การประเมินผลกระทบการโจมตีระบบโทรศัพท์ผ่านอินเตอร์เน็ต จากการปฏิเสธการให้บริการด้วยการยิงข้อความ SIP INVITE

ภูวิช แก้วหาญ

สารนิพนธ์นี้เป็นส่วนนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาตรมหาบัณฑิต
สาขาวิชาวิศวกรรมคอมพิวเตอร์ วิทยาลัยนวัตกรรมด้านเทคโนโลยีและวิศวกรรมศาสตร์
มหาวิทยาลัยธุรกิจบัณฑิตย์
ปีการศึกษา 2564

IMPACT ASSESSMENT OF ATTACKING THE VOICE OVER INTERNET PROTOCOL SYSTEM FROM A DENIAL OF SERVICE (DoS) THREAT BY FLOODING SIP INVITE MESSAGE

PHUWISH KEAOHAN

A Thematic Paper Submitted in Partial Fulfillment of the Requirements for the Degree of Master Engineering Department of Computer Engineering

College of Innovative Technology And Engineering,

Dhurakij Pundit University

Academic Year 2021

ใบรับรองสารนิพนธ์

วิทยาลัยนวัตกรรมด้านเทคโนโลยีและวิศวกรรมศาสตร์ มหาวิทยาลัยธุรกิจบัณฑิตย์

ปริญญา วิศวกรรมศาสตรมหาบัณฑิต สาขาวิชาวิศวกรรมคอมพิวเตอร์

หัวข้อสารนิพนธ์	การประเมินผลกระทบการโจมตีระบบโทรศัพท์ผ่านอินเตอร์เน็ต จากการปฏิเสธการให้บริการด้วยการยิงข้อความ SIP INVITE
เสนอโดย	นายภูวิช แก้วหาญ
สาขาวิชา	วิศวกรรมคอมพิวเตอร์
อาจารย์ที่ปรึกษาสารนิพนธ์	อาจารย์ ดร.ชัยพร เขมะภาตะพันธ์

ได้พิจารณาเห็นชอบโดยคณะกรรมการสอบสารนิพนธ์แล้ว

.....ประธานกรรมการ

(รองศาสตราจารย์ ดร.สัญฉกร วุฒิสิทธิกุลกิจ)

..... กรรมการและอาจารย์ที่ปรึกษาสารนิพนธ์

(อาจารย์ ดร.ชัยพร เขมะภาตะพันธ์)

.....กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.มัชฉิกา อ่องแตง)

วิทยาลัย นวัตกรรมด้านเทคโนโลยีและวิศวกรรมคอมพิวเตอร์รับรองแล้ว

.....คณบดีวิทยาลัย นวัตกรรมด้านเทคโนโลยีและวิศวกรรมศาสตร์

(อาจารย์ ดร.ชัยพร เขมะภาตะพันธ์)

วันที่ 21 เดือน ก.ค. พ.ศ. 2565

หัวข้อสารนิพนธ์	การประเมินผลการทบการโจมตีระบบโทรศัพท์ผ่านอินเตอร์เน็ต จากการปฏิเสธการให้บริการด้วยการยิงข้อความ SIP INVITE
ชื่อผู้เขียน	ภูวิช แก้วหาญ
อาจารย์ที่ปรึกษา	อาจารย์ ดร.ชัยพร เขมะภาตะพันธ์
หลักสูตร	วิศวกรรมคอมพิวเตอร์
ปีการศึกษา	2564

บทคัดย่อ

สารนิพนธ์นี้มีจุดประสงค์ในการศึกษา ประเมินผลกระทบของช่องโหว่ของระบบโทรศัพท์ผ่านอินเตอร์เน็ต(IPPBX SERVER) จากการคุกคามแบบ Denial of Service(DoS) โดยใช้โปรแกรมทดสอบการโจมตีด้วยการส่งคำสั่งร้องขอการเชื่อมต่อ(SIP INVITE) จำนวนมากไปยัง IPPBX SERVER โดยเปรียบเทียบกับกรณีโจมตีผ่านระบบเชื่อมต่อสัญญานโทรศัพท์ผ่านอินเตอร์เน็ต(SIP PROXY SERVER) ที่มีคุณสมบัติโปรแกรมป้องกันการคุกคาม

ผลลัพธ์จากศึกษาแสดงให้เห็นว่า SIP PROXY SERVER ที่มีการเปิดใช้งานโมดูล PIKE สามารถตอบสนองต่อการโจมตีได้โดยสามารถหยุดส่งคำสั่ง SIP INIVTE ไปยัง IPPBX SERVER เมื่ออัตราการโทรศัพท์ต่อวินาทีอยู่ในระหว่างค่าอัตราการรับคำสั่งต่อวินาทีที่กำหนดบนโมดูล PIKE ในขณะที่ IPPBX SERVER ที่ไม่มีระบบป้องกันไม่สามารถจัดการปัญหา DoS นี้ได้เลย การป้องกันทำให้ปริมาณการใช้ทรัพยากรของ IPPBX SERVER ไม่เพิ่มขึ้นและไม่มีผลกระทบต่อการให้บริการของระบบ มีผลให้ IPPBX SERVER สามารถต้านทานต่อการคุกคามแบบ DoS โดยใช้คำสั่งร้องขอการเชื่อมต่อ SIP INIVTE ได้ โดยการป้องกันจาก SIP PROXY SERVER

Thematic Paper Title	IMPACT ASSESSMENT OF ATTACKING THE VOICE OVER INTERNET PROTOCOL SYSTEM FROM A DENIAL OF SERVICE (DoS) THREAT BY FLOODING SIP INVITE MESSAGE
Author	Phuwish Keaohan
Thematic Paper Advisor	Dr.Chaiyaporn Khemapatapan
Department	Computer Engineering
Academic Year	2021

ABSTRACT

The purpose of this thematic research is to assess the impact of Internet telephone system (IPPBX SERVER) from Denial of Service (DoS) threats by sending bulk SIP invite messages to Internet telephone system by comparing the cases with and without SIP proxy server that has anti-attack program features.

The results of testing show that the SIP proxy server, bundled with the Pike module feature, is able to handle request from attacker by dropping the SIP invite message to the Internet telephony system when number of calls per second equal to call per second parameter which is defined in the Pike module while an Internet telephone system without protection feature cannot absolutely handle this DoS traffic. Resource consumption of the Internet telephony system with SIP proxy does not increase and not impact to service of system. Finally, the Internet telephone system can be protected by SIP proxy server from DoS threats which flood by SIP invite messages.

กิตติกรรมประกาศ

สารนิพนธ์ฉบับนี้สำเร็จลุล่วงและบรรลุวัตถุประสงค์ เพราะได้รับความอนุเคราะห์จาก ดร. ชัยพร เขมะภาตะพันธ์ อาจารย์ที่ปรึกษาสารนิพนธ์ ที่ได้กรุณาให้คำแนะนำ ข้อคิดเห็น และชี้แนะแนวทางที่เป็นประโยชน์ต่อสารนิพนธ์ฉบับนี้ ผู้วิจัยขอขอบคุณเป็นอย่างสูงมา ณ โอกาสนี้

ผู้วิจัยขอขอบคุณคณะอาจารย์ผู้สอนที่ประสิทธิ์ประสาทวิชาความรู้ เจ้าหน้าที่ที่เอาใจใส่อำนวยความสะดวก และเพื่อนร่วมรุ่นที่ช่วยเหลือ เอื้อเฟื้อ แบ่งปัน ตลอดระยะช่วงเวลาของการศึกษา

สุดท้ายนี้ผู้วิจัยขอขอบพระคุณบิดา มารดา อีกทั้งสมาชิกในครอบครัว ภรรยา และบุตรที่เป็นกำลังใจและสนับสนุนเพื่อให้เกิดความสำเร็จในทุกๆด้าน

ภูวิช แก้วหาญ

สารบัญ

หน้า

สารบัญ (ต่อ)

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญภาพ

ภาพที่ **หน้า**

สารบัญภาพ (ต่อ)

ภาพที่ **หน้า**

สารบัญภาพ (ต่อ)

ภาพที่ **หน้า**

สารบัญภาพ (ต่อ)

ภาพที่ **หน้า**

สารบัญภาพ (ต่อ)

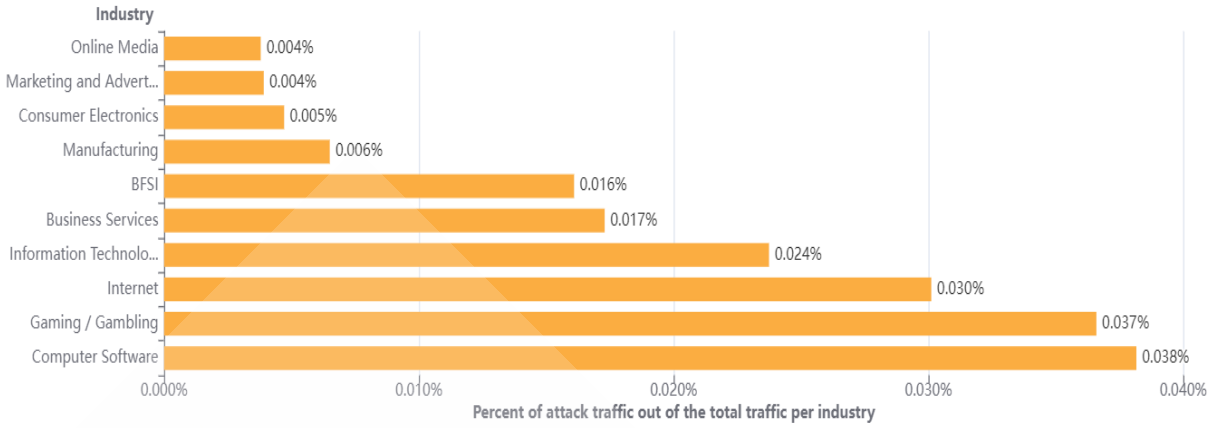
ภาพที่ **หน้า**

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

การที่ในปัจจุบันการสื่อสารข้อมูลต่างๆส่วนมากอาศัยการสื่อสารผ่านอินเตอร์เน็ตความเร็วสูงซึ่งถือได้ว่าเป็นโครงข่ายการสื่อสารข้อมูลที่ได้รับความนิยมทั้งในแง่ความสะดวกรวดเร็วในการติดตั้ง การเข้าถึงได้ง่ายของผู้ให้บริการข้อมูลในแต่ละพื้นที่ ทำให้รูปแบบการบริการข้อมูลบนอินเตอร์เน็ตมีหลากหลายมากขึ้น ซึ่งระบบการสื่อสารโทรศัพท์เช่นเดียวกันได้มีการเปลี่ยนแปลงระบบจากการสื่อสัญญานผ่านโครงข่ายระบบ การสื่อสารแบบแพคเกจสวิตช์ (Package switched Telephone) แบบ ISDN(integrated services digital network) หรือแบบอนาล็อก(CO Line) เป็นโทรศัพท์ที่รองรับการเชื่อมต่อผ่านอินเตอร์เน็ต(Voice Over Internet Protocol)

ความต้องการเชื่อมต่อระบบโทรศัพท์ผู้ให้บริการหรือสำนักงานที่มีการทำงานจากที่บ้านหรือสถานที่ภายนอกเป็นรูปแบบที่มีความจำเป็นในช่วงที่มีโรคโควิด 2019 ระบาด การปรับรูปแบบการสื่อสารเพื่อไม่ให้มีผลกระทบต่อภาระกิจหรือธุรกิจจะมีความสำคัญอันดับต้นในการดำเนินกิจการให้มีความต่อเนื่อง การปรับเปลี่ยนระบบโทรศัพท์ผ่านอินเตอร์เน็ต จะต้องมีการเตรียมพร้อมในส่วนของเชื่อมต่อสัญญาณให้มีประสิทธิภาพทั้งด้านคุณภาพของการให้บริการและความปลอดภัยของระบบโทรศัพท์ทั้งผู้ให้บริการและผู้ใช้บริการ การป้องกันความปลอดภัยของระบบมีความสำคัญอย่างยิ่งดังรายงานการโจมตีระบบเครือข่ายคอมพิวเตอร์ดังภาพที่ 1.1 นี้



ภาพที่ 1.1 รายงานการโจมตีแบบ DDOS ในไตรมาส 3 ของปี 2564 แยกกลุ่มตามธุรกิจ

ที่มา: https://blog.cloudflare.com/ddos-attack-trends-for-2021-q3/

จากภาพที่ 1.1 การโจมตีโปรแกรมคอมพิวเตอร์และอินเตอร์เน็ตรวมกันแล้วมีอัตราการถูกโจมตีมากที่สุด ซึ่งภัยคุกคามจากสื่อสารผ่านอินเตอร์เน็ตมีหลากหลายรูปแบบที่เป็นภัยต่อระบบการทำงานขององค์กรและผู้ใช้งาน ซึ่งผู้คุกคามจะใช้ประโยชน์จากช่องโหว่ที่มีในระบบสื่อสารข้อมูล เช่นเดียวกันระบบโทรศัพท์ผ่านอินเตอร์เน็ตหลีกเลี่ยงไม่ได้ที่จะโดนคุมคามโจมตีจากบุคคลประสงค์ร้าย โดยอาศัยช่องโหว่หรือจุดอ่อนของระบบโทรศัพท์ผ่านอินเตอร์เน็ต ซึ่งผลกระทบมีทั้งทางตรงและทางอ้อมระดับความรุนแรงของภัยดังกล่าวจะแตกต่างกันตามรูปแบบของภัยคุกคาม ดังนั้นการออกแบบหรือพัฒนาระบบโทรศัพท์ผ่านอินเตอร์เน็ต ให้มีความต้านทานภัยต่อคุกคาม หรือหาแนวทางป้องกัน ก็จะทำให้ลดผลกระทบ ในการให้บริการ ความสูญเสียทรัพยากรของระบบ และยังคงทำให้ระบบโทรศัพท์ผ่านอินเตอร์เน็ตให้บริการด้วยความเสถียร มีคุณภาพของการให้บริการที่ดี และมีความมั่นคงปลอดภัยน่าเชื่อถือยิ่งขึ้น

1.2 วัตถุประสงค์ของการวิจัย

1.2.1 เพื่อศึกษาจุดอ่อนและช่องโหว่ของระบบโทรศัพท์ผ่านอินเตอร์เน็ตที่มีจุดอ่อนในการรักษาความปลอดภัย

1.2.2 เพื่อศึกษาวิธีการโจมตีและใช้ประโยชน์จากช่องโหว่ของระบบโทรศัพท์ผ่านอินเตอร์เน็ต

1.2.3 เพื่อการพัฒนาระบบป้องกันการโจมตีระบบโทรศัพท์ผ่านอินเตอร์เน็ตได้

1.2.4 เพื่อการกำหนดรูปแบบนโยบายความปลอดภัยของระบบโทรศัพท์ผ่านอินเตอร์เน็ตได้

1.3 ขอบเขตของการวิจัย

ผู้วิจัยได้กำหนดขอบเขตของการวิจัยไว้ดังนี้

1.3.1 ศึกษาช่องโหว่หรือจุดอ่อนของระบบโทรศัพท์อินเตอร์เน็ต

1.3.2 ศึกษาวิธีการโจมตีและภัยคุกคามระบบโทรศัพท์อินเตอร์เน็ตในรูปแบบต่างๆ

1.3.3 ศึกษาวิธีป้องกันรักษาความปลอดภัยระบบโทรศัพท์อินเตอร์เน็ต

1.3.4 ศึกษาและพัฒนาระบบป้องกันการโจมตีระบบโทรศัพท์อินเตอร์เน็ตจากระบบเชื่อมต่อสัญญานโทรศัพท์ผ่านอินเตอร์เน็ต

1.3.5 ทำการทดสอบการโจมตีระบบโทรศัพท์อินเตอร์เน็ต

1.3.6 ทำการทดสอบการโจมตีระบบโทรศัพท์อินเตอร์เน็ตผ่านระบบเชื่อมต่อสัญญานโทรศัพท์ผ่านอินเตอร์เน็ต

1.3.7 ทำการเปรียบเทียบผลการทดสอบโจมตีระบบโทรศัพท์อินเตอร์เน็ต

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1.4.1 สามารถทราบถึงช่องโหว่หรือจุดอ่อนของระบบโทรศัพท์อินเตอร์เน็ต

1.4.2 สามารถเข้าใจวิธีการโจมตีและภัยคุกคามระบบโทรศัพท์อินเตอร์เน็ตในรูปแบบต่างๆ จากผู้บุกรุก

1.4.3 สามารถทราบถึงผลกระทบที่เกิดขึ้นระบบโทรศัพท์อินเตอร์เน็ตกรณีระบบถูกโจมตีจากผู้บุกรุก

1.4.4 สามารถเข้าใจวิธีป้องกันรักษาความปลอดภัยระบบโทรศัพท์อินเตอร์เน็ต

1.4.5 สามารถสร้างระบบรักษาความปลอดภัยและป้องกันการโจมตีระบบโทรศัพท์อินเตอร์เน็ต รวมถึงการบริหารจัดการความเสี่ยงบนระบบโทรศัพท์อินเตอร์เน็ต

1.5 ขั้นตอนการศึกษาและวิธีการวิจัย

1.5.1 ศึกษาข้อมูลการทำงานระบบโทรศัพท์ผ่านอินเตอร์เน็ต

1.5.2 ศึกษาข้อมูลช่องโหว่หรือจุดอ่อนของระบบโทรศัพท์อินเตอร์เน็ต

1.5.3 ศึกษาข้อมูลวิธีการโจมตีและภัยคุกคามระบบโทรศัพท์อินเตอร์เน็ตในรูปแบบต่างๆ

1.5.4 ศึกษาข้อมูลวิธีป้องกันรักษาความปลอดภัยระบบโทรศัพท์อินเตอร์เน็ต

1.5.5 พัฒนาปรับปรุงคุณสมบัติระบบป้องกันการโจมตีจากระบบเชื่อมต่อสัญญานโทรศัพท์ผ่านอินเตอร์เน็ต

1.5.6 ติดตั้งระบบโทรศัพท์ผ่านอินเตอร์เน็ตและสร้างข้อมูลบัญชีลูกข่าย (SIP Client) เพื่อรองรับการเชื่อมต่อสัญญานโทรศัพท์ผ่านอินเตอร์เน็ต

1.5.7 ติดตั้งโปรแกรมสื่อสารโทรศัพท์ผ่านอินเตอร์เน็ต(Softphone)

1.5.8 ติดตั้งอุปกรณ์โทรศัพท์ผ่านอินเตอร์เน็ต(IP phone)

1.5.9 ติดตั้งโปรแกรมทดสอบการผู้โจมตีระบบโทรศัพท์ผ่านอินเตอร์เน็ตและพัฒนาคำสั่งสำหรับการโจมตีในรูปแบบที่กำหนด

1.5.10 ติดตั้งโปรแกรมดักจับข้อมูลและแสดงผลการสื่อสารข้อมูลผ่านโครงข่ายอินเตอร์เน็ต

1.5.11 ทดสอบการโจมตีระบบโทรศัพท์ผ่านอินเตอร์เน็ตตามรูปแบบที่กำหนด โดยใช้โปรแกรมทดสอบการผู้โจมตี พร้อมการเก็บข้อมูล เพื่อประเมินผลการกระทบ และสรุปผลการทดสอบ

1.5.12 ทดสอบการโจมตีระบบโทรศัพท์ผ่านอินเตอร์เน็ต โดยใช้โปรแกรมทดสอบการผู้โจมตีผ่านระบบเชื่อมต่อสัญญานโทรศัพท์ผ่านอินเตอร์เน็ตตามรูปแบบที่กำหนด พร้อมการเก็บข้อมูลเพื่อประเมินผลการกระทบ และสรุปผลการทดสอบ

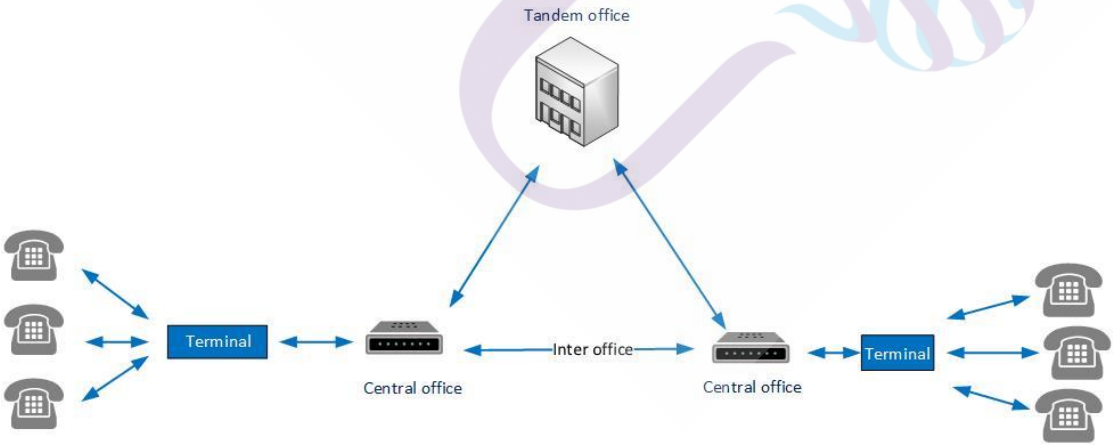
1.5.13 ทำการเปรียบเทียบผลกระทบและสรุปผลการโจมตีในแต่ละรูปแบบ

บทที่ 2
แนวคิด ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ในสารนิพนธ์ฉบับนี้เป็นการศึกษาภัยคุกคามและรักษาความปลอดภัยต่อระบบโทรศัพท์ผ่านอินเตอร์เน็ต (Voice Over Internet Protocol) จะประกอบด้วยข้อมูล แนวคิด ทฤษฎี ข้อมูลพื้นฐาน และงานวิจัยที่เกี่ยวข้องดังนี้

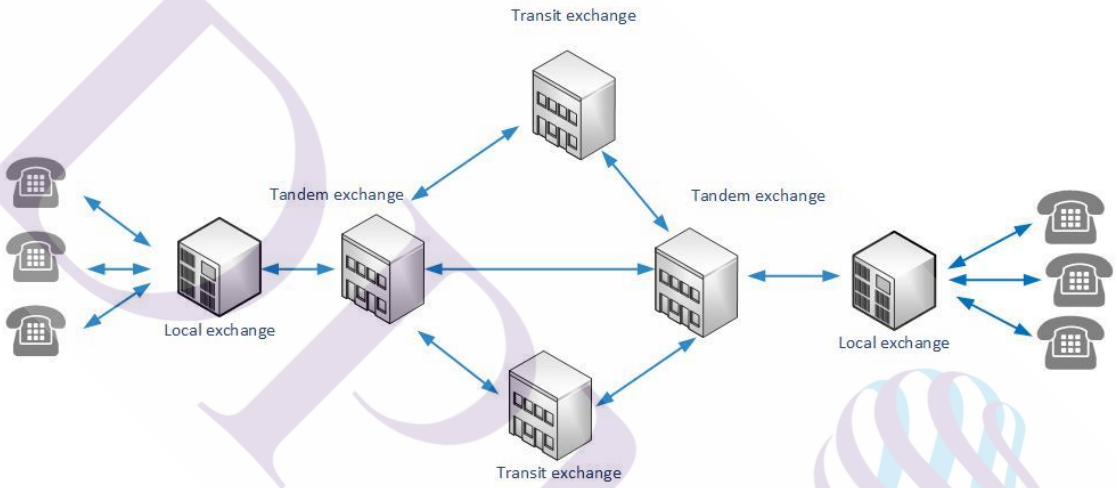
2.1 การสื่อสารโทรศัพท์แบบพื้นฐาน

เทคโนโลยีการสื่อสารโทรศัพท์ในช่วงยุคเริ่มต้น จะใช้หลักการทำงานบนโครงข่ายสื่อสัญญานโทรศัพท์แบบวงจรสวิตช์(Circuit Switched Telephone) จะอาศัยแบบวงจรสลับในการสร้างเส้นทางการติดต่อระหว่างต้นทางไปยังปลายทาง โดยมีชุมสายโทรศัพท์(Central office) ที่มีวงจรสลับติดตั้งและควบคุมการเชื่อมต่อสัญญาน ในการเชื่อมต่อสัญญานแต่ละครั้งเส้นทางการเชื่อมต่อจะถูกจองใช้งานจนกว่าการสื่อสารจะสิ้นสุด ทำให้มีข้อจำกัดในกรณีมีปริมาณการใช้งานเกินจำนวนช่องสัญญานที่ชุมสายโทรศัพท์รองรับได้



ภาพที่ 2.1 โครงข่ายสื่อสัญญานโทรศัพท์แบบวงจรสวิตช์ (Circuit Switched Telephone)

การเปลี่ยนแปลงเทคโนโลยีการสื่อสารโทรศัพท์ถูกพัฒนาเป็นการสื่อสารแบบแพคเกจสวิตช์ (Package switched Telephone) เป็นวิธีการสื่อสารข้อมูลแบบแบ่งกลุ่มข้อมูลเรียกว่าแพคเกจ โดยกำหนดชนิดและโครงสร้างข้อมูล, ข้อกำหนดหรือมาตรฐานที่ใช้ร่วมกัน(Protocol) แล้วส่งผ่านสื่อสัญญานจากต้นทางไปยังปลายทางและสามารถติดต่อสื่อสารได้หลายช่องสัญญานในเวลาเดียวกัน หลักการนี้เรียกว่าการรวมสัญญาณแบบแบ่งเวลา(Time Division Multiplexing) โดยมีชุมสายโทรศัพท์ควบคุมด้วยระบบคอมพิวเตอร์(Store Program Control) ทำหน้าที่บริหารจัดการการเชื่อมต่อแบบอัตโนมัติ ทำให้มีความรวดเร็ว แม่นยำในการเชื่อมต่อ รวมถึงรองรับปริมาณการใช้งานสูงได้



ภาพที่ 2.2 โครงข่ายสื่อสัญญานโทรศัพท์แบบแพคเกจสวิตช์ (Package switched Telephone)

ในส่วนระบบชุมสายโทรศัพท์ยังได้มีการพัฒนาเป็นระบบชุมสายโทรศัพท์แบบเครือข่ายดิจิตอลร่วม (Integrated Service Digital Network :ISDN) เพื่อให้มีขีดความสามารถเพิ่มเติมจาการสื่อสารเสียง เป็นการสื่อสารข้อมูล ภาพเคลื่อนไหว การประชุมทางไกลผ่านจอภาพ การให้บริการอินเตอร์เน็ตความเร็วสูงเป็นต้น ทั้งนี้ระบบชุมสายโทรศัพท์แบบเครือข่ายยุคใหม่ (Next Generation Network) หรือซอฟต์สวิตช์ (Soft switch) ที่ซึ่งอาศัยการสื่อสารบนโครงข่ายของอินเตอร์เน็ต (Internet protocol) ได้ถูกนำมาใช้งานในยุคของการสื่อสารอินเตอร์ความเร็วสูงเป็นความต้องการขั้นพื้นฐาน โดยยังคงรูปแบบบริการของโทรศัพท์ไว้เหมือนเดิมและเพิ่มคุณสมบัติอย่างอื่นที่ตอบโจทย์การสื่อสารข้อมูลหลากหลายมากขึ้น เช่น ข้อมูล ภาพเคลื่อนไหว บริการอื่นๆ ที่มาจากช่องทางการสื่อสารข้อมูลผ่านอินเตอร์เน็ต เช่นการโทรศัพท์ผ่านเว็บเป็นต้น

2.2 การสื่อสารโทรศัพท์ผ่านอินเตอร์เน็ต

การสื่อสารโทรศัพท์ผ่านอินเตอร์เน็ต เป็นการปรับเปลี่ยนรูปแบบและวิธีการสื่อสารโทรศัพท์ โดยอาศัยเครือข่ายอินเทอร์เน็ต(Internet protocol) เป็นตัวกลางในการสื่อสารข้อมูลเสียง ซึ่งจะต้องใช้อุปกรณ์(Hardware) หรือโปรแกรม(Software) ที่มีการใช้มาตรฐานการสื่อสาร (Protocol) ที่สามารถทำงานเข้ากันได้ทำการส่งสัญญาณโทรศัพท์จากต้นทางไปยังปลายทาง ดังข้อมูลข้างต้นการโทรศัพท์ผ่านอินเตอร์เน็ตมีลำดับชั้นของการสื่อสารเหมือนกับการสื่อสารข้อมูลผ่านอินเทอร์เน็ตที่เป็น ISO Model (Open Systems Interconnection Model) โดยมีข้อมูลเปรียบเทียบดังนี้

ภาพที่ 2.3 แสดงลำดับชั้นการสื่อสารข้อมูลโทรศัพท์ผ่านอินเตอร์เน็ตกับ ISO Model

2.2.1 มาตรฐานการสื่อสารโทรศัพท์ผ่านอินเตอร์เน็ต (VOIP Protocol)

