www.ez-admin.com

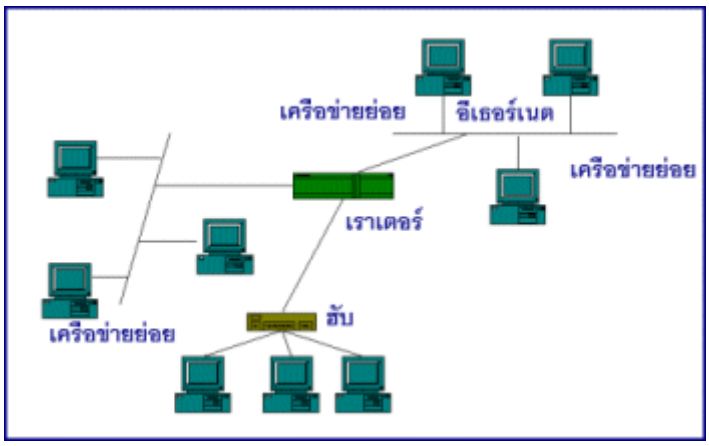
ศูนย์อบรมสำหรับผู้ต้องการก้าวสู่อาชีพผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ โดยเรียนรู้จากการปฏิบัติงานจริง

"เราจะทำเรื่องยากให้เข้าใจง่ายด้วยสิ่งเหล่านี้"

- บทความเจาะลึกด้านระบบเครือข่ายคอมพิวเตอร์
- เว็บบอร์ดถามตอบปัญหา
- คู่มือทางด้านระบบเครือข่ายคอมพิวเตอร์และ **Hacking**
- หลักสูตรอบรมที่เน้นการเรียนรู้จากการปฏิบัติงานจริงโดยผู้เชี่ยวชาญในราคาไม่แพง

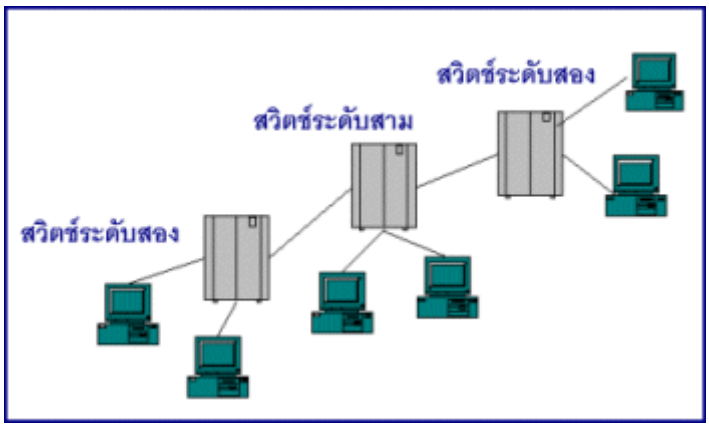
VLAN เทคโนโลยีที่ใช้ในการจำลองสร้างเครือข่าย LAN

ก่อนอื่นเราต้องมาทำความเข้าใจความหมายของ VLAN ก่อน VLAN ย่อมาจาก Virtual LAN เป็นเทคโนโลยีที่ใช้ในการจำลองสร้างเครือข่าย LAN แต่ไม่ขึ้นอยู่กับการต่อทางกายภาพเช่น สวิตช์หนึ่งตัว (Switch) สามารถใช้จำลองเครือข่าย LAN ได้ห้าเครือข่าย หรือสามารถใช้สวิตช์สามตัวจำลองเครือข่าย LAN เพียงหนึ่งเครือข่าย

