรับให้ผู้ใช้ซื้อบู๊ตรอมมาติดตั้งเพิ่มเติม บู๊ตรอมก็คือ หน่วยความจำรอม (ROM) ที่มีการบันทึกระบบปฏิบัติการเอาไว้ จึงสามารถบู๊ตเครื่องจากบู๊ตรอมนี้แทนฮาร์ดดิสก์ในเครื่องได้
4. อินเตอร์เฟส ก็คือ ส่วนที่ใช้เสียบเข้ากับสล็อตบนเมนบอร์ด ซึ่งช่วงแรกที่การ์ดแลนยังมีความเร็วเพียง 10 Mbps จะมีทั้งรุ่นที่ใช้กับสล็อต ISA และ PCI แต่ในปัจจุบันได้เปลี่ยนไปใช้สล็อตแบบ PCI ทั้งหมดแล้ว

ฮับ (Hub)

ฮับ (Hub) หรือบางทีก็เรียกว่า “รีพีตเตอร์ (Repeater)” คือ อุปกรณ์ที่ใช้เป็นศูนย์กลางในการเชื่อมต่อกลุ่มของคอมพิวเตอร์ ฮับมีหน้าที่รับส่งเฟรมข้อมูลทุกเฟรมที่ได้รับจากพอร์ตใดพอร์ตหนึ่งไปยัง ทุกๆ พอร์ตที่เหลือ คอมพิวเตอร์ที่เชื่อมต่อเข้ากับฮับ จะแชร์แบนด์วิธหรืออัตราข้อมูลของเครือข่าย ฉนั้นยิ่งมีคอมพิวเตอร์เชื่อมต่อเข้ากับฮับมากเท่าใด ยิ่งทำให้แบนด์วิธต่อคอมพิวเตอร์แต่ละเครื่องลดลง ในท้องตลาดปัจจุบัน มีฮับหลายชนิดจากหลายบริษัท ข้อแตกต่างระหว่างฮับเหล่านี้จะเป็นจำนวนพอร์ต สายสัญญาณที่ใช้ ประเภทของเครือข่าย และอัตราข้อมูลที่ฮับรองรับได้ อีเธอร์เน็ตฮับแบบ 10/100 Mbps ซึ่งคำว่า “10/100 Mbps” หมายความว่า ฮับเครื่องนี้รองรับการส่งข้อมูลได้ทั้งความเร็วที่ 10 Mbps และ 100 Mbps

รูปที่ 2.4.3 อุปกรณ์ฮับ

ที่มา : http://www.sanwa.co.jp

การที่อุปกรณ์เครือข่ายอีเธอร์เน็ตสามารถทำงานได้ที่ความเร็ว 2 ระดับ เช่น 10/100Mbpsนั้น ก็เนื่องจากอุปกรณ์เครื่องนั้นมีฟังก์ชันที่สามารถเช็คได้ว่าอุปกรณ์ หรือคอมพิวเตอร์ที่มาเชื่อมต่อกับฮับ นั้นสามารถรับส่งข้อมูลได้ที่ความเร็วสูงสุดเท่าใด และอุปกรณ์นั้นก็จะเลือกอัตราข้อมูลสูงสุดที่รองรับทั้งสองฝั่ง ฟังก์ชันนี้จะเรียกว่า “การเจรจาอัตโนมัติ (Auto-Negotiation)” ส่วนใหญ่ฮับหรือสวิตช์ที่ผลิตในปัจจุบัน

จะมีฟังก์ชันนี้อยู่ เพื่อให้สามารถเชื่อมต่อเครือข่ายอีเธอร์เน็ตที่ความเร็วต่างกันได้ ถ้ามีอุปกรณ์เครือข่ายหรือคอมพิวเตอร์หลายๆ เครื่องเชื่อมต่อเข้ากับฮับ และแต่ละโหนดสามารถรับส่งข้อมูลได้ในอัตราข้อมูลที่ต่างกัน ฮับก็จะเลือกอัตราส่งข้อมูลที่อัตราความเร็วต่ำสุด เนื่องจากคอมพิวเตอร์เหล่านี้จัดอยู่ในคอลลิชันโดเมน (Collision Domain) เดียวกันตัวอย่างเช่น ถ้า LAN การ์ดของคอมพิวเตอร์เครื่องหนึ่งสามารถรับส่งข้อมูลได้ที่ 10 Mbps แล้วคอมพิวเตอร์เหล่านี้เชื่อมต่อเข้ากับฮับเดียวกันที่รองรับอัตราความเร็วที่ 10/100 Mbps เครือข่ายนี้ก็จะทำงานที่ความเร็ว 10 Mbps เท่านั้น แต่ถ้าเป็นสวิตช์อัตราความเร็ว จะขึ้นอยู่กับความเร็วของคอมพิวเตอร์ เนื่องจากสวิตช์จะแยกคอลลิชันโดเมน

ปัจจุบันจะถือว่าฮับ (HUB) เป็นอุปกรณ์ที่ล้าสมัยไปแล้ว หรือแทบจะไม่มีใครผลิตออกมาวางขายกันอีก เนื่องจากมันถูกแทนที่โดยสวิตช์ ฮับ(HUB) ที่ยังมีวางขายอยู่ตามท้องตลาดนั้นก็มักจะเป็นฮับตัวเล็กๆ ราคาถูกๆเพียงไม่กี่ร้อยบาท นอกจากนี้ยังพบอุปกรณ์ประเภท DSL Modem หรือ DSL Router บางรุ่นบางยี่ห้อจะมีพอร์ตของฮับจำนวนหนึ่งติดมาให้ในตัว

สวิตช์ (Switch)

สวิตช์(Switch) หรือบางทีก็เรียกว่า สวิตชิ่งฮับ (Switching Hub) เป็นอุปกรณ์ที่ทำหน้าที่เป็นศูนย์กลางในการเชื่อมต่อของอุปกรณ์คอมพิวเตอร์ต่างๆ เข้ากับระบบแลนสวิตช์จะฉลาดกว่าฮับคือ สวิตช์สามารถส่งข้อมูลที่ได้รับมาจากพอร์ตหนึ่งไปยังเฉพาะพอร์ตที่เป็นปลายทางเท่านั้นทำให้คอมพิวเตอร์ ที่เชื่อมต่อกับพอร์ตที่เหลือสามารถส่งข้อมูลถึงกันและกันได้ในเวลาเดียวกันการทำเช่นนี้ทำให้อัตราการรับส่งข้อมูลหรือแบนด์วิธไม่ขึ้นอยู่กับจำนวนคอมพิวเตอร์ที่เชื่อมต่อเข้ากับสวิตช์ คอมพิวเตอร์ทุกเครื่องจะมีแบนด์วิธเท่ากับแบนด์วิธของสวิตช์ด้วยข้อดีนี้เครือข่ายที่ติดตั้งใหม่ในปัจจุบันส่วนใหญ่จะนิยมใช้สวิตช์มากกว่าฮับ เพราะจะไม่มีปัญหาเกี่ยวกับการชนกันของข้อมูลในเครือข่าย

รูปที่ 2.4.4 อุปกรณ์สวิทช์

ที่มา : http://www.synaptech.com

รูปทรงภายนอกของฮับกับสวิตช์ ดูภายนอกจะคล้ายๆ กัน คือมีลักษณะกล่องสี่เหลี่ยมที่ด้านหน้าจะมีพอร์ตแบบ RJ-45 ไว้สำหรับเสียบเข้ากับสายแลน สำหรับจำนวนพอร์ตก็แตกต่างกันไปซึ่งมีตั้งแต่ 4, 5, 8, 12, 16, 24, 48 พอร์ตหรือมากกว่านั้นขึ้นอยู่กับแต่ละยี่ห้อและแต่ละรุ่นสำหรับรูปทรงภายนอกของสวิตช์นั้นมีทั้งแบบตั้งโต๊ะหรือแบบแขวนกับผนังและแบบที่ใส่ไว้ในตู้อุปกรณ์คอมพิวเตอร์ (Rack Mountable)

