โปรแกรมสร้างและทำซ้ำทราฟฟิกบนเครือข่าย

Network Traffic Replay and Generator Tool

บทคัดย่อ

โดยทั่วไปอุปกรณ์เน็ตเวิกต้องมีความสามารถในการประมวลผล การไหล ของ ข้อมูล หรือทราฟฟิกที่มาจากหลาย ๆ ทางได้ และเพื่อตรวจสอบการทำงานที่เหมาะสมของตัวอุปกรณ์ จึงทำการทดสอบโดยการสร้างทราฟฟิกไปยังอุปกรณ์เหล่านั้นโดยที่มีการกำหนดลักษณะการทำงานที่ซับซ้อนได้

วิทยานิพนธ์นี้อธิบายหน้าที่ของโปรแกรมสร้างและทำซ้ำทราฟฟิกบนเครือข่ายซึ่งถูกใช้เพื่แสดงลักษณะของประสิทธิภาพของพิธีการสื่อสารเครือข่ายแบบแพ็กเก็ตสวิชต์โดยสร้างหรือดักจับแพ็คเก็แบบทางเดียวที่ผ่านไปมาบนเครือข่ายและการทดสอบโปรโตคอลที่แตกต่างกันเพื่อหาความแตกต่างกันของประสิทธิภาพ ซึ่งผลของการทำงานของโปรแกรมจะช่วยในการวิเคราะห์ประสิทธิภาพของระบบ, ประเมินประสิทธิภาพของอุปกรณ์บนเครือข่ายเพื่อใช้ในการปรับปรุงเครือข่ายให้ทำงานได้อย่างเหมาะสม นอกจากนั้นยังใช้เพื่อศึกษาการทำงานของโปรโตคอลในระดับชั้นต่างๆในระบบเครือข่ายศึกษาลักษการโจมตีแบบต่างๆ ในระบบเครือข่าย เพื่อใช้ในการวิเคราะห์ลักษณะของเครือข่ายและแก้ไขให้เหมาะสม

ความสำคัญและที่มา

เนื่องจากในปัจจุบันการใช้งานอินเตอร์เน็ตมีการใช้งานกันอย่างแพร่หลายและข้อมูลที่ส่งในระบบเครือข่ายก็มีมากมายหลายแบบระบบความปลอดภัยจึงเป็นสิ่งสำคัญเนื่องจากมีคนใช้งาอินเตอร์เน็ตมากมาย มีทั้งผู้ใช้งาน และผู้ที่บุกรุก ทำให้ต้องมีจัดหาอุปกรณ์ที่หรือระบบที่จะป้องกันผู้ที่จะบุกรุกเข้ามา

สิ่งที่ต้องคำนึงถึงในโลกของอินเตอร์เน็ตในปัจจุบันอย่างหนึ่งคือเรื่องของความปลอดภัยทางเครือข่ายคอมพิวเตอร์ ดังนั้นก่อนที่จะเปิดให้บริการบนระบบเครือข่ายเราจึงต้องมีการทดสอบอุปกรณ์หรือระบบรักษาความปลอดภัยต่างๆก่อนที่จะเปิดให้บริการโดยการจำลองสภาวะนั้นๆกับอุปกรณ์หรือระบบที่เราต้องการทดสอบและ ทำซ้ำสภาวะเหล่านั้นเพื่อที่จะได้นำเอาผลของการตรวจสอบมาเปรียบเทียบหาข้อบกพร่องต่างๆ และนำมาวิเคราะห์แก้ไขได้ก่อนที่จะเปิดให้บริการ

จากเหตุผลข้างต้นจึงจำเป็นที่จะต้องมีโปรแกรมที่ช่วยในการทดสอบและสร้างสภาวะต่างๆของระบบเครือข่ายและทำซ้ำสภาวะนั้นๆเพื่อเป็นการเปรียบเทียบผลที่ออกมาทำให้ระบบนั้นหรืออุปกรณ์นั้นสามารถทำงานได้ตามที่เราต้องการหรือตามที่เรากำหนดไว้

ปริญญานิพนธ์นี้จึงมุ่งเน้นการศึกษาขั้นตอนการสร้างแพ็กเก็ตในรูปแบบต่างๆและการทำซ้ำสภาวะทางเครือข่ายซึ่งสามารถจำลองการทำงานบนเครือข่ายในช่วงเวลาหนึ่งๆได้อย่างถูกต้องแม่นยำรวมถึงการศึกษาลักษณะของแพ็กเก็ตการโจมตีแต่ละประเภทเพื่อพัฒนาโปรแกรมสร้างและทำซ้ำทราฟฟิกของเครือข่ายบนระบบปฏิบัติการลีนุกซ์ให้สามารถจำลองสภาวะดังกล่าวได้อย่างมีประสิทธิภาพ