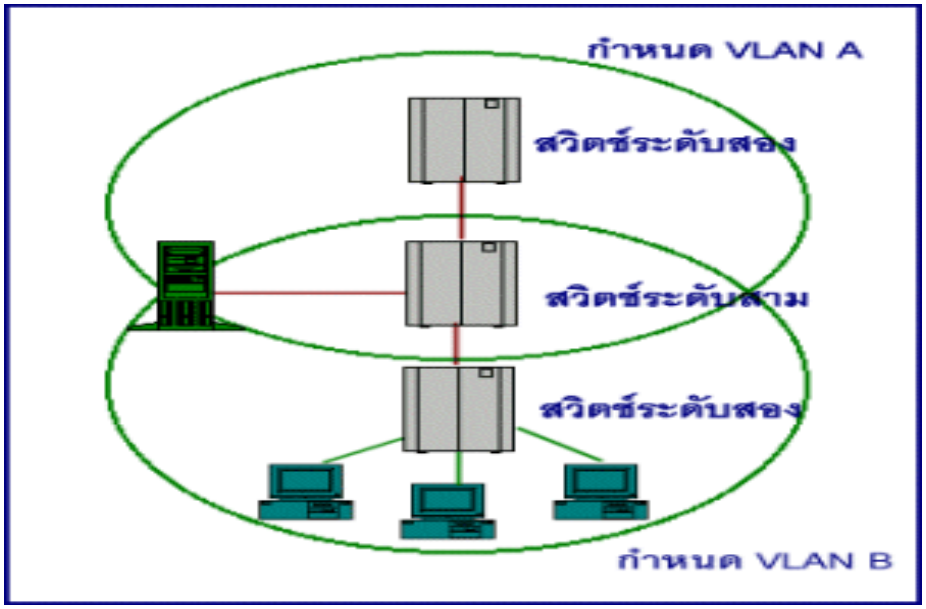


เครือข่ายย่อยที่แบ่งแยกกันด้วยเราเตอร์

การสร้าง LAN ในเครือข่ายสวิตชิ่งหรือเอทีเอ็ม เพื่อทำให้กลุ่มของคอมพิวเตอร์และอุปกรณ์สามารถเชื่อมโยงกันเป็นกลุ่มแบบ Logical โดยมีสถานภาพการทำงานเหมือน LAN คือ ในกลุ่ม VLAN เดียวกันสามารถกระจายข่าวสารระหว่างกัน สถานะการทำงานโดยรวมจะทำให้เหมือนหรือคล้ายสถานะ LAN ที่ใช้ในการเชื่อมโยงแบบเราเตอร์เดิม



การใช้สวิตช์ในเครือข่าย



การกำหนด VLAN ในเครือข่าย ATM

จะเห็นได้ว่า VLAN ก็คือการสร้างเครือข่ายสวิตช์ให้แบ่งแยกเป็นเครือข่ายย่อยตามสถานะการทำงาน โดยกำหนดให้เป็นเสมือนแลนที่ต่อกันเป็นกลุ่ม ๆ ดังที่เคยเป็นในระบบที่ใช้เราเตอร์
การกำหนดกลุ่ม VLAN แต่ละกลุ่ม ก็เพื่อให้สถานะการทำงานเหมือนเป็นกลุ่มเครือข่ายย่อยหนึ่งเครือข่าย และหากต้องการส่งข้อมูลข้ามเครือข่าย VLAN ก็จะทำได้เสมือนการมีฟังก์ชันของการกำหนดเส้นทาง เช่น จากรูปที่ 3 เราได้ทำการกำหนด VLAN สองเครือข่ายคือ VLAN A และ VLAN B

สังเกตว่าอุปกรณ์บางตัวเรากำหนดคาบเกี่ยวกันได้ คือให้เป็นทั้งเครือข่าย A และ B หากมีการส่งข้อมูลข้าม VLAN อุปกรณ์สวิตชิ่งจะดำเนินการให้เหมือนสถานะคล้ายเราเตอร์ คือให้ข้อมูลข้าม VLAN กันได้ ในการสร้าง VLAN โดยใช้อุปกรณ์เครือข่ายหลายตัว จะมีพอร์ตที่ทำหน้าที่เชื่อมต่อระหว่างอุปกรณ์เครือข่ายแต่ละตัว เรียก Trunk port ซึ่งเสมือนมีท่อเชื่อม หรือ Trunk เป็นตัวเชื่อมด้วย เนื่องจาก VLAN เป็น LAN แบบจำลอง ถึงแม้ว่าจะต่อทางกายภาพอยู่บนอุปกรณ์เครือข่ายตัวเดียวกัน แต่การติดต่อกันนั้นจำเป็นต้องใช้อุปกรณ์ที่มีความสามารถในการค้นหาเส้นทาง เช่น เราเตอร์ หรือสวิตช์เลเยอร์สาม

