เขียนโดย Administrator
วันพุธที่ 22 มีนาคม 2017 เวลา 23:38 น. - แก้ไขล่าสุด วันพฤหัสบดีที่ 23 มีนาคม 2017 เวลา 22:50 น.

รับซ่อมระบบ Network ติดตั้งระบบ วางระบบ VPN Site To Site จัดการระบบ VLAN จัดการระบบ อินเตอร์เน็ต Server

พื้นที่ให้บริการ

> กรุงเทพมหานคร

- เขตคลองเตย แขวงคลองเตย แขวงคลองตัน แขวงพระโขนง
- เขตคลองสาน แขวงคลองต้นไทร แขวงคลองสาน แขวงบางลำภูล่าง แขวงสมเด็จเจ้าพระยา
- เขตคลองสามวา แขวงทรายกองดิน แขวงทรายกองดินใต้ แขวงบางชัน แขวงสามวาตะวันตก แขวงสามวาตะวันออก
- เขตคันนายาว แขวงคันนายาว
- เขตจตุจักร แขวงจตุจักร แขวงจอมพล แขวงจันทรเกษม แขวงลาดยาว แขวงเสนานิคม
- เขตจอมทอง แขวงจอมทอง แขวงบางขุนเทียน แขวงบางค้อ แขวงบางมด
- เขตดอนเมือง แขวงสีกัน
- เขตดินแดง แขวงดินแดง
- เขตดุสิต แขวงดุสิต แขวงถนนนครไชยศรี แขวงวชิรพยาบาล แขวงสวนจิตรลดา แขวงสี่แยกมหานาค
- เขตตลิ่งชัน แขวงคลองชักพระ แขวงฉิมพลี แขวงตลิ่งชัน แขวงบางเชือกหนัง แขวงบางพรม แขวงบางระมาด
- เขตทวีวัฒนา แขวงทวีวัฒนา แขวงศาลาธรรมสพน์
- เขตทุ่งครุ แขวงทุ่งครุ แขวงบางมด
- เขตธนบุรี แขวงดาวคะนอง แขวงตลาดพลู แขวงบางยี่เรือ แขวงบุคคโล แขวงวัดกัลยาณ์ แขวงสำเหร่ แขวงหิรัญรูจี
- เขตบางเขน แขวงท่าแร้ง แขวงอนุสาวรีย์
- เขตบางแค แขวงบางแค แขวงบางแคเหนือ แขวงบางไผ่ แขวงหลักสอง
- เขตบางกอกใหญ่ แขวงวัดท่าพระ แขวงวัดอรุณ
- เขตบางกอกน้อย แขวงบางขุนนนท์ แขวงบางขุนศรี แขวงบ้านช่างหล่อ แขวงศิริราช แขวงอรุณอมรินทร์
- เขตบางกะปิ แขวงคลองจั่น แขวงหัวหมาก
- เขตบางขุนเทียน แขวงท่าข้าม แขวงแสมดำ
- เขตบางคอแหลม แขวงบางโคล่ แขวงบางคอแหลม แขวงวัดพระยาไกร
- เขตบางซื่อ แขวงบางซื่อ
- เขตบางนา แขวงบางนา
- เขตบางบอน แขวงบางบอน
- เขตบางพลัด แขวงบางบำหรุ แขวงบางพลัด แขวงบางยี่ขัน แขวงบางอ้อ
- เขตบางรัก แขวงบางรัก แขวงมหาพฤฒาราม แขวงสี่พระยา แขวงสีลม แขวงสุริยวงศ์
- เขตบึงกุ่ม แขวงคลองกุ่ม แขวงนวลจันทร์
- เขตปทุมวัน แขวงปทุมวัน แขวงรองเมือง แขวงลุมพินี แขวงวังใหม่
- เขตประเวศ แขวงดอกไม้ แขวงประเวศ แขวงหนองบอน
- เขตป้อมปราบศัตรูพ่าย แขวงคลองมหานาค แขวงบ้านบาตร แขวงป้อมปราบ แขวงวัดเทพศิรินทร์ แขวงวัดโสมนัส
- เขตพญาไท แขวงสามเสนใน
- เขตพระโขนง แขวงบางจาก
- เขตพระนคร แขวงชนะสงคราม แขวงตลาดยอด แขวงบวรนิเวศ แขวงบางขุนพรหม แขวงบ้านพานถม แขวงพระบรมมหาราชวัง แขวงวังบูรพาภิรมย์ แขวงวัดราชบพิธ แขวงวัดสามพระยา แขวงศาลเจ้าพ่อเสือ แขวงสำราญราษฎร์ แขวงเสาชิงช้า
- เขตภาษีเจริญ แขวงคลองขวาง แขวงคูหาสวรรค์ แขวงบางจาก แขวงบางด้วน แขวงบางแวก แขวงบางหว้า แขวงปากคลองภาษีเจริญ
- เขตมีนบุรี แขวงมีนบุรี แขวงแสนแสบ
- เขตยานนาวา แขวงช่องนนทรี แขวงบางโพงพาง
- เขตราชเทวี แขวงถนนเพชรบุรี แขวงถนนพญาไท แขวงทุ่งพญาไท แขวงมักกะสัน
- เขตราษฎร์บูรณะ แขวงบางปะกอก แขวงราษฎร์บูรณะ
- เขตลาดกระบัง แขวงขุมทอง แขวงคลองสองต้นนุ่น แขวงคลองสามประเวศ แขวงทับยาว แขวงลาดกระบัง แขวงลำปลาทิว
- เขตลาดพร้าว แขวงจรเข้บัว แขวงลาดพร้าว
- เขตวังทองหลาง แขวงวังทองหลาง

เขียนโดย Administrator
วันพุธที่ 22 มีนาคม 2017 เวลา 23:38 น. - แก้ไขล่าสุด วันพฤหัสบดีที่ 23 มีนาคม 2017 เวลา 22:50 น.

- เขตวัฒนา แขวงคลองเตยเหนือ แขวงคลองตันเหนือ แขวงพระโขนงเหนือ
- เขตสวนหลวง แขวงสวนหลวง
- เขตสะพานสูง แขวงสะพานสูง
- เขตสัมพันธวงศ์ แขวงจักรวรรดิ แขวงตลาดน้อย แขวงสัมพันธวงศ์
- เขตสาทร แขวงทุ่งมหาเมฆ แขวงทุ่งวัดดอน แขวงยานนาวา
- เขตสายไหม แขวงคลองถนน แขวงสายไหม แขวงออเงิน
- เขตหนองแขม แขวงหนองแขม แขวงหนองค้างพลู
- เขตหนองจอก แขวงกระทุ่มราย แขวงคลองสิบ แขวงคลองสิบสอง แขวงคู้ฝั่งเหนือ แขวงโคกแฝด แขวงลำต้อยติ่ง แขวงลำผักชี แขวงหนองจอก
- เขตหลักสี่ แขวงตลาดบางเขน แขวงทุ่งสองห้อง
- เขตห้วยขวาง แขวงบางกะปิ แขวงสามเสนนอก แขวงห้วยขวาง

> จังหวัดนนทบุรี

> จังหวัดปทุมธานี

> จังหวัดสมุทรปราการ

> จังหวัดสมุทรสาคร

บทความ : เครือข่ายคอมพิวเตอร์ (ที่มา https://th.wikipedia.org/wiki)

จากวิกิพีเดีย สารานุกรมเสรี

ตัวอย่างแผนผังการเชื่อมต่อคอมพิวเตอร์แบบ Token Ring

เครือข่ายคอมพิวเตอร์ หรือ คอมพิวเตอร์เน็ตเวิร์ก (อังกฤษ: computer network; ศัพท์บัญญัติว่า ข่ายงานคอมพิวเตอร์)

คือเครือข่ายการสื่อสารโทรคมนาคมระหว่างคอมพิวเตอร์จำนวนตั้งแต่สองเครื่องขึ้นไปสามารถแลกเปลี่ยนข้อมูลกันได้

การเชื่อมต่อระหว่างอุปกรณ์คอมพิวเตอร์ต่างๆในเครือข่าย (โหนดเครือข่าย) จะใช้สื่อที่เป็นสายเคเบิลหรือสื่อไร้สาย เครือข่ายคอมพิวเตอร์ที่รู้จักกันดีคือ อินเทอร์เน็ต

การที่ระบบเครือข่ายมีบทบาทสำคัญมากขึ้นในปัจจุบัน เพราะมีการใช้งานคอมพิวเตอร์อย่างแพร่หลาย จึงเกิดความต้องการที่จะเชื่อมต่อคอมพิวเตอร์เหล่านั้นถึงกัน

เพื่อเพิ่มความสามารถของระบบให้สูงขึ้น และลดต้นทุนของระบบโดยรวมลง

การโอนย้ายข้อมูลระหว่างกันในเครือข่าย ทำให้ระบบมีขีดความสามารถเพิ่มมากขึ้น การแบ่งการใช้ทรัพยากร เช่น หน่วยประมวลผล, หน่วยความจำ,

หน่วยจัดเก็บข้อมูล, โปรแกรมคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ที่มีราคาแพงและไม่สามารถจัดหามาให้ทุกคนได้ เช่น เครื่องพิมพ์ เครื่องกราดภาพ (scanner)

ทำให้ลดต้นทุนของระบบลงได้

อุปกรณ์เครือข่ายที่สร้างข้อมูล, ส่งมาตามเส้นทางและบรรจบข้อมูลจะเรียกว่าโหนดเครือข่าย. โหนดประกอบด้วยโฮสต์เช่นเซิร์ฟเวอร์,

คอมพิวเตอร์ส่วนบุคคลและฮาร์ดแวร์ของระบบเครือข่าย

อุปกรณ์สองตัวจะกล่าวว่าเป็นเครือข่ายได้ก็ต่อเมื่อกระบวนการในเครื่องหนึ่งสามารถที่จะแลกเปลี่ยนข้อมูลกับกระบวนการในอีกอุปกรณ์หนึ่งได้

เครือข่ายจะสนับสนุนแอปพลิเคชันเช่นการเข้าถึงเวิลด์ไวด์เว็บ, การใช้งานร่วมกันของแอปพลิเคชัน, การใช้เซิร์ฟเวอร์สำหรับเก็บข้อมูลร่วมกัน,

การใช้เครื่องพิมพ์และเครื่องแฟ็กซ์ร่วมกันและการใช้อีเมลและโปรแกรมส่งข้อความโต้ตอบแบบทันทีร่วมกัน