สวิตช์ในสมัยแรกเริ่มจะรองรับความเร็วได้สูงสุดเพียง 10 Mbps ต่อมามีการพัฒนามาตรฐานที่เรียกว่า Fast Ethernet ซึ่งรองรับความเร็วได้สูงสุด 100 Mbps และเพื่อให้สามารถใช้ได้กับอุปกรณ์รุ่นเก่าที่รองรับความเร็วได้เพียง 10 Mbps สวิตช์แบบ Fast Ethernet จึงถูกออกแบบให้รองรับความเร็วได้ทั้งสองระดับคือทั้ง 10 และ 100 Mbps (หรือเขียนเป็น 10/100 Mbps) และเรียกว่า Dual Speed Auto-Sensing หรือ Auto-Negotiation

ในปัจจุบันสวิตช์สามารถรองรับความเร็วได้สูงถึงระดับ 1,000 Mbps หรือที่เรียกว่าGigabit Ethernet Switch ซึ่งสามารถรองรับความเร็วได้ทั้ง 3 ระดับคือ 10/100/1,000 Mbps และล่าสุดสวิตช์ได้พัฒนาถึงขั้นรองรับความเร็วระดับ 10 Gigabit Ethernet (10GbE) หรือ 1,000 Mbpsไปแล้ว รายละเอียดของสวิตช์และระดับความเร็วได้แสดงไว้ในตารางดังนี้

Switch	**ความเร็ว (Mbps)**
Ethernet Switch	10
Fast Ethernet Switch	100
Dual Speed Auto-Sensing (Auto-Negotiation) Ethernet Switch	10/100
Gigabit Ethernet Switch	10/100/1000

ปัจจุบันราคาของสวิตช์ แบบ 10/100 Mbps นั้นถูกลงมาก ในขณะที่ฮับแทบจะไม่มีขายกันแล้ว เพราะถูกแทนที่โดยสวิตช์ นั่นเองสำหรับบริษัทผู้ผลิตอุปกรณ์ ฮับ/สวิตช์ ที่เรารู้จักกันดีเช่น CISCO, INTEL, 3COM, D-LINK, SMC, NETGEAR และ LINKSYS เป็นต้น

การเปรียบเทียบการทำงาน ฮับ/สวิตซ์

ฮับจะทำการส่งข้อมูลในลักษณะการส่ง กระจาย (Broadcast) โดยข้อมูลที่ส่งจากคอมพิวเตอร์เครื่องใดเครื่องหนึ่ง (หรือจากพอร์ตใดพอร์ตหนึ่งของฮับ) จะถูกส่งกระจายให้กับเครื่องอื่นๆ ที่ต่อกับพอร์ตอื่นๆ ในฮับตัวนั้นทุกเครื่อง คือรับมาแล้วปล่อยกระจายออกไปทุกพอร์ตโดยไม่สนใจว่าข้อมูลนั้นควรจะส่งไปให้เครื่องใดหรือพอร์ตใด

รูปที่ 2.4.5 อุปกรณ์ฮับและสวิทซ์

ที่มา : www.magmareport.com

ในขณะที่สวิตซ์ นั้น ข้อมูลจะถูกเลือกส่งไปให้กับเครื่องคอมพิวเตอร์ที่เป็นจุดหมายปลายทางโดยตรง หรือจากพอร์ตต้นทางไปหาพอร์ตปลายทาง เครื่องคอมพิวเตอร์อื่นที่ไม่เกี่ยวข้องจะไม่ได้รับข้อมูล ดังนั้นเราสามารถเรียก สวิตซ์ ว่าเป็นฮับ ที่ฉลาดขึ้นมาหน่อยก็ได้

ฮับจะทำงานในระดับ Physical Layer หรือ Layer1 ของโมเดล OSI ดังนั้นเราจะเรียก ฮับ (Hub) ว่า รีพีตเตอร์ (Repeater) ก็ได้ เนื่องจากมันเพียงแต่ทำหน้าที่รับสัญญาณมาแล้วปล่อยออกไปคล้ายๆ กับเครื่องทวนสัญญาณนั่นเอง สำหรับสวิตซ์นั้นจะทำงานในระดับ Data Link Layer หรือLayer 2 ของโมเดล OSI โดยมันจะต้องอาศัย Mac Address ในการทำงาน ดังนั้นเราอาจจะได้ยินคนเรียก สวิตซ์ ว่า Layer 2 Switch (L2 Switch) เพื่อให้แตกต่างจากอุปกรณ์รุ่นใหม่ในปัจจุบัน เช่นLayer 3 Switch (L3 Switch) ที่ทำงานในระดับของ Network Layer หรือ Layer 3 ของโมเดล OSI

การพ่วง ฮับ/สวิตซ์ เข้าด้วยกัน

ฮับ/สวิตซ์ รุ่นเก่าๆ สามารถนำมาพ่วงต่อกันได้โดยใช้สายแลนเชื่อมต่อกับพอร์ตพิเศษที่เรียกว่า Uplink ของตัวที่ 1 ไปยังพอร์ตธรรมดาของตัวที่ 2 โดยใช้สายแลนแบบธรรมดา (Straight Through Cable) หรือถ้าไม่มีพอร์ต Uplink ก็สามารถใช้สายแลนแบบไขว้ (Crossover Cable) เชื่อมระหว่างพอร์ตธรรมดาของ ฮับ/สวิตซ์ ทั้งสองตัวเข้าด้วยกันได้

รูปที่ 2.4.6 การพ่วงฮับผ่านช่อง Strackable

ที่มา : http://garrettcom.com/3000_series.htm

แต่ในปัจจุบัน ฮับ/สวิตซ์ รุ่นใหม่ๆ สามารถพ่วงกันได้โดยผ่านพอร์ตธรรมดาด้วยสายแลนแบบธรรมดา (Straight Through Cable) โดยไม่จำเป็นต้องใช้สายแลนแบบไขว้ (Crossover Cable) ก็ได้เนื่องจากมันสามารถที่จะปรับวงจรภายในให้เข้ากับประเภทของสายแลนที่ใช้ได้โดยอัตโนมัติ ความสามารถดังกล่าวนี้เรียกว่า Auto MDI/MDIX หรือ Auto Uplink แต่ข้อเสียของการพ่วง ฮับ/สวิตซ์ ดังกล่าวก็คือ จะต้องเสียพอร์ตของ ฮับ/สวิตซ์ ไป 1 พอร์ตต่อการพ่วง ฮับ/สวิตซ์ 1 ตัวด้วย

ฮับ/สวิตซ์ บางรุ่นสามารถนำมาพ่วงต่อกันได้เพื่อให้มองเห็นเป็นตัวเดียวกันโดยใช้สายเคเบิ้ลพิเศษเชื่อมต่อกับพอร์ตพิเศษด้านหลัง ซึ่งเราจะเรียก ฮับ/สวิตซ์ ที่มีคุณสมบัตินี้ว่า StrackableHub/Switch ทำให้ไม่ต้องเปลืองพอร์ตทางด้านหน้า และยังทำให้ได้ความเร็วระหว่าง ฮับ/สวิตซ์ ที่สูงกว่าการพ่วงผ่านพอร์ต RJ-45 ด้านหน้าเสียอีก บางยี่ห้อสามารถที่จะเชื่อมต่อกันได้ถึง 32 ตัวหรือมากกว่านั้น สำหรับการพ่วงต่อ ฮับ/สวิตซ์ ในกรณีนี้จะมีข้อจำกัดคือมักจะต้องเป็นสวิตซ์ ยี่ห้อเดียวกันหรือรุ่นเดียวกัน เนื่องจากลักษณะของสายเคเบิ้ลที่ใช้พ่วงต่อด้านหลังนั้นจะไม่มีมาตรฐานที่แน่นอน หรืออาจจะแตกต่างกันไปตามรุ่นหรือยี่ห้อนั้นๆ