วัตถุประสงค์ของปริญญานิพนธ์

ปริญญานิพนธ์ที่จัดทำขึ้นนี้ จัดทำภายใต้วัตถุประสงค์หลัก 4 ประการ ได้แก่

(1) เพื่อศึกษาการทำงานของโปรโตคอลในระดับชั้นต่างๆ

(2). เพื่อสร้างแพ็คเกจในรูปแบบต่างๆได้ตามที่ต้องการ

(3). เพื่อทำซ้ำข้อมูลของระบบเครือข่ายจากไฟล์ที่ดักจับมาได้

(4).เพื่อใช้ตรวจสอบอุปกรณ์และทดสอบระบบเครือข่ายในสภาวะแวดล้อมที่เหมือนเดิมหลายๆ ครั้งได้ เพื่อใช้ในการเปรียบเทียบ ทำให้ระบบมีประสิทธิภาพมากขึ้น

ขอบเขตของปริญญานิพนธ์

ขอบเขตการทำงานของปริญญานิพนธ์นี้ ได้แก่

(1) โปรแกรมสามารถสร้างเพ็จเก็ต ในรูปแบบต่างๆ ทั้งที่เป็นรูปแบบปกติ และ รูปแบบการโจมตีเพื่อสร้างสภาวะแวดล้อมในการทดสอบประสิทธิภาพของระบบการรักษาความปลอดภัยขององค์กรและความสามารถในการรองรับการทำงานของอุปกรณ์ในระบบเครือข่ายได้

(2) โปรแกรมสามารถนำข้อมูลในเครือข่ายที่บันทึกไว้มาส่งซ้ำได้ตามที่ต้องการ

(3) เป็นโปรแกรมที่ทำงานบนระบบปฏิบัติการที่เป็นลีนุกซ์ (Linux)

(4) โปรแกรมสามารถใช้งานง่าย โดยมีการทำกราฟฟิกยูสเซอร์อินเทอร์เฟซที่เหมาะสม

ขั้นตอนการดำเนินงาน

(1) ศึกษารายละเอียดเกี่ยวกับทีซีพี/ไอพีเบื้องต้น

(2) ศึกษาการสร้างแพ็คเก็ต (packet) โดยใช้ library libnet

(3) ศึกษารายละเอียดและการลักษณะของการโจมตีเพื่อจำลองสภาวะเครือข่ายได้

(4) ศึกษาโครงสร้างของไฟล์ที่ดักจับข้อมูลมาได้โดยโปรแกรม ethereal หรือ tcpdump

(5) ศึกษาการทำซ้ำของไฟล์ข้อมูลที่ดักจับมาได้จาก library tcpreplay

(6) ออกแบบโครงสร้างของโปรแกรมสร้างและทำซ้ำทราฟฟิกบนเครือข่ายคอมพิวเตอร์

(7) ศึกษาการเขียนโปรแกรมผ่านเครือข่าย

(8) ออกแบบขั้นตอนการทำงานของโปรแกรมสร้างและทำซ้ำทราฟฟิกบนเครือข่ายคอมพิวเตอร์

(9) พัฒนาโปรแกรมสร้างและทำซ้ำทราฟฟิกบนเครือข่ายคอมพิวเตอร์

(10) ทดสอบและปรับปรุงโปรแกรมสร้างและทำซ้ำทราฟฟิกบนเครือข่ายคอมพิวเตอร์

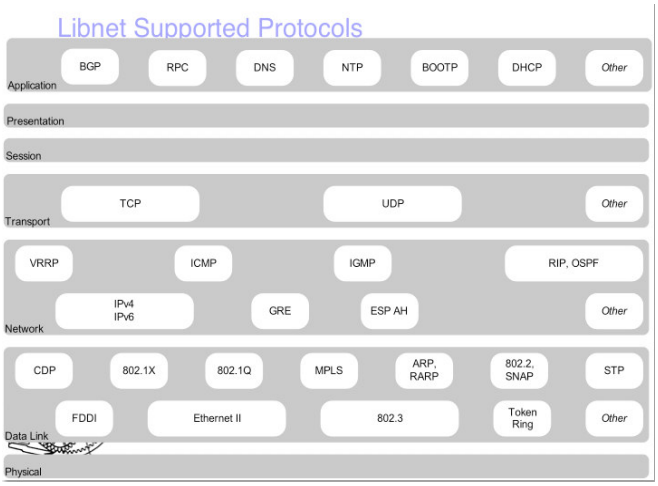
หลักการทำงานย่อยของโปรแกรม

1 หลักการสร้างแพ็คเก็ต (Packet)