การเชื่อมโยงเครือข่าย

สื่อกลางการสื่อสารที่ใช้ในการเชื่อมโยงอุปกรณ์เพื่อสร้างเป็นเครือข่ายคอมพิวเตอร์ประกอบด้วยสายเคเบิลไฟฟ้า (HomePNA, สายไฟฟ้าสื่อสาร, G.hn), ใยแก้วนำแสง และคลื่นวิทยุ (เครือข่ายไร้สาย) ในโมเดล OSI สื่อเหล่านี้จะถูกกำหนดให้อยู่ในเลเยอร์ที่ 1 และที่ 2 หรือชั้นกายภาพและชั้นเชื่อมโยงข้อมูล ครอบครัวของสื่อการสื่อสารที่ถูกพัฒนาอย่างกว้างขวางและถูกนำมาใช้ในเทคโนโลยีเครือข่ายท้องถิ่น (LAN) เรียกว่า อีเธอร์เน็ต มาตรฐานของสื่อกลางและของโพรโทคอลที่ช่วยในการสื่อสารระหว่างอุปกรณ์ในเครือข่ายอีเธอร์เน็ตถูกกำหนดโดยมาตรฐาน IEEE 802. อีเธอร์เน็ตในโลกไซเบอร์มีทั้งเทคโนโลยีของ LAN แบบใช้สายและแบบไร้สาย อุปกรณ์ของ LAN แบบใช้สายจะส่งสัญญาณผ่านสื่อกลางที่เป็นสายเคเบิล อุปกรณ์ LAN ไร้สายใช้คลื่นวิทยุหรือสัญญาณอินฟราเรดเป็นสื่อกลางในการส่งผ่านสัญญาณ

เทคโนโลยีแบบใช้สาย

เทคโนโลยีแบบใช้สายต่อไปนี้เรียงลำดับตามความเร็วจากช้าไปเร็วอย่างหยาบๆ

รูปแสดงสาย UTP

สายคู่บิดเป็นสื่อที่ใช้กันอย่างแพร่หลายที่สุดสำหรับการสื่อสารโทรคมนาคมทั้งหมด สายคู่บิดประกอบด้วยกลุ่มของสายทองแดงหุ้มฉนวนที่มีการบิดเป็นคู่ๆ สายโทรศัพท์ธรรมดาที่ใช้ภายในบ้านทั่วไปประกอบด้วยสายทองแดงหุ้มฉนวนเพียงสองสายบิดเป็นคู่ สายเคเบิลเครือข่ายคอมพิวเตอร์ (แบบใช้สายอีเธอร์เน็ตตามที่กำหนดโดยมาตรฐาน IEEE 802.3) จะเป็นสายคู่บิดจำนวน 4 คู่สายทองแดงที่สามารถใช้สำหรับการส่งทั้งเสียงและข้อมูล การใช้สายไฟสองเส้นบิดเป็นเกลียวจะช่วยลด crosstalk และการเหนี่ยวนำแม่เหล็กไฟฟ้าระหว่างสายภายในเคเบิลชุดเดียวกัน ความเร็วในการส่งอยู่ในช่วง 2 ล้านบิตต่อวินาทีถึง 10 พันล้านบิตต่อวินาที สายคู่บิดมาในสองรูปแบบคือคู่บิดไม่มีตัวนำป้องกัน(การรบกวนจากการเหนี่ยวนำแม่เหล็กไฟฟ้าภายนอก) (unshielded twisted pair หรือ UTP) และคู่บิดมีตัวนำป้องกัน (shielded twisted pair หรือ STP) แต่ละรูปแบบออกแบบมาหลายอัตราความเร็วในการใช้งานในสถานการณ์ต่างกัน

รูปแสดง STP จะเห็น sheath ที่เป็นตัวนำป้องกันอยู่รอบนอก

สายโคแอคเชียลถูกใช้อย่างแพร่หลายสำหรับระบบเคเบิลทีวี, ในอาคารสำนักงานและสถานที่ทำงานอื่นๆ ในเครือข่ายท้องถิ่น สายโคแอคประกอบด้วยลวดทองแดงหรืออะลูมิเนียมเส้นเดี่ยวที่ล้อมรอบด้วยชั้นฉนวน (โดยปกติจะเป็นวัสดุที่มีความยืดหยุ่นกับไดอิเล็กทริกคงที่สูง) และล้อมรอบทั้งหมดด้วยตัวนำอีกชั้นหนึ่งเพื่อป้องกันการเหนี่ยวนำแม่เหล็กไฟฟ้าจากภายนอก ฉนวนไดอิเล็กทริกจะช่วยลดสัญญาณรบกวนและความผิดเพี้ยน ความเร็วในการส่งข้อมูลอยู่ในช่วง 200 ล้านบิตต่อวินาทีจนถึงมากกว่า 500 ล้านบิตต่อวินาที

รูปแสดงสายโคแอคเชียล

'ITU-T G.hn เป็นเทคโนโลยีที่ใช้สายไฟที่มีอยู่ในบ้าน (สายโคแอค, สายโทรศัพท์และสายไฟฟ้า) เพื่อสร้างเครือข่ายท้องถิ่นความเร็วสูง (ถึง 1 Gb/s) ใยแก้วนำแสง เป็นแก้วไฟเบอร์ จะใช้พัลส์ของแสงในการส่งข้อมูล ข้อดีบางประการของเส้นใยแสงที่เหนือกว่าสายโลหะก็คือมีการสูญเสียในการส่งน้อยและมีอิสรภาพจากคลื่นแม่เหล็กไฟฟ้าและมีความเร็วในการส่งรวดเร็วมากถึงล้านล้านบิตต่อวินาที เราสามารถใช้ความยาวคลื่นที่แตกต่างของแสงที่จะเพิ่มจำนวนของข้อความที่ถูกส่งผ่านสายเคเบิลใยแก้วนำแสงพร้อมกันในเส้นเดียวกัน

เทคโนโลยีไร้สาย

'ไมโครเวฟบนผิวโลก - การสื่อสารไมโครเวฟบนผิวโลกจะใช้เครื่องส่งและเครื่องรับสัญญาณจากสถานีบนผิวโลกที่มีลักษณะคล้ายจานดาวเทียม ไมโครเวฟภาคพื้นดินอยู่ในช่วงกิกะเฮิรตซ์ที่ต่ำ ซึ่งจำกัดการสื่อสารทั้งหมดด้วยเส้นสายตาเท่านั้น สถานีทวนสัญญาณมีระยะห่างประมาณ 48 กิโลเมตร (30 ไมล์) ดาวเทียมสื่อสาร - การสื่อสารดาวเทียมผ่านทางคลื่นวิทยุไมโครเวฟที่ไม่ได้เบี่ยงเบนโดยชั้นบรรยากาศของโลก ดาวเทียมจะถูกส่งไปประจำการในอวกาศ ที่มักจะอยู่ในวงโคจร geosynchronous ที่ 35,400 กิโลเมตร (22,000 ไมล์) เหนือเส้นศูนย์สูตร ระบบการโคจรของโลกนี้มีความสามารถในการรับและถ่ายทอดสัญญาณเสียง, ข้อมูลและทีวี

ระบบเซลลูลาร์และ PCS ใช้เทคโนโลยีการสื่อสารวิทยุหลายเทคโนโลยี ระบบแบ่งภูมิภาคที่ครอบคลุมออกเป็นพื้นที่ทางภูมิศาสตร์หลายพื้นที่ แต่ละพื้นที่มีเครื่องส่งหรืออุปกรณ์เสาอากาศถ่ายทอดสัญญาณวิทยุพลังงานต่ำเพื่อถ่ายทอดสัญญาณเรียกจากพื้นที่หนึ่งไปยังอีกพื้นที่หนึ่งข้างหน้า เทคโนโลยีวิทยุและการแพร่กระจายสเปกตรัม - เครือข่ายท้องถิ่นไร้สายจะใช้เทคโนโลยีวิทยุความถี่สูงคล้ายกับโทรศัพท์มือถือดิจิทัลและเทคโนโลยีวิทยุความถี่ต่ำ.

เขียนโดย Administrator
วันพุธที่ 22 มีนาคม 2017 เวลา 23:38 น. - แก้ไขล่าสุด วันพฤหัสบดีที่ 23 มีนาคม 2017 เวลา 22:50 น.