ในการสื่อสารข้อมูลจะต้องมีการกำหนดรูปแบบข้อมูล ข้อกำหนดต่างๆที่ให้ผู้สื่อสารและผู้รับสารได้เข้าใจและแปลความหมายให้ตรงกัน ในส่วนการสื่อสารโทรศัพท์ผ่านอินเตอร์เน็ตได้กำหนดมาตรฐานการสื่อสารในหัวข้อวิจัยจะกล่าวถึงมาตรฐานที่นิยมใช้กันทั่วไปดังนี้

2.2.1.1 มาตรฐานแบบ H.323(H323)

เป็นมาตรฐานที่สหภาพโทรคมนาคมระหว่างประเทศ(International Telecommunications Union : ITU) เป็นผู้กำหนดคุณสมบัติทางเทคนิคสำหรับการสื่อสารด้านเสียงบนเครือข่ายท้องถิ่น(Local Area Network) ซึ่งจะไม่มีข้อกำหนดในด้านคุณภาพของการให้บริการ (Quality of Service : QOS) และเป็นจุดเริ่มต้นของการพัฒนาสำหรับการประชุมเสียง วีดีโอ ภาพบนเครือข่ายท้องถิ่น(Local Area Network) มาตรฐานแบบ H.323 ถูกพัฒนาต่อขยายเพื่อครอบคลุมการสื่อสารโทรศัพท์ผ่านอินเตอร์เน็ตในภายหลัง

ส่วนประกอบของ มาตรฐานแบบ H.323 สำหรับรองรับการเชื่อมต่อสัญญานมีดังนี้

- อุปกรณ์ต้นทางหรือปลายทาง(Terminals) สำหรับการสื่อสารแบบ 2 ทาง ของข้อมูล เสียง วีดีโอ ทำหน้าที่ติดต่อรับคำสั่งและแสดงผลกับผู้ใช้งาน

- เกตเวย์(Gateways) เป็นอุปกรณ์สำหรับรองรับการเชื่อมต่อระหว่างอุปกรณ์อื่นที่อยู่บนเครือข่าย แบบ H.323 หรือ ปรับเปลี่ยนรูปแบบสัญญาน ข้อมูล เพื่อเชื่อมต่อกับโครงข่ายสื่อสัญญานโทรศัพท์แบบแพคเกจสวิตช์ (Package switched Telephone)

- เกตคีปเปอร์(Gatekeepers) เป็นอุปกรณ์ที่มีความสำคัญสำหรับการสื่อสารโทรศัพท์แบบ H.323 ทำหน้าที่บริหารจัดการ ควบคุม ตรวจสอบและยืนยันการลงทะเบียนใช้งานรักษาความปลอดภัย ควบคุมปริมาณข้อมูลของอุปกรณ์แบบ H.323 ภายใต้พื้นที่การให้บริการของเกตคีปเปอร์ (Gatekeepers) นอกจากนี้ยังทำหน้าที่ตามมาตรฐานแบบ H.323 ดังนี้

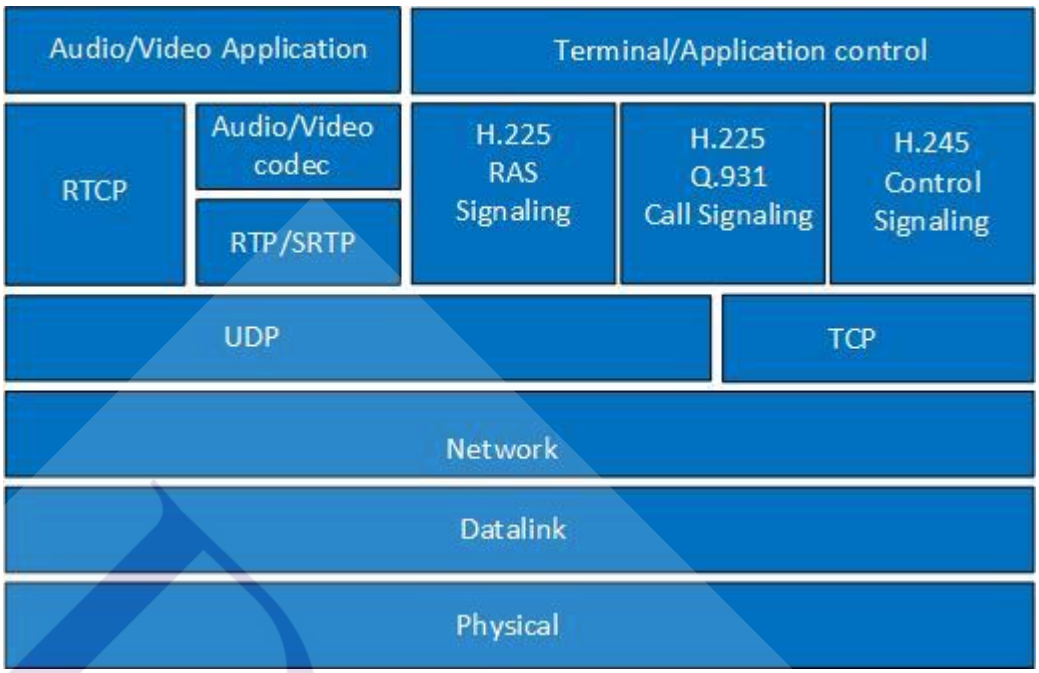
- การแปลงแอดเดรส (Address translation) เกตคีปเปอร์ (Gatekeepers) แปลง alias addressให้เป็น transport address อุปกรณ์จะทำการส่ง alias พร้อมกับการลงทะเบียน
- การควบคุมการเข้า/ออก (Admission control) ภายในโซนโดยจะทำการตรวจสอบจากเงื่อนไขต่างๆ เช่น การยืนยันตัวตน แบนด์วิดท์ ต้นทาง/ปลายของที่อยู่ หรือเงื่อนไขอื่นตามที่กำหนด
- การควบคุมแบนด์วิดท์ (Bandwidth control) อนุญาตหรือไม่อนุญาตการร้องขอแบนด์วิดท์จากอุปกรณ์ที่เชื่อมต่อ
- การจัดการโซน (Zone management and Directory service) ทำหน้าที่ในการดูแลและจัดการให้ลงทะเบียนกับทุกอุปกรณ์ H.323 ที่อยู่ในภายในโซน
- การควบคุมการส่งสัญญาณ (call control signaling) ในการส่งระหว่างอุปกรณ์ต้นทางหรือปลายทาง(Terminals)
- การอนุญาต (Call Authorization) ในการเชื่อมต่อการเข้าถึงอุปกรณ์ H.323 ตามเงื่อนไขที่กำหนดหรือตามช่วงเวลา

- การจัดการสัญญาน(Call Management) ทำการควบคุม คงสภาพรายการเชื่อมต่อของสัญญานที่เกิดขึ้นบนอุปกรณ์ H.323 ทั้งหมด
- หน่วยควบคุมการเชื่อมต่อหลายจุด (Multipoint Control Unit : MCU) ทำหน้าที่ควบคุม จัดการการเชื่อมต่อสัญญานประชุมแบบเสียง วีดีโอ จากหลายอุปกรณ์ตั้งแต่ 3 อุปกรณ์ ขึ้นไปและทำหน้าที่ในการผสม (multiplexing) เสียง วีดีโอ ข้อมูล

ลำดับชั้น (Protocol stack) ของมาตรฐานแบบ H.323

- ลำดับชั้นของการสื่อสารมาตรฐานแบบ H.323 จะอ้างอิงตามรูปแบบการสื่อสารข้อมูลผ่านอินเทอร์เน็ต มีส่วนประกอบที่สำคัญดังนี้

- ส่วนการควบคุมการสื่อสาร(Application control) โดยมีส่วนประกอบย่อยดังนี้
- H.225 RAS Signaling เป็นส่วนควบคุมสัญญาณเชื่อมต่อเพื่อลงทะเบียนการอุปกรณ์ต้นทางหรือปลายทาง (Terminals)
- H.225/Q.931 Call Signaling เป็นส่วนเพื่อสร้างการเชื่อมต่อควบคุมการรับส่งข้อมูลให้เหมาะสม รวมถึงการแปลงข้อมูล เสียง วีดีโอ
- H.245 Control Signaling เป็นส่วนจัดการสร้างเส้นทางสำหรับ ควบคุมการ แลกเปลี่ยนข้อมูล ในแต่ต้นทางและปลายทางทีเชื่อมต่อ
- ส่วนการประมวลผลข้อมูลเสียงและวีดีโอ(Audio/Video Application) โดยมีส่วนประกอบย่อยดังนี้
- Real-time Transport Protocol (RTP) เป็นส่วนควบคุมรับส่งข้อมูลเสียงวีดีโอบนเครือข่ายอินเตอร์เน็ต
- Secure Real-time Transport Protocol (SRTP) เป็นส่วนควบคุมรับส่งข้อมูลเสียง วีดีโอบนเครือข่ายอินเตอร์เน็ตที่มีการเข้ารหัสเพื่อรักษาความปลอดภัย
- Real-Time Transport Control Protocol (RTCP) เป็นส่วนที่ทำงานร่วมกับ Real-time Transport Protocol (RTP) เพื่อเก็บข้อมูลและควบคุมการเชื่อมต่อ เสียงและวีดีโอ
- Audio/Video codec เป็นการเข้ารหัสเสียงตามมาตรฐานของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) เช่น G.711, G.729, G.723 และการเข้ารหัสวีดีโอ เช่น VP8, MPEG4, H263, H264 เป็นต้น

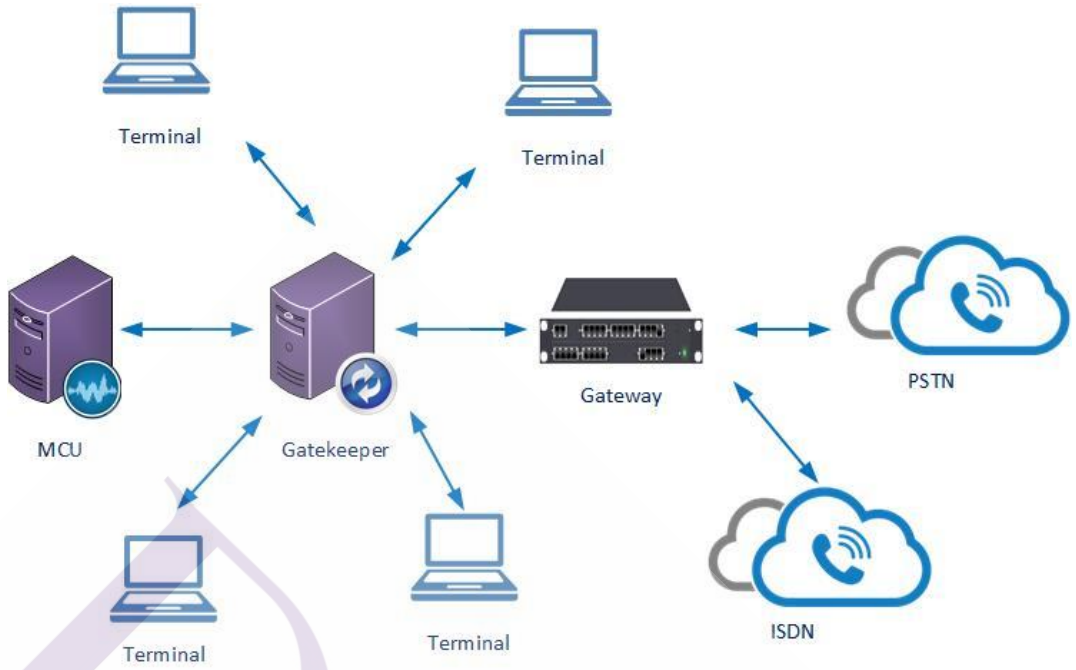


ภาพที่ 2.4 แสดงลำดับชั้นการสื่อสารข้อมูลมาตรฐานแบบ H.323 (Protocol stack)

การเชื่อมต่อ(Network Connection) ของ มาตรฐานแบบ H.323

- ส่วนประกอบของระบบในการเชื่อมต่อตามมาตรฐานแบบ H.323 มีดังนี้

  - เกตคีปเปอร์ (Gatekeepers) เป็นอุปกรณ์หลักในการจัดการการเชื่อมต่อ
  - อุปกรณ์ต้นทางหรือปลายทาง(Terminals) เป็นเครื่องลูกข่ายในระบบ
  - เกตเวย์(Gateways) ทำหน้าที่เป็นอุปกรณ์แปลงสัญญานการสื่อสารโทรศัพท์ให้เป็นแบบแบบแพคเกจสวิตช์ (Package switched Telephone) เพื่อเชื่อมต่อกับโครงข่ายโทรศัพท์สาธารณะ (Public System Telephone Network : PSTN) หรือตู้ชุมสายโทรศัพท์แบบเครือข่ายดิจิตอลร่วม (Integrated Service Digital Network :ISDN)
  - หน่วยควบคุมการเชื่อมต่อหลายจุด(Multipoint Control Unit : MCU) บริหารจัดการข้อมูลประชุมแบบเสียงและวีดีโอ



ภาพที่ 2.5 แสดงการเชื่อมต่อ(Network Connection) ของมาตรฐานแบบ H.323

การสื่อสัญญาณและควบคุมแบบ H.323 (Control and signaling)

- มีมาตรฐาน(Protocol) ที่เป็นส่วนประกอบที่ทำหน้าที่ควบคุมการส่งสัญญานและควบคุมการทำงานดังนี้

- H.225.0 RAS เป็นมาตรฐาน (Protocol) สำหรับการสร้างการเชื่อมต่อระหว่าง อุปกรณ์ต้นทางหรือปลายทาง (Terminals) และเกตคีปเปอร์ (Gatekeepers) ที่ทำหน้าที่ดังนี้

- ค้นหาเกตคีปเปอร์ (Gatekeeper discovery) ที่จะทำการลงทะเบียน
- ทำการลงทะเบียน (Endpoint registration) ให้กับอุปกรณ์ต้นทางหรือปลายทาง(Terminals)
- เก็บข้อมูลที่อยู่(Endpoint location) ของอุปกรณ์ต้นทางหรือปลายทาง (Terminals)
- ควบคุมการเข้าถึง(Admission control) การเปลี่ยนแปลงสถานะ การปฏิเสธการร้องรอใช้งาน แบนด์วิดท์

- H.225/Q.931 Call Signaling เป็นมาตรฐาน(Protocol) สำหรับสัญญาณการสื่อสารเพื่อสร้างการเชื่อมต่อโดยดัดแปลงมาจากมาตรฐาน(Protocol) Q.931 เป็นการส่งข้อมูลผ่าน TCP ทำหน้าที่ควบคุมการรับส่งข้อมูลให้เหมาะสม รวมถึงการแปลงข้อมูล เสียง วีดีโอด้วย
- H.245 เป็นมาตรฐาน(Protocol) ที่ใช้ควบคุมข้อมูลเสียง วีดีโอ ที่ใช้สื่อสาร จัดการ สร้างเส้นทางสำหรับ ควบคุม การ แลกเปลี่ยนข้อมูล ในแต่ต้นทางและปลายทางที่เชื่อมต่อ

2.2.1.2 มาตรฐานแบบ Session Initial Protocol (SIP)

เป็นมาตรฐานที่คณะทำงานเฉพาะกิจด้านวิศวกรรมอินเทอร์เน็ต (Internet Engineering Task Force: IETF) เป็นผู้พัฒนาสำหรับการสื่อสารข้อมูลเสียง วีดีโอบนเครือข่ายอินเตอร์เน็ต กำหนดในข้อกำหนด RFC3161 ซึ่งจะมีลักษณะการทำงานเหมือนกับมาตรฐาน HTTP (Hyper Text Transfer Protocol) ในส่วนของการเชื่อมต่อจากเครื่องลูกข่ายไปเครื่องแม่ข่าย(Client-Server) โดยการร้องขอการเชื่อมต่อ (Request) และการตอบกลับ(Response) อีกทั้งมาตรฐาน แบบ Session Initial Protocol (SIP) ยังมีการใช้ข้อมูลส่วนหัว (Header), วิธีการเข้ารหัสขอมูล (Encryption) และสถานการณ์สื่อสารข้อมูล(Status code) เหมือนกันอีกด้วย โดยจะมี Session Description Protocol (SDP) เป็นตัวกำหนดรายละเอียดในการเชื่อมต่อ(Session) และใช้ Real time Transfer Protocol (RTP) ในการควบคุมรับส่งข้อมูลเสียง วีดีโอบนเครือข่ายอินเตอร์เน็ต

ส่วนประกอบของมาตรฐานแบบ Session initial protocol(SIP)

- User Agent(UA) ส่วนของผู้ใช้งานที่เป็นอุปกรณ์หรือโปรแกรมที่ทำหน้าที่รับส่งข้อความ และจัดการการเชื่อมต่อโดยสามาทำงานได้ 2 แบบ คือ

- User Agent Client (UAC) ผู้ใช้งานส่วนที่ส่งการร้องขอ (Request) ขอเชื่อมต่อปลายทางที่เป็น User Agent SERVER(UAS) ซึ่งเป็นแม่ข่ายผู้ใช้งาน

- User Agent Server (UAS) เป็นแม่ข่ายผู้ใช้งาน จะรับการร้องขอ (Request) และตอบกลับ(Response) ข้อมูลไปหา User Agent Client (UAC)

- Network Server เป็นส่วนแม่ข่ายซึ่งมีความแตกต่างตามรูปแบบการทำงาน 3 แบบ ดังนี้

- Proxy Server เป็นแม่ข่ายที่รับการร้องขอ (Request) จาก User Agent (UA) และส่งต่อไปยัง User Agent (UA) อื่น ทำหน้าที่ส่งต่อข้อมูลไปยังปลายทาง โดยจะมีการทำงานอยู่ 2 แบบ คือ Stateless Proxy Server ทำหน้าที่รับส่งข้อมูลอย่างเดียว และ State full Proxy Server ทำการรับส่งข้อมูลและเก็บข้อมูลการเชื่อมต่อไว้เพื่อใช้ทำงานอื่น เช่นการส่งข้อมูลซ้ำ การเปลี่ยนปลายทางที่จะส่งข้อมูลเป็นต้น

- Registrar Server เป็นแม่ข่ายที่รับการร้องขอลงทะเบียน (Request Register) จาก User Agent (UA) ทำการตรวจสอบสิทธิ บันทึกข้อมูลตำแหน่งที่อยู่ ข้อมูล Uniform Resource Identifier (URI) ลงบนระบบฐานข้อมูล

- Redirect Server เป็นแม่ข่ายทำหน้าที่รับการร้องขอ (Request) จาก User Agent (UA) ทำการตรวจสอบเส้นทางถัดไปและตอบกลับตำแหน่งที่อยู่ให้กับ User Agent (UA)

2.2.1.3 SIP Messages เป็นข้อมูลหรือคำสั่งที่ใช้สำหรับสื่อสารระหว่าง User Agent (UA) และ Network Server มีดังนี้

- INVITE : คำสั่งสำหรับเริ่มต้นการเชื่อมต่อสัญญานและเสียงสนทนา

- BYE : คำสั่งในสิ้นสุดการเชื่อมต่อระหว่างอุปกรณ์ต้นทางกับปลายทางที่มีการเชื่อมต่อเรียบร้อยแล้ว

- ACK : คำสั่งตอบกลับคำสั่ง INVITE

- OPTIONS : คำสั่งที่ใช้ค้นหาข้อมูลของ User Agent หรือข้อมูลของ Network Server

- REGISTER : คำสั่งสำหรับ User Agent ทำการลงทะเบียนกับ Network serves แบบ Register Server

- CANCEL : คำส่งยกเลิกการร้องขอการเชื่อมต่อในกรณีที่การเชื่อมต่อยังไม่สำเร็จ

- SUBSCRIBE : คำสั่งที่ User agent ใช้เพื่อรับการแจ้งเตือนระหว่างต้นอุปกรณ์ต้นทางกับปลายทาง

- NOTIFY : คำสั่งที่ User agent ใช้แจ้งเหตุการณ์

- PUBLISH : คำสั่งเพื่อใช้แจ้งเหตุการณ์ต่างๆไปที่ Network Server

- REFER : คำสั่งใช้สำหรับโอนสาย

- INFO : คำสั่งส่งข้อมูลโดยไม่แก้ไขสถานการเชื่อมต่อ

- UPDATE : คำสั่งส่งข้อมูลเพื่อแก้ไขสถานการเชื่อมต่อแต่ไม่เปลี่ยนสถานะการทำงาน

- PRACK : คำสั่งเพิ่มความน่าเชื่อถือในการตอบกลับของ SIP MESSSAGE

2.2.1.4 ลำดับชั้น (Protocol Stack) ของมาตรฐานแบบ Session Initial Protocol (SIP)

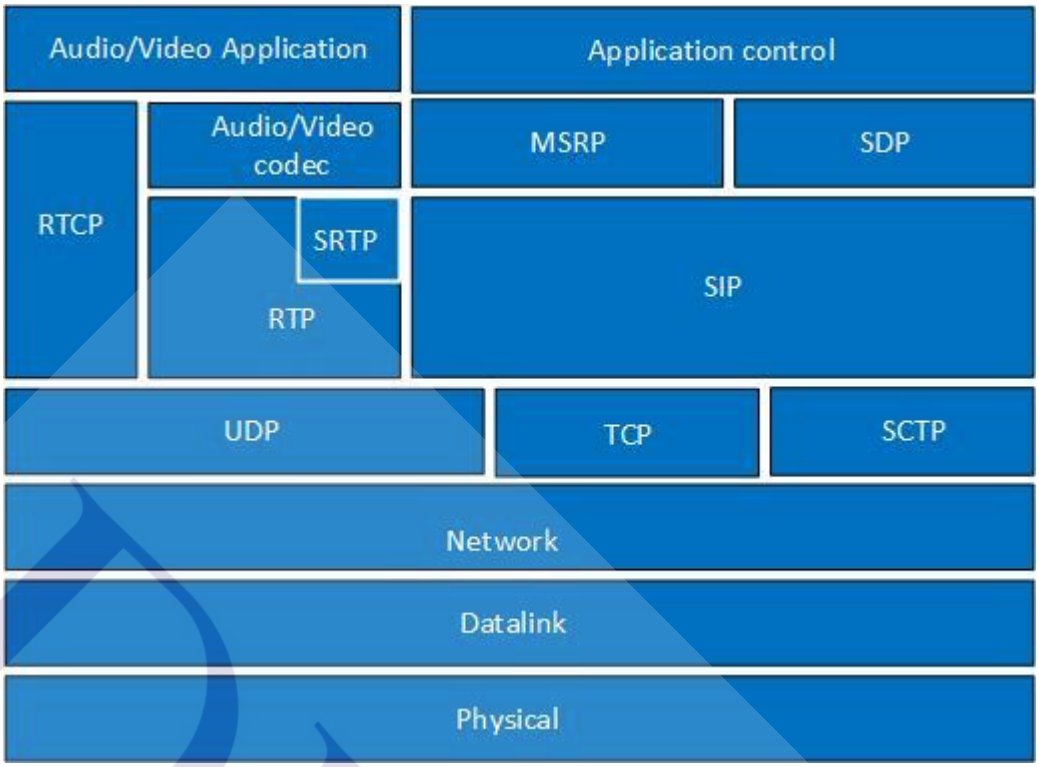
ลำดับชั้นของการสื่อสารมาตรฐานแบบ Session Initial Protocol (SIP) จะอ้างอิงตามรูปแบบการสื่อสารข้อมูลผ่านอินเทอร์เน็ต มีส่วนประกอบสำคัญ 2 ส่วนคือ

- ส่วนการควบคุมการสื่อสาร(Application control) โดยมีส่วนประกอบย่อยดังนี้

  - Session Initial Protocol(SIP) เป็นส่วนควบคุมการเชื่อมต่อสัญญาณ
  - Message Session Relay Protocol(MSRP) เป็นมาตรฐานในการรับส่งข้อความบนเครือข่ายอินเตอร์เน็ต
  - Session Description Protocol(SDP) เป็นส่วนกำหนดรายละเอียดในการเชื่อมต่อ (Session)

- ส่วนการประมวลผลข้อมูลเสียงและวีดีโอ (Audio/Video Application) โดยมีส่วนประกอบย่อยดังนี้

  - Real-time Transport Protocol(RTP) เป็นส่วนควบคุมรับส่งข้อมูลเสียง วีดีโอบนเครือข่ายอินเตอร์เน็ต
  - Secure Real-time Transport Protocol(SRTP) เป็นส่วนควบคุมรับส่งข้อมูลเสียง วีดีโอบนเครือข่ายอินเตอร์เน็ตที่มีการเข้ารหัสเพื่อรักษาความปลอดภัย
  - Real-Time Transport Control Protocol(RTCP) เป็นส่วนที่ทำงานร่วมกับ Real-time Transport Protocol(RTP) เพื่อเก็บข้อมูลและควบคุมการเชื่อมต่อ เสียงและวีดีโอ
  - Audio/Video codec เป็นการเข้ารหัสเสียงตามมาตรฐานของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) เช่น G.711, G.729, G.723 และการเข้ารหัสวีดีโอ เช่น VP8, MPEG4, H263, H264 เป็นต้น

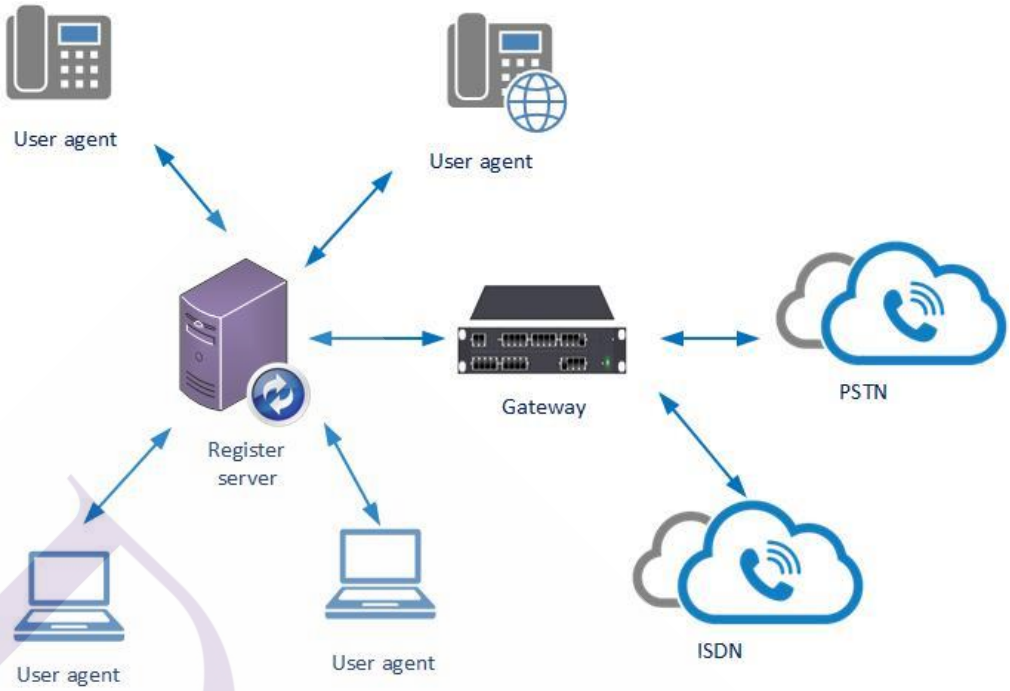


ภาพที่ 2.6 แสดงลำดับชั้นการสื่อสารข้อมูลมาตรฐานแบบ Session Initial Protocol (SIP)

2.2.1.5 การเชื่อมต่อ (Network Connection) ของมาตรฐานแบบ Session Initial Protocol (SIP)

- ส่วนประกอบของระบบตามมาตรฐานแบบ Session Initial Protocol(SIP) มีดังนี้

  - Registrar Server เป็นแม่ข่ายที่รับการร้องขอลงทะเบียนของ User Agent(UA) เป็นอุปกรณ์หลักในการจัดการการเชื่อมต่อทั้งหมด
  - User Agent(UA) เป็นเครื่องลูกข่ายในระบบ
  - เกตเวย์ (Gateways) ทำหน้าที่เป็นอุปกรณ์แปลงสัญญานการสื่อสารโทรศัพท์ให้เป็นแบบแบบแพคเกจสวิตช์ (Package switched Telephone) เพื่อเชื่อมต่อกับโครงข่ายโทรศัพท์สาธารณะ (Public System Telephone Network : PSTN) หรือ ตู้ชุมสายโทรศัพท์แบบเครือข่ายดิจิตอลร่วม (Integrated Service Digital Network :ISDN)



ภาพที่ 2.7 แสดงการเชื่อมต่อ (Network Connection) ของมาตรฐานแบบ Session Initial Protocol (SIP)