1.1 **ความหมายและหลักการทำงานของลิปเน็ต** (Libnet)

ลิปเน็ตเป็นไลบรารี่ (Library) ของภาษาซีที่เตรียมเอาไว้เพื่อใช้ในการเชื่อมต่อระดับสูง (high-level)เพื่อส่งผ่านแพ็กเก็ตจากตำแหน่งต้นทางปยังอีกฝั่งปลายทางซึ่งลิปเน็ตมีตัวอย่างเอกสารอธิบายด้วยไว้อย่างชัดเจนเกี่ยวกับเอพีไอ (API) ที่ใช้ได้อย่างง่ายดายและเรียกใช้ในโปรแกมได้อย่างเหมาะสม

ปัจจุบันตัวไลบรารี่สิปเน็ตเป็นไลบรารี่ของภาษาซีที่ออกแบบมาให้เล็กและง่ายต่อการใช้ โดยจุดประสงค์หลักของตัวลิปเน็ตเองคือการสร้างแพ็คเก็ตปัจจุบันมีโปรดตคอลที่สนับสนุน ดังรูป



รูปที่ 1 แสดงโปรโตคอลที่ลิปเน็ตสนับสนุน

1.2 **ขั้นตอนการดำเนินการ**

เพื่อสร้างและส่งแพ็กเก็ตออกไป จะต้องมีคำสั่งพื้นฐานดังนี้

1.2.1 สร้างคอนเท็กซ์ (Context) ของตัวแพ็คเก็ต เป็นการเลือกเน็ตเวิร์กการ์ด (Network card) และระดับการควบคุมแพ็คเก็ตตามที่ต้องการว่าต้องการควบคุมตั้งแต่ลิงค์เลเยอร์ (Link layer) หรือไอพีเลเยอร์ (IP Layer) ขึ้นไป

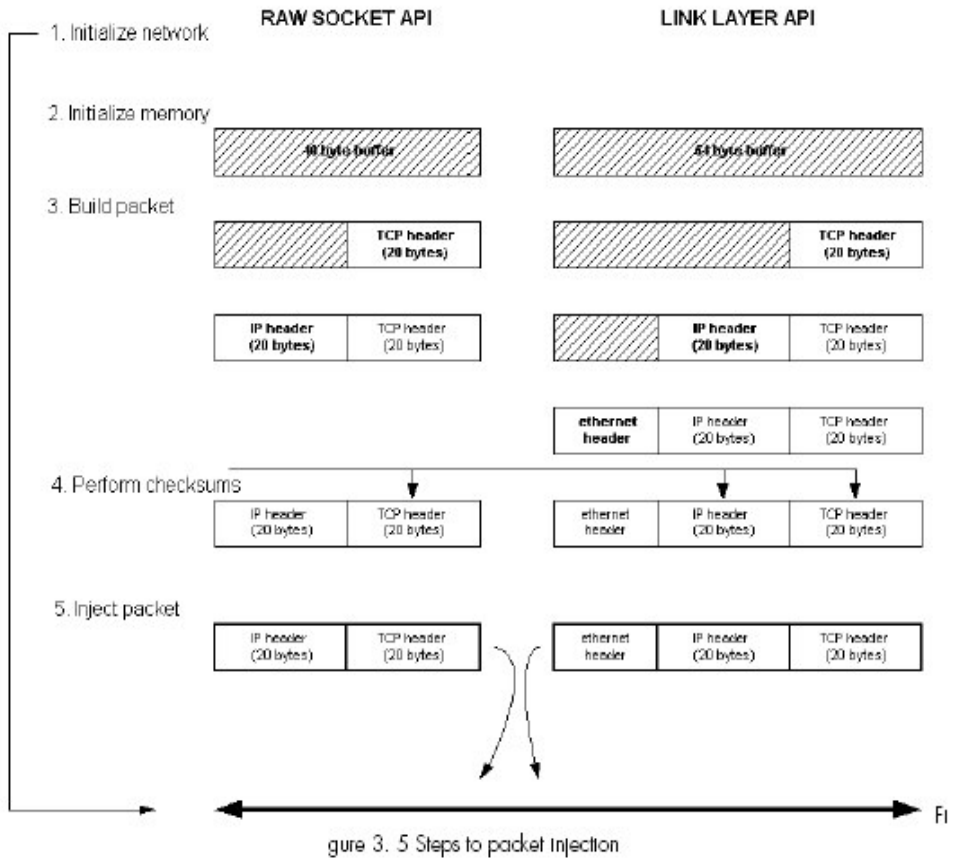
1.2.2 สร้างแต่ละโพรโตคอลบล็อก (Protocol block)