ลักษณะพิเศษของ VLAN ทั่วๆ ไปคือ

1. VLAN แต่ละเครือข่ายที่ติดต่อกันนั้น จะมีลักษณะเหมือนกับต่อแยกกันด้วยบริดจ์
2. VLAN สามารถต่อข้ามสวิตช์หลายตัวได้
3. ท่อเชื่อม (Trunks) ต่างๆ จะรองรับทราฟฟิกที่คับคั่งของแต่ละ VLAN ได้

ชนิดของ VLAN

1. Layer 1 VLAN : Membership by ports

ในการแบ่ง VLAN จะใช้พอร์ตบอกว่าเป็นของ VLAN ใด เช่นสมมุติว่าในสวิตช์ที่มี 4 พอร์ต กำหนดให้ พอร์ต 1, 2 และ 4 เป็นของ VLAN เบอร์ 1 และพอร์ตที่ 3 เป็นของ VLAN เบอร์ 2 ดังรูปที่ 1

Port	VLAN
1	1
2	1
3	2
4	1

การกำหนดพอร์ตให้กับ VLAN

2. Layer 2 VLAN : Membership by MAC Address

ใช้ MAC Address ในการแบ่ง VLAN โดยให้สวิตช์ตรวจหา MAC Address จากแต่ละ VLAN ดูรูปที่ 2

MAC Address	VLAN
1212354145121	1
2389234873743	2
3045834758445	2
5483573475843	1

การกำหนด MAC Address ให้กับ VLAN ต่างๆ

3. Layer 2 VLAN : Membership by Protocol types

แบ่ง VLAN โดยใช้ชนิดของ protocol ที่ปรากฏอยู่ในส่วนของ Layer 2 Header ดูรูปที่ 3

Protocol	VLAN
IP	1
IPX	2

การแบ่ง VLAN โดยใช้ชนิดของ Protocol กำหนด

4. Layer 3 VLAN : Membership by IP subnet Address

แบ่ง VLAN โดยใช้ Layer 3 Header นั่นก็คือใช้ IP Subnet เป็นตัวแบ่ง

IP Subnet	VLAN
23.2.24	1
26.21.35	2

การแบ่ง VLAN โดยใช้ IP Subnet

5. Higher Layer VLAN's

VLAN ทำได้โดยใช้โปรแกรมประยุกต์หรือ service แบ่ง VLAN เช่นการใช้โปรแกรม FTP สามารถใช้ได้ใน VLAN 1 เท่านั้น และถ้าจะใช้ Telnet สามารถเรียกใช้ได้ใน VLAN 2 เท่านั้น เป็นต้น

ข้อดีของ VLAN

1. เพิ่มประสิทธิภาพของเครือข่าย

ในระบบเครือข่ายทั่วไปจะมีการส่งข้อมูล Broadcast จำนวนมาก ทำให้เกิดความคับคั่ง (Congestion) และ VLAN มีความสามารถช่วยเพิ่มประสิทธิภาพของเครือข่ายได้เนื่องจาก VLAN จะจำกัดให้ส่งข้อมูล Broadcast ไปยังผู้ที่อยู่ใน VLAN เดียวกันเท่านั้น

2. ง่ายต่อการบริหารการใช้งาน

VLAN อำนวยความสะดวกในการบริหารจัดการโครงสร้างของระบบเครือข่ายให้ง่าย มีความยืดหยุ่น และเสียค่าใช้จ่ายน้อย โดยเพียงเปลี่ยนโครงสร้างทางตรรกะ (Logical) เท่านั้น ไม่จำเป็นต้องเปลี่ยนโครงสร้างทางกายภาพ กล่าวคือ ถ้าต้องการเปลี่ยนโครงสร้างของ VLAN ก็ทำโดยการคอนฟิกที่อุปกรณ์เครือข่ายใหม่ ไม่จำเป็นเปลี่ยนรูปแบบทางกายภาพของการเชื่อมต่อเครือข่ายที่มีอยู่เดิม

3. เพิ่มการรักษาความปลอดภัยมากขึ้น

เนื่องจากการติดต่อระหว่างอุปกรณ์เครือข่ายจะสามารถทำได้ภายใน VLAN เดียวกันเท่านั้น ถ้าต้องการที่จะติดต่อข้าม VLAN ต้องติดต่อผ่านอุปกรณ์ค้นหาเส้นทางหรือสวิตช์เลเยอร์สาม