2.3 ปัญหาของการสื่อสารโทรศัพท์ผ่านอินเตอร์เน็ต

แม้ในปัจจุบันการสื่อสารโทรศัพท์ผ่านอินเตอร์เน็ตได้รับความนิยมเป็นอย่างมาก แต่ยังคงมีปัญหาหลายอย่างที่จะต้องได้รับการแก้ไขโดยสาเหตุของระบบเครือข่ายอินเตอร์เน็ต ซึ่งเป็นโครงข่ายพื้นฐานในการให้บริการ ระบบโทรศัพท์ผ่านอินเตอร์เน็ต การรักษาความปลอดภัย และมาตรฐานการเชื่อมต่อโดยมีรายละเอียดดังนี้

2.3.1 คุณภาพของการบริการ(Quality of service) เครือข่ายอินเตอร์เน็ตถูกพัฒนาเพื่อการสื่อสารข้อมูล ซึ่งไม่มีการรับประกันเรื่องเวลาการให้บริการ แต่จะเป็นการทำงานโดยใช้ความเหมาะสม หรือความเป็นไปได้สูงสุดของบริการ แต่การให้การสื่อสารโทรศัพท์เป็นการสื่อสารที่มีการตอบสนองแบบทันที (Real time) ดังนั้นเพื่อให้มีการยอมรับของผู้ใช้งานระยะเวลาการส่งข้อมูลเสียงจะต้องไม่ต่ำค่าสุดที่กำหนดไว้ และต้องเป็นไปข้อกำหนดของ มาตรฐานที่คณะทำงานเฉพาะกิจด้านวิศวกรรมอินเทอร์เน็ต (Internet Engineering Task Force: IETF) รวมถึงการจัดลำดับความสำคัญของการส่งข้อมูล(Packet Prioritization) ก็มีผลต่อคุณภาพของการให้บริการเช่นกัน

2.3.2 การทำงานร่วมกันของมาตรฐานการสื่อสาร(Interoperability) ในการเชื่อมต่อระบบโทรศัพท์ผ่านอินเตอร์เน็ตผ่านโครงข่ายที่แตกต่าง และมีผลิตภัณฑ์ต่างยี่ห้อเพื่อที่จะทำให้อุปกรณ์สามารถเชื่อมต่อกันได้ จึงมีความจำเป็นที่จะต้องกำหนดให้เจ้าของผลิตภัณฑ์ทำการพัฒนาไปในแนวทางที่ IETF กำหนด ซึ่งปัญหาดังกล่าวนี้จะพบได้มากในช่วงเริ่มต้นของการระบบโทรศัพท์ผ่านอินเตอร์เน็ต

2.3.3 ความปลอดภัยของบริการ(Security) ปัญหาหลักจากสื่อสารข้อมูลบนโครงข่ายอินเตอร์เน็ต ซึ่งสามารถดักจับข้อมูลได้ง่าย ดังนั้นการเพิ่มความปลอดภัย,การเข้ารหัสข้อมูลของ, การป้องกันการโจมตีระบบโทรศัพท์ผ่านอินเตอร์เน็ตก็จะทำให้บริการมีความเชื่อถือมากขึ้น

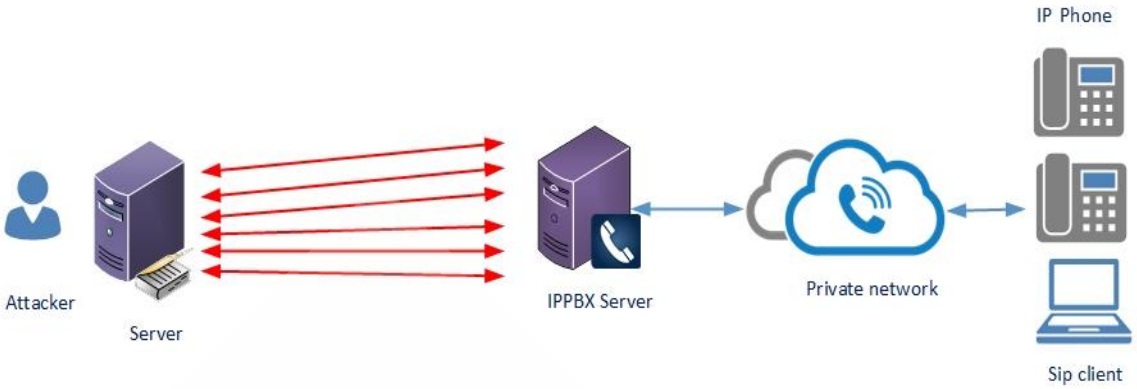
2.3.4 การเชื่อมต่อกับระบบโทรศัพท์สาธารณะ (PSTN Integration) ในการใช้งานระบบโทรศัพท์ผ่านอินเตอร์เน็ตยังเป็นการใช้บริการเฉพาะส่วนดังนั้นการเชื่อมต่อกับระบบโทรศัพท์สาธารณะจำเป็นต้องมีอุปกรณ์แปลงสัญญานการสื่อสารโทรศัพท์ให้เป็นแบบแพคเกจสวิตช์ (Package switched Telephone) เหมือนกับมาตรฐาน H.323

2.3.5 การขยายระบบ (Scalability)ในการให้บริการระบบโทรศัพท์ผ่านอินเตอร์เน็ตมีค่าใช้จ่ายที่ต่ำ ถ้าสามารถควบคุมคุณภาพของการให้บริการได้เทียบเท่ากับการสื่อสารโทรศัพท์แบบแพคเกจสวิตช์ (Package switched Telephone) การขยายโครงข่ายโทรศัพท์ผ่านอินเตอร์เน็ตสำหรับส่วนตัวและสาธารณะก็จะได้รับความนิยมมากยิ่งขึ้น ดังเช่นปัจจุบันในประเทศไทยมีบริการอินเตอร์เน็ตความเร็วสูงครอบคลุมพื้นที่สำคัญทางธุรกิจ การสื่อสารในรูปแบบอื่นๆ ที่อาศัยอินเตอร์เน็ต รวมถึงระบบโทรศัพท์อินเตอร์เน็ตก็จะถูกใช้บริการมากขึ้น

2.4 ภัยคุกคามของระบบโทรศัพท์ผ่านอินเตอร์เน็ต

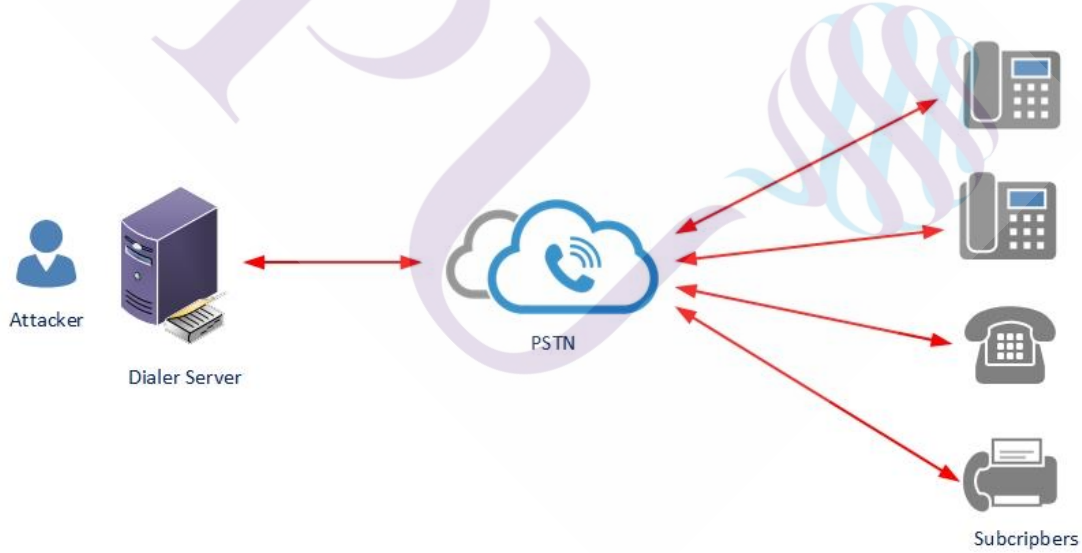
รูปแบบภัยคุกคามต่อระบบโทรศัพท์ผ่านอินเตอร์เน็ตมีรูปแบบหลักๆดังนี้

2.4.1 การคุกคามแบบ Denial of Service (DoS) เป็นภัยคุกคามที่โจมตีต่อระบบโดยใช้อุปกรณ์โจมตีเครื่องเดียว หรือหลายๆเครื่องพร้อมกันโดยส่งคำสั่งไปที่เครื่องคอมพิวเตอร์แม่ข่าย (SERVER) เพื่อระบบมีการรับคำสั่งจำนวนมากพร้อมกันทำให้มีการใช้ทรัพยากรในระบบเกินข้อจำกัด มีผลทำให้ระบบทำงานช้าลง คุณภาพเสียงไม่ดี ไม่ตอบสนองต่อผู้ใช้งานจริง และไม่สามารถให้บริการได้ในที่สุด ตัวอย่างเช่น การโทรเข้าระบบพร้อมกันเกินจำนวนคู่สายทำให้ผู้ใช้งานจริงโทรไม่ได้ หรือการส่งคำสั่งบางอย่างเช่น SIP Options ,SIP Register, SIP INVITE มาจำนวนมากทำให้ระบบต้องทรัพยากรจำนวนมากต่อการตอบสนองต่อคำสั่งที่เข้ามาจำนวนมากมีผลทำให้เกิดสภาวะความแออัดของการเชื่อมต่อ(Congestion) มีผลให้ระบบทำงานผิดปกติและไม่สามารถให้บริการได้ในที่สุด



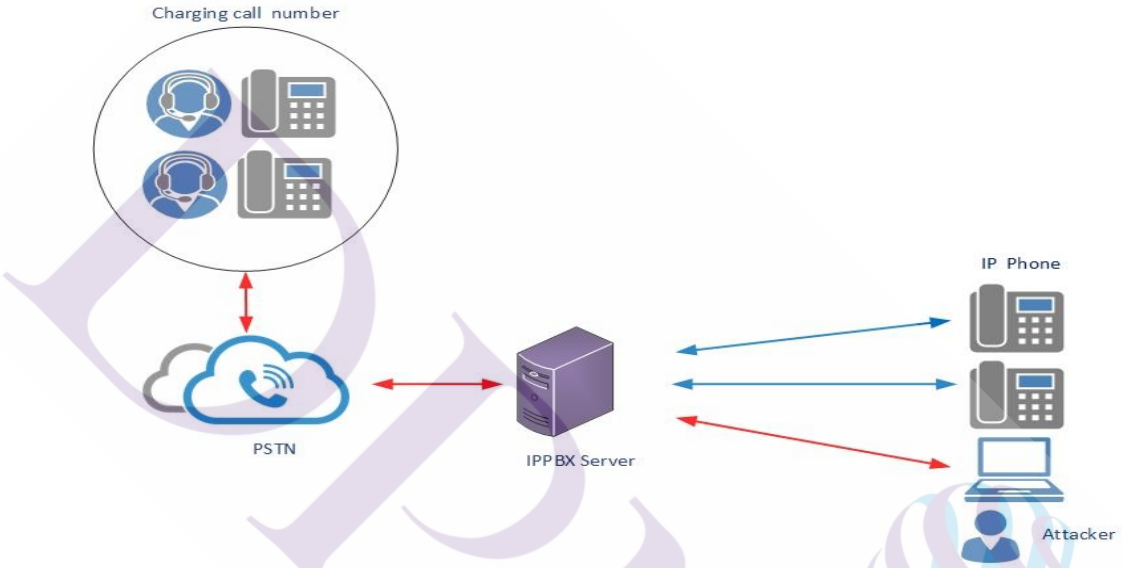
ภาพที่ 2.8 การคุกคามแบบ Denial of Service (DoS)

2.4.2 การคุมคามแบบ War dialing เป็นภัยคุกคามที่เข้าควบคุมระบบโทรศัพท์(IPPBX) โดยทำการค้นหา กำหนดหรือสุ่ม โทรไปยังหมายเลขโทรศัพท์ที่กำหนดโดยอัตโนมัติ ค้นหาและตรวจสอบสัญญานที่เป็นโมเด็ม คอมพิวเตอร์ โทรสาร ซึ่งผู้คุกคามอาจจะนำผลที่ได้ไปสร้างภัยคุมคามอย่างอื่นได้ อีกทั้งเป็นการรบกวนและสร้างความรำคาญผู้ใช้บริการในการรับโทรศัพท์จากปลายทางที่ไม่ใช่ผู้ติดต่อจริง และยังผลให้คู่สายถูกใช้งานโดยไม่เกิดประโยชน์ใดๆ



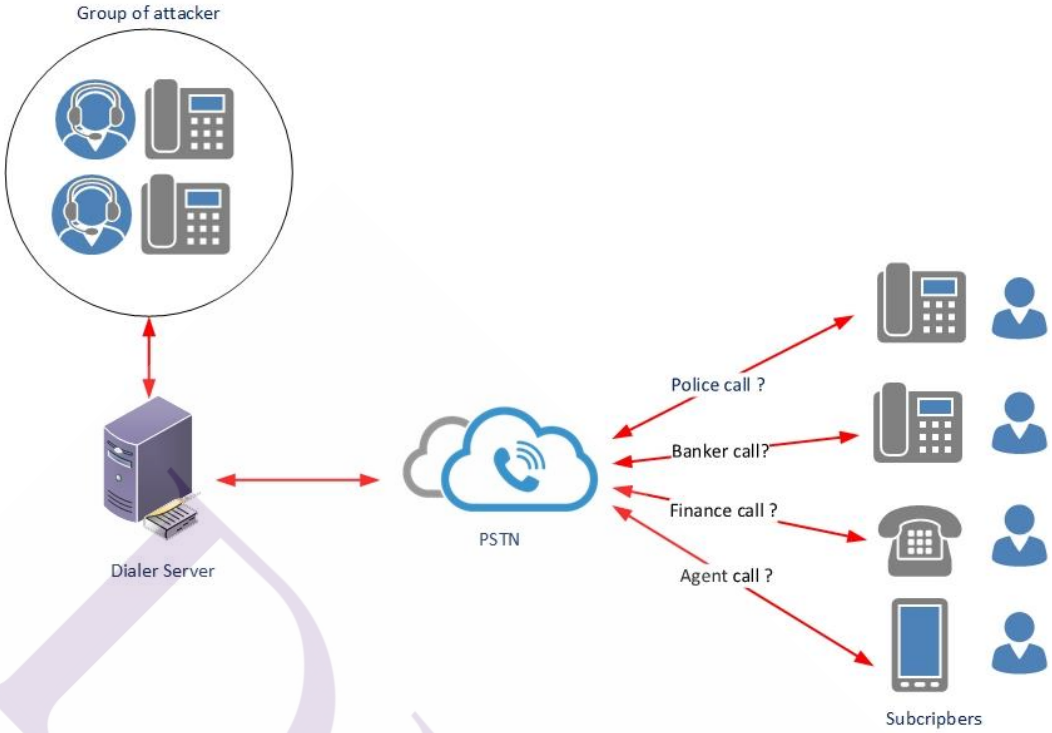
ภาพที่ 2.9 การคุมคามแบบ War dialing

2.4.3 การคุกคามแบบ Toll fraud เป็นภัยคุกคามที่มีลักษณะเหมือน War dialing แต่จะเป็นการอาศัยระบบโทรศัพท์(IPPBX) ในการโทรออกไปยังเลขหมายภายนอก หรือโทรไปยังต่างประเทศที่มีการเรียกเก็บเงินปลายทางที่มีอัตราค่าบริการต่อนาทีสูง ซึ่งภัยคุกคามแบบจะทำให้เกิดความเสียหายต่อองค์กรณ์ที่ทำให้ถูกเรียกเก็บค่าบริการโทรศัพท์จากผู้รับปลายทางโดยไม่ได้ใช้งานจริง หรือทำให้ผู้ใช้งานจริงโทรศัพท์ออกภายนอกไม่ได้กรณีถูกคุกคามแบบ Toll fraud จนเกินวงเงินค่าบริการ



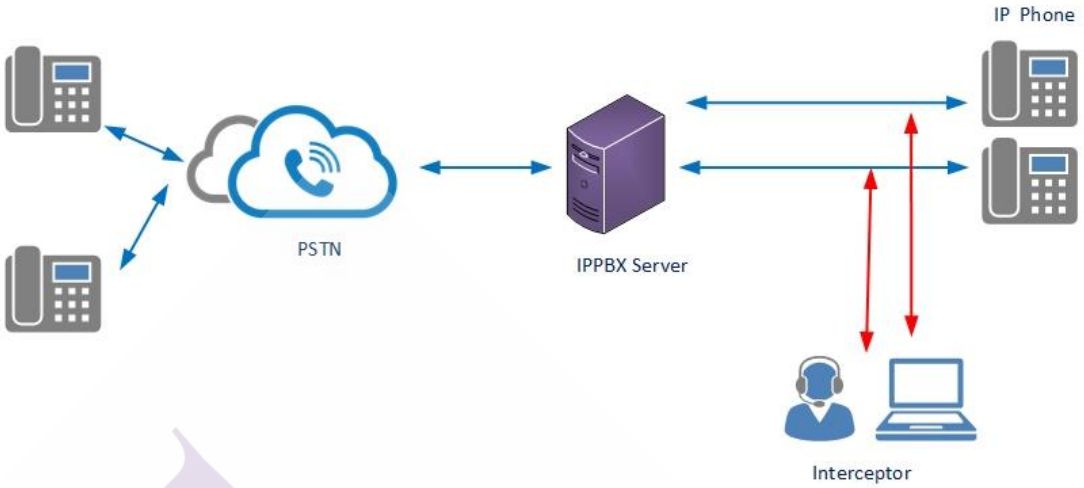
ภาพที่ 2.10 การคุกคามแบบ Toll fraud

2.4.4 การคุกคามแบบ Phishing เป็นภัยคุกคามที่มีการโทรศัพท์ติดต่อเหยื่อ โดยแอบอ้างและแสดงเลขหมายโทรศัพท์จากต้นทางที่เหยื่อมีความไว้วางใจ เช่นการอ้างว่าโทรมาจากธนาคารที่เหยื่อมีบัญชี และทำการหลอกล่อให้เหยื่อบอกหมายเลข และรหัสเอทีเอ็ม หรือรหัสผ่าน หรืออ้างว่าโทรมาจากสำนักงานตำรวจ โดยผู้คุกคามนำข้อมูลดังกล่าวไปใช้ประโยชน์ ต่างๆ การถอนหรือโอนเงิน ทำให้เหยื่อสูญเสียทรัพย์ได้



ภาพที่ 2.11 การคุกคามแบบ Phishing

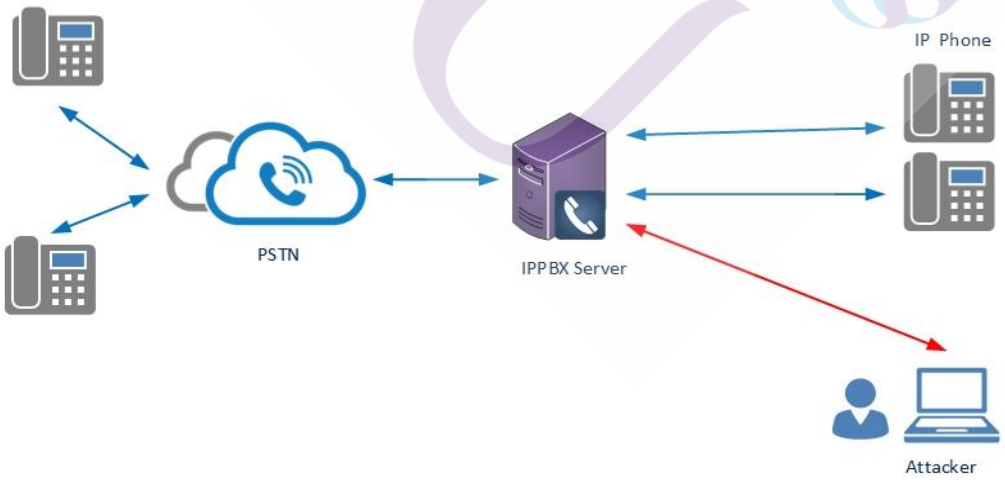
2.4.5 การคุกคามแบบ Call interception เป็นภัยคุกคามที่อาศัยระบบโทรผ่านอินเตอร์เน็ตที่มีการรักษาความปลอดภัยน้อยไม่มีการเข้ารหัสเสียง ทำให้ผู้คุกคามสามารถดักฟังและบันทึกเสียงสนทนา แล้วนำข้อมูลที่ได้ไปใช้ประโยชน์อย่างอื่นได้ เช่นข้อมูลคู่แข่งทางการค้า ความลับทางราชการ หรืออีกกรณีที่ปลายทางเป็นระบบบริการธนาคารผ่านโทรศัพท์ ผู้คุกคามสามารถดักจับข้อมูลหลายเลขบัญชี รหัสเอทีเอ็มได้ ทั้งนี้การดักฟังสามารถดักข้อมูลการโทรศัพท์แบบวีดีโอได้เช่นกัน



ภาพที่ 2.12 การดุกคามแบบ Call interception

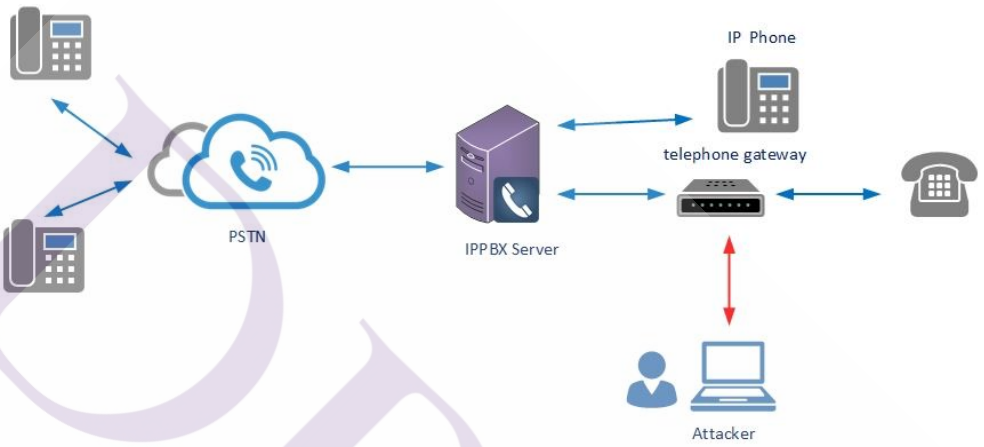
2.4.6 การดุกคามแบบ Theft of service เป็นภัยดุกคามที่มีลักษณะคล้ายกับ Toll fraud โดยผู้ดุกคามอาศัยช่องโหว่ของเกิดจากการระบบโทรผ่านอินเตอร์เน็ต เข้าไปเปลี่ยนแปลงการตั้งค่าที่สำคัญ โดยมีตัวอย่างดังนี้

- การทำ Call forwarding hack ผู้ดุกคามจะใช้สิทธิ์การเข้าจัดการระบบผ่านหน้าจอบริหารระบบโทรศัพท์ (web portal) โดยบัญชีและรหัสผ่านที่ได้จากการคาดเดา แล้วตั้งค่าการโอนสายไปยังต่างประเทศที่มีการเก็บค่าบริการปลายทาง



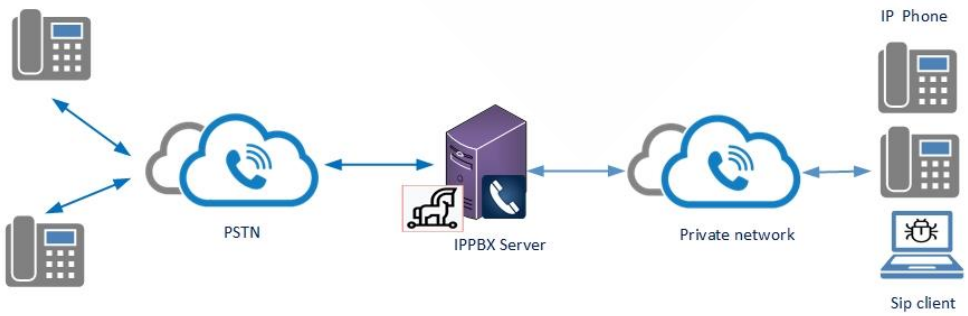
ภาพที่ 2.13 การดุกคามแบบ Theft of service การทำ Call forwarding hack

- การทำ Buffer overflow ATA attack ปกติการในเชื่อมต่อสัญญานโทรศัพท์อนาล็อกกับระบบโทรศัพท์ผ่านอินเตอร์เน็ตจะใช้อุปกรณ์แปลงสัญญาน (Analog Telephone Adapters) ซึ่งจะมีหน้าจอการบริหารจัดการผ่านเว็บ (Web Interface) ทำให้ผู้คุกคามมีโอกาสเข้าไปควบคุมเปลี่ยนแปลงการตั้งค่าเกี่ยวกับการเชื่อมต่อโทรศัพท์ได้ ทั้งนี้การคุกคามลักษณะนี้จะรวมถึงอุปกรณ์เชื่อมต่อสัญญานโทรศัพท์ผ่านอินเตอร์เน็ต แบบอื่นๆ เช่น อุปกรณ์แปลงสัญญานแบบดิจิตอล (Voice Gateway) เครื่องโทรศัพท์ผ่านอินเตอร์เน็ต (IP phone) เป็นต้น



ภาพที่ 2.14 การคุกคามแบบ Theft of service การทำ Buffer overflow ATA attack

2.4.7 การคุกคามแบบ Malware โดยผู้คุกคามจะใช้โปรแกรมที่มีจุดประสงค์ร้ายต่อคอมพิวเตอร์ในหลายรูปแบบเช่น ไวรัส(Virus),วอร์ม (Worm),สปายแวร์(Spyware) ,โทรจัน (Trojan) เพื่อให้ได้มาซึ่ง หมายเลขโทรศัพท์ บัญชีผู้ใช้ รหัสผ่าน เพื่อนำข้อมูลที่ได้ใช้ประโยชน์จากระบบโทรศัพท์ผ่านอินเตอร์เน็ตในรูปแบบอื่น



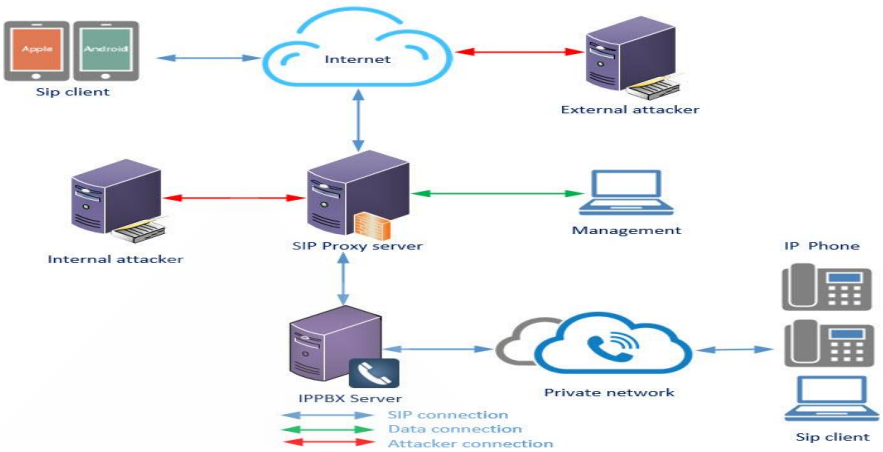
ภาพที่ 2.15 การคุกคามแบบ Malware

บทที่ 3
การศึกษาข้อมูลและระเบียบวิจัย

ในบทนี้จะกล่าวถึงขั้นตอนและแนวทางการดำเนินการวิจัย การออกแบบ เครื่องมือที่นำมาใช้ในการวิจัย แผนการดำเนินงาน รวมถึงการติดตั้งเครื่องและระบบที่เกี่ยวข้องเพื่อประเมินการประเมินผลกระทบการโจมตีระบบโทรศัพท์ผ่านอินเตอร์เน็ตจากการปฏิเสธการให้บริการด้วยการยิงข้อความ SIP INVITE ในการโจมตีระบบโทรศัพท์ผ่านอินเตอร์เน็ต (IPPBX SERVER) ผู้บุกรุกสามารถเลือกใช้ได้หลายคำสั่ง เช่น INVITE,OPTION,NOTIFY,CANCEL,BYE หรือคำสั่งอื่นที่เป็นมาตรฐานของ SIP อย่างไรก็ตามคำสั่ง INVITE จะมีความสะดวกมากกว่าเพราะส่วนประกอบของ SIP ตามมาตฐาน RFC 3261 จะรองรับคำส่ง INVITE ยิ่งกว่านั้นทุกอุปกรณ์หรือระบบถูกออกแบบให้รับคำสั่ง INVITE โดยไม่ต้องส่งคำสั่งล่วงหน้า ดังนั้นคำสั่ง INVITE สามารถทำให้การใช้ทรัพยากรณ์บนอุปกรณ์หรือระบบให้หมดลงได้ง่าย รวมถึงระบบจะต้องมีการตอบกลับสถานะของคำสั่ง INIVTE ไปยังต้นทางเสมอ ด้วยค่า 1XX หรือ 2XX [19] ซึ่งทำให้คำสั่ง SIP ทั้งหมดมีจำนวนเพิ่มมากขึ้นในช่วงเวลาของการโจมตี โดยมีหัวข้อหลักดังนี้