ในการสร้างแต่ละแพ็คเก็ตต้องมีการสร้างโปรโตคอลของแต่ละชั้นในการสร้างแพ็คเก็ตเรียกว่าโพรโตคอลบล็อกเช่น ถ้าต้องการสร้างแพ็คเก็ตดีเอ็นเอสคิวรี่ (DNS query) ก็ต้องสร้างโพรโตคอลบล็อกของชั้นแอฟพลิเคชั่นคือ ดีเอนเอสและต้องการส่งแบบยูดีพี (UDP) ต้องสร้างโพรโตคอลบล็อกของยูดีพีเป็นต้น

1.2.3 เป็นขั้นตอนในการส่งแพ็คเก็ต

ถ้าในการส่งต้องมีการทำเช็คซัม(Checksum) ซึ่งค่าเช็คซัมจะถูกคำนวณโดยอัตโนมัติเมื่อสร้างโพรโตคอลบล็อกสร็จ

1.2.4 เป็นขั้นตอนในการลบข้อมูลทั้งหมดที่สร้างไว้ออกจากหน่วยความจำ



รูปที่ 2 แสดงการขั้นตอนการสร้างและส่ง Packet ลงบนเครือข่าย

2 การทำซ้ำทราฟฟิกบนเครือข่าย

2.1 **ความหมายของการทำซ้ำแพ็กเก็ตลงบนเครือข่าย** (Replay packet)

หมายถึง การนำไฟล์ที่ดักจับแพ็คเก็ตมาได้จะเป็นไฟล์นามสกุล *.pcap จากระบบเน็ตเวิร์ก โดยวิธีการหรือโปรแกรมต่างๆ และนำมาแก้ไข หรือส่งแพ็คเก็ตออกไปตามไฟล์ที่ดักจับมาได้ ก่อนที่จะส่งออกไปลงบนเครือข่าย

2.2 **องค์ประกอบของการทำซ้ำทราฟฟิกบนเครือข่าย**

ในส่วนของการทำซ้ำทราฟฟิกบนเครือข่ายต้องมีไลบรารี่ที่เกี่ยวข้องคือลิปเน็ตและลิปพีแค็ปเพื่อทำให้การจัดการทำงานของการทำซ้ำทราฟฟิกบนเครือข่าย

2.3 **การทำงานของการทำซ้ำทราฟฟิกบนเครือข่าย**

การทำงานของการทำซ้ำทราฟฟิกบนเครือข่ายอาศัยไลบรารี่ลิปพีแค็ปในการอ่านข้อมูลจากจากไฟล์ที่ดักจับมาได้ และใช้ไลบรารี่ลิปเน็ตในการสร้างแพ็คเก็ตออกไปบนเครือข่าย

2.4 **ประโยชน์ของการทำซ้ำทราฟฟิกบนเครือข่าย**

2.4.1 ในการตรวจสอบเครือข่าย (Network Debugging Tools) ในการตรวจสอบแอพพิเคชั่น หรือไฟล์วอล (firewall) และการทำการตรวจสอบเหมือนเดิมหลายๆครั้งเพื่อทำการเปรียบเทียบผลที่ได้ออกมาเพื่อวัดประสิทธภาพของเครือข่ายหรือวิเคราะห์ปัญหาที่เกิดขึ้น สามารถทำให้แก้ก่อนการเปิดให้บริการได้

2.4.2 เพื่อใช้ในการศึกษาการทำงานของโปรโตคอลในระดับชั้นต่างๆ ในระบบเครือข่าย ศึกษาลักษณะการโจมตีแบบต่างๆ ในระบบเครือข่าย

3 หลักการดักจับแพ็กเก็ต

3.1 ความหมายของแพ็คเก็ตแคปเจอร์ (Packet sniffer)

แพ็กเก็ตแคปเจอร์คืออุปกรณ์ที่ทำหน้าที่ดักจับแพ็กเก็ตที่วิ่งอยู่บนเน็ตเวิร์กโดยจะทำงานร่วมกับเน็ตเวิร์กอินเทอร์เฟซการ์ด (Network Interface card) ในโหมดโพรมิสคิวอัส (Promiscuous-mode) โดยการทำงานร่วมกับโหมดนี้การทำงานของเน็ตเวิร์กอินเทอร์เฟซการ์ดในโหมดนี้จะไม่มีการเปรียบเทียบแอดเดรสปลายทางของแพ็กเก็ตกับแอดเดรสของเน็ตเวิร์กอินเทอร์เฟซการ์ดนั่นคือทุกๆแพ็กเก็ตมาถึงยังเน็ตเวิร์กอินเทอร์เฟซการ์ดจะถูกจับแพ็กเก็ตขึ้นมาได้ทั้งหมดไม่เลือกว่าจะระบุแอดเดรสปลายทางของการ์ดเน็ตเวิร์กอินเทอร์เฟซอันไหน