ข้อเสียและปัญหาที่พบของการใช้ VLAN

1. ถ้าเป็นการแบ่ง VLAN แบบ Port-Based นั้นจะมีข้อเสียเมื่อมีการเปลี่ยนพอร์ตนั้นอาจจะต้องทำการคอนฟิก VLAN ใหม่

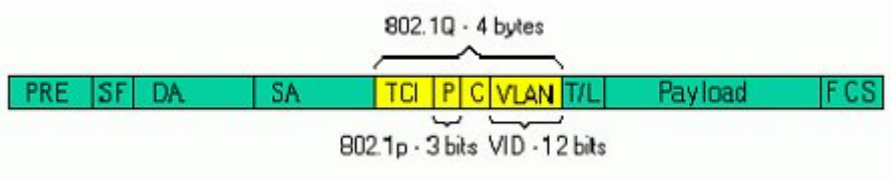
2. ถ้าเป็นการแบ่ง VLAN แบบ MAC-based นั้นจะต้องให้ค่าเริ่มต้นของ VLAN membership ก่อน และปัญหาที่เกิดขึ้นคือในระบบเครือข่ายที่ใหญ่มาก จำนวนเครื่องนับพันเครื่อง นอกจากนี้ถ้ามีการใช้เครื่อง Notebook ด้วย ซึ่งก็จะมีค่า MAC และเมื่อทำการเปลี่ยนพอร์ตที่ต่อก็ต้องทำการคอนฟิก VLAN ใหม่

มาตรฐานของ VlLAN คือ 802.1Q นั้นมีลักษณะอย่างไร

มาตรฐาน IEEE 802.1Q นั้นเป็นมาตรฐานในการนำข้อมูลของ VLAN membership ใส่เข้าไปใน Ethernet Frame หรือที่เรียกว่า การ Tagging และโปรโตคอล 802.1Q นี้ถูกพัฒนาเพื่อแก้ปัญหาเรื่องการบริหารจัดการด้าน

เครือข่ายที่เพิ่มขึ้น 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 ซึ่งมีไดอะแกรมของเฟรมมาตรฐาน 802.3 ดังรูปด้านล่าง และไดอะแกรมของมาตรฐาน 802.3 ac ดังรูปสุดท้าย (ส่วนสีเหลืองแทนส่วนของ tag 802.1Q)



รูปแบบของเฟรม 802.3 ก่อนที่จะทำ VLAN Tagging และหลังจากที่มีการ tagging 802.1Q แล้ว

Label	Field Name	Size	Description
PRE	Preamble	7 bytes	Used to synchronize traffic between nodes
SF	Start Frame Delimiter	1 bytes	Marks the beginning of the header
DA	Destination Address	6 bytes	The MAC address of the next/final hop
SA	Source Address	6 bytes	The MAC address of the source
TCI	Tag Control Info	2 bytes	When set to '8100', indicates this frame uses 802.1p and Q tags
P	Priority	3 bits	Indicates 802.1p priority level 0-7
C	Canonical Indicator	1 bit	Indicates if the MAC addresses are in canonical format – Ethernet uses "0"
VLAN	VLAN Identifier (VID)	12 bits	Indicates which VLAN this frame belongs to (0-4095)
T/L	Type/Length Field	2 bytes	Ethernet II "type" or 802.3 "length" information
Payload	Payload	≤1500 bytes	User data or higher layer protocol information
FCS	Frame Check Sequence	4 bytes	Error checking on the frame's contents – also known as "CRC" (Cyclical Redundancy Check)