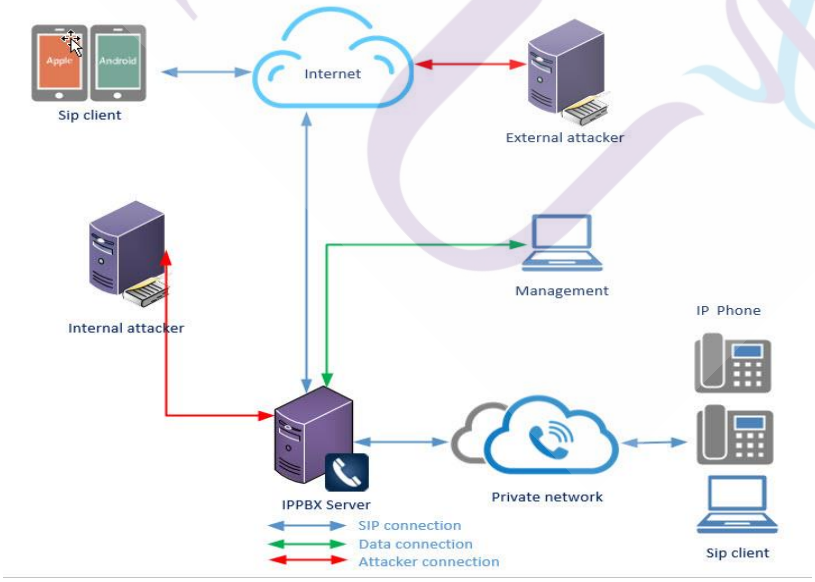
3.1 การกำหนดโครงสร้างที่ใช้ในการวิจัย

ในการศึกษาข้อมูลและระบบ ผู้วิจัยได้กำหนดโครงสร้างและองค์ประกอบของระบบทั้งหมดเพื่อสนับสนุนการวิจัยดังภาพที่ 3.1



ภาพที่ 3.1 โครงสร้างและองค์ประกอบของระบบเชื่อมต่อสัญญานโทรศัพท์ผ่านอินเตอร์เน็ต (SIP PROXY SERVER)

ซึ่งจะเป็นการกำหนดโครงสร้างการเชื่อมต่อที่มีระบบเชื่อมต่อสัญญานโทรศัพท์ผ่านอินเตอร์เน็ต (SIP PROXY SERVER) และกำหนดโครงสร้างการเชื่อมต่อเพื่อทดสอบโดยไม่มีระบบเชื่อมต่อสัญญานโทรศัพท์ผ่านอินเตอร์เน็ต (SIP PROXY SERVER) มาจัดการเส้นทางการเชื่อมต่อ



ภาพที่ 3.2 โครงสร้างและองค์ประกอบแบบไม่มีระบบเชื่อมต่อสัญญานโทรศัพท์ผ่านอินเตอร์เน็ต (SIP PROXY SERVER)

โดยมีรายละเอียดคุณสมบัติของระบบที่ใช้ในการศึกษาวิจัยดังนี้

3.1.1 ระบบเชื่อมต่อสัญญานโทรศัพท์ผ่านอินเตอร์เน็ต (SIP PROXY SERVER) ระบบโทรศัพท์ผ่านอินเตอร์เน็ต พัฒนาจากโปรแกรม Kamailio® [1] ซึ่งเป็นซอฟต์แวร์ระบบสื่อสารแบบโอเพ่นซอร์ส ที่รองรับการพัฒนาเป็นระบบโทรศัพท์ผ่านอินเตอร์เน็ต (Internet Telephony) รองรับการสื่อสารในเวลาจริง หรือ Real Time Communications (RTC) ซึ่งเป็นการสื่อสารข้อมูลแบบตอบกลับทันที สามารถรับส่ง ข้อความ รูปภาพ ภาพเคลื่อนไหว เสียง

3.1.2 รองรับการพัฒนาเป็นระบบเชื่อมต่อและแปลงสัญญาณโทรศัพท์ผ่านอินเตอร์เน็ตเป็นสัญญาณโทรศัพท์แบบสลับวงจร (Circuit Switching) ได้

3.1.3 ระบบโทรศัพท์ผ่านอินเตอร์เน็ต (IPPBX SERVER) เป็นซอฟต์แวร์ระบบสื่อสารแบบโอเพ่นซอร์สชื่อ Free SWITCH® [2] ที่สามารถปรับค่าระบบให้ทำงานเป็นระบบตู้สาขาโทรศัพท์ผ่านโครงข่ายอินเตอร์เน็ต หรือ Internet Protocol Private Branch Exchange (IPPBX) รองรับการเชื่อมต่อสัญญานโทรศัพท์แบบ Session Initial Protocol (SIP) หรือ มาตรฐาน H.323 ทั้งนี้ยังสามารถบริหารจัดการข้อมูลบัญชี การลงทะเบียนเครื่องลูกข่าย (SIP Client) ได้ ทั้งนี้ระบบโทรศัพท์ผ่านอินเตอร์เน็ตยังมีหน้าที่ควบคุมและจัดการการเชื่อมต่อข้อมูลเสียงและวีดีโอผ่านโครงข่ายอินเตอร์เน็ต (RTP SERVER)

3.1.4 โปรแกรมสื่อสารโทรศัพท์ผ่านอินเตอร์เน็ต (Softphone) โดยใช้โปรแกรม Microsip ติดตั้งบนเครื่องคอมพิวเตอร์ และโปรแกรม Zoiper สำหรับติดตั้งบนเครื่องโทรศัพท์เคลื่อนที่ ซึ่งจะทำเป็นเครื่องลูกข่าย (SIP Client) ที่ใช้เพื่อเชื่อมต่อสัญญาณโทรศัพท์จากภายนอกและภายในเครือข่ายอินเตอร์เน็ตของระบบ

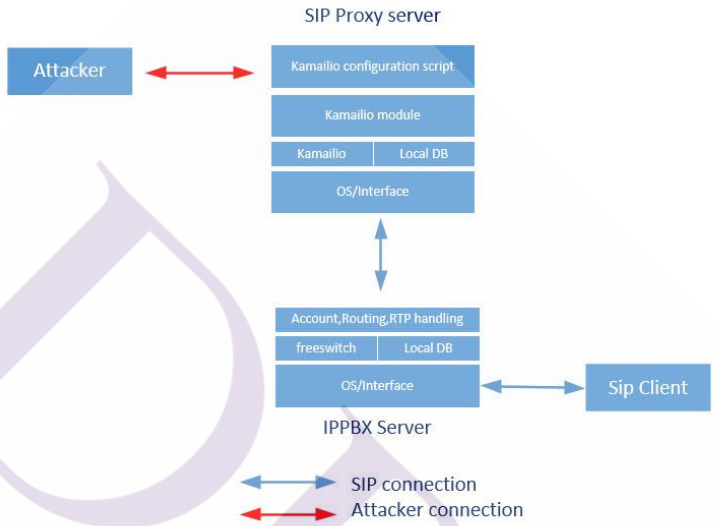
3.1.5 อุปกรณ์โทรศัพท์ผ่านอินเตอร์เน็ต (IP phone) ที่รองรับการเชื่อมต่อสัญญานแบบ Session Initial Protocol (SIP) ซึ่งจะทำเป็นเครื่องลูกข่าย (SIP Client) ที่ใช้เพื่อเชื่อมต่อสัญญาณโทรศัพท์จากภายในเครือข่ายอินเตอร์เน็ตของระบบ

3.1.6 โปรแกรมทดสอบการผู้โจมตีระบบโทรศัพท์ผ่านอินเตอร์เน็ต โดยจะใช้โปรแกรม SIPP ซึ่งเป็นซอฟต์แวร์ทดสอบสื่อสารแบบโอเพ่นซอร์ส ทำหน้าที่โจมตีระบบโทรศัพท์ผ่านอินเตอร์เน็ตจากภายในเครือข่ายอินเตอร์เน็ตของระบบ (Internal attacker)

3.1.7 ผู้โจมตีระบบโทรศัพท์ผ่านอินเตอร์เน็ตจากภายนอกเครือข่ายอินเตอร์เน็ตของระบบ (External attacker) กลุ่มของระบบหรือบุคคลที่ไม่สามารถกำหนดตัวตนและกำหนดรูปแบบการโจมตีได้

3.2 องค์ประกอบของระบบที่ใช้ในการศึกษาวิจัย

ในส่วนนี้จะแสดงให้เห็นส่วนองค์ประกอบของแต่ละระบบที่เป็นส่วนสำคัญต่อการวิจัยนี้ซึ่งผู้วิจัยจะกำหนดคุณสมบัติในแต่ละระบบเพื่อให้ทำงานตรงกับจุดประสงค์ของงานวิจัย โดยมีแผนผังดังภาพประกอบที่ 3.3



ภาพที่ 3.3 องค์ประกอบของแต่ละระบบของการวิจัย

โดยมีรายละเอียดขององค์ประกอบของระบบที่ใช้ในการศึกษาวิจัยดังนี้

3.2.1 ระบบเชื่อมต่อสัญญานโทรศัพท์ผ่านอินเตอร์เน็ต (SIP PROXY SERVER) ประกอบด้วยส่วนย่อย ดังนี้

- OS/Interface เป็นส่วนของฮาดแวร์และอุปกรณ์ที่เกี่ยวข้องกับเครือข่าย รวมถึงระบบปฏิบัติการ
- Kamailio® เป็นของโปรแกรมประมวลผลการเชื่อมต่อสัญญานโทรศัพท์ผ่านอินเตอร์เน็ต (Voice over IP)ในรูปแบบ SIP Protocol
- Local DB เป็นระบบฐานข้อมูลที่ใช้เก็บข้อมูลการเชื่อมต่อของสัญญานโทรศัพท์ทั้งหมดของโปรแกรม Kamailio®
- Kamailio® Module เป็น ส่วนของโปรแกรมที่ถูกพัฒนาเพิ่มเติมให้กับโปรแกรม Kamalio® เพื่อรองรับการทำงานในส่วนอื่นๆตามจุดประสงค์ของผู้พัฒนา

- Kamailio configuration script เป็นการกำหนดค่าการทำงานของโปรแกรม Kamalio® เพื่อให้ทำงานเป็น SIP PROXY โดยมี Pike , htable เป็น โมดูลสำหรับตรวจสอบจำนวนคำสั่ง SIP Message ต่อ IP Address ในแต่ละช่วงเวลาได้ ซึ่งสามารถนำคุณสมบัตินี้กำหนดเงื่อนไขในการเชื่อมต่อไปยังระบบโทรศัพท์ผ่านอินเตอร์เน็ตได้

- Signaling routing and controlling เป็นส่วนที่ทำหน้าที่ควบคุม จัดการการร้องขอเชื่อมต่อของ Kamailio® การส่งต่อข้อมูลทั้งในส่วนที่เป็น data packageไปยัง Management , SIP package ระหว่าการเชื่อมต่อภายนอกกับ ระบบโทรศัพท์ผ่านอินเตอร์เน็ต (IPPBX SERVER) และ RTP package ระหว่างระบบเชื่อมต่อสัญญานโทรศัพท์ผ่านอินเตอร์เน็ต(SIP PROXY SERVER) กับ ระบบโทรศัพท์ผ่านอินเตอร์เน็ต (IPPBX SERVER)

3.2.2 ระบบโทรศัพท์ผ่านอินเตอร์เน็ต (IPPBX SERVER) ประกอบด้วยส่วนย่อยดังนี้

- OS/Interface เป็นส่วนของฮาดแวร์และอุปกรณ์ที่เกี่ยวข้องกับเครือข่าย รวมถึงระบบปฏิบัติการ

- Local DB เป็นระบบฐานข้อมูลที่ใช้เก็บข้อมูลการเชื่อมต่อของสัญญานโทรศัพท์ทั้งหมด และเก็บข้อมูลการตั้งค่าเส้นทางการเชื่อมต่อ ค่าสถิติ สถานะการเชื่อมต่อแบบ Real time

- Free switch เป็นโปรแกรมที่ทำหน้าที่บริหารจัดการ ประมวลผลข้อมูลสัญญานโทรศัพท์อินเตอร์เน็ตระหว่างเครื่องลูกข่ายและเชื่อมต่อสัญญานไปยังอุปกรณ์อื่นได้

- Account ,routing ,RTP handling เป็นส่วนประกอบของโปรแกรม Free switch ที่ทำหน้าที่จัดการบัญชีเครื่องลูกข่าย การจัดเส้นทางของสัญญานโทรศัพท์ รวมถึงการจัดการเชื่อมต่อสัญญานเสียงและวีดีโอ ในการใช้งานระบบโทรศัพท์ผ่านอินเตอร์เน็ต

3.3 เครื่องมือและอุปกรณ์ที่ในการวิจัย

ผู้วิจัยได้แยกรายการอุปกรณ์และซอฟต์แวร์เพื่อรองรับการพัฒนางานวิจัยนี้ออกเป็น 2 ส่วน ดังนี้

3.3.1 อุปกรณ์ (Hardware) ที่เป็นอุปกรณ์หลัก มีดังนี้

- เครื่องคอมพิวเตอร์เสมือน (Virtual SERVER) สำหรับติดตั้งระบบเชื่อมต่อสัญญานโทรศัพท์ผ่านอินเตอร์เน็ต (SIP PROXY SERVER) ของระบบโทรศัพท์ผ่านอินเตอร์เน็ตมีคุณสมบัติดังนี้

- หน่วยประมวลผลกลาง 2 ชุด (vCPUs)

- หน่วยความจำ 2 กิกะไบต์ (Gigabyte)

- หน่วยจัดเก็บข้อมูล 30 กิกะไบต์ (Gigabyte)

- อุปกรณ์เครือข่ายเสมือน 2 หน่วย

- เครื่องคอมพิวเตอร์เสมือน (Virtual SERVER) สำหรับติดตั้งระบบโทรศัพท์ผ่านอินเตอร์เน็ต (IPPBX SERVER) มีคุณสมบัติดังนี้

- หน่วยประมวลผลกลาง 2 ชุด (vCPUs)

- หน่วยความจำ 2 กิกะไบต์ (Gigabyte)

- หน่วยจัดเก็บข้อมูล 30 กิกะไบต์ (Gigabyte)

- อุปกรณ์เครือข่ายเสมือน 1 หน่วย

- อุปกรณ์โทรศัพท์ผ่านอินเตอร์เน็ต (IP phone) เป็นอุปกรณ์ที่รองรับการเชื่อมสัญญาณโทรศัพท์

- เครื่องคอมพิวเตอร์สำหรับติดตั้งโปรแกรมสื่อสารโทรศัพท์ผ่านอินเตอร์เน็ต (Softphone) โดยมีคุณสมบัติดังนี้

- หน่วยประมวลผลกลาง 1 ชุด (CPU)

- หน่วยความจำ 16 กิกะไบต์ (Gigabyte)

- พื้นที่สำหรับติดตั้งติดตั้งโปรแกรมสื่อสารโทรศัพท์ผ่านอินเตอร์เน็ต (Softphone) 50 เมกะไบต์ (Megabyte)

- เครื่องคอมพิวเตอร์เสมือน (Virtual SERVER) สำหรับติดตั้งโปรแกรมทดสอบการผู้โจมตีระบบโทรศัพท์ผ่านอินเตอร์เน็ต มีคุณสมบัติดังนี้

- หน่วยประมวลผลกลาง 2 ชุด (vCPUs)

- หน่วยความจำ 2 กิกะไบต์ (Gigabyte)

- หน่วยจัดเก็บข้อมูล 30 กิกะไบต์ (Gigabyte)

- อุปกรณ์เครือข่ายเสมือน 1 หน่วย

3.3.2 ซอฟต์แวร์ (Software) โดยจะมีส่วนประกอบย่อยดังนี้

- ระบบปฏิบัติการ(Operating system) เป็นระบบหลักในการควบคุมและประมวลผลในด้านต่างๆตามหน้าที่หลักของแต่ละส่วนในหัวข้อศึกษานี้โดยจะระบบปฏิบัติการเดเบียนลีนุกซ์ รุ่น 11.0 (Debian GNU/Linux OS Release 11.0) และระบบปฏิบัติการวินโดวน์ 10 (Windows 10 OS)

- ระบบเชื่อมต่อสัญญานโทรศัพท์ผ่านอินเตอร์เน็ต (SIP PROXY SERVER) ที่ผู้วิจัยใช้โปรแกรม Kamailio® ทำหน้าที่รักษาความรักษาความปลอดภัย และทำหน้าที่แบบตัวกลาง (SIP Proxy) ในการเชื่อมต่อสัญญานโทรศัพท์ระหว่างแม่ข่ายกับเครื่องลูกข่าย (SIP Client) จากเครือข่ายอินเตอร์เน็ต

- ระบบโทรศัพท์ผ่านอินเตอร์เน็ต (IPPBX SERVER) ทำหน้าที่เป็นเครื่องแม่ข่ายบริหารจัดการเชื่อมต่อสัญญานโทรศัพท์ผ่านอินเตอร์เน็ตระหว่างแม่ข่ายกับเครื่องลูกข่าย (SIP Client) ในรูปแบบ SIP

- โปรแกรมสื่อสารโทรศัพท์ผ่านอินเตอร์เน็ต (Softphone) เป็นโปรแกรมสำหรับสื่อสารข้อมูลเสียงและวีดีโอโครงข่ายอินเตอร์เน็ต โดยรองรับการเชื่อมต่อกับระบบโทรศัพท์ผ่านอินเตอร์เน็ต (IPPBX SERVER) ในรูปแบบ SIP

- โปรแกรมทดสอบการผู้โจมตีระบบโทรศัพท์ผ่านอินเตอร์เน็ต (SIPP) เป็นโปรแกรมสำหรับสื่อสารข้อมูลเสียงและวีดีโอโครงข่ายอินเตอร์เน็ตที่รองรับการสร้างจำนวนครั้งในการเชื่อมต่อไปยังระบบเชื่อมต่อสัญญานโทรศัพท์ผ่านอินเตอร์เน็ต (SIP PROXY SERVER) และระบบโทรศัพท์ผ่านอินเตอร์เน็ต (IPPBX SERVER) แบบจำนวนมากได้ รวมทั้งสามารถกำหนดค่าพารามิเตอร์และคุณสมบัติของการเชื่อมต่อได้

- โปรแกรมดักจับข้อมูลและแสดงผลการสื่อสารข้อมูลผ่านโครงข่ายอินเตอร์เน็ตที่รองรับการดักจับข้อมูลประเภท Session Initial Protocol (SIP) และ Real time transport protocol(RTP) ได้ เช่นโปรแกรม ไวร์ชาร์ก (Wire shark) หรือคำสั่ง tcpdump เป็นต้น

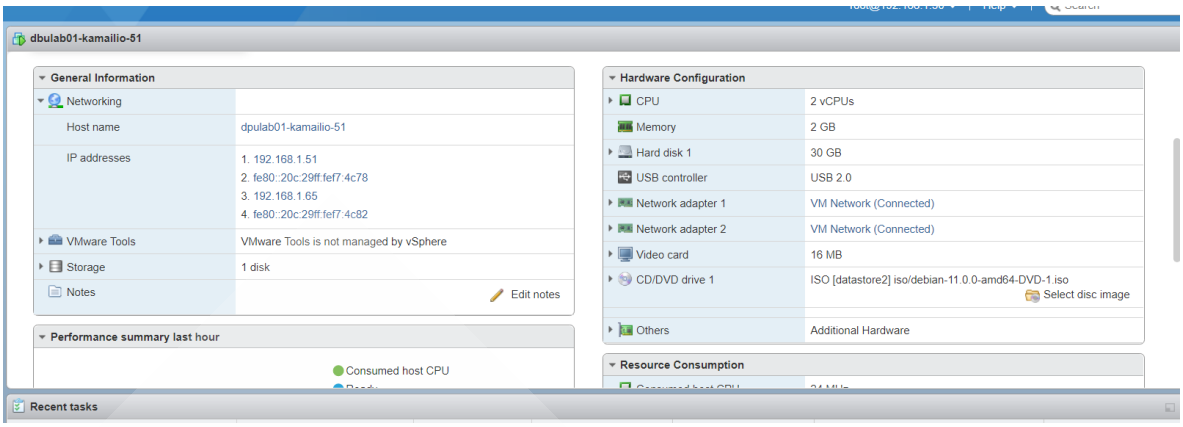
3.4 การติดตั้งระบบและโปรแกรมที่ในการวิจัย

ผู้วิจัยได้สรุปการรายละเอียดการติดตั้งดังนี้

3.4.1 การติดตั้งโปรแกรม Kamailio®

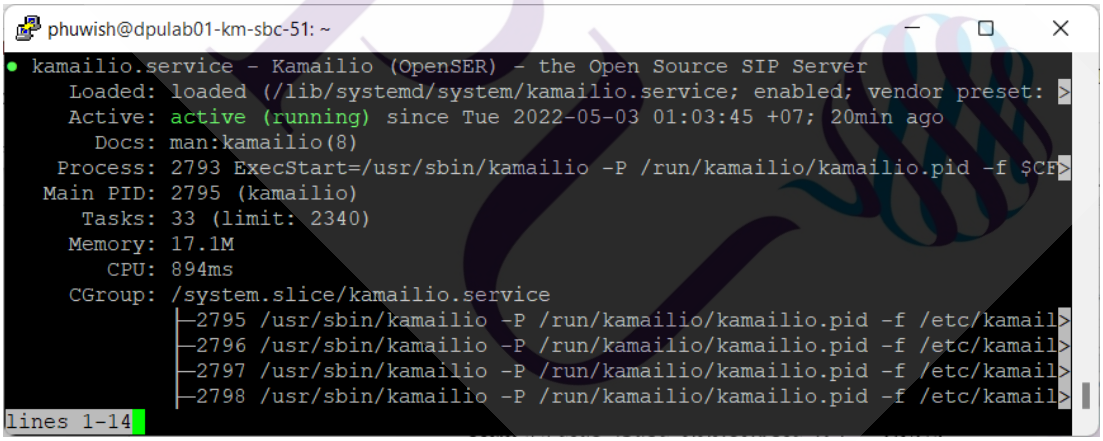
โดยมีส่วนประกอบและขั้นตอนย่อยดังนี้

- ติดตั้งระบบปฏิบัติการ Debain GNU/Linux โดยทำการดาวน์โหลดโปรแกรมจาก https://www.debian.org/CD/http-ftp/ และปรับปรุงโปรแกรมเป็นเวอร์ชั่นล่าสุด เพื่อรองรับโปรแกรม Kamailio®



ภาพที่ 3.4 รายละเอียดระบบปฏิบัติการ Debain GNU/Linux

- ติดตั้งโปรแกรม Kamailio® โดยอ้างอิงข้อมูลจาก https://kamailio.org/docs/tutorials/-5.5.x/kamailio-install-guide-git/ เพื่อใช้ระบบเชื่อมต่อสัญญาณโทรศัพท์ผ่านอินเตอร์เน็ต (SIP Proxy SERVER) และปรับค่าระบบเพื่อรักษาความปลอดภัยและป้องกันการโจมตีทางระบบโทรศัพท์อินเตอร์เน็ต

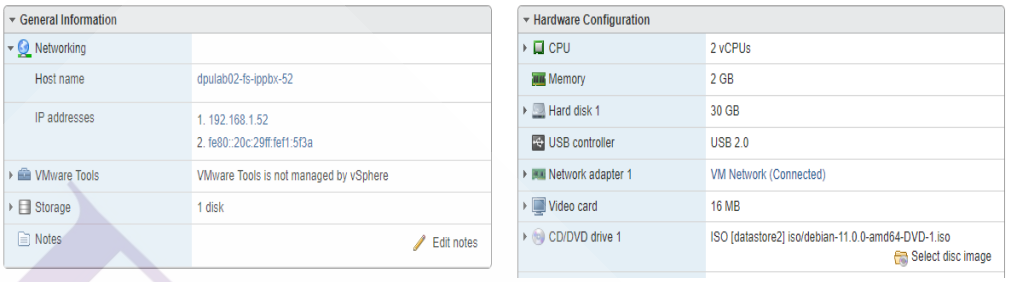


ภาพที่ 3.5 การทำงานของโปรแกรม Kamailio®

3.4.2 การติดตั้งโปรแกรม Free SWITCH® เพื่อเป็นระบบโทรศัพท์ผ่านอินเตอร์เน็ต (IPPBX SERVER) และสร้างข้อมูลบัญชีลูกข่าย (SIP Client)

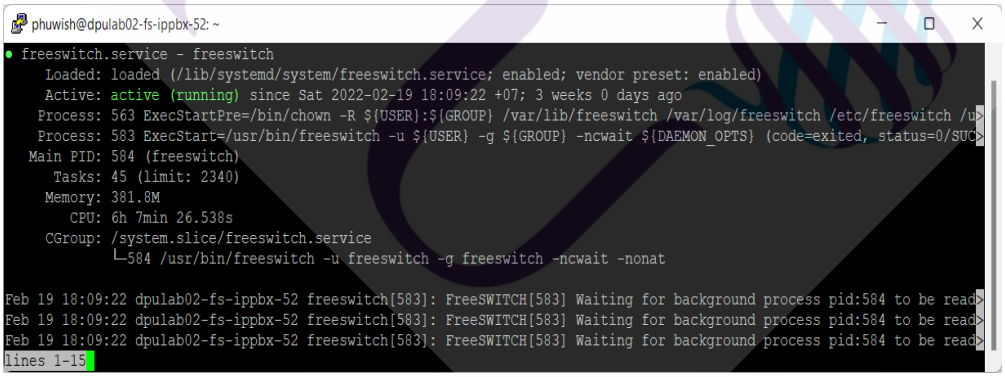
โดยมีส่วนประกอบและขั้นตอนย่อยดังนี้

- ติดตั้งระบบปฏิบัติการ Debain GNU/Linux โดยทำการดาวน์โหลดโปรแกรมจาก https://www.debian.org/CD/http-ftp/ และปรับปรุงโปรแกรมเป็นเวอร์ชั่นล่าสุด เพื่อรองรับโปรแกรม Free SWITCH®



ภาพที่ 3.6 รายละเอียดระบบปฏิบัติการ Debain GNU/Linux

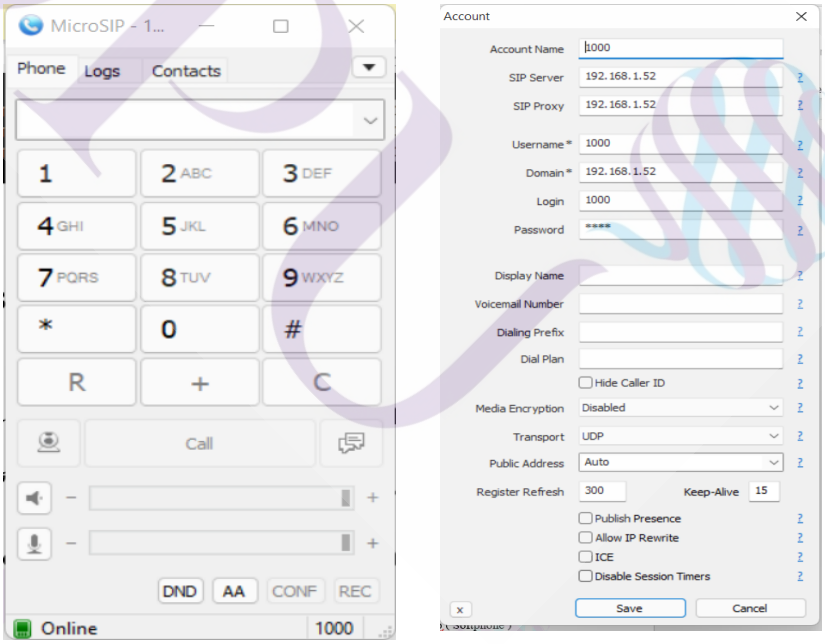
- ติดตั้งโปรแกรม Free SWITCH® โดยอ้างอิงข้อมูลจาก https://freeswitch.org/-confluence/display/FREESWITCH/Installation และทำการตั้งค่าระบบเพื่อให้ทำงานเป็นระบบโทรศัพท์ผ่านอินเตอร์เน็ต



ภาพที่ 3.7 ระบบโทรศัพท์ผ่านอินเตอร์เน็ต (IPPBX SERVER)

ภาพที่ 3.8 ระบบโทรศัพท์ผ่านอินเตอร์เน็ต (IPPBX SERVER) แสดงสถานการณ์เชื่อมต่อกับเครื่องลูกข่าย