แพ็กเก็ตแคปเจอร์จะถูกใช้ในการเฝ้าดูการจารจรในเครือข่ายให้มีประสิทธิภาพและแก้ไขปัญหาต่างๆที่เกิดจากการทำงานผิดพลาดของเครือข่ายและยังเป็นเครื่องมือในการศึกษาการทำงานของโพรโตคอลรวมถึงการดูแลความปลอดภัยของระบบ

3.2 องค์ประกอบของแพ็กเก็ตแคปเจอร์

3.2.1 ฮาร์ดแวร์ (Hardware)

หมายถึงอุปกรณ์อิเล็กทรอนิคส์ที่สามารถดักอ่านสัญญาณจากเน็ตเวิร์กเข้ามาได้และสามารถนำสัญญาณที่ให้ส่งต่อไปประมวลผลออกมาเป็นข้อมูลทางคอมพิวเตอร์ได้หน้าที่หลักคือจัดการกับการรับข้อมูลในระดับฟิสิกคอล (Physical) อุปกรณ์นี้โดยทั่วไปคือเน็ตเวิร์กอะแดปเตอร์

3.2.2 ไดรเวอร์(Driver)

เป็นโปรแกรมระดับล่างที่ควบคุมการดักจับข้อมูลของฮาร์ดแวร์ไปเก็บเป็นข้อมูลดิบรอการประมาวลผลในลำดับถัดไป

3.2.3 บัฟเฟอร์(Buffer)

เป็นหน่วยความจำที่ใช้พักข้อมูลจากการดักจับมาได้ของDriver โดยจะทำงานการจัดเก็บเพียงชั่วคราว และหมุนเวียนข้อมูลใหม่เข้ามาเสมอกลไกลการนำข้อมูลขากไดรเวอร์มาเก็บในบัฟเฟอร์จะเป็นตัวบอกสมรรถนะของการดักข้อมูลได้ความเร็วสูงสุดเท่าใดหากกระบวนการนำข้อมูลไปเก็บเป็นไปอย่างล่าช้าย่อมทำให้แพ็กเก็ตแคปเจอร์ไม่สามารถดักจับข้อมูลที่อยู่บนเน็ตเวิร์กได้ทันและต้องปล่อยข้อมูลนั้นทิ้งไป

3.2.4 ซอฟต์แวร์ (Software)

เพื่อทำหน้าที่จัดการข้อมูลที่ได้เข้าโดยการประมวลผลตามวัตถุประสงค์ของการดักอ่านข้อมูลนั้น เนื่องจากข้อมูลดิบที่ดักได้นั้นจะเป็นข้อมูลในระดับต่ำคือ เน็ตเวิร์กอินเทอร์เฟซเลเยอร์ (Network Interface Layer) ซึ่งจะมีข้อมูลที่ยังไม่ผ่านการมัลติเพล็กซ์และจัดรูปแบบให้เข้าใจได้ส่วนที่ได้จะเป็นข้อมูลเลขฐานสอง 0 กับ1จำนวนมหาศาลที่ต้องนำมาหาความหมายและอีกหน้าที่หนึ่งคือข้อมูลที่ดักได้นันเป็นการสื่อสารของทุกโฮสต์ที่อยู่ภายในเน็ตเวิร์กนั้นร่วมกันอยู่อย่างไม่เป็นระเบียบและไม่มีการแยกแยะว่าเป็นการสื่อสารเรื่องอะไรระหว่างโฮสต์ใดกับโฮสต์ใดการที่จะแปลความหมายของข้อมูลนี้ได้ก็จำเป็นต้องมีโปรแกรมสำหรับทำหน้าที่แปลความหมายของข้อมูลให้อยู่ในรูปแบบที่สามารถเข้าใจได้มากขึ้นนั่นคือการทำหน้าที่คล้ายกับดีมัลติเพล็กซ์ของโพรโตคอลปกติแต่จะเป็นการดีมัลติเพล็กซ์ของข้อมูลทุกๆโฮสต์โดยไม่สนใจว่าเป็นข้อมูลของโฮสต์ใด