Managed Switch และ Unmanaged Switch

รูปที่ 2.4.7 Unmanaged Switch และ Managed Switch

ที่มา : http://www.dcomputer.com

โดยทั่วไปสวิตซ์ ที่ใช้กันอย่างแพร่หลายและราคาไม่แพงมากนักจะเป็นแบบ Unmanaged Switch กล่าวคือจะไม่มีเฟิร์มแวร์หรือซอฟต์แวร์อยู่ในตัวให้สามารถปรับแต่งหรือตั้งค่าอะไรก็ได้ ในขณะที่ สวิตซ์อีกประเภทหนึ่งที่เรียกว่า Managed Switch (หรือ Intelligent Switch) จะมีเฟิร์มแวร์อยู่ภายในตัวทำให้สามารถปรับแต่งหรือบริหารจัดการผ่านเครือข่ายได้ง่ายขึ้น เช่น

- สามารถใช้โปรแกรมเว็บบราวเซอร์เข้าไปปรับแต่งหรือควบคุมการทำงาน (Web Management Utility)
- สนับสนุนการทำ VLAN
- สามารถเชื่อมต่อกับระบบบริหารและจัดการเครือข่าย (Network Management System)
- สนับสนุนการทำ Port Mirroring และ Port Trunking
- สามารถเปิด/ปิด หรือจำกัดความเร็วของพอร์ตแต่ละพอร์ตได้

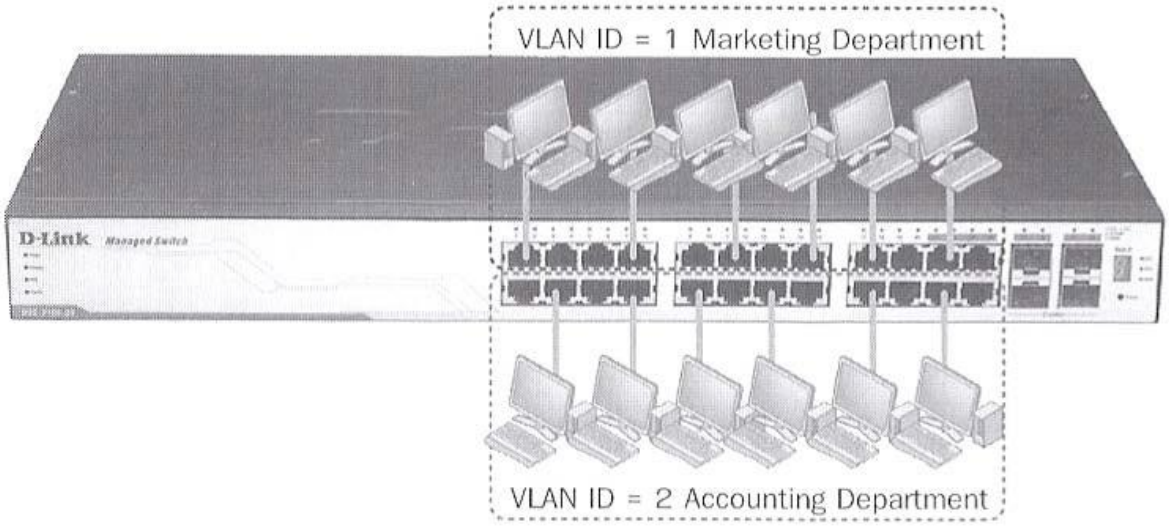
ดังนั้น Managed Switch จึงมีราคาแพงและมักใช้ในองค์กรหรือบริษัทใหญ่ๆ หรือใช้ในศูนย์คอมพิวเตอร์ (Data Center) นอกจากนี้อาจเคยได้ยินคำว่า Smart Switch ที่วางขายกันตามท้องตลาด ซึ่งก็คือ Managed Switch ที่มีความสามารถจำกัดหรือน้อยกว่า Managed Switch ปกตินั่นเอง

เทคโนโลยีใหม่ๆ ในสวิตซ์

VLAN

VLAN (Virtual LAN) คือการจัดกลุ่มพอร์ตของสวิตซ์ เป็นกลุ่มๆ โดยอาศัยเฟิร์มแวร์หรือซอฟต์แวร์ภายในตัวของมัน เพื่อจำกัดหรือควบคุมการติดต่อสื่อสารระหว่างกลุ่มของพอร์ตที่จัดแบ่งไว้

VLAN เปรียบเสมือนการนำสวิตซ์ ตัวใหญ่ๆ 1 ตัวมาแบ่งย่อยให้กลายเป็นสวิตซ์ ย่อยๆ หลายตัว เช่น สวิตซ์ขนาด 24 พอร์ต 1 ตัว หากมีการจัดแบ่งพอร์ตออกเป็น 2 กลุ่มๆ ละ 12 พอร์ต ก็จะได้สวิตซ์ ย่อยๆ 2 ตัว ตัวละ 12 พอร์ตนั่นเอง หลังจากนั้นสามารถที่จะใช้ซอฟต์แวร์ในสวิตซ์ทำการจัดระเบียบหรือควบคุมการทำงานของสวิตซ์ ย่อยๆ เหล่านั้นได้



รูปที่ 2.4.8 การแบ่ง VLAN ในสวิตซ์

ที่มา : คู่มือดูแลระบบ Network ฉบับมืออาชีพ, 2551 : 72

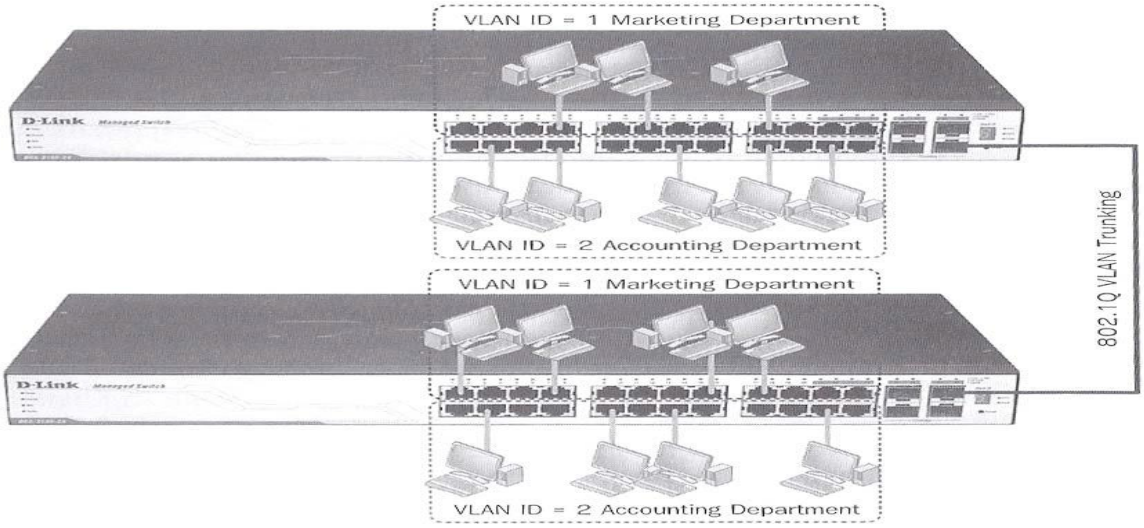
สวิตซ์ย่อยๆ แต่ละตัวนั้นหากมีการนำเอาอุปกรณ์คอมพิวเตอร์เข้าไปเชื่อมต่อก็จะเกิดเป็นระบบแลนวงย่อยๆ ขึ้น ซึ่งระบบแลนวงย่อยๆ เหล่านั้นก็จะเรียกว่า “Virtual LAN” หรือ VLAN นั่นเอง

ประโยชน์ที่ได้จากการใช้ VLAN

- เพื่อให้เกิดความปลอดภัย หรือเป็นการจำกัดการเข้าใช้ทรัพยากรของคอมพิวเตอร์ที่อยู่คนละกลุ่มกัน