3.4.3 การติดตั้งโปรแกรมสื่อสารโทรศัพท์ผ่านอินเตอร์เน็ต (Softphone) โปรแกรม Microsip เป็นโปรแกรมที่รองรับการติดตั้งบนระบบปฏิบัติการวินโดวน์ (Window 11) โดยสามารถดาวน์โหลดได้จาก https://www.microsip.org/ และทำการลงทะเบียนบัญชีหมายเลขโทรศัพท์บนระบบโทรศัพท์ผ่านอินเตอร์เน็ต



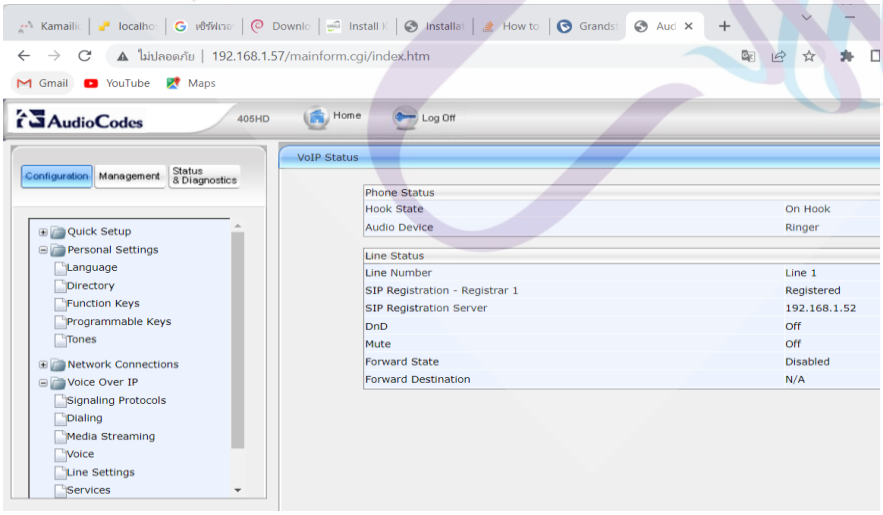
ภาพที่ 3.9 โปรแกรมสื่อสารโทรศัพท์ผ่านอินเตอร์เน็ต Microsip (Softphone)

3.4.4 การติดตั้งอุปกรณ์โทรศัพท์ผ่านอินเตอร์เน็ต (IP phone)

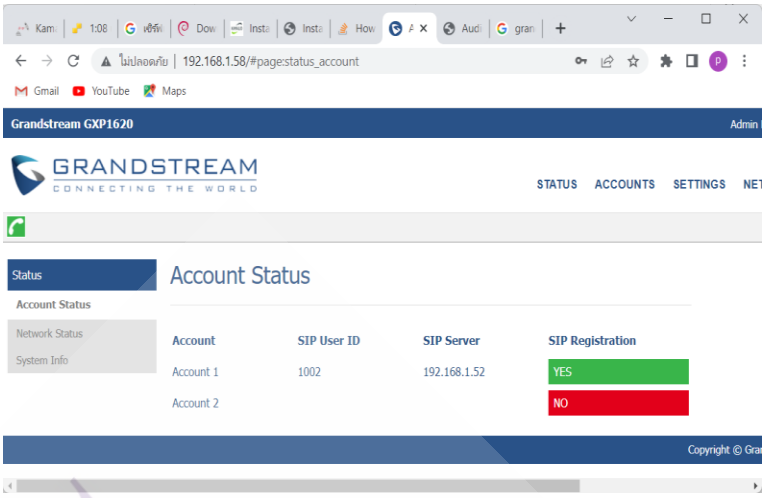
โดยมีอุปกรณ์ที่ใช้ในการศึกษาวิจัยจำนวน 2 เครื่องที่รองรับการเชื่อมต่อแบบ SIP

ภาพที่ 3.10 อุปกรณ์โทรศัพท์ผ่านอินเตอร์เน็ต (IP phone) ที่ใช้ในการศึกษาวิจัย

ทำการลงทะเบียนบัญชีหมายเลขโทรศัพท์ของแต่ละเครื่องบนระบบโทรศัพท์ผ่านอินเตอร์เน็ต โดยมีข้อมูลสถานการณ์เชื่อมต่อระบบดังนี้



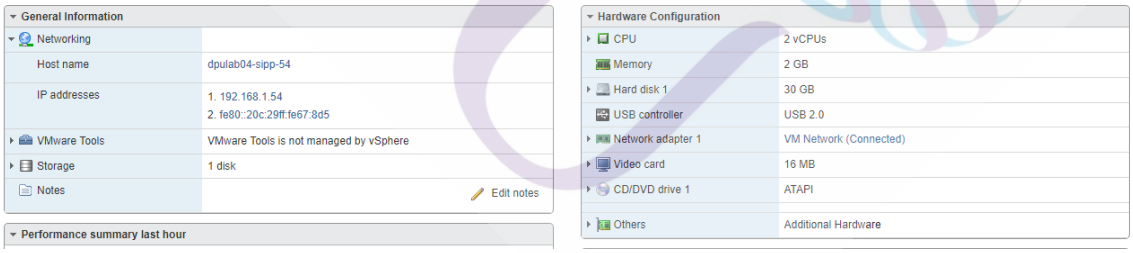
ภาพที่ 3.11 แสดงสถานการณ์เชื่อมต่อระบบของ อุปกรณ์โทรศัพท์ผ่านอินเตอร์เน็ต(IP phone) เครื่องที่ 1



ภาพที่ 3.12 แสดงสถานการณ์เชื่อมต่อระบบของอุปกรณ์โทรศัพท์ผ่านอินเตอร์เน็ต(IP phone) เครื่องที่ 2

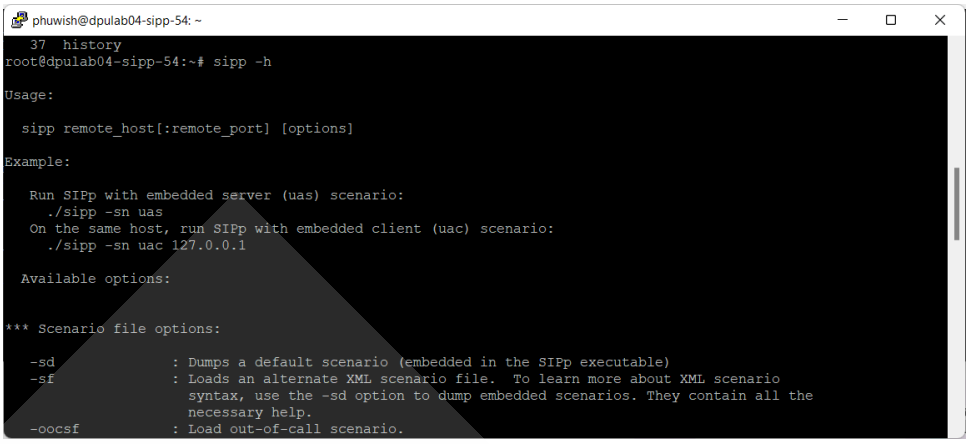
3.4.5 การติดตั้งโปรแกรมทดสอบการผู้โจมตีระบบโทรศัพท์ผ่านอินเตอร์เน็ตโปรแกรม SIPP โดยมีส่วนประกอบและขั้นตอนย่อยดังนี้

- ติดตั้งระบบปฏิบัติการ Debain GNU/Linux โดยทำการดาวน์โหลดโปรแกรมจาก https://www.debian.org/CD/http-ftp/ และปรับปรุงโปรแกรมเป็นเวอร์ชั่นล่าสุด เพื่อรองรับโปรแกรม SIPP



ภาพที่ 3.13 รายละเอียดระบบปฏิบัติการ Debain GNU/Linux

- ติดตั้งโปรแกรม SIPP โดยสามารถดาวน์โหลดและอ้างอิงข้อมูลจาก https://sipp.-readthedocs.io/en/latest/installation.html



ภาพที่ 3.14 แสดงข้อมูลการทำงานของโปรแกรม SIPP

3.5 การปรับระบบเชื่อมสัญญาณโทรศัพท์ผ่านอินเตอร์เน็ต (SIP PROXY SERVER)เพื่อรองรับทดสอบความปลอดภัยระบบโทรศัพท์ผ่านอินเตอร์เน็ต

3.5.1 การปรับค่าและคำสั่งบนโปรแกรม Kamailio® ในไฟล์ตั้งค่า kamailio.cfg โดยแบ่งเป็นส่วนๆ ดังนี้

- เปิด module WITH_ANTIFLOOD, WITH_FREESWITCH สำหรับใช้งานในโปรแกรม

ภาพที่ 3.15 แสดงข้อมูลเปิด module สำหรับใช้งานในโปรแกรม Kamailio®

- กำหนดค่าตัวแปร IP Address ,Port สำหรับการเชื่อมต่อไปยัง IPPBX SERVER โดยมี IP Address 192.168.1.52 และ Port สำหรับ SIP Protocol เป็น 5060

ภาพที่ 3.16 แสดงข้อมูลกำหนดค่าตัวแปรที่ใช้งานในโปรแกรม Kamailio®

- กำหนดค่าเริ่มต้นใช้งานสำหรับ โมดูล Pike และ โมดูล htable

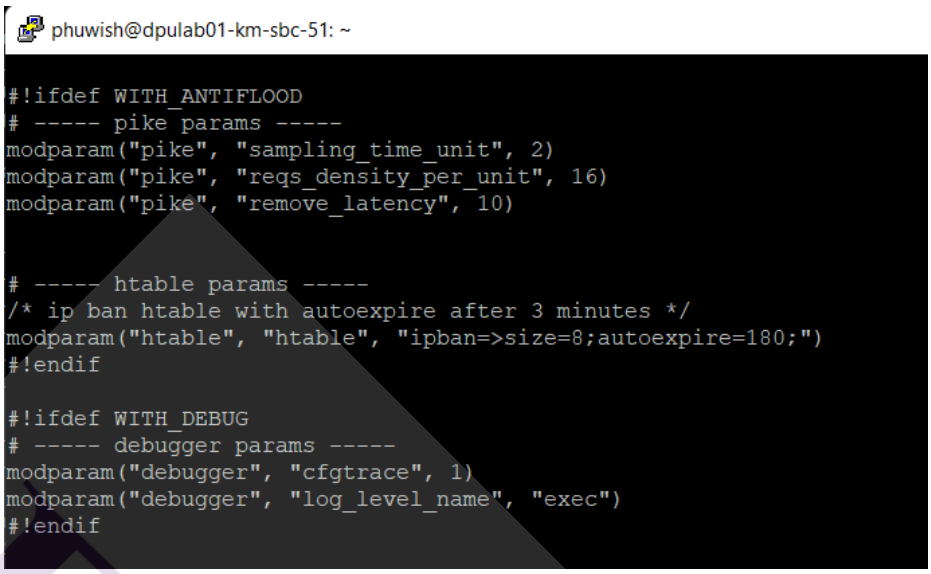
- โมดูล Pike เป็นโมดูลสำหรับกำหนดค่าการเชื่อมต่อของ IPAddress ผ่าน SIP PROXY SERVER โดยมีการกำหนดค่าดังนี้

- sampling_time_unit คือค่าเวลาในหน่วยวินาทีของการตรวจสอบการเชื่อมต่อจาก IP Address ต้นทาง โดยค่าเริ่มต้นคือ 2 วินาที

- reqs_density_per_unit คือจำนวนครั้งที่เชื่อมต่อจากต้นทางต่อ sampling_time_unit ก่อนที่จะปฏิเสธการเชื่อมต่อจาก IP Address โดยมีค่าเริ่มต้นที่ 30 หมายถึงอัตราการเชื่อมต่อเป็น 30 ครั้ง ต่อ sampling_time_unit 2 วินาที โดยที่ค่าปฏิเสธการเชื่อมต่อจาก IP Address จะอยู่ในช่วง reqs_density_per_unit ที่กำหนดถึง 3 เท่าสำหรับ IPV4 และ 8 เท่าสำหรับ IPV6

- remove_latency คือการกำหนดเระยะเวลาให้ระบบเก็บข้อมูล IP Address ที่มีการเชื่อมต่อล่าสุดไว้ มีหน่วยเป็นวินาทีมีค่าเริ่มต้นที่ 120 วินาที แต่ไม่ใช่ระยะเวลาของการปฏิเสธการเชื่อมต่อสำหรับ IP Address นั้นๆ การปรับสถานะให้เป็นอนุญาตเชื่อมต่อก็ต่อเมื่อ sampling_time_unit ไม่เกิน reqs_density_per_unit การเก็บข้อมูล IP Address ไว้ในหน่วยความจำทำให้มีความรวดเร็วในการค้นหา IP Address ที่อยู่ในสถานะปฏิเสธการเชื่อมต่อ

- โมดูล htable เป็นโมดูลที่ทำหน้าที่สร้างตารางสำหรับเก็บข้อมูล IP Address ชั่วคราวซึ่งจะถูกเก็บในหน่วยความจำชั่วคราว โดยมี ipban=>size คือ ขนาดของตารางเก็บข้อมูลโมดูล htable มีค่าเป็น 8 ช่อง(Array) autoexpire คือ ระยะเวลาในการเก็บข้อมูลมีหน่วยเป็นวินาที



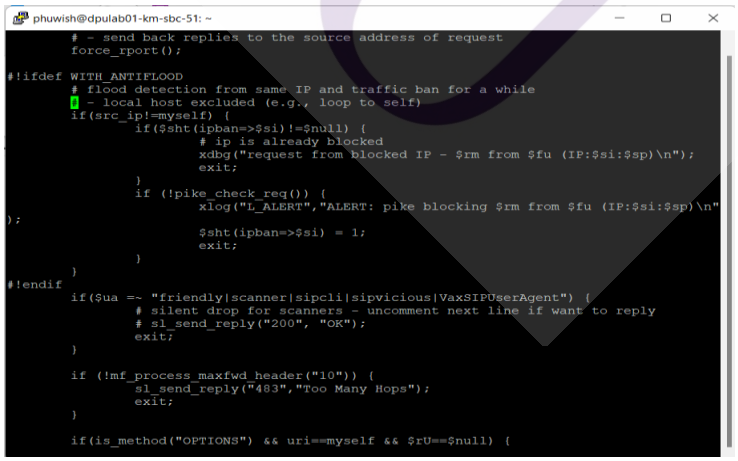
ภาพที่ 3.17 แสดงข้อมูลกำหนดค่าเริ่มต้นของ module pike และ htable

- รายละเอียดคำส่งการตรวจสอบสถานะการเชื่อมต่อของ IP Address สำหรับโมดูล Pike มีฟังก์ชั่น pike_check_req() ที่ใช้ในการตรวจสอบ IP Address ที่ขอเชื่อมต่อซึ่งจะมีค่าได้กลับมาดังนี้

1 = IP Address อยู่ในสถานะอนุญาตเชื่อมต่อ หรือเกิดปัญหาอย่างอื่น

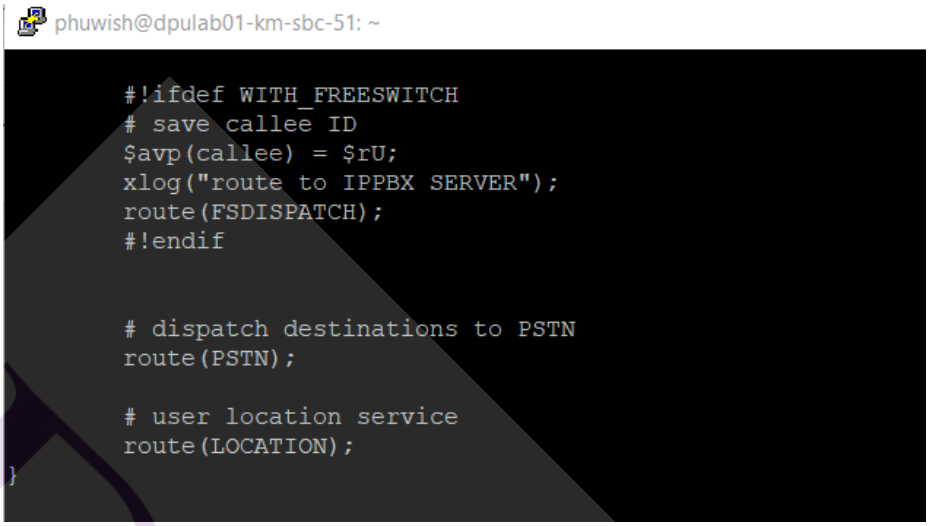
-1 = IP Address อยู่ในสถานะปฏิเสธเชื่อมต่อก่อนหน้านี้แล้ว

-2 = IP Address ใหม่มีการเชื่อมต่อเกินที่กำหนดและเปลี่ยนให้เป็นสถานะปฏิเสธเชื่อมต่อ



ภาพที่ 3.18 แสดงข้อมูลคำสั่งการตรวจสอบสถานะของ IP Address

- ปรับคำสั่งการทำ Routing เพื่อเชื่อมต่อกับ IPPBX SERVER ดังภาพ 3.19



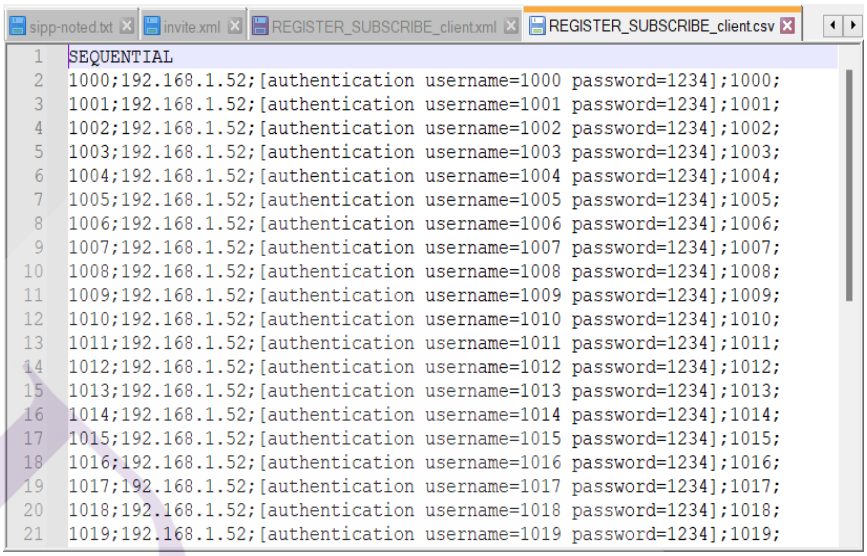
ภาพที่ 3.19 แสดงข้อมูล script สำหรับจัดการเส้นทางการเชื่อมต่อ IPPBX

3.5.2 การสร้างไฟล์ข้อมูลสำหรับโปรแกรม SIPP

- ไฟล์คำสั่งเพื่อรองรับ คำสั่ง SIP Register

ภาพที่ 3.20 แสดงข้อมูล script สำหรับคำสั่ง SIP Register

- ไฟล์รายชื่อบัญชีเพื่อรองรับคำสั่ง SIP Register



ภาพที่ 3.21 แสดงข้อมูลบัญชีหมายเลขโทรศัพท์สำหรับคำสั่ง SIP Register

- คำสั่ง SIPP เพื่อลงทะเบียนบัญชีผู้ใช้งานบน IPPBX SERVER .

  /sipp192.168.1.52-sfREGISTER_SUBSCRIBE_client.xml-inf

  REGISTER _SUBSCRIBE_client.csv-m100-l2-r2

- คำสั่ง SIPP สำหรับการทดสอบการโทรศัพท์ไปยัง IPPBX SERVER

  sipp -r XXX -sn uac 192.168.1.52 หมายเหตุ: XXX = จำนวนครั้งที่โทรศัพท์พร้อมกันต่อวินาที

- คำสั่ง SIPP สำหรับการทดสอบการโทรศัพท์ไปยัง IPPBX SERVER

  sipp -r XXX -sn uac 192.168.1.51 หมายเหตุ: XXX = จำนวนครั้งที่โทรศัพท์พร้อมกันต่อวินาที

3.5.3 การเตรียมคำสั่งดักจับข้อมูลบนเครือข่ายโปรแกรม TCPDUMP

- คำสั่งบันทึกข้อมูลการใช้งานเครือข่ายบน IPPBX SERVER port 5060

  tcpdump-iens192-n-s0 port 5060-vvv -w /home/phuwish/ippbx_no_ddos.pcap

- คำสั่งบันทึกข้อมูลการใช้งานเครือข่ายบน SIP PROXY SERVER port 5060

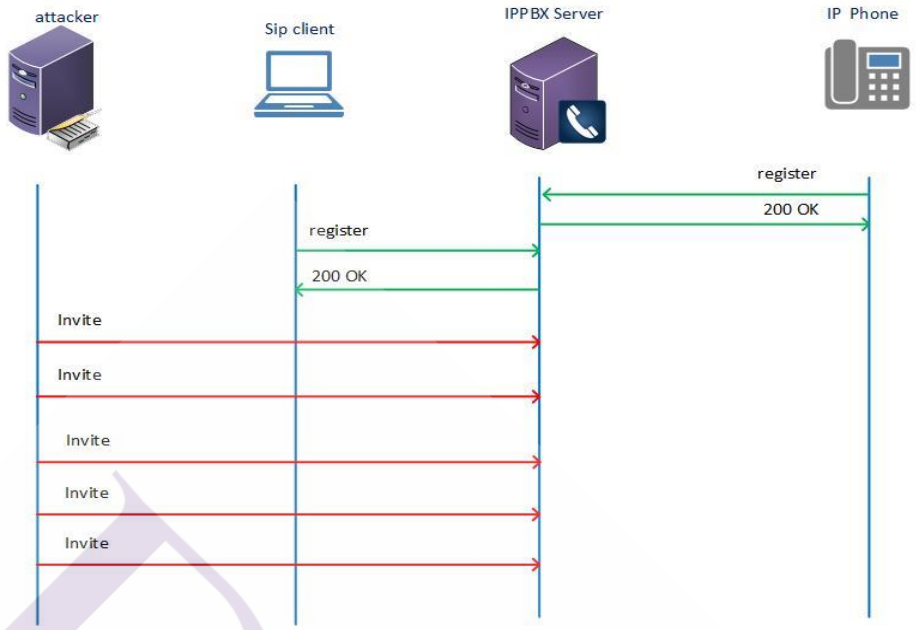
  tcpdump-iens192-n-sport506-vvv -w /home/phuwish/ippbx_wproxy_ddos.pcap

บทที่ 4
การผลทดสอบงานวิจัย

การทดสอบวิจัยนี้เพื่อการเปรียบเทียบระหว่างการโจมตีระบบโทรศัพท์ผ่านอินเตอร์เน็ต (IPPBX SERVER) ในแต่ละเงื่อนเพื่อให้เห็นข้อมูลการทำงานของระบบและสรุปข้อมูลการทดสอบ โดยแบ่งการทดสอบเป็น 3 ส่วนดังนี้

4.1 การทดสอบโจมตีระบบโทรศัพท์ผ่านอินเตอร์เน็ต (IPPBX SERVER) จากโปรแกรมทดสอบการโจมตี SIPP

การดำเนินการทดสอบส่วนนี้จะเป็นการส่งคำสั่งร้องขอการเชื่อมต่อ (SIP INVITE) จากโปรแกรมทดสอบการโจมตี SIPP ไปยังระบบโทรศัพท์ผ่านอินเตอร์เน็ต (IPPBX SERVER) จากเครือข่ายอินเตอร์เน็ตท้องถิ่น(LAN) โดยกำหนดค่าอัตราการในการโทรศัพท์ต่อวินาที (CALL RATE) และระยะเวลาในการโจมตีเป็นเงื่อนไขในการทดสอบ อีกทั้งยังทำการส่งคำสั่งเพื่อลงทะเบียนการงาน (SIP REGISTER) ของตามจำนวนบัญชีผู้ใช้งานจริง เพื่อให้เห็นข้อมูลการใช้ทรัพยากรของระบบโทรศัพท์ผ่านอินเตอร์เน็ต (IPPBX SERVER) ที่ตอบสนองต่อการโจมตีจากโปรแกรม SIPP โดยมีแผนผังการเชื่อมต่อทดสอบการโจมตีดังภาพที่ 4.1



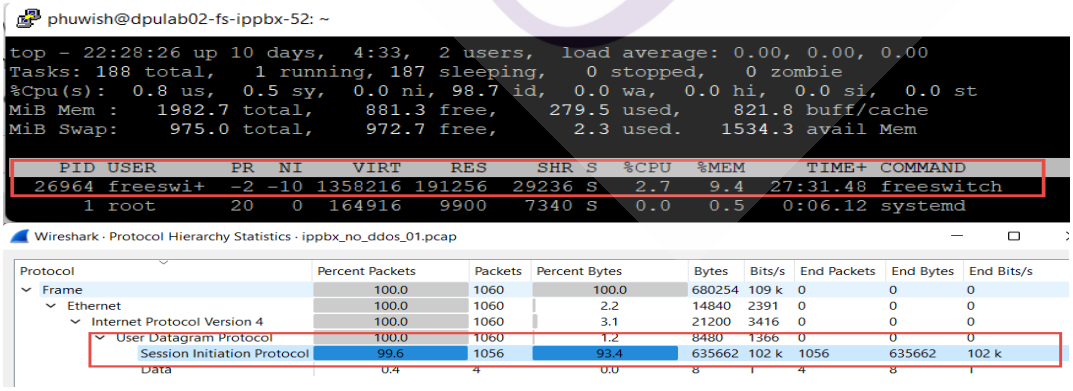
ภาพที่ 4.1 แสดงแผนผังการเชื่อมต่อทดสอบการโจมตี IPPBX SERVER จากโปรแกรม SIPP

ซึ่งจะมีผลข้อมูลที่ได้จากการทดสอบเป็นดังนี้

4.1.1 ข้อมูลการทดสอบ

4.1.1.1 ข้อมูลการใช้ทรัพยากรของ IPPBX SERVER ในสถานะการใช้งานปกติ

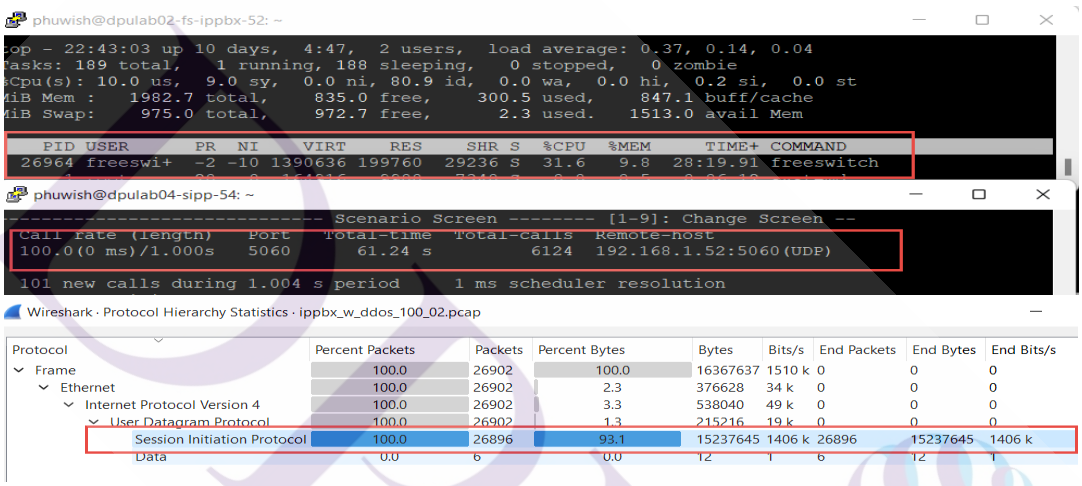
- หน่วยประมวลผลกลาง (CPU) 2.7 เปอร์เซ็นต์(%)
- หน่วยความจำ (Memory) 9.4 เปอร์เซ็นต์(%)
- อัตราการส่งข้อมูลของ SIP Protocol 102 กิโลบิตต่อวินาที (Kbps)



ภาพที่ 4.2 แสดงข้อมูลการใช้ทรัพยากร IPPBX SERVER ในสถานการณ์ใช้งานปกติ

4.1.1.2 ข้อมูลการใช้ทรัพยากรของ IPPBX SERVER ต่ออัตราการโทรศัพท์(CALL RATE) เป็น 100 ครั้งต่อวินาที