LAN ไร้สายใช้เทคโนโลยีการแพร่กระจายคลื่นความถี่เพื่อการสื่อสารระหว่างอุปกรณ์หลายชนิดในพื้นที่จำกัด. IEEE 802.11
กำหนดคุณสมบัติทั่วไปของเทคโนโลยีคลื่นวิทยุไร้สายมาตรฐานเปิดที่รู้จักกันคือ Wifi
การสื่อสารอินฟราเรด สามารถส่งสัญญาณระยะทางสั้นๆมักไม่เกิน 10 เมตร ในหลายกรณีส่วนใหญ่ การส่งแสงจะใช้แบบเส้นสายตา
ซึ่งจำกัดตำแหน่งการติดตั้งของอุปกรณ์การสื่อสาร
เครือข่ายทั่วโลก (global area network หรือ GAN) เป็นเครือข่ายที่ใช้สำหรับการสนับสนุนการใช้งานมือถือข้ามหลายๆ LAN ไร้สาย
หรือในพื้นที่ที่ดาวเทียมครอบคลุมถึง ฯลฯ ความท้าทายที่สำคัญในการสื่อสารเคลื่อนที่คือการส่งมอบการสื่อสารของผู้ใช้จากพื้นที่หนึ่งไปอีกพื้นที่หนึ่ง ใน IEEE 802
การส่งมอบนี้เกี่ยวข้องกับความต่อเนื่องของ LAN ไร้สายบนผิวโลก .
เทคโนโลยีที่แปลกใหม่
มีความพยายามต่างๆที่ขนส่งข้อมูลผ่านสื่อที่แปลกใหม่ ได้แก่:
IP over Avian Carriers เป็นอารมณ์ขันของ April's fool เป็น RFC 1149 มันถูกนำมาใช้ในชีวิตจริงในปี 2001.
ขยายอินเทอร์เน็ตเพื่อมิติอวกาศผ่านทางคลื่นวิทยุ.
ทั้งสองกรณีมีการหน่วงเวลาสูงอันเนื่องมาจากสัญญาณต้องเดินทางไปกลับ ซึ่งจะทำให้การสื่อสารสองทางล่าช้ามาก แต่ก็ไม่ได้ขัดขวางการส่งข้อมูลจำนวนมาก
ชนิดของเครือข่าย
ระบบเครือข่ายจะถูกแบ่งออกตามขนาดของเครือข่าย ซึ่งปัจจุบันเครือข่ายที่รู้จักกันดีมีอยู่ 6 แบบ ได้แก่
เครือข่ายภายใน หรือ แลน (Local Area Network: LAN) เป็นเครือข่ายที่ใช้ในการ เชื่อมโยงกันในพื้นที่ใกล้เคียงกัน เช่นอยู่ในห้อง หรือภายในอาคารเดียวกัน
เครือข่ายวงกว้าง หรือ แวน (Wide Area Network: WAN) เป็นเครือข่ายที่ใช้ในการ เชื่อมโยงกัน ในระยะทางที่ห่างไกล อาจจะเป็น กิโลเมตร หรือ หลาย ๆ
กิโลเมตร
เครือข่ายงานบริเวณนครหลวง หรือ แมน (Metropolitan area network : MAN)
เครือข่ายของการติดต่อระหว่างไมโครคอนโทรลเลอร์ หรือ แคน (Controller area network) : CAN) เป็นเครือข่ายที่ใช้ติดต่อกันระหว่างไมโครคอนโทรลเลอร์
(Micro Controller unit: MCU)
เครือข่ายส่วนบุคคล หรือ แพน (Personal area network) : PAN) เป็นเครือข่ายระหว่างอุปกรณ์เคลื่อนที่ส่วนบุคคล เช่น โน้ตบุ๊ก มือถือ อาจมีสายหรือไร้สายก็ได้
เครือข่ายข้อมูล หรือ แซน (Storage area network) : SAN) เป็นเครือข่าย (หรือเครือข่ายย่อย)
ความเร็วสูงวัตถุประสงค์เฉพาะที่เชื่อมต่อภายในกับอุปกรณ์จัดเก็บข้อมูลชนิดต่างกันด้วยแม่ข่ายข้อมูลสัมพันธ์กันบนคัวแทนเครือข่ายขนาดใหญ่ของผู้ใช้
อุปกรณ์เครือข่าย
เซิร์ฟเวอร์ (Server) หรือเรียกอีกอย่างหนึ่งว่า เครื่องแม่ข่าย เป็นเครื่องคอมพิวเตอร์หลักในเครือข่าย ที่ทำหน้าที่จัดเก็บและให้บริการไฟล์ข้อมูลและทรัพยากรอื่นๆ
กับคอมพิวเตอร์เครื่องอื่น ๆ ใน เครือข่าย โดยปกติคอมพิวเตอร์ที่นำมาใช้เป็นเซิร์ฟเวอร์มักจะเป็นเครื่องที่มีสมรรถนะสูง
และมีฮาร์ดดิสก์ความจำสูงกว่าคอมพิวเตอร์เครื่องอื่น ๆ ในเครือข่าย
ไคลเอนต์ (Client) หรือเรียกอีกอย่างหนึ่งว่า เครื่องลูกข่าย เป็นคอมพิวเตอร์ในเครือข่ายที่ร้องขอ บริการและเข้าถึงไฟล์ข้อมูลที่จัดเก็บในเซิร์ฟเวอร์ หรือพูดง่าย ๆ
ก็คือ ไคลเอนต์ เป็นคอมพิวเตอร์ ของผู้ใช้แต่ละคนในระบบเครือข่าย
ฮับ (HUB) หรือ เรียก รีพีตเตอร์ (Repeater) คืออุปกรณ์ที่ใช้เชื่อมต่อกลุ่มคอมพิวเตอร์ ฮับ มีหน้าที่รับส่งเฟรมข้อมูลทุกเฟรมที่ได้รับจากพอร์ตใดพอร์ตหนึ่ง
ไปยังพอร์ตที่เหลือ คอมพิวเตอร์ที่เชื่อมต่อเข้ากับฮับจะแชร์แบนด์วิธหรืออัตราข้อมูลของเครือข่าย
เพราะฉะนั้นถ้ามีคอมพิวเตอร์เชื่อมต่อมากจะทำให้อัตราการส่งข้อมูลลดลง
เนทเวิร์ค สวิตช์ (Switch) คืออุปกรณ์เครือข่ายที่ทำหน้าที่ในเลเยอร์ที่ 2 และทำหน้าที่ส่งข้อมูลที่ได้รับมาจากพอร์ตหนึ่งไปยังพอร์ตเฉพาะที่เป็นปลายทางเท่านั้น
และทำให้คอมพิวเตอร์ที่เชื่อมต่อกับพอร์ตที่เหลือส่งข้อมูลถึงกันในเวลาเดียวกัน ดังนั้น อัตราการรับส่งข้อมูลหรือแบนด์วิธจึงไม่ขึ้นอยู่กับคอมพิวเตอร์
ปัจจุบันนิยมเชื่อมต่อแบบนี้มากกว่าฮับเพราะลดปัญหาการชนกันของข้อมูล
เราท์เตอร์ (Router)เป็นอุปรณ์ที่ทำหน้าที่ในเลเยอร์ที่ 3 เราท์เตอร์จะอ่านที่อยู่ (Address) ของสถานีปลายทางที่ส่วนหัว (Header) ข้อแพ็กเก็ตข้อมูล
เพื่อที่จะกำหนดและส่งแพ็กเก็ตต่อไป เราท์เตอร์จะมีตัวจัดเส้นทางในแพ็กเก็ต เรียกว่า เราติ้งเทเบิ้ล (Routing Table)
หรือตารางจัดเส้นทางนอกจากนี้ยังส่งข้อมูลไปยังเครือข่ายที่ให้โพรโทคอลต่างกันได้ เช่น IP (Internet Protocol) , IPX (Internet Package Exchange) และ
AppleTalk นอกจากนี้ยังเชื่อมต่อกับเครือข่ายอื่นได้ เช่น เครือข่ายอินเทอร์เน็ต
บริดจ์ (Bridge) เป็นอุปกรณ์ที่มักจะใช้ในการเชื่อมต่อวงแลน (LAN Segments) เข้าด้วยกัน ทำให้สามารถขยายขอบเขตของ LAN ออกไปได้เรื่อยๆ
โดยที่ประสิทธิภาพรวมของระบบ ไม่ลดลงมากนัก เนื่องจากการติดต่อของเครื่องที่อยู่ในเซกเมนต์เดียวกันจะไม่ถูกส่งผ่าน ไปรบกวนการจราจรของเซกเมนต์อื่น
และเนื่องจากบริดจ์เป็นอุปกรณ์ที่ทำงานอยู่ในระดับ Data Link Layer จึงทำให้สามารถใช้ในการเชื่อมต่อเครือข่ายที่แตกต่างกันในระดับ Physical และ Data Link
ได้ เช่น ระหว่าง Eternet กับ Token Ring เป็นต้น
บริดจ์ มักจะถูกใช้ในการเชื่อมเครือข่ายย่อย ๆ ในองค์กรเข้าด้วยกันเป็นเครือข่ายใหญ่ เพียงเครือข่ายเดียว เพื่อให้เครือข่ายย่อยๆ
เหล่านั้นสามารถติดต่อกับเครือข่ายย่อยอื่นๆ ได้
เกตเวย์ (Gateway) เป็นอุปกรณ์ฮาร์ดแวร์ที่เชื่อมต่อเครือข่ายต่างประเภทเข้าด้วยกัน เช่น การใช้เกตเวย์ในการเชื่อมต่อเครือข่าย ที่เป็นคอมพิวเตอร์ประเภทพีซี (PC)

เข้ากับคอมพิวเตอร์ประเภทแมคอินทอช (MAC) เป็นต้น
โพรโทคอลการสื่อสาร
คือชุดของกฎหรือข้อกำหนดต่างๆสำหรับการแลกเปลี่ยนข้อมูลในเครือข่าย ในโพรโทคอลสแต็ค (ระดับชั้นของโพรโทคอล ดูแบบจำลองโอเอสไอ) แต่ละโพรโทคอลยกระดับการให้บริการของโพรโทตคลที่อยู่ในชั้นล่าง ตัวอย่างที่สำคัญในโพรโทคอลสแต็คได้แก่ HTTP ที่ทำงานบน TCP over IP ผ่านข้อกำหนด IEEE 802.11 (TCP และ IP ที่เป็นสมาชิกของชุดโปรโตคอลอินเทอร์เน็ต. IEEE 802.11 เป็นสมาชิกของชุดอีเธอร์เน็ตโพรโทคอล.)
สแต็คนี้จะถูกใช้ระหว่างเราต์เตอร์ไร้สายกับคอมพิวเตอร์ส่วนบุคคลของผู้ใช้ตามบ้านเมื่อผู้ใช้จะท่องเว็บ
โพรโทคอลการสื่อสารมีลักษณะต่างๆกัน ซึ่งอาจจะเชื่อมต่อแบบ connection หรือ connectionless, หรืออาจจะใช้ circuit mode หรือแพ็กเกตสวิตชิง, หรืออาจใช้การ addressing ตามลำดับชั้นหรือแบบ flat
มีโพรโทคอลการสื่อสารมากมาย บางส่วนได้อธิบายไว้ด้านล่างนี้
อีเธอร์เน็ต
OSI model
7. Application layer
NNTP SIP SSI DNS FTP Gopher HTTP NFS NTP SMPP SMTP SNMP Telnet DHCP Netconf (more)
6. Presentation layer
MIME XDR
5. Session layer
Named pipe NetBIOS SAP PPTP RTP SOCKS SPDY TLS/SSL
4. Transport layer
TCP UDP SCTP DCCP SPX
3. Network layer
IP IPv4 IPv6 ICMP IPsec IGMP IPX AppleTalk X.25 PLP
2. Data link layer
ATM ARP SDLC HDLC CSLIP SLIP GFP PLIP IEEE 802.2 LLC L2TP IEEE 802.3 Frame Relay ITU-T G.hn DLL PPP X.25 LAPB Q.921 LAPD Q.922 LAPF
1. Physical layer
EIA/TIA-232 EIA/TIA-449 ITU-T V-Series I.430 I.431 PDH SONET/SDH PON OTN DSL IEEE 802.3 IEEE 802.11 IEEE 802.15 IEEE 802.16 IEEE 1394 ITU-T G.hn PHY USB Bluetooth RS-232 RS-449
ด พ ก
อีเธอร์เน็ตเป็นครอบครัวของโพรโทคอลที่ใช้ในระบบ LAN, ตามที่อธิบายอยู่ในชุดของมาตรฐานที่เรียกว่า IEEE 802
เผยแพร่โดยสถาบันวิศวกรไฟฟ้าและอิเล็กทรอนิกส์ ซึ่งมีวิธีการ addressing แบบ flat และจะดำเนินการส่วนใหญ่ที่ระดับ 1 และ 2 ของแบบจำลอง OSI.
สำหรับผู้ใช้ที่บ้านในวันนี้ สมาชิกส่วนใหญ่ของครอบครัวของโปรโตคอลที่รู้จักกันดีนี้คือ IEEE 802.11 หรือที่เรียกว่า Wireless LAN (WLAN). IEEE 802 โพรโทคอลชุดสมบูรณ์จัดให้มีความหลากหลายของความสามารถเครือข่าย ตัวอย่างเช่น MAC bridging (IEEE 802.1D) ทำงานเกี่ยวกับการ forwarding ของแพ็กเกตอีเธอร์เน็ตโดยใช้โพรโทคอล Spanning tree, IEEE 802.1Q อธิบาย VLANs และ IEEE 802.1X
กำหนดโพรโทคอลที่ใช้ควบคุมการเข้าถึงเครือข่ายแบบพอร์ตซึ่งฟอร์มตัวเป็นพื้นฐานสำหรับกลไกการตรวจสอบที่ใช้ใน VLANs (แต่ก็ยังพบในเครือข่าย WLANs อีกด้วย) - มันเป็นสิ่งที่ผู้ใช้ตามบ้านเห็นเมื่อผู้ใช้จะต้องใส่ "wireless access key".
ชุดโพรโทคอลอินเทอร์เน็ต
ชั้นโปรแกรมประยุกต์
BGP DHCP DNS FTP HTTP IMAP LDAP MGCP NNTP NTP POP ONC/RPC RTP RTSP RIP SIP SMTP SNMP SSH Telnet TLS/SSL XMPP ดูเพิ่ม...
Transport layer
TCP UDP DCCP SCTP RSVP
Internet layer
IP IPv4 IPv6 ICMP ICMPv6 ECN IGMP IPsec
Link layer
ARP NDP OSPF Tunnels L2TP PPP MAC Ethernet DSL ISDN FDDI
Internet protocol suite
อินเทอร์เน็ตโปรโตคอลสวีท, หรือที่เรียกว่า TCP / IP, เป็นรากฐานของระบบการเชื่อมโยงเครือข่ายที่ทันสมัย ทำให้มีการเชื่อมต่อแบบ connection-less