- สามารถควบคุมหรือบริหารระบบแลนได้อย่างสะดวกและมีประสิทธิภาพ เช่น ทำให้ไม่จำเป็นต้องไปสลับสายหรือย้ายสายแลนที่พอร์ตของสวิตซ์จริงๆ
- สามารถประหยัดค่าใช้จ่ายในการติดตั้งอุปกรณ์ Router ซึ่งโดยปกติการติดต่อข้ามวงแลนคนละกลุ่มกันจะต้องใช้อุปกรณ์ Router เท่านั้น นอกจากนี้การใช้ VLAN ยังช่วยให้การติดต่อข้ามวงแลนทำได้รวดเร็วกว่าการใช้ Router ด้วย

เราสามารถนำเอาสวิตซ์ที่มีการกำหนด VLAN เอาไว้แล้ว 2 ตัวหรือมากกว่านั้นมาพ่วงกัน เพื่อทำให้ VLAN ที่อยู่บนสวิตซ์คนละตัวกันสามารถติดต่อกันได้ การติดต่อข้าม สวิตซ์ ของ VLAN จะเรียกว่า “VLAN Trunking” โดยปัจจุบันมีการกำหนดมาตรฐานที่เรียกว่า IEEE 802.1Q

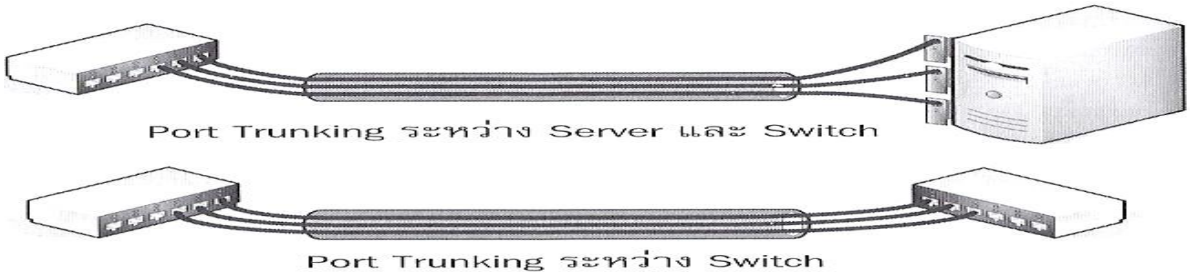


รูปที่ 2.4.9 VLAN Trunking

ที่มา : คู่มือดูแลระบบ Network ฉบับมืออาชีพ, 2551 : 73

Port Trunking หรือ Link Aggregation

ยังมีชื่อเรียกแตกต่างกันไปอีก เช่น Port Aggregation, Port Teaming, MultilinkTrunking, NIC Teaming, NIC Bonding หรือ Link Aggregation Group คือ มาตรฐาน IEEE802.3ad ซึ่งหมายถึงการอาศัยการ์ดแลนหลายๆ อันติดตั้งไว้ในเครื่องคอมพิวเตอร์ให้ช่วยกันรับส่งข้อมูลเสมือนราวกับว่าเป็นการ์ดแลนใบเดียวกัน ทำให้สามารถรับส่งข้อมูลได้ทีละมากๆ ซึ่งส่งผลให้ความเร็วในการส่งข้อมูลเพิ่มสูงขึ้นมากกว่าการรับส่งด้วยการ์ดแลนเพียงอันเดียว



รูปที่ 2.4.10 Port Trunking

ที่มา : คู่มือดูแลระบบ Network ฉบับมืออาชีพ, 2551 : 74

การทำ Port Trunking ระหว่างคอมพิวเตอร์เซิร์ฟเวอร์และพอร์ตของสวิตซ์ ตัวคอมพิวเตอร์เซิร์ฟเวอร์จะต้องติดตั้งซอฟต์แวร์สำหรับการทำ Port Trunking ด้วย แต่หากเป็นการทำระหว่างสวิตซ์นั้น ทั้ง 2 ตัวจะต้องสนับสนุนคุณสมบัติของ Port Trunking ด้วยประโยชน์ของการทำ Port Trunking นอกจากจะได้ความเร็วที่สูงขึ้นแล้ว ยังได้ประโยชน์ทางด้าน False Tolerant และ Load Balancing ด้วย

Layer3 Switch และ Multilayer Switch

รูปที่ 2.4.11 Netgear ProSafe 24-Port Layer 3 Managed Stackable Switch, 10/100Mbps

ที่มา : http://www.directron.com

Layer 3 Switch (หรือ L3 Switch) จริงๆ แล้วก็คือ สวิตซ์ทั่วๆ ไปที่ทำงานใน Layer 2 นั่นเอง แต่ได้เพิ่มความสามารถในการจัดการหรือลำเลียงแพ็กเก็ตใน Layer 3 โดยเฉพาะโปรโตคอล IP เป็นหลัก ซึ่งความสามารถที่เพิ่มขึ้นมานี้ที่แท้จริงแล้วคือหน้าที่ของอุปกรณ์ Routerนั่นเอง เราจึงมักจะเรียก Layer 3 สวิตซ์ในกรณีนี้ว่า Routing Switch อธิบายง่ายๆ คือ Layer 3Switch ก็คือ สวิตซ์ที่มีความสามารถในการทำตัวเป็น Router ด้วย แต่จะแตกต่างจาก Router ก็คือมันจะทำหน้าที่ของ Router ได้รวดเร็วกว่าหรือด้วยวิธีที่ฉลาดกว่า กล่าวคือมันจะเรียนรู้เส้นทางในการลำเลียงข้อมูลของอุปกรณ์ทุกตัวที่ต่อกับตัวมันเองก่อนในช่วงแรกๆ เช่น ข้อมูลที่ว่าพอร์ตไหนมี IP Address อะไรผ่านเข้าออกบ้าง หลังจากที่ได้รับข้อมูลเพียงพอ

แล้วมันจะเปลี่ยนมาใช้วิธีการลำเลียงข้อมูลใน Layer 2 เหมือน สวิตช์ทั่วๆ ไปนั่นเอง ทำให้สามารถลดขั้นตอนในการทำงานลงได้ ซึ่งผลก็คือความเร็วในการส่งผ่านข้อมูลจะเพิ่มสูงขึ้นด้วย Layer 3 Switch จึงเหมาะที่จะนำมาใช้ในระบบแลนที่มีความเร็วสูง

ในบางกรณี Layer 3 Switch อาจจะหมายถึงอุปกรณ์ Router ที่เรียกกันว่า SwitchingRouter ซึ่งหมายถึง Router ที่ได้รับการเพิ่มความสามารถของสวิตช์เข้าไปในตัวด้วย อย่างไรก็ตามSwitching Router ยังได้รับการปรับปรุงวงจรการทำงานภายในจากเดิมที่ใช้ไมโครโปรเซสเซอร์ หรือ CPU ในการคัดเลือกเส้นทางและลำเลียงแพ็กเก็ต ก็เปลี่ยนมาใช้ฮาร์ดแวร์ที่มีวงจรการทำงานโดยเฉพาะ ซึ่งเรียกว่า ASIC (Application Specific Integrated Circuit) ทำให้การทำงานของ Router เพิ่มสูงมากขึ้น

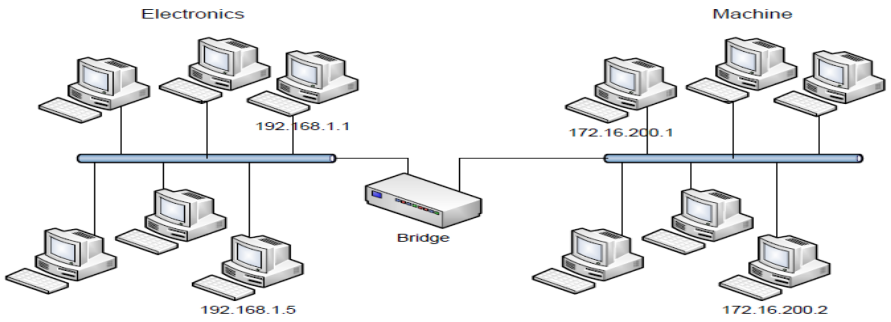
รูปที่ 2.4.12 D-Link Multilayer Switch 48 Port 10/100/1000