ตารางของคำอธิบายส่วนต่างๆ ของมาตรฐาน 802.3

สถาปัตยกรรมเครือข่ายที่ใช้สวิตช์และใช้ VLAN

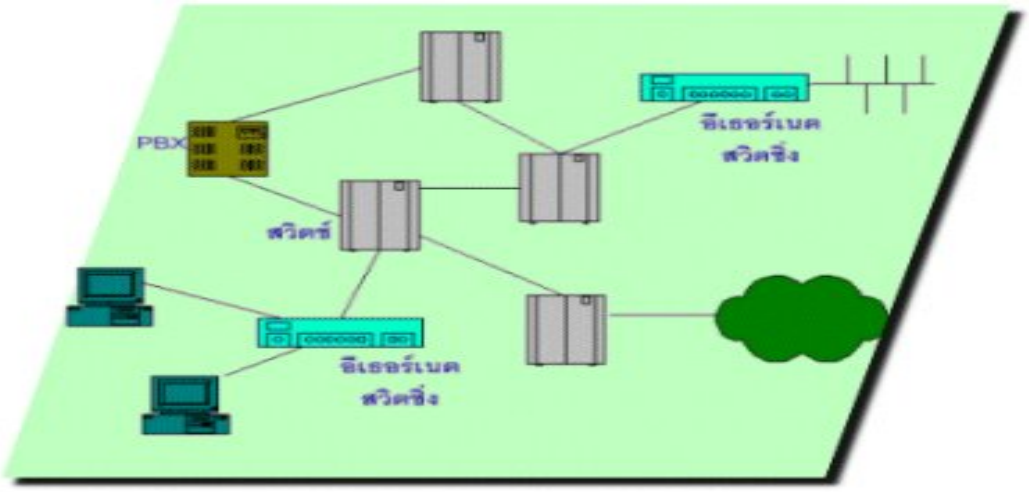
การทำงานของระบบเครือข่ายจะประสบผลสำเร็จได้ด้วยซอฟต์แวร์ที่ใช้ในการจัดการ การที่สวิตช์ทั้งการแยกแพคเกจข้อมูลได้เร็ว มิได้หมายความว่าสวิช์จะประสบผลสำเร็จได้ เพราะการสวิตช์อย่างเดียวไม่เพียงพอ จำเป็นต้องมีการควบคุมการสวิตช์ เพื่อส่งผ่านข้อมูลให้ถูกช่องทาง การดำเนินการในระดับช่วยจัดการจึงอยู่ที่ซอฟต์แวร์จัดการในระดับที่อยู่เหนือจากสวิตช์ขึ้นไป ซอฟต์แวร์จัดการเหล่านี้ทำให้สามารถเชื่อมโยงเครือข่ายเสมือนแลนได้ (VLAN) ช่วยในการปรับเปลี่ยนโครงสร้างเครือข่ายตามความต้องการ

ช่วยให้มีการแบ่งแถบกว้างสัญญาณแต่ละช่องตามความต้องการอย่างเหมาะสม และสนองความต้องการ รวมถึงการจัดการเรื่องความปลอดภัยของข้อมูล และทำให้ลดข้อยุ่งยากในการจัดการเครือข่าย

โครงสร้างการทำงานของเครือข่าย

โครงสร้างการจัดการเหล่านี้จึงต้องเป็นไปตามโครงสร้างระบบการแบ่งชั้นของเครือข่ายตามมาตรฐาน OSI