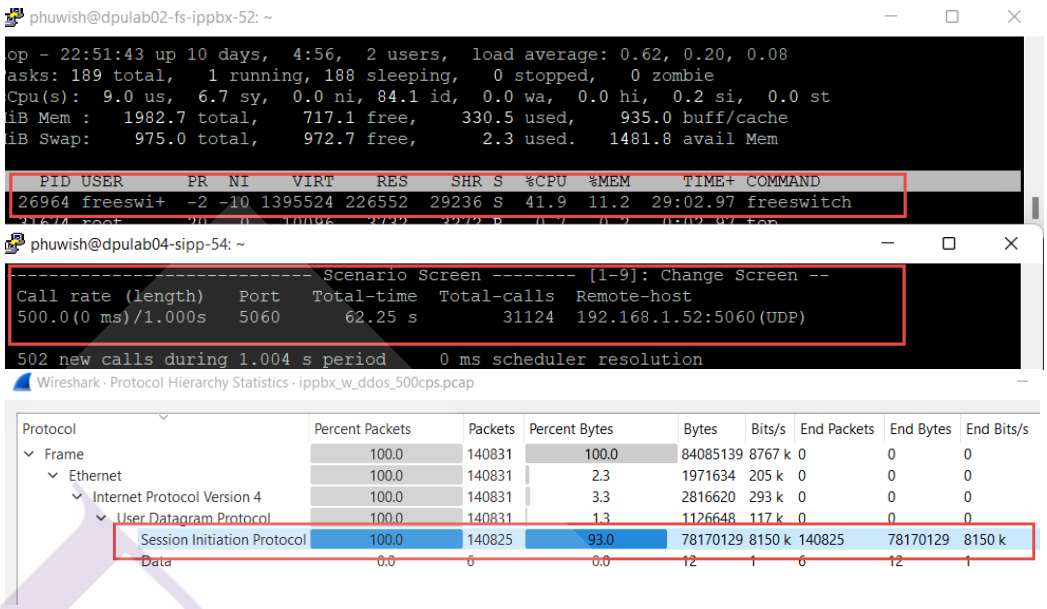
- จำนวนครั้งที่โทรศัพท์ (Total call) 6,124 ครั้ง
- ระยะเวลาในการโทรศัพท์ทั้งหมด (Total time) 61.24 วินาที
- หน่วยประมวลผลกลาง (CPU) 31.6 เปอร์เซ็นต์(%)
- หน่วยความจำ (Memory) 9.80 เปอร์เซ็นต์(%)
- อัตราการส่งข้อมูลของ SIP Protocol 1,406 กิโลบิตต่อวินาที (Kbps)



ภาพที่ 4.3 แสดงข้อมูลการใช้ทรัพยากรของ IPPBX SERVER ต่ออัตราการโทรศัพท์ (Call rate) เป็น 100 ครั้งต่อวินาที

4.1.1.3 ข้อมูลการใช้ทรัพยากรของ IPPBX ต่ออัตราการโทรศัพท์(Call rate) เป็น 500 ครั้งต่อวินาที

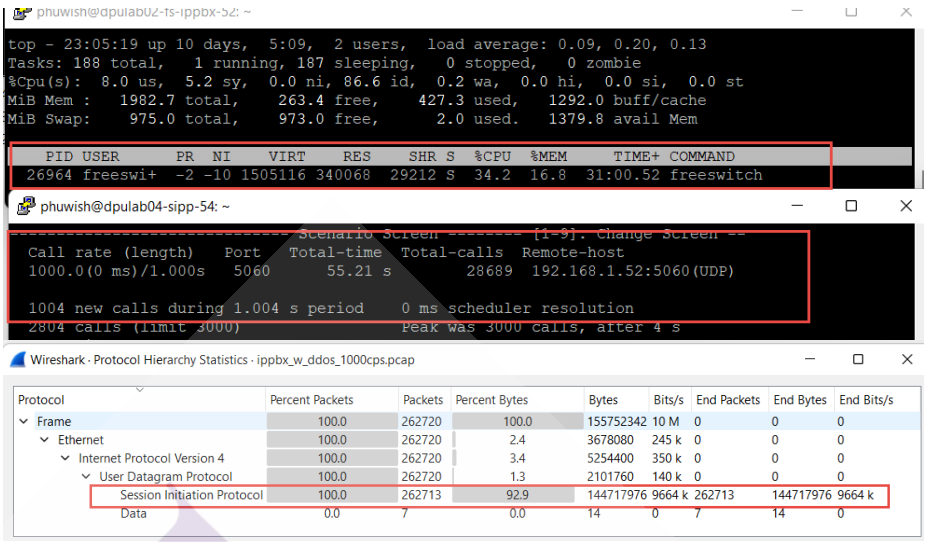
- จำนวนครั้งที่โทรศัพท์ (Total call) 31,124 ครั้ง
- ระยะเวลาในการโทรศัพท์ทั้งหมด (Total time) 62.25 วินาที
- หน่วยประมวลผลกลาง (CPU) 41.9 เปอร์เซ็นต์(%)
- หน่วยความจำ (Memory) 11.2 เปอร์เซ็นต์(%)
- อัตราการส่งข้อมูลของ SIP Protocol 8,150 กิโลบิตต่อวินาที (Kbps)



ภาพที่ 4.4 แสดงข้อมูลการใช้ทรัพยากรของ IPPBX SERVER ต่ออัตราการโทรศัพท์ต่อวินาที (Call rate) เป็น 500 ครั้งต่อวินาที

4.1.1.4 ข้อมูลการใช้ทรัพยากรของ IPPBX SERVER ต่ออัตราการโทรศัพท์(Call rate) เป็น 1,000 ครั้งต่อวินาที

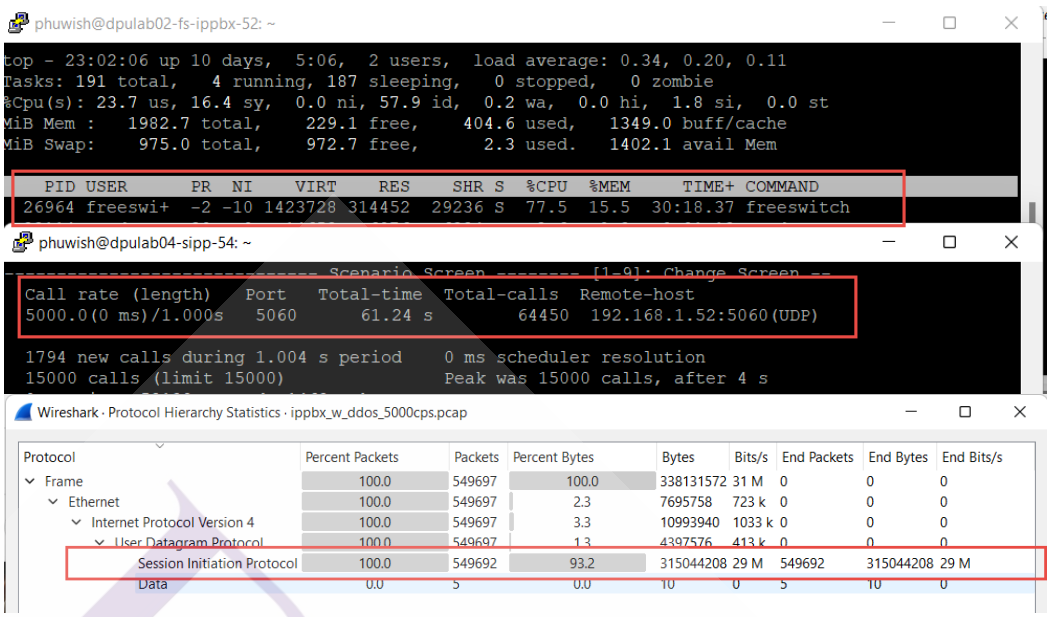
- จำนวนครั้งที่โทรศัพท์ (Total call) 28,689 ครั้ง
- ระยะเวลาในการโทรศัพท์ทั้งหมด (Total time) 55.21 วินาที
- หน่วยประมวลผลกลาง (CPU) 34.2 เปอร์เซ็นต์(%)
- หน่วยความจำ (Memory) 16.8 เปอร์เซ็นต์(%)
- อัตราการส่งข้อมูลของ SIP Protocol 9,664 กิโลบิตต่อวินาที (Kbps)



ภาพที่ 4.5 แสดงข้อมูลการใช้ทรัพยากรของ IPPBX SERVER ต่ออัตราการโทรศัพท์ (Call rate) เป็น 1,000 ครั้งต่อวินาที

4.1.1.5 ข้อมูลการใช้ทรัพยากรของ IPPBX SERVER ต่ออัตราการโทรศัพท์ (Call rate) เป็น 5,000 ครั้งต่อวินาที

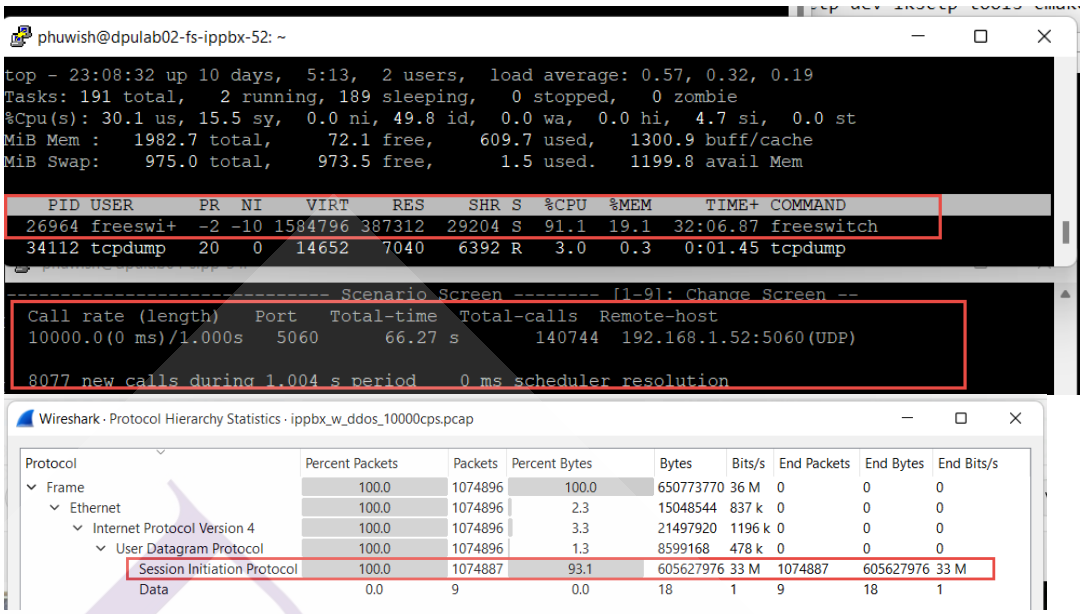
- จำนวนครั้งที่โทรศัพท์ (Total call) 64,450 ครั้ง
- ระยะเวลาในการโทรศัพท์ทั้งหมด (Total time) 61.25 วินาที
- หน่วยประมวลผลกลาง (CPU) 77.5 เปอร์เซ็นต์(%)
- หน่วยความจำ (Memory) 15.5 เปอร์เซ็นต์(%)
- อัตราการส่งข้อมูลของ SIP Protocol 29 เมกะบิตต่อวินาที (Mbps)



ภาพที่ 4.6 แสดงข้อมูลการใช้ทรัพยากรของ IPPBX SERVER ต่ออัตราการโทรศัพท์ (Call rate) เป็น 5,000 ครั้งต่อวินาที

4.1.1.6 ข้อมูลการใช้ทรัพยากรของ IPPBX SERVER ต่ออัตราการโทรศัพท์ (Call rate) เป็น 10,000 ครั้งต่อวินาที

- จำนวนครั้งที่โทรศัพท์ (Total call) 140,744 ครั้ง
- ระยะเวลาในการโทรศัพท์ทั้งหมด (Total time) 66.27 วินาที
- หน่วยประมวลผลกลาง (CPU) 91.1 เปอร์เซ็นต์(%)
- หน่วยความจำ (Memory) 19.1 เปอร์เซ็นต์(%)
- อัตราการส่งข้อมูลของ SIP Protocol 33 เมกะบิตต่อวินาที (Mbps)

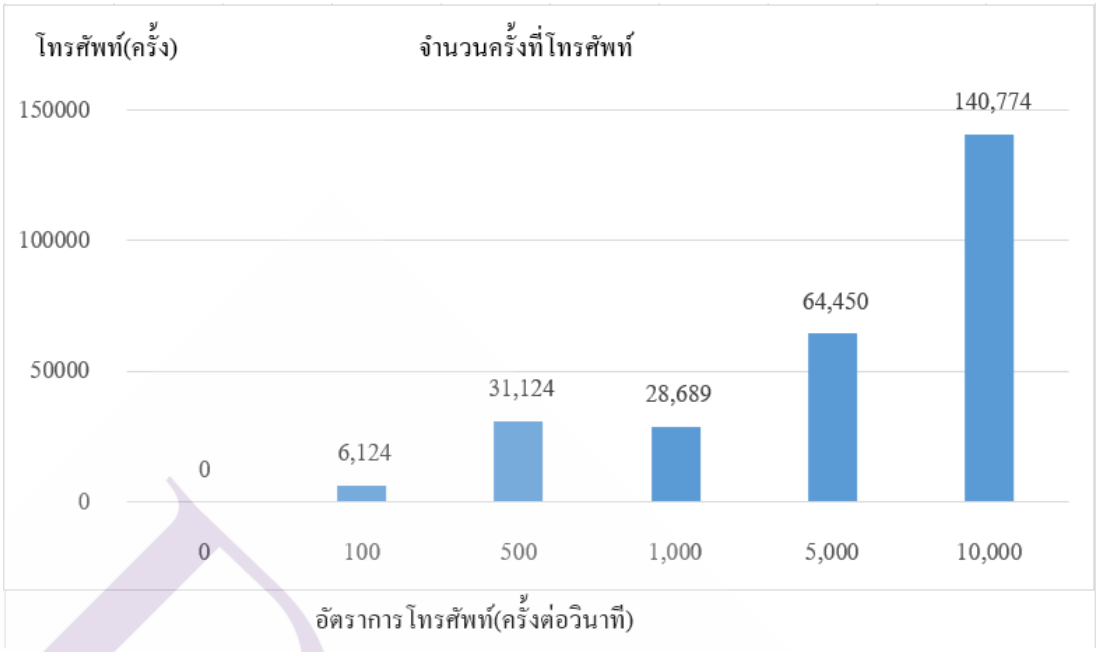


ภาพที่ 4.7 แสดงข้อมูลการใช้ทรัพยากรของ IPPBX SERVER ต่ออัตราการโทรศัพท์ (Call rate) เป็น 10,000 ครั้งต่อวินาที

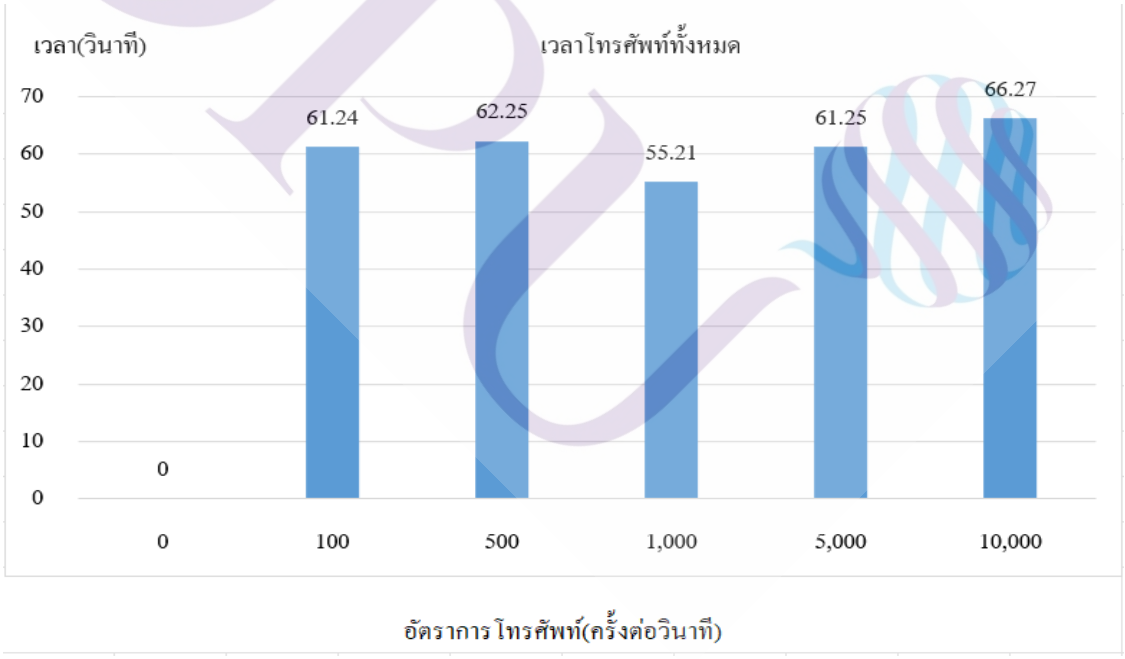
4.1.2 สรุปข้อมูลการใช้ทรัพยากรของ IPPBX SERVER เป็นดังนี้

ตารางที่ 4.1 แสดงข้อมูลทรัพยากรของ IPPBX SERVER ต่ออัตราการโทรศัพท์ (Call Rate) ในแต่ละครั้งที่กำหนด

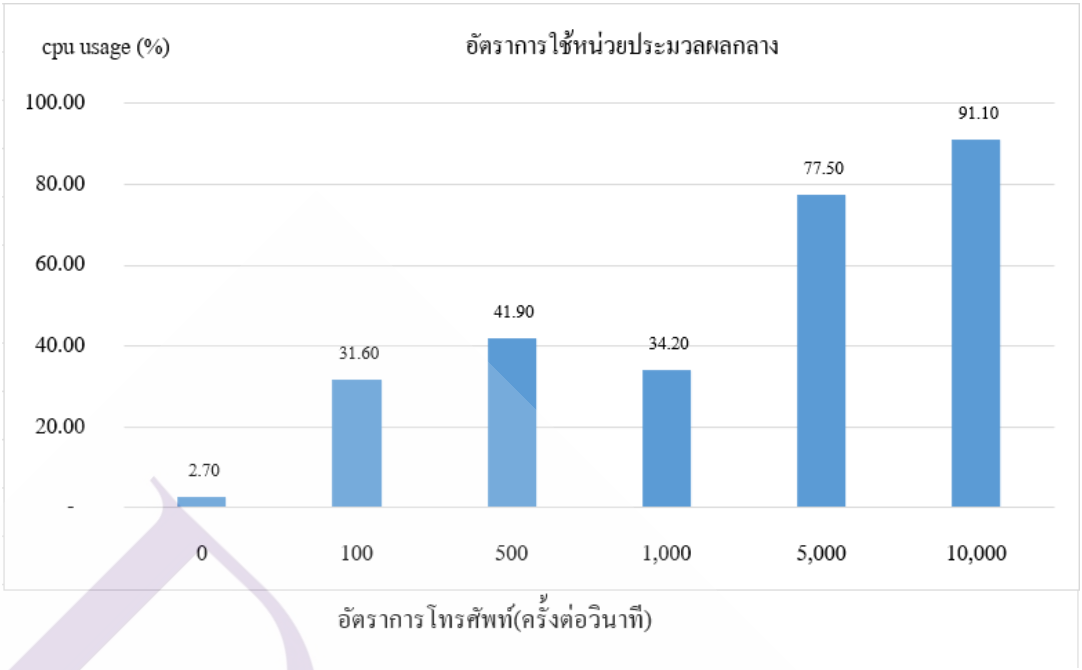
อัตราการโทรศัพท์ (ครั้งต่อวินาที)	จำนวนครั้งที่โทรศัพท์ (ครั้ง)	เวลาโทรศัพท์ทั้งหมด (วินาที)	อัตราการใช้หน่วยประมวลผลกลาง (%)	อัตราการใช้หน่วยความจำหลัก (%)	อัตราการส่งข้อมูลของ SIP Protocol (กิโลบิต/วินาที)
-	0	0	2.70	9.40	102
100	6,124	61.24	31.60	9.80	1,406
500	31,124	62.25	41.90	11.20	8,150
1,000	28,689	55.21	34.20	16.80	9,664
5,000	64,450	61.25	77.50	15.50	29,000
10,000	140,774	66.27	91.10	19.10	33,000



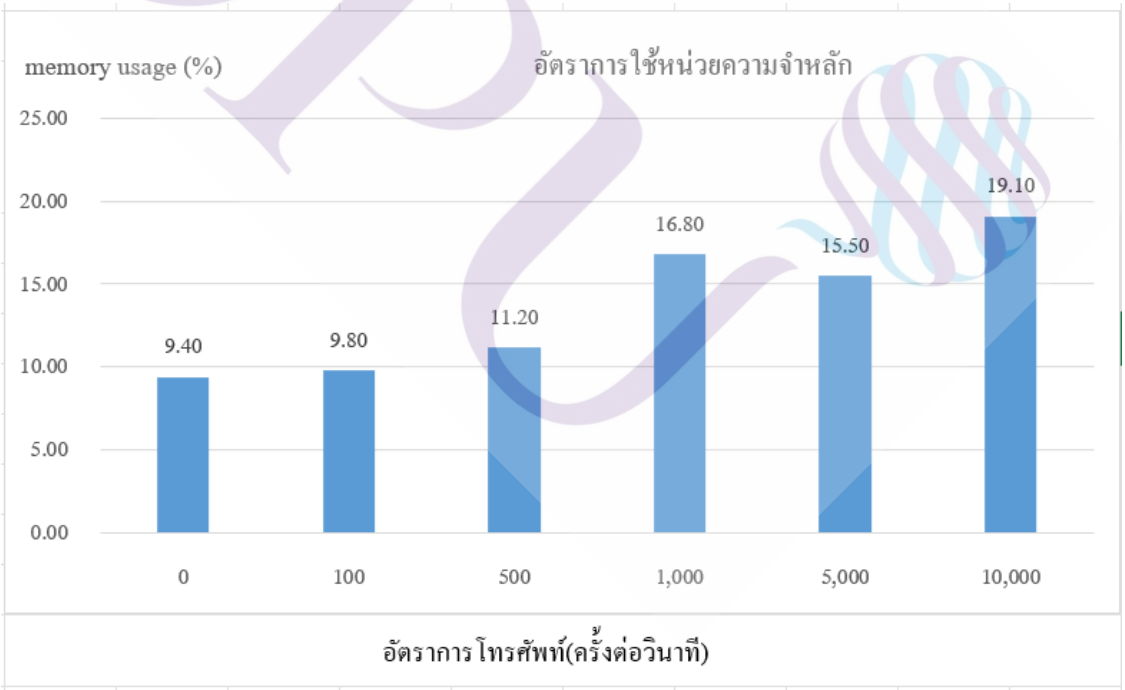
ภาพที่ 4.8 กราฟแสดงจำนวนครั้งที่โทรศัพท์



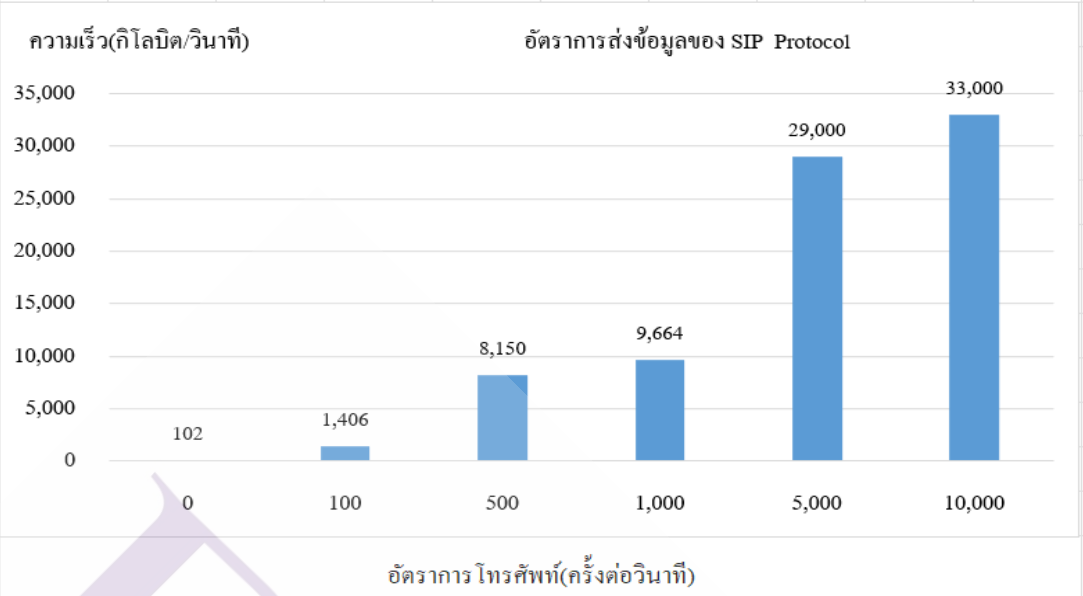
ภาพที่ 4.9 กราฟแสดงระยะเวลาในการทดสอบโทรศัพท์โจมตี



ภาพที่ 4.10 กราฟแสดงการใช้หน่วยประมวลผลกลาง

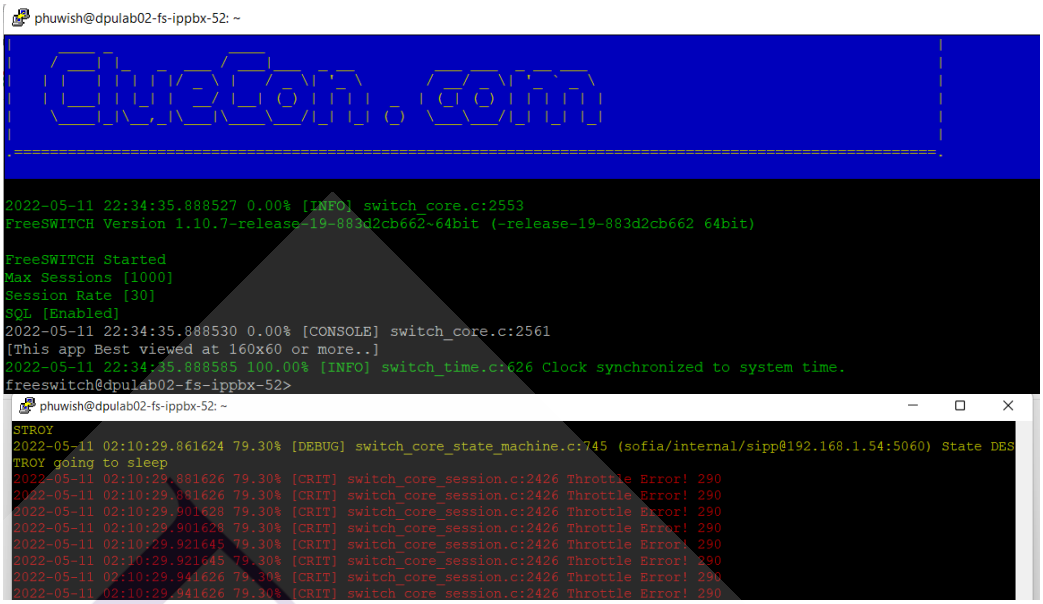


ภาพที่ 4.11 กราฟแสดงการใช้หน่วยความจำหลัก

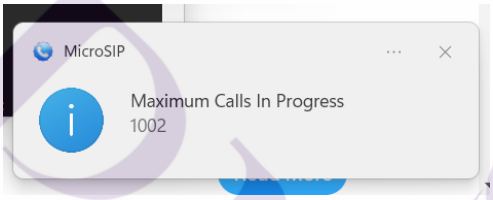


ภาพที่ 4.12 กราฟแสดงอัตราการส่งข้อมูลของ SIP Protocol

จากตารางที่ 4.1 และภาพที่ 4.8 ถึง 4.12 จะเห็นได้ว่าการใช้ทรัพยากรเครื่องคอมพิวเตอร์แม่ข่ายของโปรแซส (Process) IPPBX SERVER มีอัตราสูงขึ้นตามอัตราการโทรศัพท์ (Call rate) และจำนวนครั้งที่โทรศัพท์ (Total call) ที่เพิ่มขึ้นโดยมีระยะเวลาในการโทรศัพท์ทั้งหมด (Total time) ใกล้เคียงกัน โดยเฉพาะการใช้หน่วยประมวลผลกลาง (CPU) ,หน่วยความจำ (Memory) และ และ อัตราการส่งข้อมูลของ SIP Protocol มีอัตราการใช้งานเพิ่มขึ้นอย่างเป็นสัดส่วน การทดลองในหัวข้อวิจัยนี้เป็นการโทรศัพท์โดยการส่งคำสั่งร้องขอเชื่อมต่อ (SIP INVITE) เพียงครั้งเดียวแล้วสิ้นสุดการเชื่อมต่อเพื่อให้เห็นผลการใช้ทรัพยากรของระบบโทรศัพท์ผ่านอินเตอร์เน็ต (IPPBX SERVER) ต่อ 1 คำสั่งได้จากการโจมตี อีกทั้งในช่วงการทดสอบอัตราการโทรศัพท์ (Call rate) มากกว่า 30 ครั้งต่อวินาที เป็นต้นไป ระบบโทรศัพท์ผ่านอินเตอร์เน็ต (IPPBX SERVER) จะไม่สามารถทำงานได้และไม่ตอบสนองต่อการโทรศัพท์โดยใช้บัญชีเลขหมายภายในของระบบได้ดังภาพที่ 4.15 และ 4.16 ซึ่งจะตรงกับคุณสมบัติของ IPPBX SERVER ที่รองรับการเชื่อมต่อได้พร้อมกันสูงสุด 30 ครั้ง