หลังจากข้อมูลผ่านการดีมัลติเพล็กซ์แล้วก็จะอยู่ในรูปที่สามารถเข้าใจได้ง่ายขึ้นแต่จะเข้าใจมากน้อยขึ้นอยู่กับความสามารถในการดีมัลติเพล็กซ์ของโปรแกรมหากสามารถดีมัลติพล็กซ์ได้จนถึงโพรโตคอลเลเยอร์ที่สูงรวมทั้งหากมีการแยกแยะหมวดหมู่ของการสื่อสารของแต่ละโฮสต์ก็จะเห็นความต่อเนื่องของการสื่อสารได้ดีขึ้น

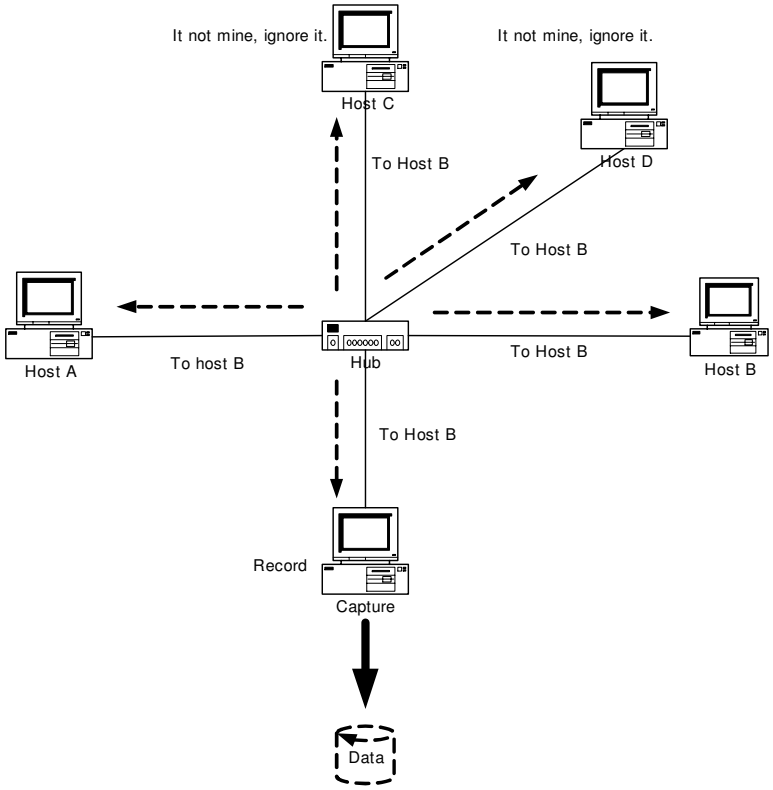
3.3 การทำงานของแพ็กเก็ตแคปเจอร์

การทำงานของแพ็กเก็ตแคปเจอร์อาศัยหลักการของโพรโตคอลอีเทอร์เน็ตที่ใช้การกระจายของข้อมูลไปยังทุกโฮสต์ที่อยู่ในเน็ตเวิร์กและอาศัยโฮสต์แต่ละตัวทำหน้าที่จำแนกการสื่อสารของตนเองนั่นหมายความว่าข้อมูลทุกแพ็กเก็ตที่ใช้สื่อสารกันได้ถูกส่งไปยังทุกโฮสต์ซึ่งจะได้รับพร้อมกันแล้วเหมือนกันเพียงแต่การที่จะสื่อสารกันได้อย่างถูกต้องนั้นโฮสต์แต่ละตัวจะต้องมีการบวนการที่สามารถรู้ได้ว่าข้อมูลแพ็กเก็ตใดเป็นของตนเองและข้อมูลแพ็กเก็ตใดมิใช่ของตนเองทุกๆแพ็กเก็ตที่กระจายลงบนเน็ตเวิร์กนั้นจะมีหมายเลขระบุชัดเจนคือ แม็คแอดเดรส (MAC Address) หรือเรียกอีกอย่างหนึ่งว่าอีเทอร์เน็ต (Ethernet Address) ซึ่งจะเป็นสิ่งที่บอกว่าแพ็กเก็ตมาจากฮาร์ดแวร์ใดในเน็ตเวิร์กทำให้สามารถระบุได้ว่าส่งมาจากโฮสต์ใดแม็คแอดเดรสจะเป็นหมายเลขเฉพาะฮาร์ดแวร์ทุกชนิดที่ใช้สื่อสารโดยโพรโตคอลอีเธอร์เน็ตและในทางทฤษฎีแล้วฮาร์ดแวร์ทุกชนิดจะไม่มีแม็คแอดเดรสซ้ำกันโดยทั่วไปแม็คแอดเดรสจะกำหนดตายตัวอยู่ในรอม(Rom) ของฮาร์ดแวร์และไม่สามารถเปลี่ยนแปลงได้ด้วยซอฟต์แวร์