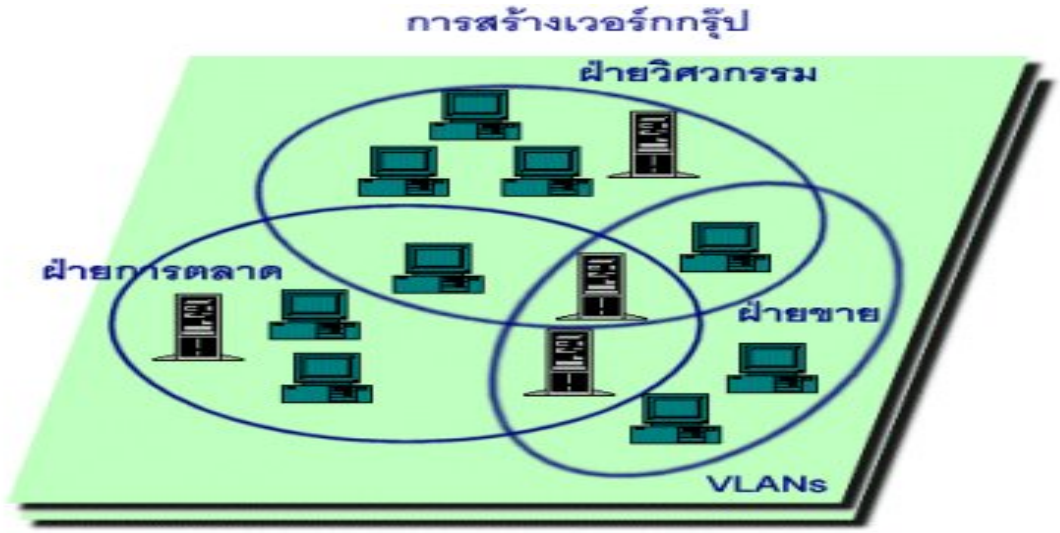
- โครงสร้างสวิตช์เริ่มจากระดับชั้นแรก เป็นวิธีการเชื่อมต่อและการสวิตช์แพคเกจที่เป็นแพคเกจขนาดเล็ก
- ระดับที่สองเป็นระดับซอฟต์แวร์ที่ดำเนินการจัดการกระทำเครือข่ายแลนแบบเสมือนที่เรียกว่า VLAN ชั้นนี้จึงเป็นชั้นสำคัญที่ทำให้เครือข่ายมีลักษณะเหมือนแลน และใช้งานได้เหมือนใช้แลน นอกจากนี้ยังทำให้เครือข่ายเชื่อมโยงกับเราเตอร์แบบเดิม เพื่อเชื่อมต่อในระดับที่ 3 ต่อไป
- ระดับสามเป็นระดับเครือข่าย เป็นระดับที่เชื่อมโยงระหว่าง VLAN กับ VLAN หรือ LAN อื่น ระดับนี้จึงใช้ซอฟต์แวร์ทำหน้าที่กำหนดเส้นทาง ฟังก์ชันการทำงานจึงเหมือนกับเครือข่ายแลนที่เชื่อมโยงกันด้วยเราเตอร์



การเชื่อมโยงระหว่างอุปกรณ์ต่าง ๆ

เมื่อสร้าง VLAN ในระดับที่สองจะมีการจัดกลุ่มเครือข่ายเข้าด้วยกัน โดยแต่ละกลุ่มทำหน้าที่เหมือนเป็นแลนหนึ่งเครือข่าย สังเกตว่าอุปกรณ์บางตัวอยู่ในเครือข่ายย่อย VLAN ได้หลายเครือข่าย หากพิจารณาเครือข่าย VLAN ตามรูปแบบ TCP/IP นั่นหมายความว่า แต่ละอุปกรณ์มีตำแหน่งแอดเดรสของตนเอง

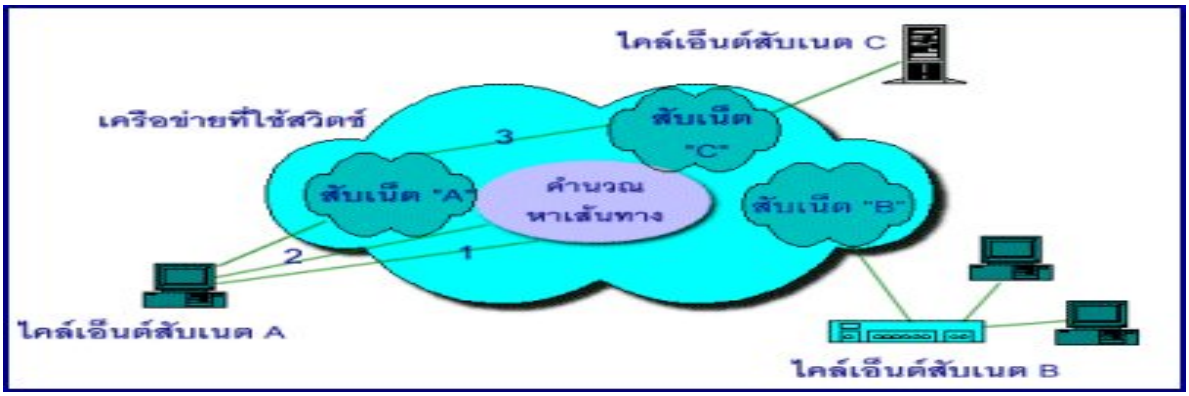
ระบบซอฟต์แวร์จะทำการกำหนดตำแหน่งต่าง ๆ ของอุปกรณ์เข้าเป็นเครือข่าย VLAN สามารถปรับเปลี่ยนและดูแลเครือข่ายโดยรวมได้ VLAN จึงเป็นซอฟต์แวร์ที่ทำให้ส่วนการทำงานเหมือนชั้น LLC ในระดับแลนเดิม และสามารถสนับสนุนให้เป็นระบบแลนได้หลายรูปแบบ