เช่นเดียวกับ connection-oriented ผ่านเครือข่ายที่ไม่น่าเชื่อถือโดยการส่งดาต้าแกรม(ข้อมูลที่ถูกแบ่งเป็นชิ้นเล็กๆ)ที่เลเยอร์โปรโตคอลอินเทอร์เน็ต (IP) ที่แกนกลางของมัน ชุดโพรโทคอลกำหนด address, การระบุตัวตน, และคุณสมบัติของการเราต์ติงสำหรับ Internet Protocol Version 4 (IPv4) และ IPv6 ซึ่งรุ่นต่อไปที่มีความสามารถในการขยายระบบ addressing อย่างมาก

SONET/SDH

Synchronous optical networking (SONET) และ Synchronous Digital Hierarchy (SDH) เป็นโพรโทคอลมาตรฐานสำหรับการ multiplexing ที่ทำการถ่ายโอนกระแสบิตดิจิตอลที่หลากหลายผ่านใยแก้วนำแสง. พวกมันแต่เดิมถูกออกแบบมาเพื่อการขนส่งในการสื่อสารแบบ circuit mode จากแหล่งที่มาที่หลากหลายแตกต่างกัน, เบื้องต้นเพื่อสนับสนุนระบบเสียงที่เป็น circuit-switched ที่เข้ารหัสในฟอร์แมท PCM (Pulse-Code Modulation) ที่เป็นเรียลไทม์และ ถูกบีบอัด. อย่างไรก็ตามเนื่องจากความเป็นกลางและคุณสมบัติที่เป็น transport-oriented, SONET/SDH ยังเป็นตัวเลือกที่ชัดเจนสำหรับการขนส่งเฟรมของ Asynchronous Transfer Mode (ATM)

Asynchronous Transfer Mode

เป็นเทคนิคการ switching สำหรับเครือข่ายการสื่อสารโทรคมนาคม ที่ใช้ asynchronous time-division multiplexing ATM จะเข้ารหัสข้อมูลที่เป็นเซลล์ขนาดเล็กคงที่ วิธีนี้จะแตกต่างจากโพรโทคอลอื่น ๆ เช่น Internet Protocol สวิทหรืออีเธอร์เน็ตที่ใช้แพ็กเกตหลายขนาด ATM มีความคล้ายคลึงกันกับ circuit switched และ packet switched networking. ATM จึงเป็นทางเลือกที่ดีสำหรับเครือข่ายที่ต้องจัดการทั้งแบบการจราจรที่มีข้อมูล throughput สูงแบบดั้งเดิมและแบบเนื้อหา real-time, ความล่าช้าแฝงต่ำเช่นเสียงและวิดีโอ. ATM ใช้รูปแบบการเชื่อมต่อแบบ connection-oriented model ในที่ซึ่งวงจรเสมือนจะต้องจัดตั้งขึ้นระหว่างจุดสิ้นสุดสองจุดก่อนที่การแลกเปลี่ยนข้อมูลที่เกิดขึ้นจริงจะเริ่มขึ้น ในขณะที่บทบาทของ ATM จะลดน้อยลงเนื่องจากความโปรดปรานของเครือข่ายรุ่นต่อไป มันยังคงมีบทบาทในการเป็นไมล์สุดท้ายซึ่งคือการเชื่อมต่อระหว่างผู้ให้บริการอินเทอร์เน็ตและผู้ใช้ตามบ้าน สำหรับรายละเอียดเพิ่มเติมของเทคโนโลยีและโปรโตคอลการสื่อสาร โปรดอ่านเพิ่มเติมในหัวข้อข้างท้าย

ขอบเขตของเครือข่าย

เครือข่ายโดยทั่วไปถูกจัดการโดยองค์กรที่เป็นเจ้าของ เครือข่ายองค์กรเอกชนอาจจะใช้รวมกันทั้งอินทราเน็ตและเอ็กซ์ทราเน็ต และยังอาจจัดให้มีการเข้าถึงเครือข่ายอินเทอร์เน็ตซึ่งไม่มีเจ้าของเดียวและให้การเชื่อมต่อทั่วโลกแทบไม่จำกัด

อินทราเน็ตและเอ็กซ์ทราเน็ต

อินทราเน็ตและเอ็กซ์ทราเน็ตเป็นส่วนหนึ่งหรือส่วนขยายของเครือข่ายคอมพิวเตอร์ที่มักจะเป็น LAN อินทราเน็ต เป็นชุดของเครือข่ายที่อยู่ภายใต้การควบคุมของหน่วยการบริหารเดียว อินทราเน็ตใช้โปรโตคอล IP และเครื่องมือที่เป็น IP-based เช่นเว็บเบราเซอร์และโปรแกรมการถ่ายโอนไฟล์ หน่วยการบริหารจำกัดการใช้อินทราเน็ตเฉพาะผู้ได้รับอนุญาตเท่านั้น ส่วนใหญ่แล้ว อินทราเน็ตจะเป็นเครือข่ายภายในองค์กร อินทราเน็ตขนาดใหญ่มักจะมีเว็บเซิร์ฟเวอร์อย่างน้อยหนึ่งตัวเพื่อให้ผู้ใช้เข้าถึงข้อมูลขององค์กรเอง เอ็กซ์ทราเน็ต เป็นเครือข่ายที่ยังอยู่ภายใต้การควบคุมของผู้ดูแลระบบขององค์กรเดียว แต่สนับสนุนการเชื่อมต่อที่จำกัดเฉพาะเครือข่ายภายนอกที่เฉพาะเจาะจง ตัวอย่างเช่นองค์กรอาจจัดให้มีการเข้าถึงบางแง่มุมของอินทราเน็ตของบริษัทเพื่อแชร์ข้อมูลร่วมกับคู่ค้าทางธุรกิจหรือลูกค้า หน่วยงานอื่น ๆ เหล่านี้ไม่จำเป็นต้องได้รับความเชื่อถือจากมุมมองของการรักษาความปลอดภัย การเชื่อมต่อเครือข่ายเอ็กซ์ทราเน็ตมักจะเป็น, แต่ไม่เสมอไป, การดำเนินการผ่านทาง WAN เทคโนโลยี

Internetwork

Internetwork คือการเชื่อมต่อของหลายเครือข่ายคอมพิวเตอร์ผ่านทางเทคโนโลยีการกำหนดเส้นทางร่วมกันโดยใช้เราต์เตอร์

อินเทอร์เน็ต

อินเทอร์เน็ตเป็นตัวอย่างที่ใหญ่ที่สุดของ Internetwork มันเป็นระบบที่เชื่อมต่อกันทั่วโลกของภาครัฐ, นักวิชาการ, องค์กรของรัฐและเอกชน, และเครือข่ายคอมพิวเตอร์ส่วนบุคคล มันขึ้นอยู่กับเทคโนโลยีระบบเครือข่ายของ Internet Protocol สวิท ซึ่งสืบทอดมาจากโครงการวิจัยขั้นสูงของหน่วยงานเครือข่าย (ARPANET) พัฒนาโดย DARPA ของกระทรวงกลาโหมสหรัฐอเมริกา อินเทอร์เน็ตยังเป็นแกนนำการสื่อสารพื้นฐานเวิลด์ไวด์เว็บ (WWW)
ผู้เข้าร่วมใน Internet ใช้ความหลากหลายของวิธีการหลายร้อยโพรโทคอลที่ถูกทำเป็นเอกสารและเป็นมาตรฐานไว้แล้ว โพรโทคอลดังกล่าวมักจะเข้ากันได้ดีกับ Internet Protocol Suite และระบบ addressing (ที่อยู่ IP) ที่ถูกบริหารงานโดยหน่วยงานกำหนดหมายเลขอินเทอร์เน็ตและทะเบียน address.
ผู้ให้บริการและองค์กรขนาดใหญ่ทำการแลกเปลี่ยนข้อมูลเกี่ยวกับความสามารถในการเข้าถึงพื้นที่ที่เป็น address ของพวกเขาผ่าน Border Gateway Protocol (BGP) ทำให้เป็นเส้นทางการส่งที่ซ้ำซ้อนของตาข่ายทั่วโลก

โทโพโลยีเครือข่าย

Network Topologies

โทโพโลยีเครือข่ายเป็นรูปแบบหรือลำดับชั้นของโหนดที่เชื่อมต่อกันของเครือข่ายคอมพิวเตอร์

รูปแบบสามัญ

รูปแบบที่พบบ่อยคือ:

เครือข่ายแบบบัส: ทุกโหนดจะถูกเชื่อมต่อกับสื่อกลางไปตลอดทั้งตัวสื่อนี้ รูปแบบนี้ใช้ในต้นฉบับอีเธอร์เน็ตที่เรียกว่า 10BASE5 และ 10Base2
เครือข่ายรูปดาว: ทุกโหนดจะเชื่อมต่อกับโหนดกลางพิเศษ รูปแบบนี้พบโดยทั่วไปใน LAN ไร้สายที่ลูกค้าแต่ละรายเชื่อมต่อแบบไร้สายกับจุดการเข้าถึง (Wireless access point)
เครือข่ายวงแหวน: แต่ละโหนดมีการเชื่อมต่อไปยังโหนดข้างเคียงด้านซ้ายและด้านขวา เพื่อที่ว่าทุกโหนดมีการเชื่อมต่อและแต่ละโหนดสามารถเข้าถึงโหนดอื่นโดยเข้าหาทางโหนดด้านซ้ายหรือโหนดด้านขวาก็ได้ ไฟเบอร์การเชื่อมต่อข้อมูลแบบกระจาย (Fiber Distributed Data Interface หรือ FDDI) ใช้โทโพโลยีแบบนี้
เครือข่ายตาข่าย: แต่ละโหนดจะเชื่อมต่อกับโหนดอื่นๆได้เกือบทั้งหมดในลักษณะที่มีอยู่อย่างน้อยหนึ่งเส้นทางไปยังโหนดใดๆ แต่อาจต้องผ่านโหนดอื่นไป
เครือข่ายที่เชื่อมต่ออย่างเต็มที่: ในแต่ละโหนดจะเชื่อมต่อกับทุกโหนดอื่น ๆ ในเครือข่าย
ต้นไม้: ในกรณีนี้โหนดทั้งหมดมีการจัดลำดับชั้น
โปรดสังเกตว่ารูปแบบทางกายภาพของโหนดในเครือข่ายอาจไม่จำเป็นต้องสะท้อนให้เห็นถึงโทโพโลยีเครือข่าย ตัวอย่างเช่น, FDDI มีโทโพโลยีเครือข่ายเป็นวงแหวน (ที่จริงสองวงหมุนสวนทางกัน) แต่โครงสร้างทางกายภาพอาจเป็นรูปดาวเพราะทุกการเชื่อมต่อกับโหนดที่อยู่ใกล้เคียงจะถูกส่งผ่านโหนดที่อยู่ตรงกลาง
เครือข่ายซ้อนทับ
เครือข่ายซ้อนทับเป็นเครือข่ายคอมพิวเตอร์เสมือนที่ถูกสร้างขึ้นทับบนเครือข่ายอื่น โหนดในเครือข่ายซ้อนทับจะถูกลิงค์เข้าด้วยกันแบบเสมือนหรือแบบลอจิก ที่ซึ่งแต่ละลิงค์จะสอดคล้องกับเส้นทางในเครือข่ายหลักด้านล่าง ที่อาจจะผ่านการลิงค์ทางกายภาพหลายลิงค์ โทโพโลยีของเครือข่ายซ้อนทับอาจ (และมักจะ) แตกต่างจากของเครือข่ายด้านล่าง. เช่น เครือข่ายแบบ peer-to-peer หลายเครือข่ายเป็นเครื่อข่ายซ้อนทับ
พวกมันจะถูกจัดให้เป็นโหนดของระบบเสมือนจริงของลิงค์ที่ทำงานบนอินเทอร์เน็ต อินเทอร์เน็ตถูกสร้างขึ้นครั้งแรกเป็นภาพซ้อนทับบนเครือข่ายโทรศัพท์.
ตัวอย่างที่โดดเด่นที่สุดของเครือข่ายซ้อนทับคือระบบของ Internet เอง. ที่เลเยอร์เครือข่ายแต่ละโหนดสามารถเข้าถึงโหนดอื่น ๆ โดยการเชื่อมต่อโดยตรงไปยัง IP address ที่ต้องการ ทำให้เกิดการสร้างเครือข่ายที่ถูกเชื่อมต่ออย่างเต็มที่ อย่างไรก็ตาม
เครือข่ายด้านล่างจะประกอบด้วยการเชื่อมต่อภายในเหมือนตาข่ายของเครือข่ายย่อยที่มี topologies (และเทคโนโลยี)ที่แตกต่างกัน การจำแนก address และการเราต์ติงค์เป็นวิธีที่ใช้ในการทำ mapping ของเครือข่ายซ้อนทับ(แบบ IP ที่ถูกเชื่อมต่ออย่างเต็มที่)ข้างบนกับเครือข่ายที่อยู่ข้างล่าง
เครือข่ายซ้อนทับเกิดขึ้นตั้งแต่มีการสร้างเครือข่ายเมื่อระบบคอมพิวเตอร์ถูกเชื่อมต่อผ่านสายโทรศัพท์โดยใช้โมเด็ม และเกิดขึ้นก่อนที่จะมีเครือข่ายข้อมูลเสียอีก
อีกตัวอย่างของเครือข่ายซ้อนทับก็คือตารางแฮชกระจายซึ่ง map คีย์(keys)ไปยังโหนดในเครือข่าย ในกรณีนี้เครือข่ายข้างใต้เป็นเครือข่าย IP และเครือข่ายทับซ้อนเป็นตาราง (ที่จริงเป็นแผนที่) ที่ถูกทำดัชนีโดยคีย์
เครือข่ายซ้อนทับยังได้รับการเสนอให้เป็นวิธีการปรับปรุงการเราต์ติงค์ในอินเทอร์เน็ต
เช่นการเราต์โดยการรับประกันคุณภาพการให้บริการเพื่อให้ได้สื่อกลางสตรีมมิ่งที่มีคุณภาพสูง ข้อเสนอก่อนหน้านี้เช่น IntServ, DiffServ และ IP Multicast ไม่ได้เห็นการยอมรับอย่างกว้างขวางเพราะข้อเสนอเหล่านี้จำเป็นต้องมีการปรับเปลี่ยนของเราต์เตอร์ทั้งหมดในเครือข่าย.
ในขณะที่เครือข่ายทับซ้อนถูกนำไปใช้งานเพิ่มขึ้นบน end-hosts ที่ run ซอฟแวร์โปรโตคอลทับซ้อนโดยไม่ต้องรับความร่วมมือจากผู้ให้บริการอินเทอร์เน็ต
เครือข่ายซ้อนทับไม่มีการควบคุมวิธีการที่แพ็คเก็ตจะถูกเราต์ในเครือข่ายข้างล่างระหว่างสองโหนดที่ซ้อนทับกัน แต่มันสามารถควบคุม, ตัวอย่างเช่น, ลำดับของโหนดซ้อนทับที่ข้อความจะลัดเลาะไปก่อนที่จะถึงปลายทาง
ตัวอย่างเช่น Akamai เทคโนโลยีทำการบริหารจัดการเครือข่ายซ้อนทับที่ดำเนินการจัดส่งเนื้อหาอย่างมีประสิทธิภาพและน่าเชื่อถือ (ชนิดหนึ่งของ multicast).
งานวิจัยที่เป็นวิชาการรวมถึงการ multicast ระบบปลาย, การเราต์ติงค์ที่มีความยืดหยุ่นและการศึกษาเรื่อง'คุณภาพของบริการ'(quality of service), ระหว่างเครือข่ายซ้อนทับอื่น ๆ

เครือข่ายส่วนตัวเสมือน (อังกฤษ: Virtual Private Network: VPN) คือ เครือข่ายเสมือนที่ยอมให้กลุ่มของ site สามารถสื่อสารกันได้. นโยบายในการใช้งานใน VPN ถูกกำหนดโดยชุดของ admin policies ที่จุดทำขึ้นโดยสมาชิกในกลุ่มนั้น หรือถูกกำหนดอย่างเบ็ดเสร็จโดย Service Provider (SP) site ดังกล่าวอาจอยู่ภายในองค์กรเดียวกันหรือต่างองค์กรก็ได้ หรือ VPN อาจเป็น intranet หรือ extranet site ดังกล่าวอาจอยู่ในมากกว่าหนึ่ง VPN ก็ได้หรือ VPN อาจทับกัน, ทุก site ไม่จำเป็นต้องอยู่ภายใต้ SP เดียวกัน, VPN อาจกระจายอยู่หลาย SP
การส่งข้อมูลที่เป็นเครือข่ายส่วนตัว (Private Network) จะมีการเข้ารหัสแพ็กเก็ตก่อนการส่ง เพื่อสร้างความปลอดภัยให้กับข้อมูล และส่งข้อมูลไปตามเส้นทางที่สร้างขึ้นเสมือนกับอุโมงค์ที่อยู่ภายในเครือข่ายสาธารณะ (Public Network) นั่นก็คือเครือข่าย อินเทอร์เน็ต นั่นเอง
เครือข่ายส่วนตัวเสมือนสามารถเชื่อมต่อเครือข่ายจากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่งได้ VPN จะช่วยให้คุณสามารถส่งข้อมูลระหว่างเครื่องคอมพิวเตอร์โดยผ่านระบบอินเทอร์เน็ต ทำให้ได้รับความสะดวกและรวดเร็วในการส่งข้อมูลในแต่ละครั้ง
เครือข่ายส่วนตัว (Private Network) เป็นระบบเครือข่ายที่จัดตั้งขึ้นไว้สำหรับหน่วยงานหรือองค์กรที่เป็นเจ้าของและมีการใช้ทรัพยากรร่วมกัน ซึ่งทรัพยากรและการสื่อสารต่างที่มีอยู่ในเครือข่ายจะมีไว้เฉพาะบุคคลในองค์กรเท่านั้นที่มีสิทธเข้ามาใช้
บุคคลภายนอกเครือข่ายไม่สามารถเข้ามาร่วมใช้งานบนเครือข่ายขององค์กรได้ ถึงแม้ว่าจะมีการเชื่อมโยงกันระหว่างสาขาขององค์กรและในเครือข่ายสาธารณะก็ตาม เพราะฉะนั้น ระบบเครือข่ายส่วนตัวจึงมีจุดเด่นในเรื่องของการรักษาความลับและเรื่องความปลอดภัย
ส่วนเครือข่ายสาธารณะ (Public Data Network) เป็นเครือข่ายที่รวมเอาเครือข่ายระบบต่างๆ ไว้ด้วยกันและสามารถแลกเปลี่ยนข้อมูลได้อย่างอิสระ เหมาะสำหรับบุคคลหรือองค์กรที่ไม่ต้องการวางเครือข่ายเอง โดยการไปเช่าช่องทางของเครือข่ายสาธารณะซึ่งองค์กรที่ได้รับสัมปทานจัดตั้งขึ้น สามารถใช้งานได้ทันทีและค่าใช้จ่ายต่ำกว่าการจัดตั้งระบบเครือข่ายส่วนตัว

เขียนโดย Administrator
วันพุธที่ 22 มีนาคม 2017 เวลา 23:38 น. - แก้ไขล่าสุด วันพฤหัสบดีที่ 23 มีนาคม 2017 เวลา 22:50 น.