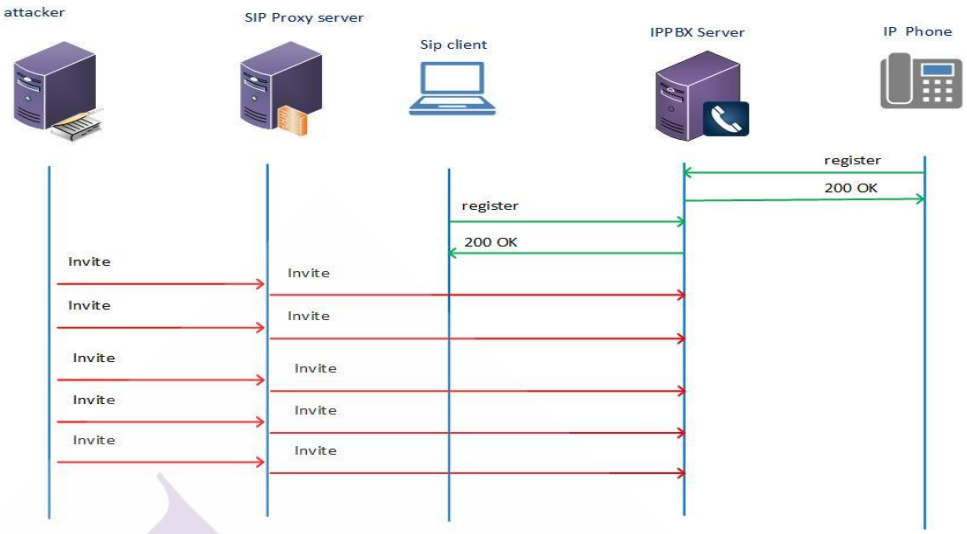
ภาพที่ 4.13 แสดงผลข้อมูลกรณีจำนวนโทรศัพท์เกินความสามารถ IPPBX SERVER



ภาพที่ 4.14 แสดงผลการโทรศัพท์จากโปรแกรมสื่อสารโทรศัพท์ผ่านอินเตอร์เน็ต (Softphone) กรณีจำนวนโทรศัพท์เกินความสามารถ IPPBX SERVER

4.2 การทดสอบโจมตีระบบโทรศัพท์ผ่านอินเตอร์เน็ต (IPPBX SERVER) จากโปรแกรมทดสอบการผู้โจมตี SIPP ผ่านระบบเชื่อมต่อสัญญาณโทรศัพท์ผ่านอินเตอร์เน็ต (SIP PROXY SERVER)

การดำเนินการทดสอบจะเป็นการส่งคำสั่งร้องขอการเชื่อมต่อ (SIP INVITE) จากโปรแกรมทดสอบการโจมตี SIPP ผ่านระบบเชื่อมต่อสัญญาณโทรศัพท์ผ่านอินเตอร์เน็ต (SIP PROXY SERVER) ไปยังระบบโทรศัพท์ผ่านอินเตอร์เน็ต (IPPBX SERVER) จากเครือข่ายอินเตอร์เน็ตท้องถิ่น (LAN) โดยมีการแผนผังการเชื่อมต่อดังภาพที่ 4.17 นี้



ภาพที่ 4.15 แสดงแผนผังการเชื่อมต่อทดสอบการโจมตี IPPBX SERVER ผ่าน SIP PROXY SERVER

โดยกำหนดค่าจำนวนครั้งในการโทรศัพท์ต่อวินาที(Call rate) และระยะเวลาในการโจมตี และเป็นเงื่อนไขในการทดสอบ มีการกำหนดค่าบนโมดูล pike ซึ่งการตั้งค่าข้างต้นจะมีผลต่ออัตราการโทรศัพท์ต่อวินาทีที่ SIP PROXY SERVER ใช้ควบคุมการร้องขอการเชื่อมต่อ (SIP INVITE) จากโปรแกรมทดสอบโจมตี SIPP ด้วย

4.2.1 ข้อมูลจาการการทดสอบ

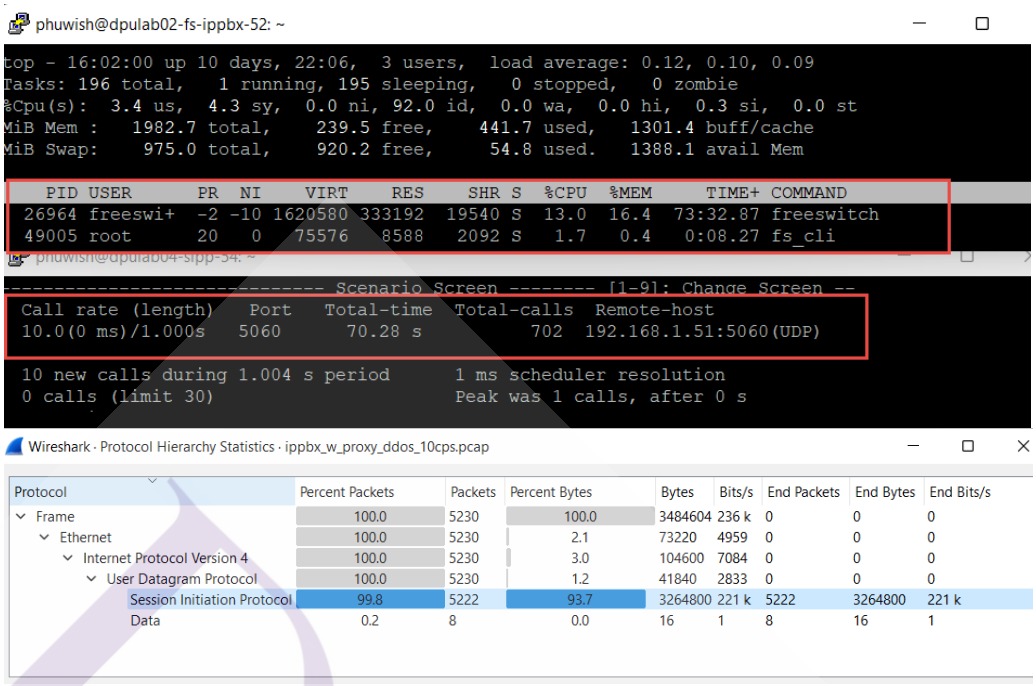
4.2.1.1 ทดสอบแบบที่ 1 โดยกำหนดค่าบนโมดูล pike ดังนี้

- Sampling time unit 2 วินาที
- Reqs_density_per_unit 100 ครั้ง
- Remove_latency 120 วินาที

4.2.1.1.1 ผลการทดสอบครั้งที่ 1 ในต่ออัตราการโทรศัพท์(Call rate) เป็น 10 ครั้งต่อวินาที โดยมีผลข้อมูลที่ได้ 2 ส่วนคือ

ข้อมูลการใช้ทรัพยากรของ IPPBX SERVER

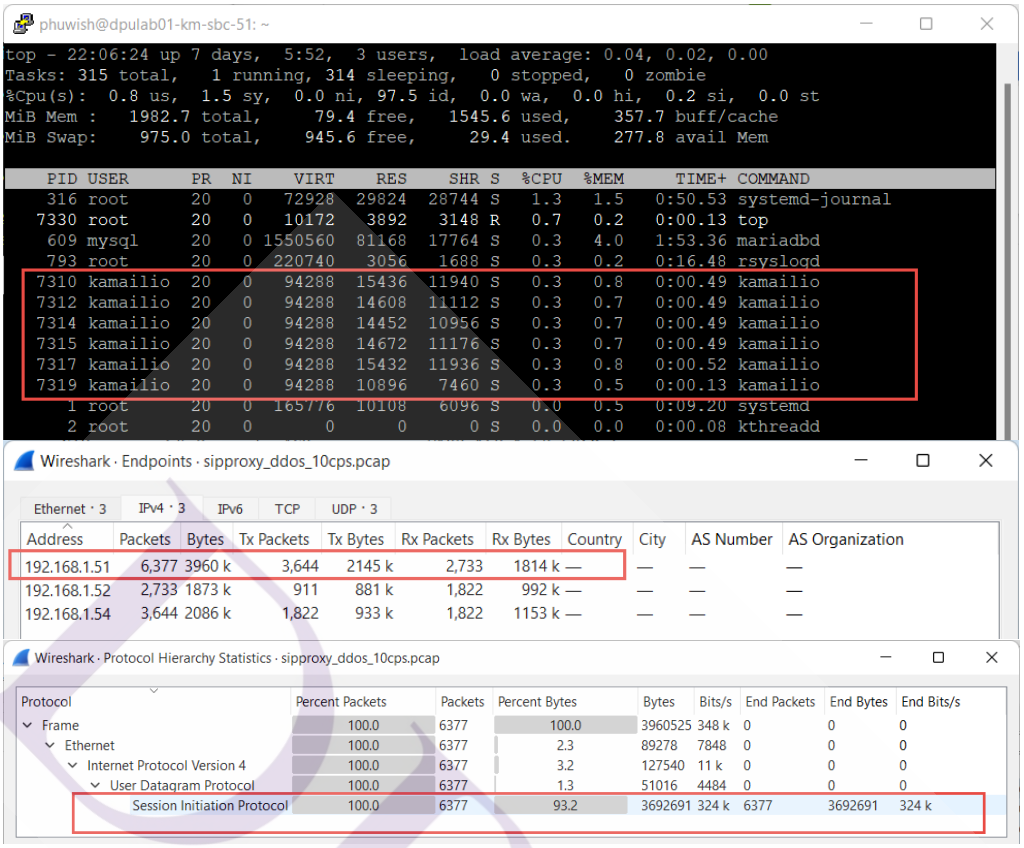
- จำนวนครั้งที่โทรศัพท์ (Total call) 702 ครั้ง
- ระยะเวลาในการโทรศัพท์ทั้งหมด (Total time) 70.28 วินาที
- หน่วยประมวลผลกลาง (CPU) 13.0 เปอร์เซ็นต์(%)
- หน่วยความจำ (Memory) 16.4 เปอร์เซ็นต์(%)
- อัตราการส่งข้อมูลของ SIP Protocol 221 กิโลบิตต่อวินาที (Kbps)



ภาพที่ 4.16 แสดงข้อมูลการใช้ทรัพยากรของ IPPBX SERVER แบบที่ 1 ครั้งที่ 1

ข้อมูลการใช้ทรัพยากรของ SIP PROXY SERVER

- หน่วยประมวลผลกลาง (CPU) จากโปรแซสทั้งหมด 1.80 เปอร์เซ็นต์(%)
- หน่วยความจำ (Memory) จากโปรแซสทั้งหมด 4.20 เปอร์เซ็นต์(%)
- อัตราการส่งข้อมูลของ SIP Protocol 324 กิโลบิตต่อวินาที (Kbps)
- การส่งคำสั่งเชื่อมต่อ (SIP Invite) จากโปรแกรมทดสอบโจมตี SIPP ไปยัง IPPBX SERVER ผ่าน SIP PROXY SERVER ยังทำงานครบตามภาพที่ 4.18



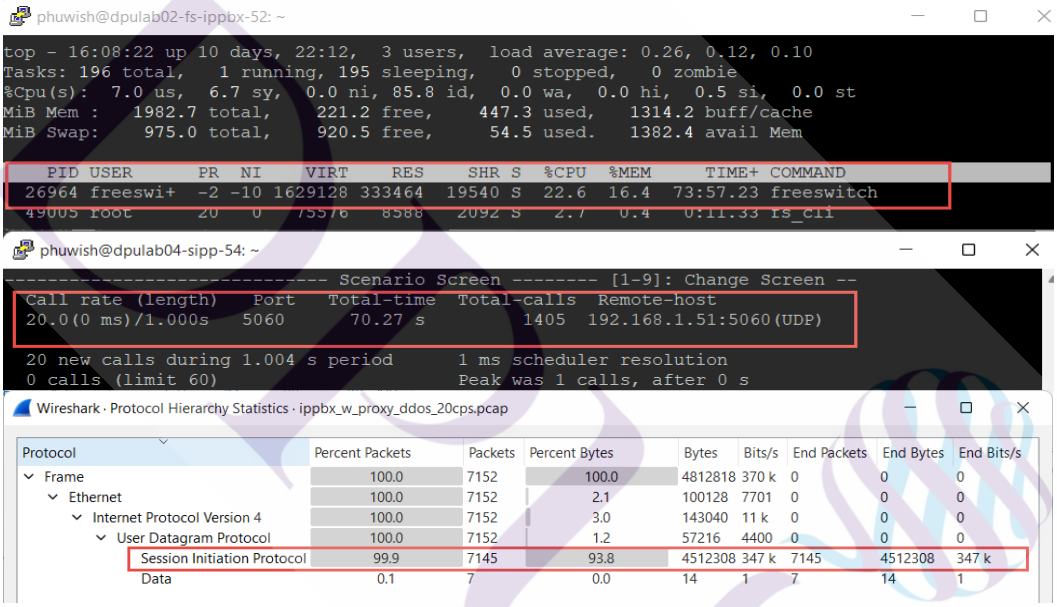
ภาพที่ 4.17 แสดงข้อมูลการใช้ทรัพยากร SIP PROXY SERVER แบบที่ 1 ครั้งที่ 1

ภาพที่ 4.18 แสดงข้อมูลการเชื่อมต่อสัญญาณระหว่างโปรแกรมทดสอบการโจมตีกับ IPPBX SERVER และ IPPBX SERVER แบบที่ 1 ครั้งที่ 1

4.2.1.1.2 ผลการทดสอบครั้งที่ 2 ในต่ออัตราการโทรศัพท์ (Call rate) เป็น 20 ครั้งต่อวินาที โดยมีผลข้อมูลที่ได้ 2 ส่วนคือ

ข้อมูลการใช้ทรัพยากรของ IPPBX SERVER

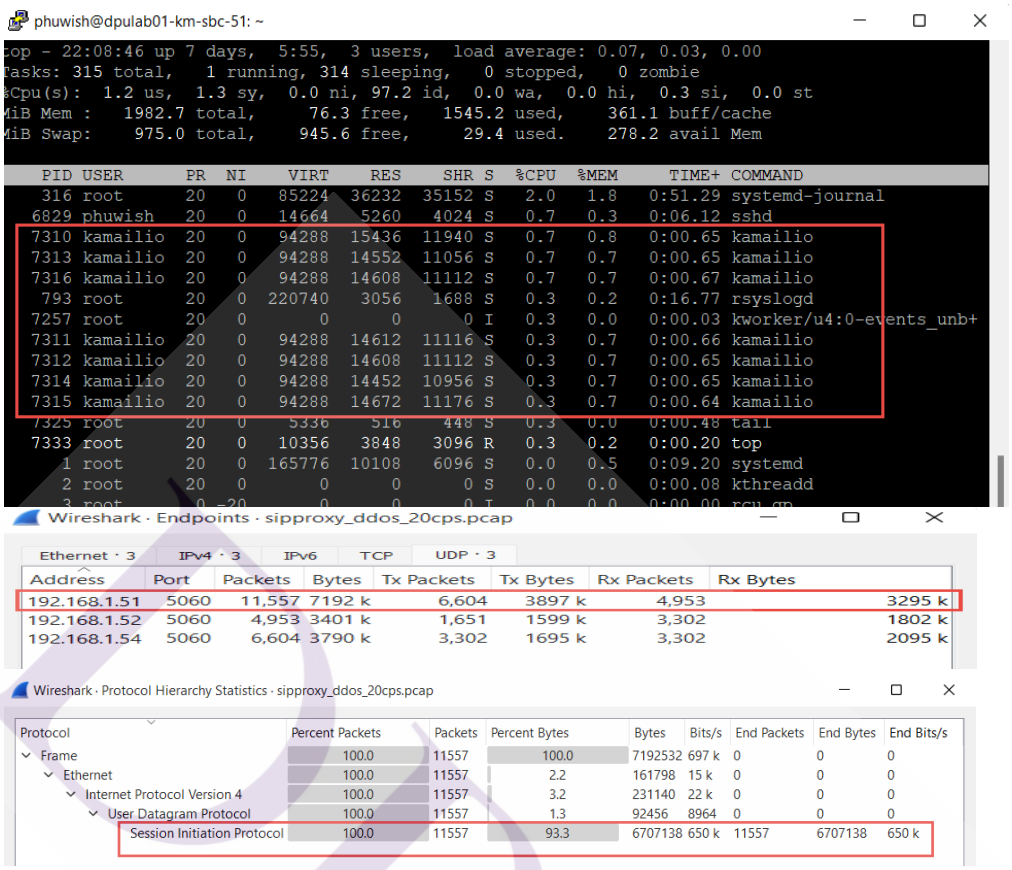
- จำนวนครั้งที่โทรศัพท์ (Total call) 1,405 ครั้ง
- ระยะเวลาในการโทรศัพท์ทั้งหมด (Total time) 70.27 วินาที
- หน่วยประมวลผลกลาง (CPU) 22.60 เปอร์เซ็นต์(%)
- หน่วยความจำ (Memory) 16.40 เปอร์เซ็นต์(%)
- อัตราการส่งข้อมูลของ SIP Protocol 347 กิโลบิตต่อวินาที (Kbps)



ภาพที่ 4.19 แสดงข้อมูลการใช้ทรัพยากรของ IPPBX SERVER แบบที่ 1 ครั้งที่ 2

ข้อมูลการใช้ทรัพยากรของ SIP PROXY SERVER

- หน่วยประมวลผลกลาง (CPU) จากโปรแซสทั้งหมด 3.30 เปอร์เซ็นต์(%)
- หน่วยความจำ (Memory) จากโปรแซสทั้งหมด 5.00 เปอร์เซ็นต์(%)
- อัตราการส่งข้อมูลของ SIP Protocol 650 กิโลบิตต่อวินาที (Kbps)
- การส่งคำสั่งเชื่อมต่อ (SIP Invite) จากโปรแกรมทดสอบโจมตี SIPP ไปยัง IPPBX SERVER ผ่าน SIP PROXY SERVER ยังทำงานครบตามภาพที่ 4.21



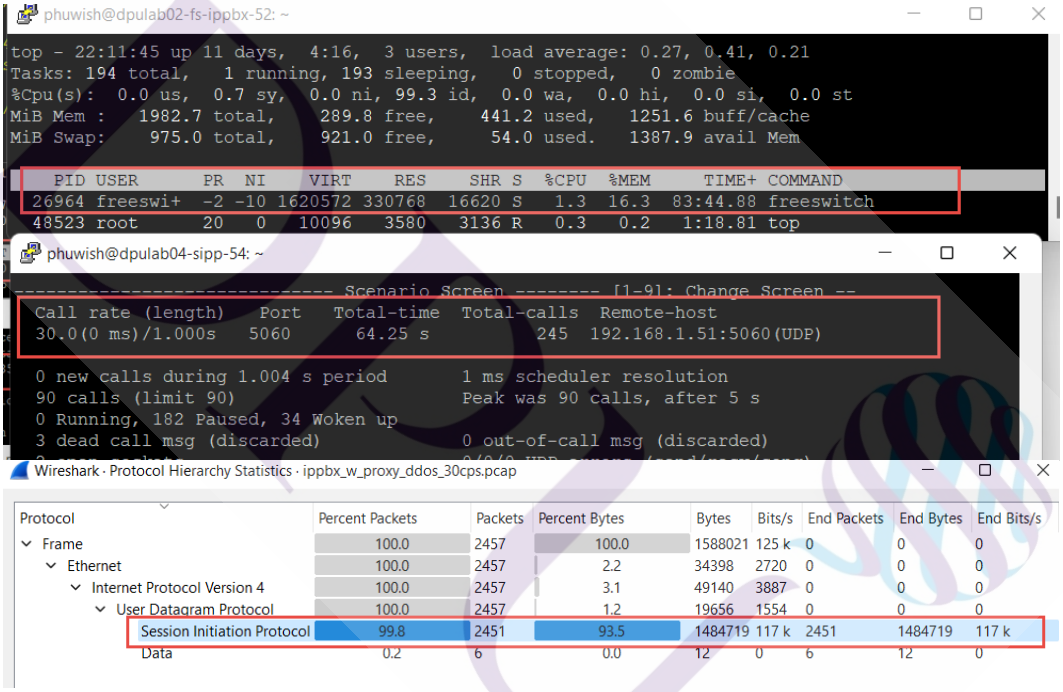
ภาพที่ 4.20 แสดงข้อมูลการใช้ทรัพยากร SIP PROXY SERVER แบบที่ 1 ครั้งที่ 2

ภาพที่ 4.21 แสดงข้อมูลการเชื่อมต่อสัญญาณระหว่างโปรแกรมทดสอบการโจมตีกับ IPPBX SERVER และ IPPBX SERVER แบบที่ 1 ครั้งที่ 2

4.2.1.1.3 ผลการทดสอบครั้งที่ 3 ในต่ออัตราการโทรศัพท์ (Call rate) เป็น 30 ครั้งต่อวินาที

ข้อมูลการใช้ทรัพยากรของ IPPBX SERVER

- จำนวนครั้งที่โทรศัพท์ (Total call) 245 ครั้ง
- ระยะเวลาในการโทรศัพท์ทั้งหมด (Total time) 62.25 วินาที
- หน่วยประมวลผลกลาง (CPU) 1.30 เปอร์เซ็นต์(%)
- หน่วยความจำ (Memory) 16.30 เปอร์เซ็นต์(%)
- อัตราการส่งข้อมูลของ SIP Protocol 117 กิโลบิตต่อวินาที (Kbps)

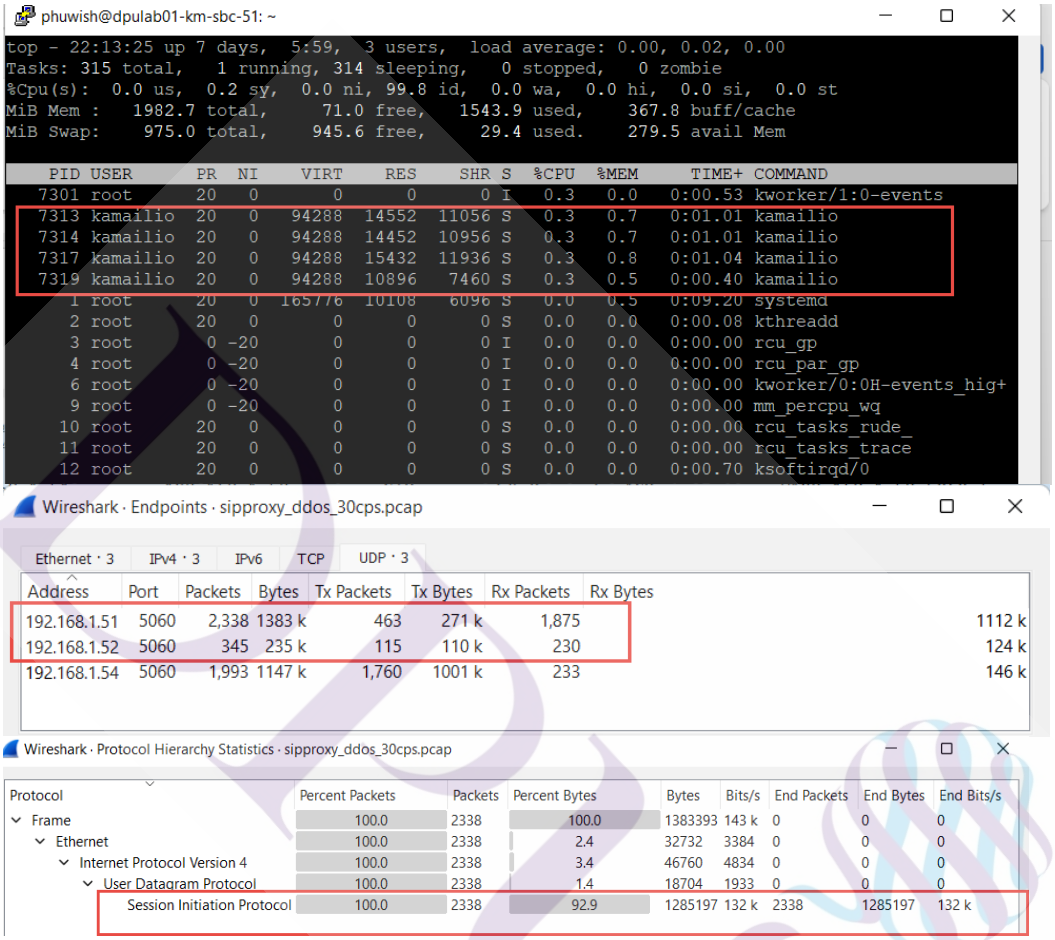


ภาพที่ 4.22 แสดงข้อมูลการใช้ทรัพยากรของ IPPBX SERVER แบบที่ 1 ครั้งที่ 3

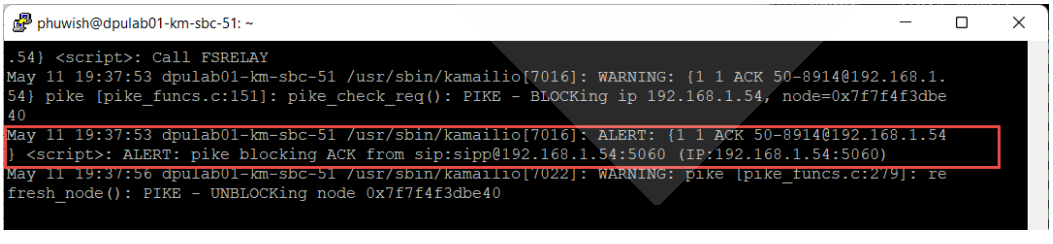
ข้อมูลการใช้ทรัพยากรของ SIP PROXY SERVER

- หน่วยประมวลผลกลาง (CPU) จากโปรแซสทั้งหมด 1.20 เปอร์เซ็นต์(%)
- หน่วยความจำ (Memory) จากโปรแซสทั้งหมด 2.70 เปอร์เซ็นต์(%)
- อัตราการส่งข้อมูลของ SIP Protocol 132 กิโลบิตต่อวินาที (Kbps)
- การส่งคำสั่งเชื่อมต่อ (SIP Invite) จากโปรแกรมทดสอบโจมตี SIPP ไปยัง IPPBX SERVER ผ่าน SIP PROXY SERVER ยังทำงานครบตามภาพที่

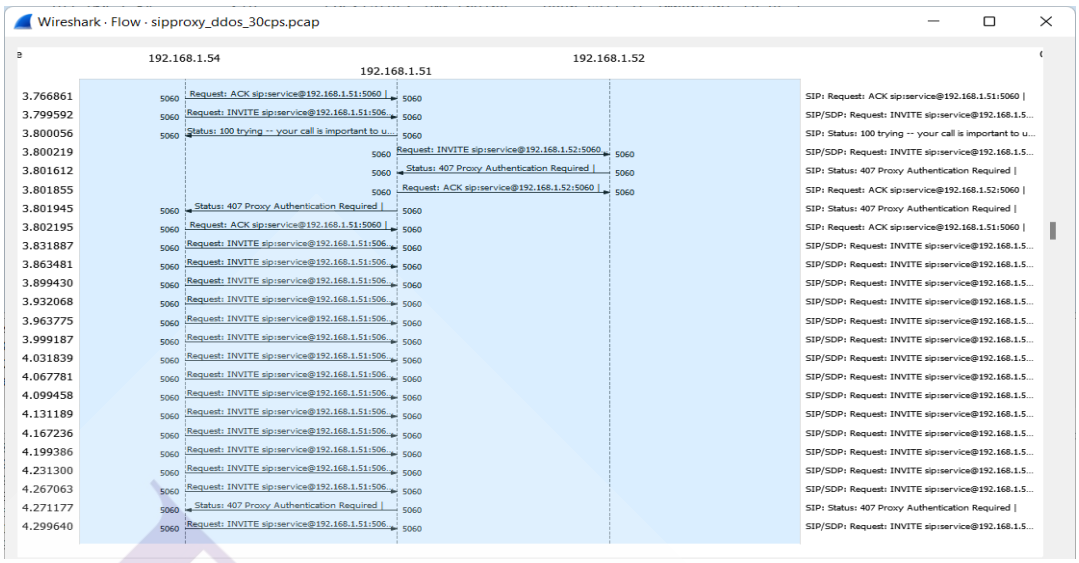
4.24 และ 4.25 ซึ่งจะมีช่วงที่ SIP PROXY SERVER ปฏิเสธการเชื่อมต่อจาก IP Address ทำให้เห็นว่ามีการหยุดส่งคำสั่ง ไปยัง IPPBX SERVER