โครงสร้างการจัดกลุ่มอุปกรณ์ให้เข้าเป็นเครือข่าย VLAN ภายใต้เครือข่ายแบบสวิตช์

การทำงานกำหนดเส้นทางเป็นซอฟต์แวร์ในระดับ 3 ที่มีความสำคัญยิ่ง เพราะในระดับสามเป็นการเชื่อม VLAN เข้าด้วยกันเป็นเครือข่าย ดังนั้นจึงต้องมีการกำหนดเส้นทางด้วยอุปกรณ์ที่จะกำหนดเส้นทางได้ถูกต้อง วิธีการหาเส้นทางจึงต้องฝากไว้กับอุปกรณ์ที่จะเป็นตัวบอกให้มีการสวิตช์ตามเส้นทางใด การหาเส้นทางจึงต้องมีการสอบถามและให้ข้อมูลเพื่อดำเนินการสร้างการเชื่อมต่อของข้อมูลผ่าน VLAN ได้ถูกต้อง

ในรูปเป็นวิธีการในการที่ไคล์เอ็นต์ A ต้องการติดต่อกับไคล์เอ็นต์ C มีวิธีการติดต่อโดยการให้การกำหนดเส้นทางผ่านอุปกรณ์ที่ใช้ในการกำหนดเส้นทางซึ่งเป็นซอฟต์แวร์



วิธีการติดต่อระหว่างไคล์เอ็นต์

เมื่อระดับการกำหนดเส้นทางมีความชัดเจนและทำงานได้ตามฟังก์ชันของเราเตอร์แล้ว การเชื่อมโยงแพคเกจระดับ IP ก็เกิดขึ้นได้ แพคเกจในระดับ IP วิ่งผ่านเข้าไปยัง VLAN และถูกตัดแบ่งเป็นเซล เมื่อสวิตช์ไปตามเส้นทางที่กำหนดได้ระดับชั้นที่เชื่อมต่อกับระดับ 3 คือ ระดับ Transport ที่จะเชื่อมโยงต่อเข้าสู่ระดับการประยุกต์ การทำงานในระดับนี้จึงเข้าใกล้กับการประยุกต์ใช้งานต่าง ๆ

ช่องโหว่ของการใช้ VLAN

โดยปกติแล้วจะไม่สามารถส่งข้อมูลข้าม VLAN ได้ถ้าไม่ใช้ เราเตอร์ สวิตช์เลเยอร์สาม หรือตัวกลางที่ช่วยค้นหาเส้นทางอื่นๆ แต่มีช่องโหว่ที่ทำให้ผู้ใช้สามารถส่งข้อมูลข้าม VLAN ได้โดยไม่ต้องอาศัยตัวกลาง เรียกว่า " การเบรค VLAN " ซึ่งช่องโหว่นี้เกิดจาก Trunking protocol ของสวิตช์บางรุ่น และวิธีการทดสอบคือทำการส่งข้อมูลตัวอย่างจาก VLAN หนึ่งไปยัง VLAN อื่น ที่อยู่บนสวิตช์คนละตัว และข้อมูลที่ส่งนั้นให้ทำการสร้าง ethernet Frame ที่มี Tag 802.1Q และเปลี่ยนค่าของหมายเลข VLAN ให้เป็นค่าของหมายเลข VLAN ปลายทางที่ต้องการเบรค เฟรมที่ถูกสร้างขึ้นใหม่นั้นจะมีลักษณะดังรูปที่ 6 และค่าของ Tag 802.1Q จะมีรูปแบบ "81 00 0n nn" โดยที่ nnn คือหมายเลขของ VLAN ซึ่งผลจากการทดสอบดังกล่างจะสามารถทำการเบรค VLAN ได้

สถานการณ์ต่อไปนี้จะทำให้เกิดช่องโหว่ของ VLAN

1.เมื่อผู้บุกรุกสามารถที่จะเข้าถึงพอร์ตในสวิตช์ที่เป็น VLAN เดียวกันกับ VLAN ของ Trunk port