ที่มา : http://global.dlink.com.sg

นอกจากนี้ยังมีการพัฒนาสวิตช์ให้มีความสามารถทำงานในระดับที่สูงกว่า Layer3 ที่เรียกว่า Multilayer Switch โดยจะเน้นเฉพาะโปรโตคอลในระดับบนที่อาศัย TCP/IP เป็นหลัก เช่น ในกรณีของ Layer 4 (Transport layer) ที่มีการเพิ่มคุณสมบัติของ Layer4 Management System,QoS(Quality of Service) และ IP Multicast และในกรณีของ Layer 7 (Application Layer) ที่ทำให้การลำเลียงแพ็กเก็ตของโปรโตคอล HTTP ระหว่างตัวเว็บเซิร์ฟเวอร์และเว็บบราวเซอร์ทำได้รวดเร็วขึ้น

บริดจ์(Bridge)

บริดจ์ (Bridge) เป็นอุปกรณ์ที่ใช้ในการเชื่อมส่วนต่างๆ ของเครือข่ายท้องถิ่นเข้าด้วยกันบริดจ์ใช้ในการติดต่อสื่อสารข้อมูลระหว่างเครือข่ายแลน 2 เครือข่ายที่มีโพรโทคอลเหมือนกันหรือต่างกัน บริดจ์จะรับแพ็กเกตข้อมูลจากสถานีส่ง ผู้ส่งในเครือข่ายต้นทางทำการตรวจสอบตำแหน่งปลายทาง จากนั้นก็จะส่งแพ็กเกตข้อมูลทั้งหมดนั้นไปยังผู้ใช้เครือข่ายปลายทาง



รูปที่ 2.5.1

หลักการทำงานของบริดจ์

บริดจ์จะทำงานอยู่ในเลเยอร์ชั้นที่ 2 หรือชั้นดาต้าลิงค์ (Data Link Layer) ของรูปแบบโอเอสไอ บริดจ์เป็นอุปกรณ์เชื่อมโยงเครือข่ายของเครือข่ายที่แยกจากกัน แต่เดิมบริดจ์ได้รับการออกแบบมาให้ใช้กับเครือข่ายประเภทเดียวกัน เช่น ใช้เชื่อมโยงระหว่างอีเทอร์เน็ตกับอีเธอร์เน็ตบริดจ์มีใช้มานานแล้ว ตั้งแต่ปี ค.ศ. 1980 บริดจ์จึงเป็นเสมือนสะพานเชื่อมระหว่างสองเครือข่ายการติดต่อภายในเครือข่ายเดียวกันมีลักษณะการส่งข้อมูลแบบกระจาย (Broadcasting) ดังนั้นจึงกระจายได้เฉพาะเครือข่ายเดียวกันเท่านั้น

การรับส่งภายในเครือข่ายมีข้อกำหนดให้แพ็กเกตที่ส่งกระจายไปยังตัวรับได้ทุกตัวแต่ถ้ามีการส่งมาที่แอดเดรสต่างเครือข่าย บริดจ์จะนำข้อมูลเฉพาะแพ็กเกตนั้นส่งให้ บริดจ์จึงเป็นเสมือนตัวแบ่งแยกข้อมูลระหว่างเครือข่ายให้มีการสื่อสารภายในเครือข่ายของตน ไม่ปะปนไปยังอีกเครือข่ายหนึ่ง เพื่อลดปัญหาปริมาณข้อมูลกระจายในสายสื่อสารมากเกินไป ในระยะหลังมีผู้พัฒนาบริดจ์ให้เชื่อมโยงเครือข่ายต่างชนิดกันได้ เช่น อีเทอร์เน็ต กับ โทเคนริง เป็นต้น หากมีการเชื่อมต่อเครือข่ายมากกว่าสองเครือข่ายเข้าด้วยกันและเครือข่ายที่เชื่อมมีลักษณะหลากหลาย ซึ่งเป็นทั้งเครือข่ายแบบแลน และแวน อุปกรณ์ที่นิยมใช้ในการเชื่อมโยงคือ เราท์เตอร์ (Router)

บริดจ์เป็นอุปกรณ์ที่จัดเก็บตารางรายการตำแหน่งที่อยู่ของเครื่องคอมพิวเตอร์ในระบบเครือข่ายแลนไว้ เมื่อมีข้อมูลเข้ามา บริดจ์จะทำการตรวจสอบข้อมูลดูว่าตำแหน่งปลายทางที่ต้องการส่งไปถึงมีอยู่ในตารางรายการเครื่องคอมพิวเตอร์ในระบบเครือข่ายแลนของบริดจ์หรือไม่ถ้าพบว่ามีอยู่ใน ตารางรายการ บริดจ์ทำการกรองออกจากแพ็กเกตที่ส่งมาแล้วส่งไปยังปลายทางในระบบเครือข่ายนั้นๆ แต่ถ้าแพ็กเกตนั้นไม่ได้อยู่ในรายการในระบบเครือข่าย บริดจ์ก็จะทำการส่งผ่านข้ามไปบริดจ์อื่นในระบบเครือข่ายอื่นต่อไป

บริดจ์จะมีการทำงานที่รวดเร็ว เนื่องจากบริดจ์ไม่ได้จัดรูปแบบข้อมูลใหม่ เพียงแต่ทำการอ่านข้อมูลปลายทาง แล้วตัดสินใจว่าจะทำการกรองหรือส่งผ่านไป

อุปกรณ์บริดจ์เป็นสิ่งที่ใช้แก้ปัญหาในเรื่องสัญญาณที่วิ่งอยู่ในเครือข่ายมากเกินไปได้โดยจะจัดแบ่งเครือข่ายออกเป็นเครือข่ายย่อย (Network Segment) และจะทำการกลั่นกรองสัญญาณเท่าที่ จำเป็นเพื่อส่งให้กับเครือข่ายย่อยที่ถูกต้องได้ ทำให้สัญญาณไม่มารบกวนกันหรือมีสัญญาณที่ไม่เกี่ยวข้องเข้ามาในเครือข่ายย่อยโดยไม่จำเป็น แต่ในทางกลับกันถ้ามีความจำเป็นต้องการสื่อสารกันข้ามเครือข่ายย่อยเป็นจำนวนมากแล้ว อุปกรณ์บริดจ์ก็อาจจะกลายเป็นเสมือนคอขวดที่ทำให้เครือข่ายมีการทำงาน ช้าลงได้

ข้อดีอย่างหนึ่งของบริดจ์ก็คือ ช่วยลดการจราจรของข้อมูลในส่วนที่ไม่จำเป็นลงได้โดยการแบ่งเครือข่ายแลนขนาดใหญ่ที่เกิดการชนของข้อมูล (Collision) ให้เป็นเซกเมนต์ที่เล็กลง การดำเนินการดังกล่าวนี้จะเป็นการช่วยลดข้อมูลที่เกิดขึ้นเนื่องจากการที่หลายๆ โหนดส่งข้อมูลออกมาพร้อมกัน

รูปที่ 2.5.2 อุปกรณ์บริดจ์

ที่มา : http://www.sys2u.com

บริดจ์นั้นมี 2 รูปแบบคือ บริดจ์ท้องถิ่น (Local Bridge) ใช้สำหรับเชื่อมต่อแลน 2 เซกเมนต์ ที่อยู่ในท้องถิ่นหรือพื้นที่เดียวกันเข้าด้วยกัน และบริดจ์ทางไกล (Remote Bridge) ใช้เชื่อมต่อแลน 2 เซกเมนต์ที่อยู่ห่างไกลกันผ่านทางเครือข่ายแบบแวน การทำงานของบริดจ์คล้ายกับเราท์เตอร์ แต่บริดจ์จะทำงานในชั้นดาต้าลิงค์ ส่วนเราท์เตอร์นั้นจะทำงานในชั้นเน็ตเวิร์ด