การใช้งานของฮาร์ดแวร์จะต้องควบคู่กับไดรเวอร์ของฮาร์ดแวร์นั้นๆโดยปกติแล้วไดรเวอร์จะถูกกำหนดให้ปฏิบัติตามโพรโตคอลอย่างเข้มงวดคือ

- ให้รับข้อมูลที่มีแม็คแอดเดรสเป็นของตนเองเท่านั้น (ห้ามอ่านข้อมูลของผู้อื่น)
- ให้ส่งข้อมูลโดยใช้แม็คแอดเดรสของตอนเองเท่านั้น (ห้ามปลอมเป็นผู้อื่น)

ดังนั้นหากใช้ไดรเวอร์ตามปกติที่มากับฮาร์ดแวร์แล้วเครื่องคอมพิวเตอร์ก็จะทำงานอยู่ในระเบียบเรียบร้อยและไม่สามารถวุ่นวายกับข้อมูลของผู้อื่นได้แพ็กเก็ตแคปเจอร์จึงจำเป็นที่ต้องใช้โหมดการทำงานพิเศษที่อนุญาตให้รับข้อมูลที่แม็คแอดเดรสไม่ใช้ของตนได้โหมดนั้นเรียกว่าโพรมิสคิวอัสโหมด(Promiscuous Mode) ที่ทำให้ฮาร์ดแวร์สามารถรับข้อมูลดิบทั้งหมดบนเน็ตเวิร์กเข้ามาได้โดยไม่สนใจว่าข้อมูลทั้งหมดเป็นของใคร ส่งให้ใคร



รูปที่ 3 การทำงานของแพ็กเก็ตแคปเจอร์

จากรูปที่ 3.1 ในเน็ตเวิร์กมีโฮสต์อยู่ 4 ตัวต่อรวมกันเป็นเน็ตเวิร์กโดยใช้ฮับ (Hub) ร่วมกัน และมีโฮสต์ตัวหนึ่งรันโปรแกรมที่ทำหน้าที่เป็นโปรแกรมแคปเจอร์เพื่อดักจับข้อมูลเสียบต่อร่วมเข้ากับฮับนั้น จากรูปแสดงให้เห็นการกระจายของข้อมูลที่โฮสต์ A ต้องการส่งให้โฮสต์ Bข้อมูลได้กระจายไปยังทุกโฮสต์ที่ต่ออยู่บนฮับ รวมถึงแพ็กเก็ตแคปเจอร์ด้วย

โฮสต์ Bเมื่อได้รับข้อมูลก็จะตรวจแม็คแอดเดรสถ้าพบว่าเป็นข้อมูลที่ถูกส่งมาหาตนเองก็ทำการอ่านและส่งต่อให้ระบบปฏิบัติการประมวลผล

โฮสต์ Cและโฮสต์Dโฮสต์ทั้งสองซึ่งมีเน็ตเวิร์กอะแดปเตอร์ทำงานอยู่ในโหมดปกติเมื่อได้ทำการตรวจสอบแล้วว่าไม่ใช่ข้อมูลของตนเองก็จะไม่สนใจข้อมูลนั้นแพ็กเก็ตแคปเจอร์สำหรับแพ็กเก็ตแคปเจอร์นั้นมีเน็ตเวิร์กอแดปเตอร์ที่ทำงานอยู่ในโพรมิสคิวอัสโหมดนั่นคือไม่สนใจว่าข้อมูลที่เข้ามาเป็นของใครแพ็กเก็ตแคปเจอร์จะรับข้อมูลทั้งหมดแล้วนำไปเก็บไว้ในบัฟเฟอร์และฐานข้อมูลเพื่อนำไปประมวลผลเพื่อหาข้อมูลที่มีประโยชน์ภายหลังจากเน็ตเวิร์กในภาพนั้นมีแพ็กเก็ตแคปเจอร์ถูกติดตั้งในตำแหน่งดังกล่าวก็จะทำให้ข้อมูลทั้งหมดที่โฮสต์ทั้ง4 สื่อสารกันโดยผ่านฮับที่ใช้งานร่วมกันไม่ว่าข้อมูลใดจะปรากฏที่ฮับก็สามารถถูกดักอ่านได้โดยแพ็กเก็ตแคปเจอร์ทันที

3.4 ประโยชน์จากแพ็กเก็ตแคปเจอร์

3.4.1 วิเคราะห์ระบบเครือข่าย (Network Analyzer)