ลักษณะการทำงาน

ลักษณะการทำงานของเครือข่ายส่วนตัวเสมือน (Virtual Private Network) เป็นเครือข่ายที่มีเส้นทางทำงานอยู่ในเครือข่ายสาธารณะ
ดังนั้นเรื่องความปลอดภัยของข้อมูลในเครือข่ายส่วนตัวจึงเป็นเรื่องที่ต้องคำนึงถึงเป็นอย่างมาก
เครือข่ายส่วนตัวเสมือนจะมีการส่งข้อมูลในรูปแบบแพ็กเก็ตออกมาที่เครือข่ายอินเทอร์เน็ต โดยมีการเข้ารหัสข้อมูล (Data Encryption)
ก่อนการส่งข้อมูลเพื่อสร้างความปลอดภัยให้กับข้อมูลและส่งข้อมูลผ่านอุโมงค์ (Tunneling) ซึ่งจะถูกสร้างขึ้นจากจุดต้นทางไปถึงปลายทางระหว่างผู้ให้บริการ VPN
กับผู้ใช้บริการการเข้ารหัสข้อมูลนี้เอง เป็นการไม่อณุญาตให้บุคคลอื่นที่ไม่เกี่ยวข้องกับข้อมูล สามารถอ่านข้อมูลได้จนสามารถที่จะส่งไปถึงปลายทาง
และมีเพียงผู้รับปลายทางเท่านั้นที่สามารถถอดรหัสข้อมูลและนำข้อมูลไปใช้ได้

การทำงานของระบบเครือข่ายส่วนตัว

Authentication VPN

เป็นการตรวจสอบและพิสูจน์เพื่อยืนยันผู้ใช้งาน หรือยืนยันข้อมูล ความมีสิทธิ์ในการเข้าถึงเพื่อใช้งานเครือข่าย ซึ่งเป็นระบบรักษาความปลอดภัยให้กับข้อมูล การ
Authentication เป็นขั้นตอนแรกในการทำงาน เมื่อมีการพิสูจน์เพื่อยืนยันผู้ใช้งานแล้ว จึงจะสามารถสร้างอุโมงค์หรือ Tunnel ได้
ถ้าหากว่าการยืนยันผิดพลาดก็ไม่สามารถที่จะสร้างอุโมงค์เพื่อเชื่อมโยงกันได้

Encryption

เป็นการเข้ารหัสข้อมูลซึ่งข้อมูลที่ส่งนั้นจะส่งไปเป็นแพ็กเก็ตและมีการเข้ารหัสข้อมูลก่อนการส่งเสมอทั้งนี้เพื่อรักษาความปลอดภัยให้กับข้อมูลและป้องกันการโจรกรรม
จากบุคคลนอกองค์กร เมื่อข้อมูลส่งถึงปลายทางอุปกรณ์ปลายทางจะทำการถอดรหัสข้อมูล ให้เป็นเหมือนเดิม เพื่อนำมาใช้งานต่อไป การเข้ารหัสมีอยู่ 2 แบบคือ แบบ
Symmetric-key encryption และ แบบPublic-key encryption

Tunneling

เป็นวิธีการสร้างอุโมงค์เพื่อเป็นช่องทางในการส่งข้อมูลระหว่างผู้ใช้กับองค์กรหรือระหว่างองค์กรทั้งสององค์กรที่มีการเชื่อมต่อกัน
ซึ่งผู้ที่จะเข้ามาใช้งานได้ต้องเป็นผู้ที่มีสิทธิ์เท่านั้น
เพราะฉะนั้นการสร้างอุโมงค์จึงเป็นการรักษาความปลอดภัยอย่างหนึ่งเนื่องจากเป็นการเชื่อมต่อเส้นทางบนเครือข่ายสาธารณะที่บุคคลอื่นมองไม่เห็น
การสร้างอุโมงค์เป็นหน้าที่ของอุปกรณ์เชื่อมต่อ

Firewall

หรือระบบรักษาความปลอดภัย มีหน้าที่ในการให้อนุญาตและไม่อนุญาตผู้ที่ต้องการเข้ามาใช้งานในระบบเครือข่าย

รูปแบบการให้บริการของ VPN

ตัวอย่างรูปแบบการให้บริการของ Intranet

ตัวอย่างรูปแบบการให้บริการของ Remote Access

Intranet VPN

เป็นรูปแบบของ VPN ที่ใช้เฉพาะภายในองค์กรเท่านั้น เช่น การเชื่อมต่อเครือข่ายระหว่างสำนักงานใหญ่กับสำนักงานย่อยในกรุงเทพและต่างจังหวัด
โดยเป็นการเชื่อมต่ออินเทอร์เน็ตผ่านผู้ให้บริการท้องถิ่นแล้วจึงเชื่อมต่อเข้ากับเครือข่ายส่วนตัวเสมือนขององค์กร จากเดิมที่ทำการเชื่อมต่อโดยใช้ Leased Line หรือ
Frame relay

Extranet VPN

มีรูปแบบการเชื่อมต่อที่คล้ายกับแบบ Intranet แต่มีการขยายวงออกไปยังกลุ่มต่างๆภายนอกองค์กร เช่น ซัพพลายเออร์ ลูกค้า เป็นต้น
การเชื่อมต่อแบบนี้ก็คือการเชื่อมต่อ LAN ต่าง LAN กันนั่นเอง

เขียนโดย Administrator
วันพุธที่ 22 มีนาคม 2017 เวลา 23:38 น. - แก้ไขล่าสุด วันพฤหัสบดีที่ 23 มีนาคม 2017 เวลา 22:50 น.

ปัญหาก็คือการรักษาความปลอดภัยให้กับข้อมูลเพราะฉะนั้นการเลือกผู้ให้บริการที่ดีจึงเป็นสิ่งที่สำคัญมากในการรักษาความปลอดภัยของข้อมูลเพราะถ้าผู้ให้บริการดีก็สามารถรักษาความปลอดภัยให้กับข้อมูลของผู้ใช้บริการได้อย่างดี

Remote Access VPN

เป็นรูปแบบการเข้าถึงเครือข่ายระยะไกลจากอุปกรณ์เคลื่อนที่ต่าง ๆ ซึ่งสามารถเข้าถึงเครือข่ายได้ใน 2 ลักษณะ ลักษณะแรก เป็นการเข้าถึงจากไคลเอ็นต์ทั่วไป ไคลเอ็นต์จะอาศัยผู้ให้บริการอินเทอร์เน็ตเป็นตัวกลางในการติดต่อและเข้ารหัสการส่งสัญญาณจากไคลเอ็นต์ไปยังเครื่องไอเอสพีและลักษณะที่สองเป็นการเข้าถึงจากเครื่องแอ็กเซสเซิร์ฟเวอร์ (Network Access Server-Nas)

รูปแบบการใช้งานของ VPN

Software-Based VPN

เป็นซอฟต์แวร์ที่ทำงานในลักษณะของไคลเอนต์และเซิร์ฟเวอร์
จะทำงานโดยการใช้ซอฟต์แวร์ทำหน้าที่สร้างอุโมงค์ข้อมูลและมีหน้าที่ในการเข้ารหัสและการถอดรหัสข้อมูลบนคอมพิวเตอร์
โดยจะมีการติดตั้งซอฟต์แวร์เข้าไปในเครื่องไคลเอนต์เพื่อเชื่อมต่อกับ เซิร์ฟเวอร์ที่ติดตั้งซอฟต์แวร์ VPN จากนั้นจึงสร้างอุโมงค์เชื่อมต่อขึ้น
ข้อดีคือสนับสนุนการทำงานบนระบบปฏิบัติการที่หลากหลาย ติดตั้งง่าย นำอุปกรณ์ที่มีอยู่เดิมมาประยุกต์ใช้ได้ ทำให้สามารถจัดการกับระบบได้ง่าย

Firewall-Based VPN

องค์กรส่วนใหญ่ที่เชื่อมต่อกับอินเทอร์เน็ตมีไฟร์วอลล์อยู่แล้วเพียงแค่เพิ่มซอฟต์แวร์ที่เกี่ยวกับการเข้ารหัสข้อมูลและซอฟต์แวร์ที่เกี่ยวข้องเข้าไปยังตัวไฟร์วอลล์ก็สามารถดำเนินงานได้ทันที Firewall-Based VPN มีส่วนคล้ายกับรูปแบบของซอฟต์แวร์และมีการเพิ่มประสิทธิภาพเข้าไปในไฟร์วอลล์
แต่ประสิทธิภาพก็ยังด้อยกว่าฮาร์ดแวร์ เป็นรูปแบบ VPN ที่นิยมใช้แพร่หลายมากที่สุด แต่ก็ไม่ได้เป็นรูปแบบที่ดีที่สุด
สนับสนุนการทำงานบนระบบปฏิบัติการที่หลากหลาย บางผลิตภัณฑ์สนับสนุน Load Balancing รวมทั้ง IPsec

Router-Based VPN

เป็นรูปแบบของ Hardware Base VPN มีอยู่ด้วยกัน 2 แบบ คือ แบบที่เพิ่มซอฟต์แวร์เข้าไปที่ตัว Router เพื่อเพิ่มการเข้ารหัสและถอดรหัสของข้อมูลที่จะวิ่งผ่าน Router เป็นการติดตั้งซอฟต์แวร์เข้าไปในชิบ แบบที่สองเป็นการเพิ่มการ์ดเข้าไปที่ตัวแท่นเครื่องของเราเตอร์ ข้อดีคือสามารถใช้เราเตอร์ของเราที่มีอยู่แล้วได้ ลดต้นทุนได้

Black Box-Based VPN

คือรูปแบบของฮาร์ดแวร์ VPN ที่มีลักษณะคล้ายกับเครื่องคอมพิวเตอร์ เป็นรูปแบบของ Hardware Base VPN อีกหนึ่งชนิด

ข้อดีและข้อเสียของการใช้งาน VPN

สถาปัตยกรรม	ข้อดี	ข้อเสีย
Software-Based VPN	สามารถนำอุปกรณ์เดิมมาประยุกต์ใช้กับเทคโนโลยี VPN ได้ ทำงานได้บนระบบปฏิบัติการที่หลากหลาย การติดตั้งง่าย ความสามารถในการเข้ารหัส (Encryption) และการทำ Tunneling ต่ำ	มีปัญหาคล้ายคลึงกับแบบ Software-Based VPN และอาจมีปัญหาเกี่ยวกับระบบความปลอดภัย
Firewall-Based VPN	สามารถใช้ได้กับอุปกรณ์ที่มีอยู่เดิมและทำงานได้บนระบบปฏิบัติการที่หลากหลายเช่นเดียวกับ Software-Based VPN	เพิ่มเทคโนโลยีของ VPN เข้าไปในอุปกรณ์ Router ที่มีอยู่ได้ทำให้ไม่จำเป็นต้องเปลี่ยน อุปกรณ์ ลดต้นทุน อาจมีปัญหาในเรื่องของประสิทธิภาพเนื่องจากมีความต้องการเพิ่มการ์ดอินเตอร์เฟส
Router-Based VPN		

เขียนโดย Administrator
วันพุธที่ 22 มีนาคม 2017 เวลา 23:38 น. - แก้ไขล่าสุด วันพฤหัสบดีที่ 23 มีนาคม 2017 เวลา 22:50 น.