2.เครื่องเป้าหมายอยู่บนสวิตช์ต่างกันแต่มีกลุ่ม trunk เดียวกัน

3.ผู้บุกรุกทราบถึง MAC address ของเครื่องเป้าหมาย

4.Layer 3 device สามารถสร้าง Connection จาก VLAN เป้าหมายกลับไปยัง VLAN ที่เป็นต้นทางได้

สรุป

เนื่องจากช่องโหว่ที่พบนั้นเป็นช่องโหว่ที่อาจจะไม่ สามารถจะป้องกันได้เพราะเป็นช่องโหว่ที่เกิดจากทางผู้พัฒนามาตรฐานและผู้ ผลิตอุปกรณ์เครือข่าย ฉะนั้นขอแนะนำว่า ไม่ควรใช้ VLAN เพื่อจุดประสงค์ในการรักษาความปลอดภัยของข้อมูลที่ส่งผ่าน เพียงแต่คุณสมบัติที่ดีของ VLAN นั้นก็ทำให้เป็นทางเลือกอีกทางที่น่าใช้ คุณสมบัติดังกล่าว เช่นสามารถทำการแบ่งเครือข่ายง่าย ลดการ broadcast และ ลดความคับคั่ง (Collision) เป็นต้น แต่ถ้าจำเป็นต้องใช้ VLAN นั้นให้พยายามเลี่ยงการใช้สวิตช์หลายตัว หรือกล่าวอีกนัยหนึ่งคือไม่ควรที่จะใช้ Trunk port

แหล่งอ้างอิง

http://article.numsai.com/index.php/computer/3389-vlan--lan

http://www.bloggang.com/viewdiary.php?id=pcgamezip&month=05-2008&date=15&group=3&gblog=9

ez-ADMIN Training Center

ดูรายละเอียดทั้งหมดที่ www.ez-admin.com โทร 02-6166422, 081-2055711

ศูนย์อบรมสำหรับมือใหม่ที่ต้องการก้าวสู่อาชีพผู้ดูแลระบบคอมพิวเตอร์แบบครบวงจร

จุดเด่นของศูนย์อบรม ez-admin

- ทุกเนื้อหาถ่ายทอดจากประสบการณ์จริงของผู้ดูแลระบบมืออาชีพ
- สอนภาคปฏิบัติ ให้ลงมือทำจริง ไม่เร่งสอนจนผู้เรียนไม่รู้เรื่อง
- เน้นสอนให้เข้าใจ ประยุกต์ใช้งานได้จริง ไม่ใช่แค่ทำตาม
- ถ่ายทอดเพื่อให้ผู้เรียนนำไปใช้งานและประกอบอาชีพได้จริง
- เน้นบรรยากาศการเรียนรู้ที่เป็นกันเองและราคาต่อหลักสูตรไม่แพง
- สมัครวันนี้ 4 หลักสูตร เรียนฟรีอีก 1 หลักสูตร และเรียนซ้ำได้ฟรี

หลักสูตรที่น่าสนใจ

- ก้าวแรกสู่อาชีพผู้ดูแลระบบเครือข่ายคอมพิวเตอร์
- ติดตั้งและบริหารจัดการ Windows Server 2008 Basic&Advance1-2
- ติดตั้งและบริหารจัดการ Windows Server 2003 Basic&Advance1
- ติดตั้งระบบรักษาความปลอดภัยด้วย ISA Server 2006 & Firewall
- ติดตั้งระบบ Genius Disk เครือข่ายแบบไร้ฮาร์ดดิสก์เพื่อควบคุมการทำงานที่ Server
- ติดตั้งและจัดการเครือข่ายอินเทอร์เน็ตคาเฟ่และเกมออนไลน์ด้วย Clark Connect
- ติดตั้งกล้อง IP Camera ดูภาพวงจรปิดผ่านอินเทอร์เน็ตได้ทั่วโลก
- เชื่อมต่อเครือข่ายข้ามสาขาระยะไกลด้วย Remote&VPN
- ติดตั้งระบบเครือข่ายไร้สายระยะไกลและการทำ Wireless Hotspot
- หลักสูตร Linux Network Administrator Basic&Advance
- หลักสูตร Hacker&Security 1,2,3,4

ทุกหลักสูตรเพียง 2,500 บาท สมัคร 4 หลักสูตร เรียนฟรี 1 หลักสูตร