บริดจ์นั้นมีความสามารถในการแปลงข้อมูลในระหว่างชั้น MAC Address ที่แตกต่างกันตัวอย่างเช่น บริดจ์นำเฟรมที่เป็นอีเทอร์เน็ตมาส่งต่อให้เป็นเฟรมของโทเคนริงในอีกพอร์ตหนึ่งได้บริดจะทำงานคล้ายกับเครื่องตรวจตำแหน่ง (Address) ของข้อมูล บริดจ์จะรับข้อมูลมาทั้งแพ็กเกตจากแลนต้นทาง และส่งทั้ง

แพ็กเกตนั้นให้กับแลนหนึ่งซึ่งอยู่ปลายทางโดยที่บริดจ์จะไม่ทำการแก้ไขหรือเพิ่มเติม ข่าวสารใดๆ ให้แก่แพ็กเกตข้อมูล

ข้อแตกต่างกันระหว่าง Bridge กับ สวิตซ์

ถึงแม้ว่า บริดจ์ (Bridge) กับสวิตซ์ (Switch) จะมีความฉลาดในการพิจารณาว่าควรส่งเฟรมข้อมูลออกทางพอร์ตไหน โดยพิจารณาจาก MAC Address ปลายทางก็ตาม แต่มีหลายๆ ปัจจัยที่ทำให้อุปกรณ์สวิตซ์มีข้อได้เปรียบมากว่าอุปกรณ์บริดจ์มาก จึงเป็นที่มาว่าทำไมปัจจุบัน เราจึงไม่ได้เห็นหน้าตาของบริดจ์กันแล้ว หลายๆ ปัจจัยที่ว่านั้นได้แก่

- ความเร็วในการทำงาน สวิตซ์นั้นทำงานได้เร็วกว่าบริดจ์
- จำนวนพอร์ตของบริดจ์มีเพียง 2 พอร์ต แต่สวิตซ์มีด้วยกันหลายพอร์ต
- ต้นทุนต่อพอร์ตของสวิทช์จะต่ำกว่าบริดจ์
- สวิตซ์มีความยืดหยุ่นในการเซตคอนฟิกูเรชั่นต่างๆ มากกว่าบริดจ์
- สวิตซ์นั้นสามารถแบ่งออกเป็น LAN เสมือนย่อยๆ ที่เรียกว่า VLAN ได้
- ในปัจจุบันไม่พบผู้ค่ารายใดจำหน่ายบริดจ์แล้ว มีแต่จำหน่ายสวิตซ์

ข้อแตกต่างกันระหว่าง Bridge กับ Router

บริดจ์ทำงานในชั้นที่ 2 (Datalink Layer) ส่วนเราเตอร์ทำงานที่ระดับสูงกว่าคือชั้นที่ 3 (Network Layer) ของรูปแบบโอเอสไอเราท์เตอร์ (Router)

เราท์เตอร์คือ อุปกรณ์ที่ทำหน้าที่ในการเชื่อมเครือข่ายหลายๆ เครือข่ายเข้าหากัน ซึ่งอาจจะเป็นวงแลนย่อยๆ ภายในบริษัทหรืออาจจะเป็นวงแลนที่อยู่ไกลกันคนละสถานที่ก็ได้ เช่น ระหว่างสาขาและสำนักงานใหญ่ เราท์เตอร์เป็นสิ่งที่ควบคู่กับโปรโตคอล TCP/IP ซึ่งหากปราศจากเราท์เตอร์แล้วระบบเครือข่ายอินเตอร์เน็ตคงไม่สามารถทำงานได้ เนื่องจากมันจะทำหน้าที่บอกเส้นทางการลำเลียงแพ็กเก็ตของโปรโตคอล TCP/IP ให้สามารถเดินทางถึงจุดหมายปลายทางได้

รูปที่ 2.5.3 เราท์เตอร์

ที่มา : http://www.ipcomsupply.com

การทำงานของ จะทำงานใน Layer 3 (Network Layer) ของโมเดล OSI หรือคือชั้นของInternet Layer ของ TCP/IP Model ดังรูป ภายในตัวเราท์เตอร์จะมีซอฟต์แวร์หรือระบบปฏิบัติการที่เปิดโอกาสให้สามารถตั้งค่าการทำงานต่างๆ ที่เกี่ยวกับเส้นทางการลำเลียงแพ็กเก็ตของโปรโตคอล TCP/IP ว่าต้องวิ่งผ่านเราท์เตอร์ ตัวไหนในระบบเครือข่ายไหนบ้าง

ปัจจุบันอุปกรณ์เราท์เตอร์ได้รับการพัฒนาไปมากทำให้การใช้งานเราท์เตอร์มีประสิทธิภาพ โดยเฉพาะเมื่อเชื่อมอุปกรณ์ เราท์เตอร์หลายๆ ตัวเข้าด้วยกันเป็นเครือข่ายขนาดใหญ่เราท์เตอร์สามารถทำงานอย่างมีประสิทธิภาพ โดยการหาเส้นทางเดินที่สั้นที่สุดเลือกตามความเหมาะสมและแก้ปัญหาที่เกิดขึ้นเองได้เมื่อเทคโนโลยีทางด้านอิเล็กทรอนิกส์ได้รับการพัฒนาให้มีขีดความสามารถในการทำงานได้เร็วขึ้น จึงมีผู้พัฒนาอุปกรณ์ที่ทำหน้าที่คัดแยกแพ็กเกตหรือเรียกว่า สวิทช์แพ็กเกตข้อมูล (Data Switched Packet) โดยลดระยะเวลาการตรวจสอบแอดเดรสลงไป การคัดแยกจะกระทำในระดับวงจรอิเล็กทรอนิกส์ เพื่อให้การทำงานมีประสิทธิภาพในด้านความเร็วและความแม่นยำสูงสุด อุปกรณ์สวิทช์ข้อมูลจึงมีเวลาหน่วงภายในตัวสวิทช์ต่ำมาก จึงสามารถนำมาประยุกต์กับงานที่ต้องการเวลาจริง เช่น การส่งสัญญาณเสียง วิดีโอ ได้ดี

จะเห็นว่าหน้าที่ของเราท์เตอร์คือ หาเส้นทางข้อมูลที่มีประสิทธิภาพสูงสุดและดีที่สุดเพื่อให้การส่งข้อมูลไปถึงปลายทางได้เร็วที่สุด โดยจะทำการคำนวณปริมาณของข้อมูล ความเร็วและระยะทางของเส้นทาง

ประกอบกัน เราท์เตอร์ที่มีประสิทธิภาพสูงสามารถปรับเปลี่ยนเส้นทางข้อมูลได้โดยอัตโนมัติในกรณีเส้นทางที่ใช้ส่งข้อมูลอยู่เกิดปัญหาในการใช้เราท์เตอร์เชื่อมโยงระหว่างเครือข่ายตั้งแต่ 2 เครือข่ายขึ้นไป ปริมาณข้อมูลที่ส่งผ่านเราท์เตอร์จึงมีจำนวนมาก เราเตอร์จึงต้องมีโปรเซสเซอร์ประมวลผลความเร็วสูงช่วยในการคำนวณหาเส้นทาง เพื่อป้องกันไม่ให้เกิดปัญหาคอคอดหรือปากขวดของข้อมูล ซึ่งจะทำให้ประสิทธิภาพในการสื่อสารข้อมูลช้าลงได้