ในบางผลิตภัณฑ์
Black Box-Based VPN ทำงานได้อย่างรวดเร็ว โดยจะ
สร้างอุโมงค์ได้หลายอุโมงค์ และ
มีการเข้ารหัสและถอดรหัสที่รวดเร็ว
การทำงานจำเป็นต้องใช้คอมพิวเตอร์
อีกเครื่อง เนื่องจาก Black Box ไม่
มีระบบบริหารจัดการโดยตรง
การทำ Tunnel
Tunneling คือการสร้างอุโมงค์เสมือนเพื่อส่งข้อมูลผ่านอุโมงค์นี้เพื่อออกสู่เน็ตเวิร์คมี 2 แบบ
Voluntary Tunneling
เป็นการทำงานของ VPN Client ซึ่งมีหน้าที่ในการติดต่อเข้าไปยัง ISP หลังจากนั้นจึงสร้าง Tunnel เชื่อมต่อไปยัง VPN Server โดยจะเป็นการติดต่อกันโดยตรง (live connection)
Compulsory Tunneling
การเชื่อมต่อ VPN ในวิธีนี้จะเป็นหน้าที่ของ ISP คือเมื่อมีผู้ใช้เชื่อมต่อเข้ามายัง ISP ISP ก็จะจะทำการตรวจสอบจนเสร็จ
จากนั้นก็จะทำการเชื่อมต่อเครื่องของผู้ใช้เข้ากับเครือข่าย VPN ของผู้ใช้
รูปแบบโพรโทคอลของการทำ Tunnel
PPTP
PPTP ย่อมาจาก Point - to - Point Tunneling Protocol เป็นโพรโทคอลที่ผลิตและ ติดมากับระบบปฏิบัติการของ Microsoft ซึ่งร่วมกับบริษัทอื่นๆ 3 บริษัท พัฒนาขึ้น PPTP เป็นส่วนต่อเติมของโพรโทคอล PPP ดังนั้นจึงสนับสนุนเฉพาะการเชื่อมต่อแบบPoint-To-Point แต่ไม่สนับสนุนการเชื่อมต่อแบบ Point-To-Multipoint PPTP มีข้อได้เปรียบตรงที่สนับสนุนทั้งไคลเอ็นต์ และทันแนลเซิร์ฟเวอร์และยังได้รับการพัฒนาเพื่อให้เพิ่มประสิทธิภาพในด้านต่างๆขึ้นมาอีก ข้อดีคือสามารถใช้ได้กับทุกระบบปฏิบัติการ ใช้งานผ่าน NAT ได้ สะดวกในการติดตั้ง
L2F
L2F ย่อมาจาก Layer 2 Forwarding protocolพัฒนาโดยบริษัท CISCO System เป็นโพรโทคอลที่ทำงานบนเลเยอร์ที่ 2 โดยใช้พวกเฟรมรีเลย์หรือ ATM รวมถึง X.25 ในการทำทันแนล PPTP สามารถใช้เป็นแบบ client-initiated (ซึ่งทรานส์พาเรนต์สำหรับ ISP) หรือใช้เป็นแบบ client-transparent ก็ได้ L2F ต้องการการสนับสนุนในแอคเซสเซิร์ฟเวอร์และในเราท์เตอร์ ระบบการป้องกันของ L2F มีการจัดเตรียมบางอย่างที่ PPTP ไม่มีเช่นการ Authentication ของปลายทั้ง 2 ข้างของทันแนล
L2TP
L2TP ย่อมาจาก Layer 2 Tunneling Protocol การทำงานคล้ายๆกับ PPTP ต่างกันตรง L2TP จะใช้ User Datagram Protocol (UDP) ในการตกลงรายละเอียดในการรับส่งข้อมูลและสร้าง Tunnel ซึ่งเป็นการนำเอาข้อดีของทั้งสองโพรโทคอลมารวมไว้ด้วยกัน โดยนำโพรโทคอลในระดับ Layer 2 หรือ PPP มาหุ้มแพ็กเก็ตใน Layer 3 ก่อนที่จะหุ้มด้วย IP Packet อีกชั้น ดังนั้นจึงใช้วิธีพิสูจน์แบบ PPP L2TP ยังสนับสนุนการทำ Tunnel พร้อมกันหลายๆ อันบนไคลเอ็นต์เพียงตัวเดียว
IPSec
IPSec หรือ IP Security เป็นการรวม Protocol หลายๆอันมาไว้ด้วยกัน ประกอบด้วยการรักษาความปลอดภัยในการเข้ารหัส การตรวจสอบตัวตนและความถูกต้องของข้อมูล โดยมีการเข้ารหัส 2 แบบด้วยกัน คือ การเข้ารหัสเฉพาะส่วนของข้อมูลจะไม่มีการเข้ารหัส Header เรียกว่า Transport mode และวิธีที่ 2 คือ การเข้ารหัสทั้งส่วนของข้อมูลและ Header เรียกว่า Tunnel mode ซึ่งวิธีนี้จะทำให้ข้อมูลมีความปลอดภัยขึ้น
OPEN VPN
OPENVPN พัฒนาจาก SSL หรือ HTTPS ซึ่ง มีความปลอดภัยสูงมาก มีต้นกำเนิดมาจากระบบ LINUX ทำให้การใช้งาน จะต้องมี SERVER เป็น LINUX เข้ามาร่วมด้วย ในปัจจุบัน ADSL ROUTER สามารถ เปลี่ยน FIRMWARE เป็น LINUX แบบ OPEN SOURCE ได้เช่น DD-WRT (ADSL ROUTER ที่ขายทั่วไปใช้ LINUX แต่ ไม่ OPEN SOURCE) ทำให้สามารถใช้งาน OPEN VPN ได้ ง่ายๆ ไม่ต้องมี SERVER LINUX ความปลอดภัยที่มากขึ้น มาจากการ GEN CODE ของ KEY CA ขึ้นมา เพื่อใช้ในการ ตรวจสอบตัวตน และ มีการแก้ไข ปรับปรุงจาก VPN แบบ PPTP หรือ IPSEC เช่นการกำหนด PORT เปลี่ยนแปลง ได้โดยง่าย หรือ สามารถใช้งาน หลายๆ PORT ได้พร้อมๆ กัน ทำให้ OPEN VPN มีทั้งความปลอดภัย ความสะดวกในการติดตั้ง ปรับปรุง แต่ เพราะมีระบบ LINUX ทำให้ ผู้ใช้ (คนไทย) ยังกลัว ๆ กันอยู่
ข้อดีและข้อเสียของระบบ VPN
ข้อดีของระบบ VPN
สามารถขยายการเชื่อมต่อเครือข่ายได้แม้ว่าเครือข่ายนั้นจะอยู่สถานที่ต่างกัน
มีความยืดหยุ่นสูงเพราะสามารถใช้ VPN ที่ใดก็ได้ และยังสามารถขยาย Bandwidth ในการใช้งานได้ง่ายดาย โดยเฉพาะในการทำ Remote Access

เขียนโดย Administrator
วันพุธที่ 22 มีนาคม 2017 เวลา 23:38 น. - แก้ไขล่าสุด วันพฤหัสบดีที่ 23 มีนาคม 2017 เวลา 22:50 น.

ให้ผู้ใช้ติดต่อเข้ามาใช้งานเครือข่ายได้จากสถานที่อื่น
สามารถเชื่อมโยงเครือข่ายและแลกเปลี่ยนข้อมูลออกภายนอกองค์กรได้อย่างปลอดภัย โดยใช้มาตรการระบบเปิดและมีการเข้ารหัสข้อมูลก่อนการส่งข้อมูลทุกครั้ง
สามารถลดค่าใช้จ่ายในการเชื่อมต่อ ง่ายต่อการดูแลรักษาการใช้งานและการเชื่อมต่อ
ข้อเสียของระบบ VPN
ไม่สามารถที่จะควบคุมความเร็ว การเข้าถึงและคุณภาพของ VPN ได้ เนื่องจากVPN ทำงานอยู่บนเครือข่ายอินเทอร์เน็ตซึ่งเป็นเรื่องที่อยู่เหนือการควบคุมของผู้ดูแล
VPN ยังถือว่าเป็นเทคโนโลยีที่ค่อนข้างใหม่สำหรับประเทศไทยและมีความหลากหลายต่างกันตามผู้ผลิตแต่ละราย
ฉะนั้นจึงยังไม่มีมาตรฐานที่สามารถใช้ร่วมกันได้แพร่หลาย
VPN บางประเภทต้องอาศัยความสามารถของอุปกรณ์เสริมเพื่อช่วยในการเข้ารหัส และต้องมีการอัพเกรดประสิทธิภาพ

แลนเสมือน (อังกฤษ: virtual LAN) เหมือนการสร้าง logical segment สวิสต์ตัวหนึ่งสามารถแบ่งออกมาเป็นหลายๆ vlanได้
เหมือนมีswitchหลายตัวหรือมีhubหลายตัว แต่จริงๆมีแค่ตัวเดียวแล้วก็แบ่งซอยออกมา โดยมากแบ่งตามพื้นที่ใช้งาน แบ่งตามแผนก แบ่งตามหน่วยงาน
แบ่งตามลักษณะการใช้งาน การจำลองสร้างเครือข่าย LAN แต่ไม่ขึ้นอยู่กับการต่อทางกายภาพเช่น สวิตช์หนึ่งตัวสามารถใช้จำลองเครือข่าย LAN ได้สิบเครือข่าย
หรือสามารถใช้สวิตช์สามตัวจำลองเครือข่าย LAN เพียงหนึ่งเครือข่าย เป็นต้น การแบ่งกลุ่มของสวิตช์ภายในเลเยอร์ 2 ที่ไม่ขึ้นกับ ลักษณะทางกายภาพใดๆ
กล่าวแบบง่ายๆ ก็คือ เราไม่จำเป็นที่จะต้องนำสวิตช์มาต่อกันเป็น ทอดๆ เพื่อจัดกลุ่มของสวิตช์ว่า สวิตช์กลุ่มนี้คือ กลุ่มเดียวกัน แต่ เราสามารถที่จะ จัดกลุ่มให้
สวิตช์ที่อยู่ห่างไกลกันออกไปนั้น เป็นสมาชิกของสวิตช์อีกกลุ่มหนึ่งทางแนวตรรกะ