การที่แพ็กเก็ตแคปเจอร์สามารถดักจับข้อมูลทั้งหมดที่อยู่บนเน็ตเวิร์กได้ทำให้เราสามารถนำข้อมูลดังกล่าวมาทำการประมวลผลวิเคราะห์คุณสมบัติต่างๆของเน็ตเวิร์กได้หลายแง่มุมไม่ว่าการกระจายการใช้งานเน็ตเวิร์กของโพรโตคอลต่างๆเช่นเอชทีทีพี(HTTP),เอสเอ็มทีพี(SMTP),เอฟทีพี(FTP)เพื่อจะได้ทราบว่ามีการใช้เน็ตเวิร์กเพื่อการใดมากน้อยเพียงใดจะทำให้สามารถจัดการเน็ตเวิร์กได้อย่างเหมาะสม หรือในด้านการใช้งานเน็ตเวิร์กตามช่วงเวลาดังกล่าวหรือในด้านการใช้งานเน็ตเวิร์กตามช่วงเวลาต่างๆ เวลาใดที่มีผู้ใช้มากเวลาใดที่มีผู้ใช้น้อย ผู้ใช้คนใดใช้แบนด์วิดธ์ไปในทางที่เป็นประโยชน์หรือไม่

3.4.2 เครื่องมือตรวจสอบเครือข่าย (Network Debugging Tools)

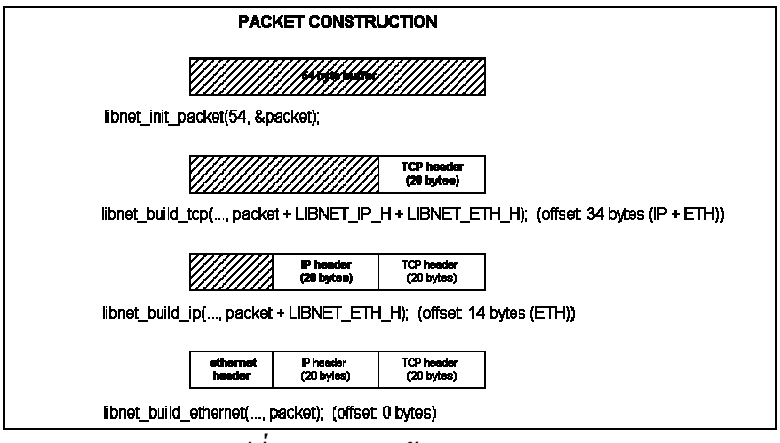
ในบางครั้งการหาสาเหตุความผิดปกติของแอพพลิเคชั่นต่างๆจำเป็นที่ต้องสืบค้นลึกลงไปถึงเนื้อข้อมูลที่รับส่งกันจริงๆบนเน็ตเวิร์กเพื่อหาว่าเหตุใดการทำงานของแอพพลิเคชั่นจึงไม่สามาถทำงานได้ตามปกติการได้เห็นข้อมูลที่ส่งกันจริงทำให้การวิเคราะห์และแก้ไขปัญหาสามาถดำเนินการอย่างรวดเร็วและตรงต่อหัญหาได้มากขึ้นโดยเฉพาะกรณีที่มีการใช้เครื่องมือในระดับเน็ตเวิร์กมาเกี่ยวข้องเช่นมีการส่งข้อมูลผ่านไฟร์วอลล์แล้วปัญหา หรือการทดสอบ ALC (Access Control List) ของเราเตอร์เป็นต้น

3.4.3 ตรวจจับแพ็กเก็ต (Packet Monitoring)

การศึกษาเทคนิคของโพรโตคอลในระดับเน็ตเวิร์กจำเป็นต้องเห็นข้อมูลที่สื่อสารกันอยู่จึงจะสามารถเข้าใจได้และเห็นภาพจริงแพ็กเก็ตมอนิเตอร์ริ่งจะเป็นเครื่องมือที่นำแพ็กเก็ตมาแสดงเห็นในรูปแบบต่างๆได้

3.4.4 ระบบตรวจจับผู้บุกรุก (Intrusion Detection System)

ระบบตรวจจับผู้บบุกรุกก็มีพื้นฐานมาจาการดักอ่านข้อมูลเพียงแต่เป็นการประยุกต์การวิเคราะห์รูปแบบการบุกรุกเข้ากับการดักอ่านข้อมูลบนเน็ตเวิร์กแบบเรียลไทม์ทำให้สามารถทราบว่ามีกิจกรรมใดบนเน็ตเยิร์กที่มีแนวโน้มว่าจะเป็นการบุกรุกหรือทำอันตรายต่อผู้อื่น



รูปที่ 4 แสดงการสร้างแบบ LIBNET_LINK