การใช้งานเราท์เตอร์(Router) สามารถแบ่งได้เป็น 3 กรณีคือ

1. ใช้เชื่อมต่ออินเตอร์เน็ตผ่านวงจรเช่า (Leased Line) โดยจะเชื่อมจากวงแลนของผู้ให้บริการ ซึ่งมักจะเป็นลูกค้าแบบองค์กรไปยังวงแลน ที่อยู่ภายในที่ทำการของผู้ให้บริการอินเตอร์เน็ต ซึ่งเชื่อมต่อกับโครงข่ายอินเตอร์เน็ตความเร็วสูง
2. ใช้เชื่อมจากวงแลนของอาคารสำนักงานใหญ่ไปยังวงแลนของอาคารสาขาในลักษณะของจุดต่อจุด (Point-to-Point) โดยผ่านวงจรเช่า (Leased Line) หรือสื่อประเภทอื่น
3. ใช้เชื่อมวงแลนย่อยภายในองค์กรที่มีการกำหนด IP Address คนละกลุ่มหรือคนละ Subnet เข้าด้วยกัน สำหรับในกรณีที่ 3 นั้น สาเหตุที่ต้องมีการแบ่งระบบแลนออกเป็นวงแลนย่อยๆ โดยการกำหนด IP Address ให้เป็นคนละกลุ่มกัน หรือที่เรียกว่า Subnet นั้นก็เพื่อ
    - เพิ่มความเร็วให้กับระบบเครือข่าย เนื่องจากหากในวงแลนมีจำนวนเครื่องมากเกินไป เวลาที่มีการส่งข้อมูลประเภท Broadcast เกิดขึ้นจะทำให้วงแลนทำงานช้าลงได้ การแบ่งวงแลนขนาดใหญ่ วงออกเป็นวงแลนย่อยๆ หลายๆ วงจะเป็นการเพิ่มประสิทธิภาพของเครือข่ายย่อยๆ แต่ละวงได้
    - เป็นการจัดระเบียบโครงสร้างองค์กร เช่น อาจมีการแบ่งวงแลนย่อยๆ หรือ Subnetออกไปตามแผนกหรือฝ่ายต่างๆ ให้สอดคล้องกับโครงสร้างขององค์กร ทำให้ง่ายต่อการบริหารจัดการและควบคุมดูแล
    - เป็นการเพิ่มความปลอดภัยให้กับระบบเครือข่าย เช่น อาจมีการแบ่งวงแลนย่อยภายในออกเป็น 2 กลุ่มคือ กลุ่มที่ 1 คือวงแลนของฝ่ายบัญชีและการเงินที่ต้องการความปลอดภัยของข้อมูลสูงและกลุ่มที่ 2 จะเป็นกลุ่มผู้ใช้ฝ่ายอื่นๆ ที่เหลือทั้งหมด
    - กำหนดนโยบายการใช้งานอินเตอร์เน็ต เช่น อาจมีการแบ่งวงแลนย่อยภายในออกเป็น 2 กลุ่มคือ กลุ่มที่ 1 จะไม่สามารถใช้งานอินเตอร์เน็ตได้และกลุ่มที่ 2 จะสามารถใช้งานอินเตอร์เน็ตได้

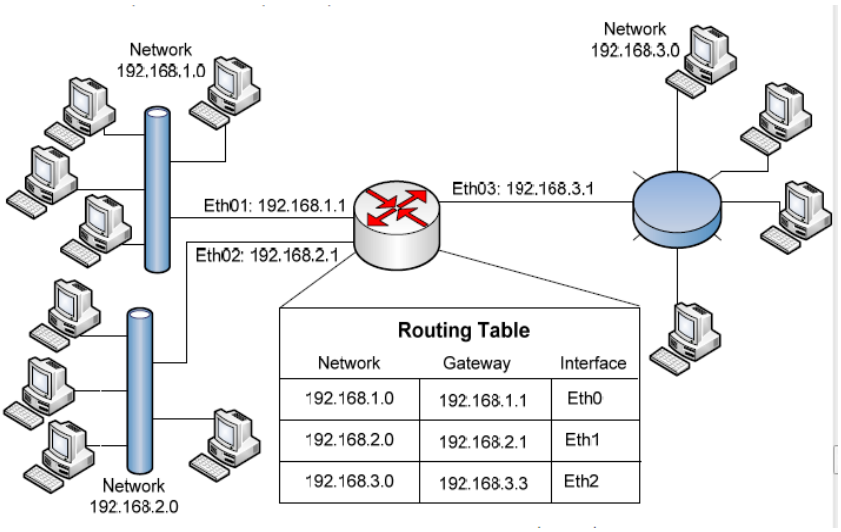
สำหรับเราท์เตอร์ ที่บริษัทหรือองค์กรต่างๆ ส่วนใหญ่นิยมเลือกใช้กันก็คือยี่ห้อ CISCO เนื่องจากเป็นเราท์เตอร์ ที่มีประสิทธิภาพและความน่าเชื่อถือสูง มีซอฟท์แวร์ภายในมารู้จักกันแพร่หลายคือ IOS (Internetwork Operating System) และมีการสนับสนุนทางด้านเทคนิคที่ดี โดยผู้ใช้สามารถหาข้อมูลเพื่อแก้ปัญหาทางด้านเทคนิคต่างๆ ได้ทางเว็บไซต์ได้ง่าย และมีให้เลือกหลายรุ่นหลายขนาดไปตามลักษณะการใช้งานและขนาดขององค์กร แต่ราคาก็สูงกว่ายี่ห้ออื่นด้วยเช่นกัน

Routing Table

หน้าที่ของเราท์เตอร์คือ การส่งผ่านแพ็กเก็ตระหว่างเครือข่าย ถ้าเปรียบเทียบระบบเครือข่ายกับระบบไปรษณีย์ เราท์เตอร์ก็เปรียบเสมือนเป็นที่ทำการไปรษณีย์นั่นเองเราท์เตอร์ต้องทราบข้อมูลเกี่ยวกับเครือข่ายต่างๆ เช่น เครือข่ายดังกล่าวสามารถส่งแพ็กเก็ตไปได้หรือไม่ ถ้าได้จะส่งไปทางใดได้บ้าง เป็นต้น

ข้อมูลเกี่ยวกับเส้นทางนี้จะถูกเก็บไว้ในตารางที่เรียกว่า เราท์ติ้งเทเบิ้ล ซึ่งตารางนี้จะมีรายการของหมายเลขไอพีของเราท์เตอร์ และหมายเลขเครือข่ายที่เราท์เตอร์สามารถสื่อสารได้เมื่อไรก็ตามที่เราท์เตอร์ต้องการจะส่งต่อแพ็กเก็ตมันจะใช้ข้อมูลในตารางนี้ในการตัดสินใจเลือกเส้นทาง

โดยทั่วไปแล้วในตารางเราท์ติ้งเทเบิลจะประกอบด้วย หมายเลขเครือข่าย (Network ID)ซับเน็ตมาส์ค (Subnet Mask) หมายเลขไอพีของเกตเวย์ (Gateway Address) เน็ตเวิร์คการ์ด (Network Interface) และเมทริก (Metric)



รูปที่ 2.5.4 การบันทึกเราท์ติ้งเทเบิ้ลของเราท์เตอร์

ที่มา : www.magmareport.com

ตารางแสดงเราท์ติ้งเทเบิล

Network ID	Subnet Mask	Gateway	Interface	Metric
192.168.1.0	255.255.255.0	192.168.1.1	Eth01	1
192.168.2.0	255.255.255.0	192.168.2.1	Eth02	1
192.168.3.0	255.255.255.0	192.168.3.1	Eth03	1

ตารางแสดงเราท์ติ้งเทเบิ้ล ซึ่งเป็นตารางภายในเราท์เตอร์ ในตารางจะประกอบด้วยรายการ ซึ่งจะเป็นข้อมูลที่จะใช้สำหรับส่งแพ็กเก็ตไปยังเครือข่ายปลายทาง เช่น เมื่อเราท์เตอร์ได้รับแพ็กเก็ตที่โฮสต์ปลายทางอยู่ในเครือข่าย 192.168.1.0 เราท์เตอร์ก็จะส่งต่อแพ็กเก็ตไปยังเครือข่ายปลายทางผ่านเน็ตเวิร์กการ์ด Eth01 ที่มีหมายเลขปลายทางเป็น 192.168.1.1 ความหมายของแต่ละคอลัมน์มีดังนี้