1 Broadcast domain
2 ชนิดของ VLAN
2.1 Static
2.2 Dynamic
3 Trunk Port
4 ข้อดีและข้อเสียของการทำ VLAN
4.1 ข้อดีของการทำ VLAN
4.2 ข้อเสียของการทำvlan
5 communication ระหว่างvlan
6 มาตรฐานของVLAN
7 แหล่งข้อมูลอื่น

Broadcast domain
กลุ่มของพอร์ตหรือuserที่อยู่ในBroadcast Domainเดียวกัน ส่วน broadcast domain นั้นจะเกี่ยวข้องกับการทำงานของ switch เป็นหลัก คือว่าโดยปกติแล้ว
switch นั้นจะทำหน้าที่ตัดสินใจเลือกพอร์ตปลายทางให้กับ frame ที่รับเข้ามาว่าจะส่งออกไปทาง port ไหน โดยที่พิจารณาจาก switch table แต่หาก switch
table ไม่มีข้อมูลที่เกี่ยวข้องกับ frame นั้นเลย switch จะส่ง frame นั้นออกไปยังทุก port ที่มีการเชื่อมต่อกับ switch วิธีการดังกล่าวเรียกว่า การ broadcast
ซึ่งสิ่งนี้เป็นที่มาของคำว่า broadcast domain ที่หมายความว่าเป็นขอบเขตที่ switch จะสามารถส่ง frame ไปได้ ซึ่งอุปกรณ์ที่จำกัดขอบเขตของ broadcast
domain คือ router
ตัวอย่างรูปการBroadcast Domain
ชนิดของ VLAN
โดยค่าดีฟอล์ท (Default) ทุกๆ พอร์ทของสวิตช์นั้น จะถูกจัดให้อยู่ใน VLAN 1 หรือ ที่เรียกกันว่า “Management VLAN” ซึ่ง ในการสร้าง-แก้ไข-ลบ VLAN นั้น
เราจะไม่สามารถลบ VLAN 1 นี้ได้ และ หมายเลข VLAN นี้ สามารถสร้างได้ตั้งแต่หมายเลข 1 – 1005
Static
สแตติก VLAN หรือ อีกชื่อหนึ่งคือ Port-Based Membership นั้น จะเป็นการพิจารณาความเป็นสมาชิกของ VLAN หนึ่งๆ โดยดูจากพอร์ท
ซึ่งพอร์ทของสวิตช์ที่เชื่อมต่ออยู่กับ Client นั้น ถึงแม้ว่าจะเป็น พอร์ทของสวิตช์เดียวกัน แต่หากพอร์ททั้งสองนั้นอยู่คนละ VLAN กัน ก็ไม่สามารถที่จะติดต่อกันได้
หากไม่มีอุปกรณ์ในเลเยอร์ 3 มาช่วยในการเราท์ทราฟฟิก ซึ่ง การเซตพอร์ทแต่ละพอร์ทให้เป็นสมาชิกของ VLAN ใดๆ นั้น จะถูกกระทำแบบ Manual จาก System
Administrator
ตัวอย่างรูปการคอนฟิกแบบ Dynamic
Dynamic
ไดนามิค VLAN เป็นการกำหนด VLAN ให้กับเครื่องClient โดยพิจารณาจากหมายเลข MAC Address ของ Client ซึ่งเมื่อ Client ทำการเชื่อมต่อไปยังสวิตช์ตัวใดๆ
สวิตช์ที่รัน Dynamic VLAN นี้ก็จะไปหาหมายเลข VLAN ที่ MAP กับ MAC Address นี้จาก Database ส่วนกลางมาให้ ซึ่ง System Administrator
สามารถที่จะเซตหมายเลข MAC Address ในการจับคู่กับ VLAN ได้ที่ VLAN Management Policy Server (VMPS)
Trunk Port

เขียนโดย Administrator
วันพุธที่ 22 มีนาคม 2017 เวลา 23:38 น. - แก้ไขล่าสุด วันพฤหัสบดีที่ 23 มีนาคม 2017 เวลา 22:50 น.

เป็นพอร์ททำหน้าที่เชื่อมต่อ Switch ตัวอื่น ๆ ที่ต้องการให้เป็นสมาชิกของ VLAN ต่าง ๆ กันให้มาอยู่ด้วยกัน และ ทำหน้าที่ส่งผ่านข้อมูล Traffic ของ หลาย ๆ VLAN ให้กระจายไปยัง Switch ตัวอื่น ๆ ที่มีพอร์ทที่ถูกกำหนดให้เป็น VLAN เดียวกันกับ Switch ตัวต้นทางได้ หรือที่เรียกกันโดยทั่วไปว่า Uplink Port ซึ่ง
ตัวอย่างในการเซตพอร์ทให้เป็น Trunk Port นี้ ก็คือ
- พอร์ทที่ทำหน้าที่คอนเนคไปยังสวิตช์ตัวอื่นๆ เช่น Uplink Port
- พอร์ทที่ทำหน้าที่เชื่อมไปยัง เราเตอร์ตัวที่ทำหน้า เราท์ทราฟฟิกระหว่าง VLAN
ตัวอย่างรูป Multiple switch VLAN
ข้อดีและข้อเสียของการทำ VLAN
ข้อดีของการทำ VLAN
1.เพิ่มประสิทธิภาพของเครือข่าย จำกัดการแพร่กระจายของbroadcastทราฟฟิคไม่ให้ส่งผลกระทบต่อประสิทธิภาพโดยรวมของเน็ตเวิร์ก
2.ง่ายต่อการใช้งาน ผู้ใช้งานสามารถที่จะเคลื่อนย้ายไปยัง VLAN (Subnet) อื่นๆ ได้โดยเพียงแค่การเปลี่ยนคอนฟิกของสวิตช์และ IP Address ของ Client เพียงนิดเดียว ไม่จำเป็นต้องมีการย้ายสวิตช์ หรือสายเคเบิลใดๆ
3.เพิ่มเครื่องง่าย สามารถรองรับการขยายตัวของระบบเน็ตเวิร์กที่จะเพิ่มขึ้นในอนาคตได้ง่าย เนื่องจากมีการวางแผนเกี่ยวกับการทำซับเน็ต และการดีไซน์ระบบที่ไม่ยึดติดกับทางกายภาพอีกต่อไป
4.เพิ่มเรื่องของความปลอดภัย สามารถสร้างกลไกด้านความปลอดภัยได้ง่ายขึ้น เช่น การสร้าง Access Control List บนอุปกรณ์เลเยอร์ 3 และ ลดความเสี่ยงเกี่ยวกับการดักจับข้อมูล (Sniffing)
ข้อเสียของการทำvlan
1. ถ้าเป็นการแบ่ง VLAN แบบ port-based นั้นจะมีข้อเสียเมื่อมีการเปลี่ยนพอร์ตนั้นอาจจะต้องทำการคอนฟิก VLAN ใหม่
2. ถ้าเป็นการแบ่ง VLAN แบบ MAC-based นั้นจะต้องให้ค่าเริ่มต้นของ VLAN membership ก่อน และปัญหาที่เกิดขึ้นคือในระบบเครือข่ายที่ใหญ่มาก จำนวนเครื่องนับพันเครื่อง นอกจากนี้ถ้ามีการใช้เครื่อง Notebook ด้วย ซึ่งก็จะมีค่า MAC และเมื่อทำการเปลี่ยนพอร์ตที่ต่อก็ต้องทำการคอนฟิก VLAN ใหม่
communication ระหว่างvlan
ตัวอย่างการMap logical เป็น physical
vlanก็คือlanวงหนึ่ง lan2 ตัวจะคุยกันตรงๆไม่ได้ต้องผ่าน router และ router ทำหน้าที่ routing subnet จาก lan วงหนึ่งไปอีก subnet vlan สร้างขึ้นมา vlan2,3,4,5 จะคุยกันไม่ได้ต้องผ่าน router โดยมีวิธีแก้ มี vlan เชื่อมต่อไปที่ไปที่ router มี vlan1 เป็น vlan2 มาเชื่อมกับ router มีกี่ vlan ก็ต้องมี link ไปที่ router ถ้าทำแบบนี้มันจะราคาแพง แต่วิธีนี้ไม่ดี router ทำงานหนัก เราต้องทำแบบ logical link เรามี physical link ให้มันอันเดียว แล้วเราสร้างเป็น logical link ยุบรวมให้เหลือเส้นเดียวให้วิ่งหลายๆ vlan ในเส้นเดียวเราเรียกแบบนี้ Trunking โดยใช้software เข้ามาควบคุม การเอา layer3
เข้ามาให้มันมีการเพิ่มความปลอดภัยของการ management
มาตรฐานของVLAN[แก้]
มาตรฐาน IEEE 802.1Q นั้นเป็นมาตรฐานในการนำข้อมูลของ VLAN membership ใส่เข้าไปใน Ethernet Frame หรือที่เรียกว่า การ Tagging และโพรโทคอล 802.1Q นี้ถูกพัฒนาเพื่อแก้ปัญหาเรื่องการบริหารจัดการด้านเครือข่ายที่เพิ่มขึ้น เช่น การกระจายเครือข่ายใหญ่ๆ ให้เป็นส่วนย่อยๆ (Segment) ทำให้ไม่สูญเสียแบนวิธให้กับการ broadcast และ multicast มากเกินไป และยังเป็นการรักษาความปลอดภัยระหว่างส่วนย่อยต่างๆ ภายในเครือข่ายให้สูงขึ้นอีกด้วย การต่อเติมเฟรม (tagging Frame) ด้วยมาตรฐาน 802.1Q นั้นจะทำในระดับ Data-Link layer และการทำ VLAN Tagging นั้นจะเป็นการเปลี่ยนรูปแบบของ Ethernet Frame มาตรฐาน 802.3 ให้เป็นรูปแบบใหม่ที่เป็นมาตรฐาน 802.3 ac