- หมายเลขเครือข่าย (Network ID) จะเป็นหมายเลขไอพี หรือหมายเลขเครือข่ายของโฮสต์ปลายทาง
- ซับเน็ตมาส์ค (Subnet Mask) หมายเลขที่เราท์เตอร์จะใช้แอนด์ (AND) กับหมายเลขไอพีของโฮสต์ปลายทาง เพื่อคำนวณหาหมายเลขเครือข่าย
- เกตเวย์ (Gateway) คือหมายเลขไอพีของเราท์เตอร์ หรือเกตเวย์ที่สามารถส่งแพ็กเก็ตข้อมูลถึงเครือข่ายปลายทาง
- อินเตอร์เฟส (Interface) คือเน็ตเวิร์กการ์ดของเราท์เตอร์ที่สามารถส่งข้อมูลถึงเกตเวย์ดังกล่าวได้
- เมทริก (Metric) เป็นตัวเลขที่เป็นหน่วยวัดเกี่ยวกับความยากง่ายในการส่งแพ็กเก็ตไปยังเครือข่ายนั้น ส่วนใหญ่จะหมายถึง จำนวนฮ็อป (HOP) หรือเราท์เตอร์ที่ต้องส่งแพ็กเก็ตผ่าน ก่อนที่จะมาถึงเครือข่ายปลายทาง

ประเภทของเราท์ติ้งโปรโตคอล

เราท์เตอร์จะใช้ข้อมูลที่อยู่ในตารางเราท์ติ้งเทเบิล สำหรับการส่งแพ็กเก็ตระหว่างเครือข่าย ส่วนเส้นทางที่ถูกเลือกนั้นจะขึ้นอยู่กับอัลกอริธึม (Algorithm) ที่ใช้ หรือที่เรียกว่า “เราท์ติ้งโปรโตคอล (Routing Protocol)” ประเภทของเราท์ติ้งโปรโตคอลสามารถแบ่งได้หลายแบบขึ้นอยู่กับลักษณะการทำงานของเราท์ติ้งโปรโตคอล ถ้าใช้ลักษณะการอัพเดตเราท์ติ้งเทเบิลก็สามารถแบ่งออกเป็น 2 ประเภทคือ

- Static Routing Protocol
- Dynamic Routing Protocol

Static IP Routing

สำหรับการจัดเส้นทางแบบนี้รายการในตารางเราท์ติ้งเทเบิ้ลจะถูกป้อนโดยผู้ดูแลระบบซึ่งข้อมูลในรายการนี้จะไม่มีการเปลี่ยนแปลง หลังจากนั้นการคอนฟิกตารางจะค่อนข้างง่าย แต่ผู้ติดตั้งระบบจะต้องป้อนข้อมูลทุกๆ ฟิลด์ในตารางเอง ซึ่งเป็นเหมือนกับการบอกเราท์เตอร์ให้ทราบว่าเครือข่ายไหนที่สามารถติดต่อได้ ความถูกต้องของข้อมูลในตารางเราท์ติ้งเทเบิลจะขึ้นอยู่กับ ความรับผิดชอบของผู้ดูแลระบบนั้นๆ โดยทั่วไปแล้วสำหรับเครือข่ายเล็กๆ จะใช้การเราท์แบบสแตติกนี้ แต่เมื่อเครือข่ยใหญ่ขึ้นก็จะใช้โปรโตคอลแบบไดนามิกซึ่งง่ายต่อการจัดการมากกว่า

Dynamic IP Routing

การจัดเส้นทางแบบไดนามิกนี้จะใช้โปโตคอลในการสร้างตารางเราท์ติ้งเทเบิ้ล แทนการป้อนข้อมูลเองโดยคน ซึ่งวิธีการสร้างนั้นจะขึ้นอยู่กับโปรโตคอล เช่น โหลดของช่องสัญญาณแบนด์วิธของลิ้งค์เป็นต้น ข้อได้เปรียบของการใช้โปรโตคอลประเภทนี้คือ รายการในตารางจะถูกอัพเดตโดยอัตโนมัติ ทำให้ผู้ดูแระบบไม่ต้องกังวลว่ารายการในตารางจะผิดพลาด ส่วนข้อเสียคือ ปริมาณการไหลของแพ็กเก็ตในเครือข่ายจะเพิ่มขึ้น

โปรโตคอลแบบไดนามิกนี้ยังแบ่งย่อยออกเป็น 2 ประเภทคือ

- Distance-Vector Routing Protocol
- Link-State Routing Protocol

Distance-Vector Routing Protocol

โปรโตคอลนี้จะเลือกเส้นทางที่ดีที่สุดโดยใช้เมทริก(Metric) เป็นเกณฑ์ โดยเมทริกนี้จะเป็นหน่วยที่วัดประสิทธิภาพของลิ้งค์ไปยังเครือข่ายนั้น และขึ้นอยู่กับโปรโตคอลที่ใช้ ซึ่งโดยส่วนใหญ่จะใช้จำนวนฮ็อป (HOP) เป็นหลัก เราท์เตอร์ที่ใช้โปรโตคอลนี้จะรักษาตารางเราท์ติ้งเทเบิ้ลโดยรายการในตารางนี้จะขึ้นอยู่กับสถานะของเครือข่ายนั้น

ข้อเสียของโปรโตคอลนี้คือ เราท์เตอร์จะต้องแลกเปลี่ยนข้อมูลซึ่งกันและกัน เพื่ออัพเดตรายการในตารางหรือเพื่อให้ตารางเราท์ติ้งเทเบิ้ลของแต่ละเราท์เตอร์ทันสมัยอยู่ตลอดเวลาเราท์เตอร์แต่ละตัวจะต้องบรอดคาสต์ในช่วงเวลาที่กำหนดเป็นประจำ ดังนั้นจึงทำให้จำนวนแพ็กเก็ตที่ไหลเวียนในเครือข่ายเพิ่มขึ้น

โปรโตคอลที่จัดอยู่ในประเภทนี้เช่น RIP (Routing Information Protocal), IGRP (Interior Gateway Routing Protocol) เป็นต้น

Link-State Routing Protocol

โปรโตคอลแบบลิงค์สเตจจะสร้างเส้นทางข้อมูลเหมือนกับต้นไม้ (Tree) โดยรากของต้นไม้นี้คือ เราท์เตอร์ตัวมันเอง โดยเราท์เตอร์แต่ละตัวจะบรอดคลาสต์ข้อมูลที่เกี่ยวกับเครือข่ายที่เชื่อมต่อตรงกับเราท์เตอร์และเมทริก เราท์เตอร์จะบรอดคลาสต์เฉพาะตอนที่มีการเปลี่ยนแปลงเท่านั้น ทำให้ลดจำนวนแพ็กเก็ตในเครือข่ายลงได้

เมื่อเราท์เตอร์ค้นพบว่ามีการเปลี่ยนแปลงเกี่ยวกับเครือข่ายที่เชื่อมต่อตรงกับเราท์เตอร์นั้น มันจะบอร์ดคาสต์ข้อมูลดังกล่าวไปยังทุกๆ เราท์เตอร์ ซึ่งกระบวนการนี้จะเรียกว่า “การฟลัดดิ้ง(Flooding)” การฟลัดดิ้งนี้จะอัพเดตฐานข้อมูลของทุกๆ เราท์เตอร์เฉพาะรายการที่มีการเปลี่ยนแปลงเท่านั้น โดยทั่วไปแล้วแพ็กเก็ตเหล่านี้จะมีขนาดเล็ก และมีการส่งไม่บ่อยมากนักโปรโตคอลที่จัดอยู่ในประเภทนี้ เช่น OSPF (Open Shortest Path first)