ภาพที่ 4.23 แสดงข้อมูลการใช้ทรัพยากร SIP PROXY SERVER แบบที่ 1 ครั้งที่ 3



ภาพที่ 4.24 แสดงข้อมูลจาก SIP PROXY SERVER เกี่ยวกับการปฏิเสธการเชื่อมต่อจาก IP Address แบบที่ 1 ครั้งที่ 3



ภาพที่ 4.25 แสดงข้อมูลการเชื่อมต่อสัญญาณระหว่างโปรแกรมทดสอบการโจมตีกับ IPPBX SERVER และ IPPBX SERVER แบบที่ 1 ครั้งที่ 3

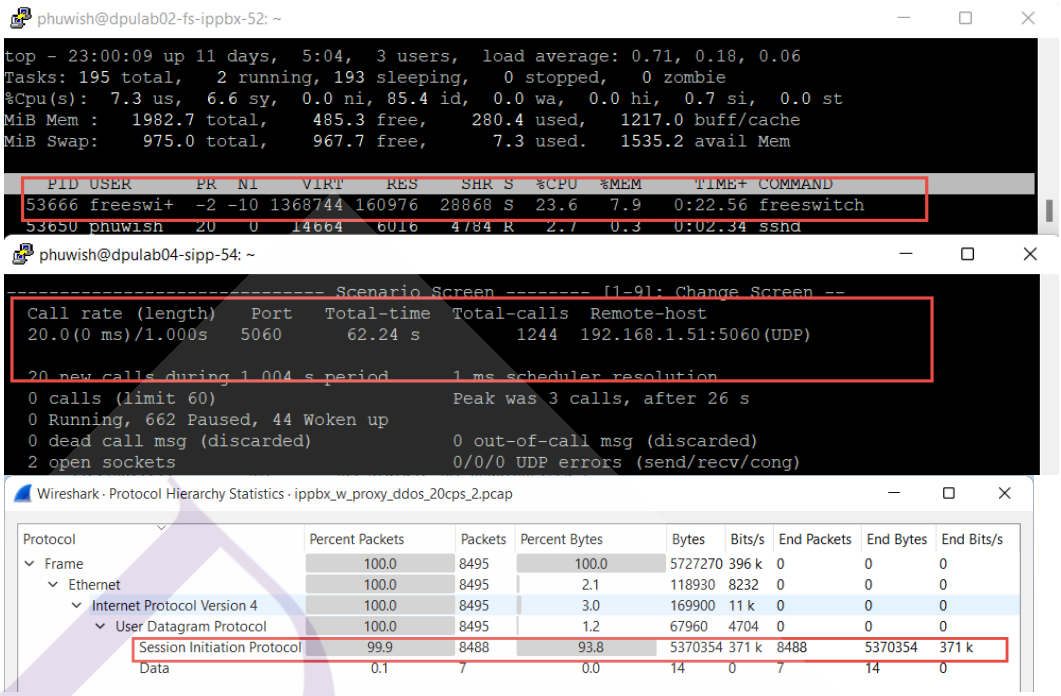
4.2.1.2 ทดสอบแบบที่ 2 โดยกำหนดค่าบนโมดูล pike ดังนี้

- Sampling time unit 2 วินาที
- Reqs_density_per_unit 200 ครั้ง
- Remove_latency 120 วินาที

4.2.1.2.1 ผลการทดสอบครั้งที่ 1 ในต่ออัตราการโทรศัพท์ (Call rate) เป็น 20 ครั้งต่อวินาที

ข้อมูลการใช้ทรัพยากรของ IPPBX SERVER

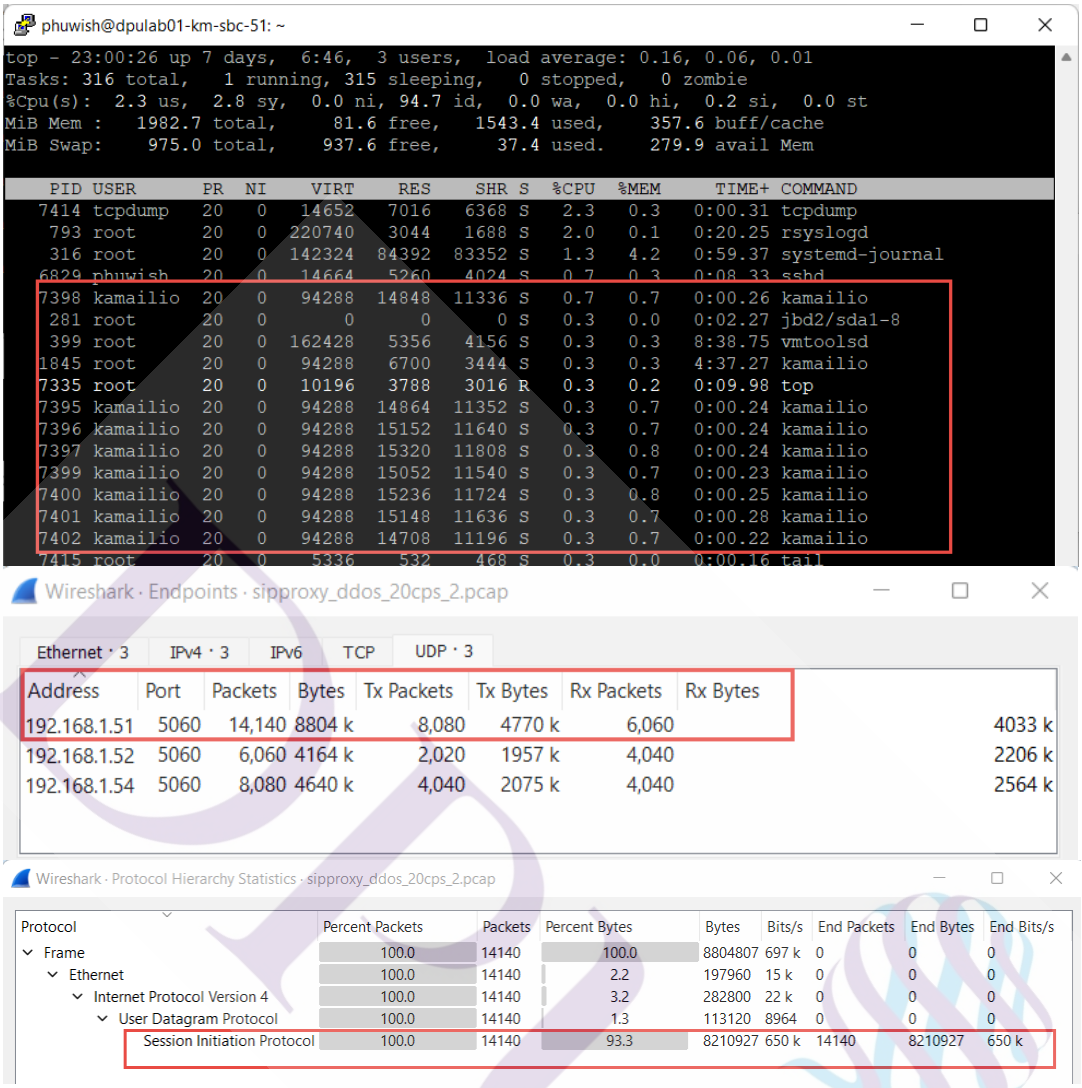
- จำนวนครั้งที่โทรศัพท์(Total call) 1,244 ครั้ง
- ระยะเวลาในการโทรศัพท์ทั้งหมด (Total time) 62.24 วินาที
- หน่วยประมวลผลกลาง (CPU) 23.60 เปอร์เซ็นต์(%)
- หน่วยความจำ (Memory) 7.90 เปอร์เซ็นต์(%)
- อัตราการส่งข้อมูลของ SIP Protocol 371 กิโลบิตต่อวินาที (Kbps)



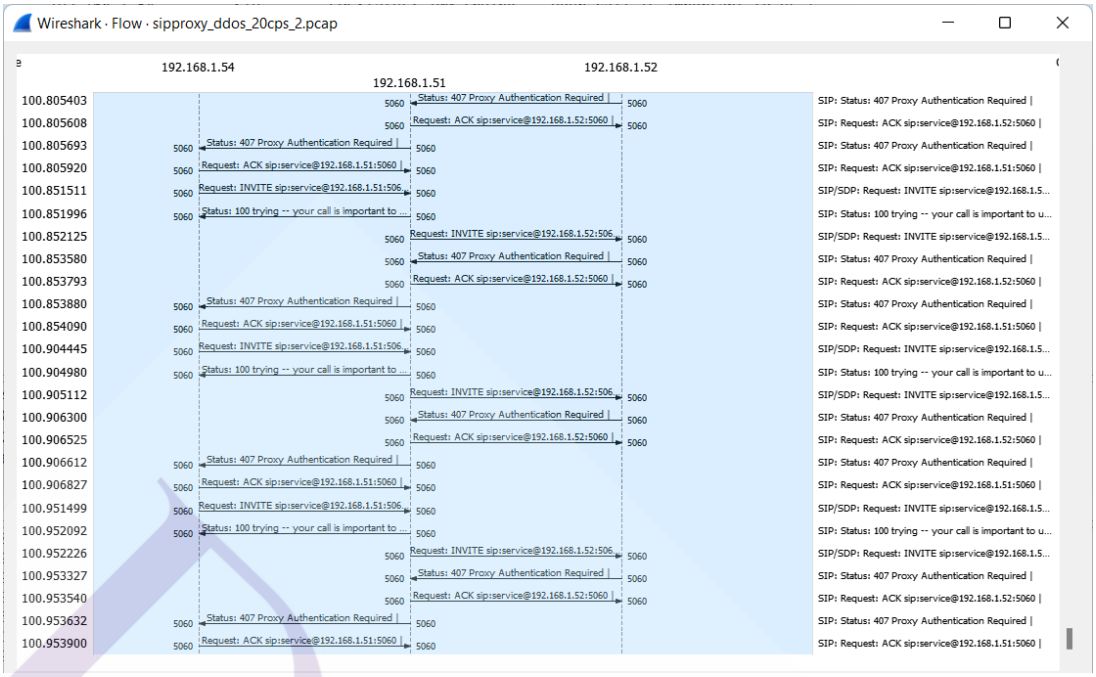
ภาพที่ 4.26 แสดงข้อมูลการใช้ทรัพยากรของ IPPBX SERVER แบบที่ 2 ครั้งที่ 1

ข้อมูลการใช้ทรัพยากรของ SIP PROXY SERVER

- หน่วยประมวลผลกลาง (CPU) จากโปรแซสทั้งหมด 3.10 เปอร์เซ็นต์(%)
- หน่วยความจำ (Memory) จากโปรแซสทั้งหมด 8.80 เปอร์เซ็นต์(%)
- อัตราการส่งข้อมูลของ SIP Protocol 650 กิโลบิตต่อวินาที (Kbps)
- การส่งคำสั่งเชื่อมต่อ (SIP INVITE) จากโปรแกรมทดสอบโจมตี SIPP ไปยัง IPPBX SERVER ผ่าน SIP PROXY SERVER ยังทำงานครบตามภาพที่ 4.28



ภาพที่ 4.27 แสดงข้อมูลการใช้ทรัพยากร SIP PROXY SERVER แบบที่ 2 ครั้งที่ 1

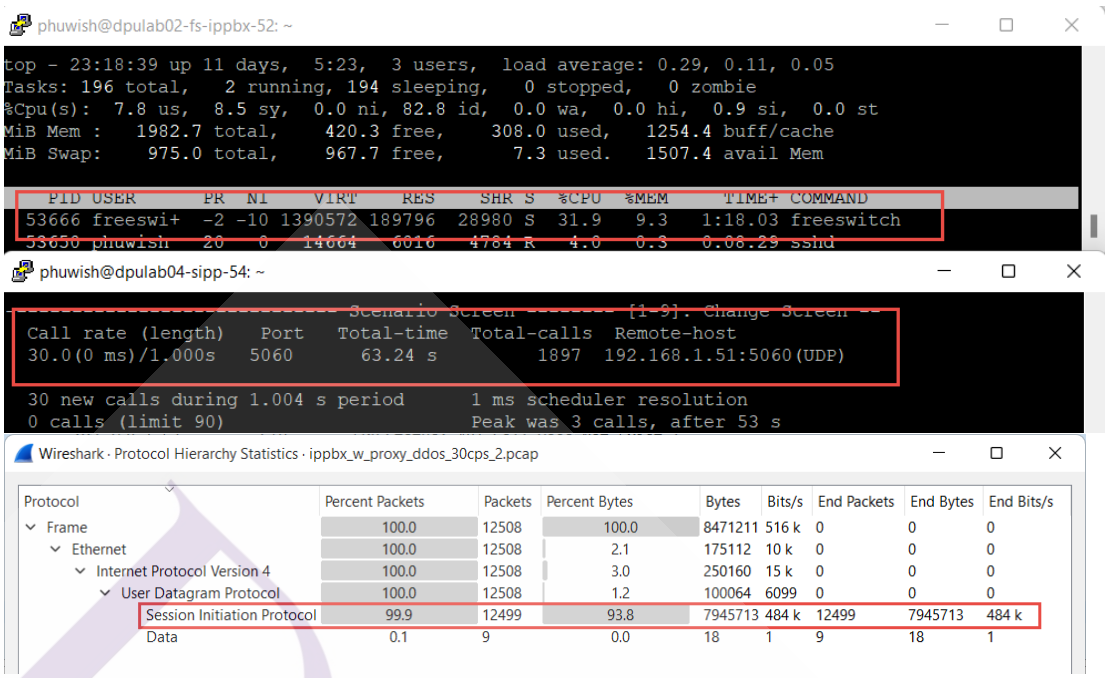


ภาพที่ 4.28 แสดงข้อมูลการเชื่อมต่อสัญญาณระหว่างโปรแกรมทดสอบการโจมตีกับ IPPBX SERVER และ IPPBX SERVER แบบที่ 2 ครั้งที่ 1

4.2.1.2.2 ผลการทดสอบครั้งที่ 2 ในต่ออัตราการโทรศัพท์ (Call rate) เป็น 30 ครั้งต่อวินาที

ข้อมูลการใช้ทรัพยากรของ IPPBX SERVER

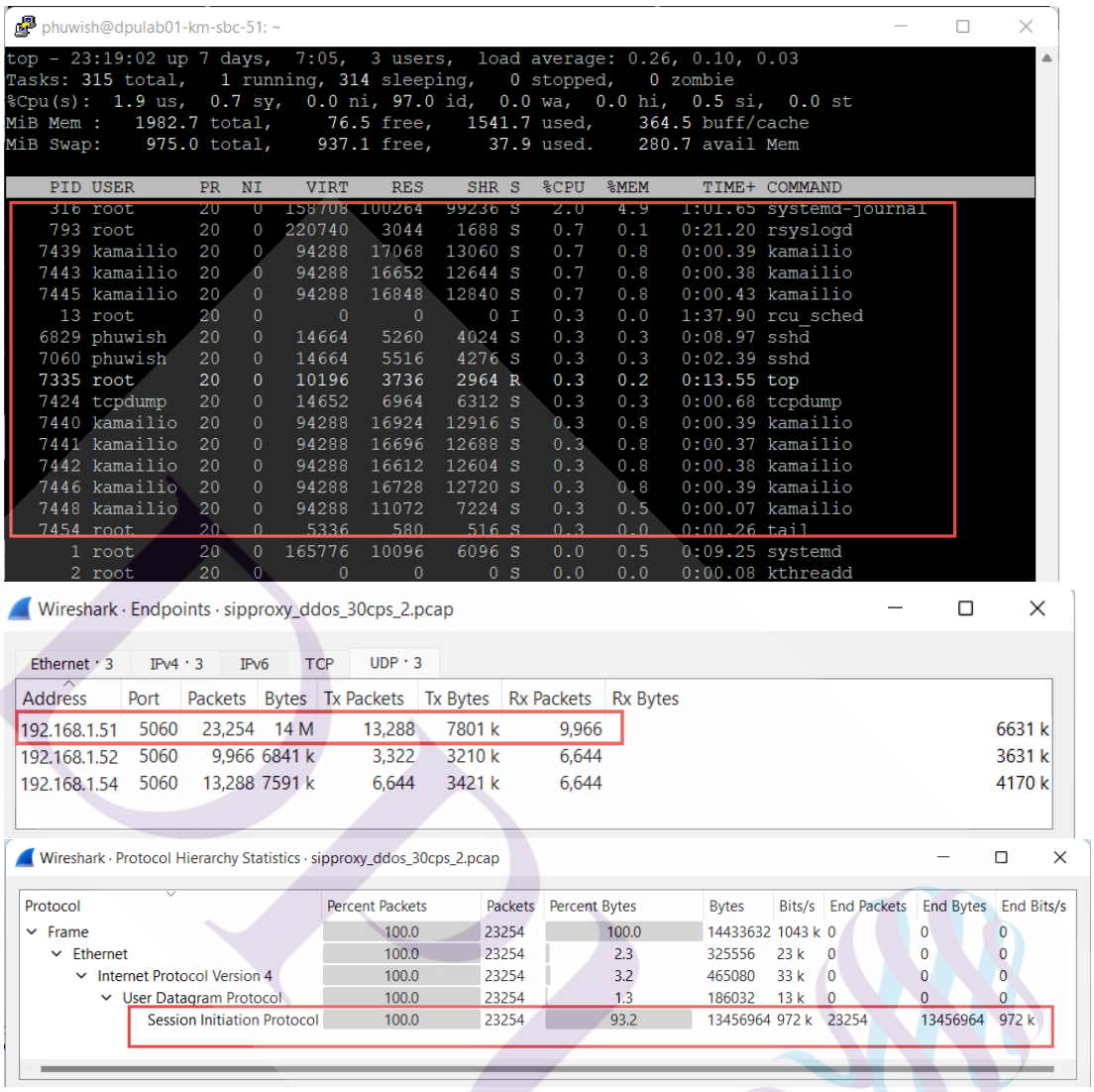
- จำนวนครั้งที่โทรศัพท์ (Total call) 1,897 ครั้ง
- ระยะเวลาในการโทรศัพท์ทั้งหมด(Total time) 63.24 วินาที
- หน่วยประมวลผลกลาง (CPU) 31.90 เปอร์เซ็นต์(%)
- หน่วยความจำ (Memory) 9.30 เปอร์เซ็นต์(%)
- อัตราการส่งข้อมูลของ SIP Protocol 484 กิโลบิตต่อวินาที (Kbps)



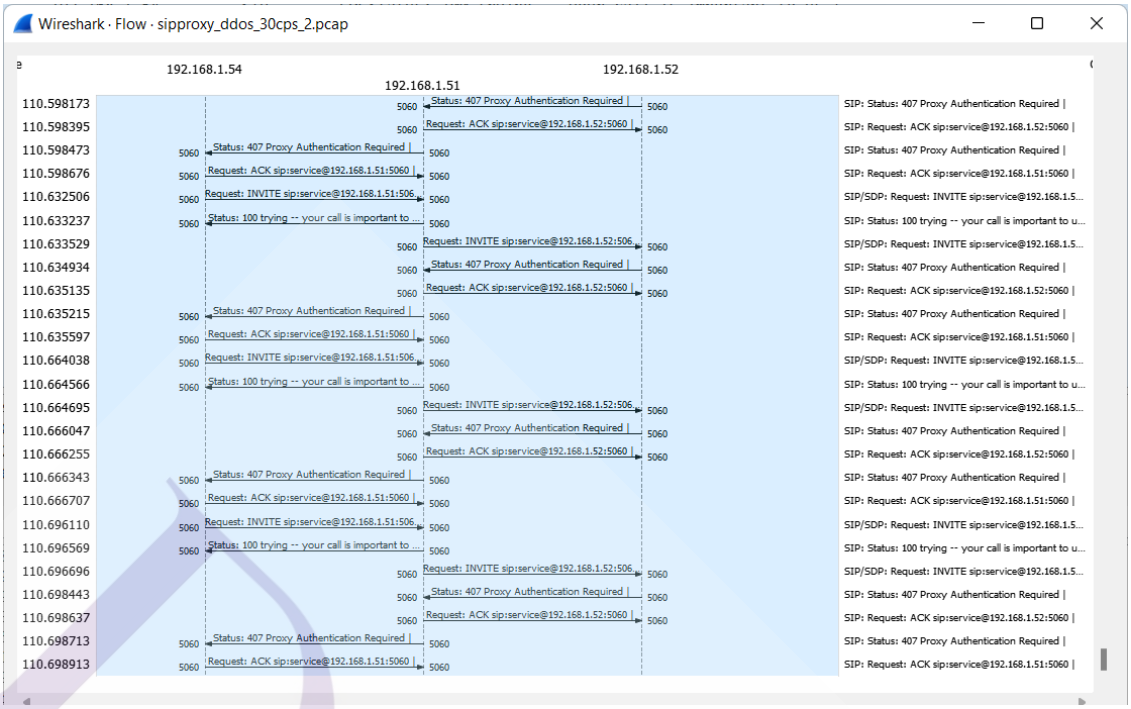
ภาพที่ 4.29 แสดงข้อมูลการใช้ทรัพยากรของ IPPBX SERVER แบบที่ 2 ครั้งที่ 2

ข้อมูลการใช้ทรัพยากรของ SIP PROXY SERVER

- หน่วยประมวลผลกลาง (CPU) จากโปรแซสทั้งหมด 3.60 เปอร์เซ็นต์(%)
- หน่วยความจำ (Memory) จากโปรแซสทั้งหมด 6.10 เปอร์เซ็นต์(%)
- อัตราการส่งข้อมูลของ SIP Protocol 972 กิโลบิตต่อวินาที (Kbps)
- การส่งคำสั่งเชื่อมต่อ (SIP INVITE) จากโปรแกรมทดสอบโจมตี SIPP ไปยัง IPPBX SERVER ผ่าน SIP PROXY SERVER ยังทำงานครบตามภาพที่ 4.31



ภาพที่ 4.30 แสดงข้อมูลการใช้ทรัพยากร SIP PROXY SERVER แบบที่ 2 ครั้งที่ 2

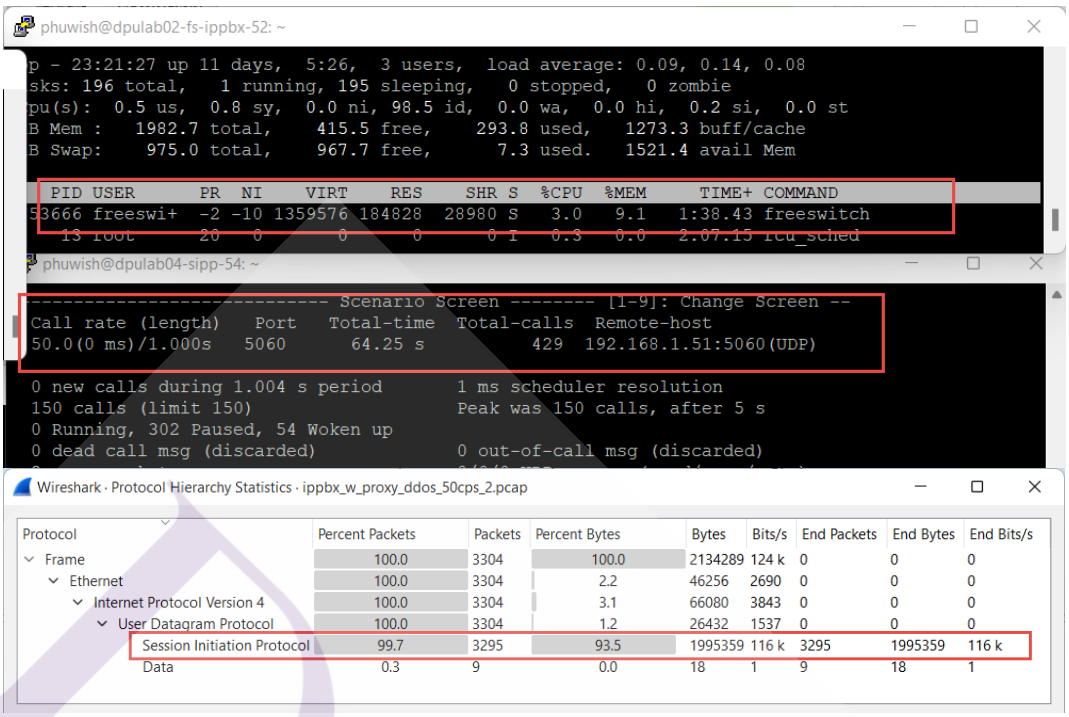


ภาพที่ 4.31 แสดงข้อมูลการเชื่อมต่อสัญญาณระหว่าง โปรแกรมทดสอบการโจมตี กับ IPPBX SERVER และ IPPBX SERVER แบบที่ 2 ครั้งที่ 2

4.2.1.2.3 ผลการทดสอบครั้งที่ 3 ในต่ออัตราการโทรศัพท์ (Call rate) เป็น 50 ครั้งต่อวินาที

ข้อมูลการใช้ทรัพยากรของ IPPBX SERVER

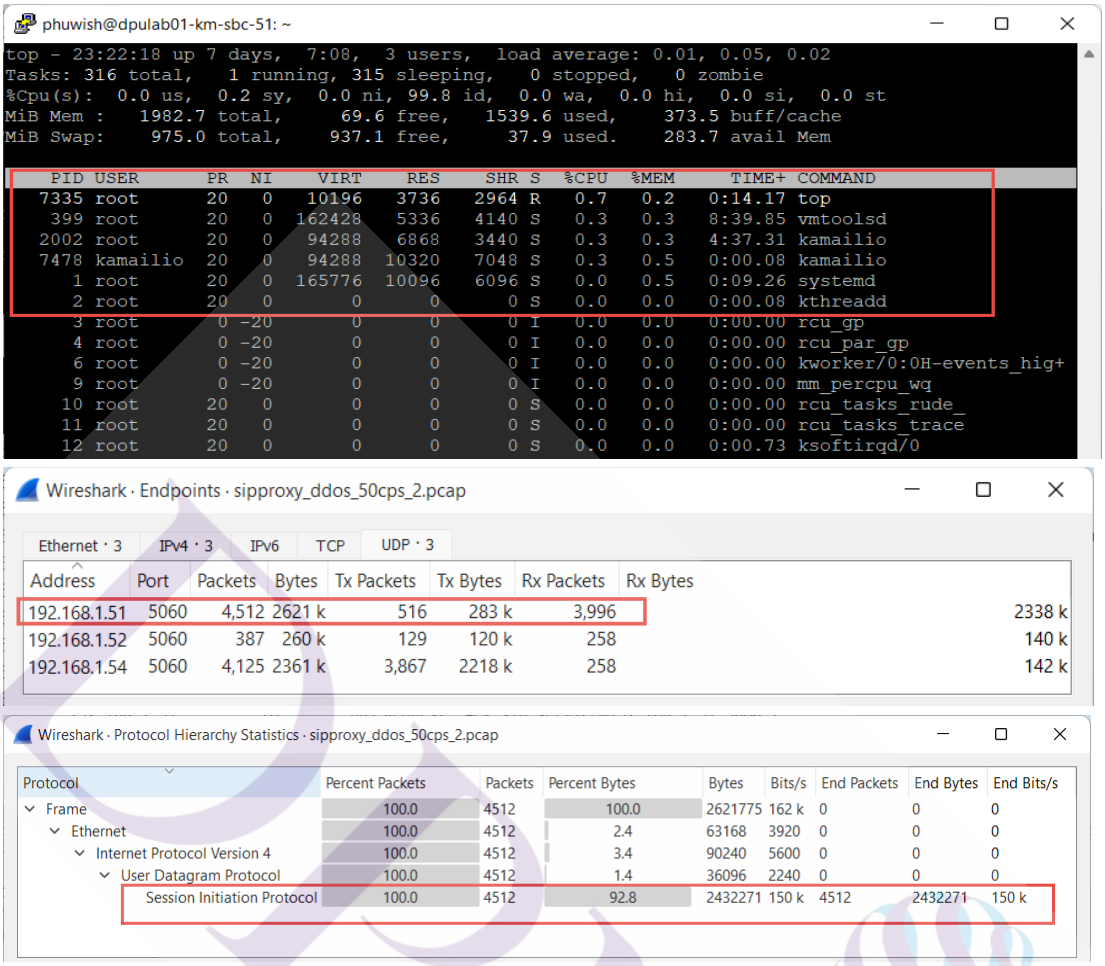
- จำนวนครั้งที่โทรศัพท์(Total call) 429 ครั้ง
- ระยะเวลาในการโทรศัพท์ทั้งหมด(Total time) 64.25 วินาที
- หน่วยประมวลผลกลาง (CPU) 3.00 เปอร์เซ็นต์(%)
- หน่วยความจำ(Memory) 9.10 เปอร์เซ็นต์(%)
- อัตราการส่งข้อมูลของ SIP Protocol 116 กิโลบิตต่อวินาที (Kbps)



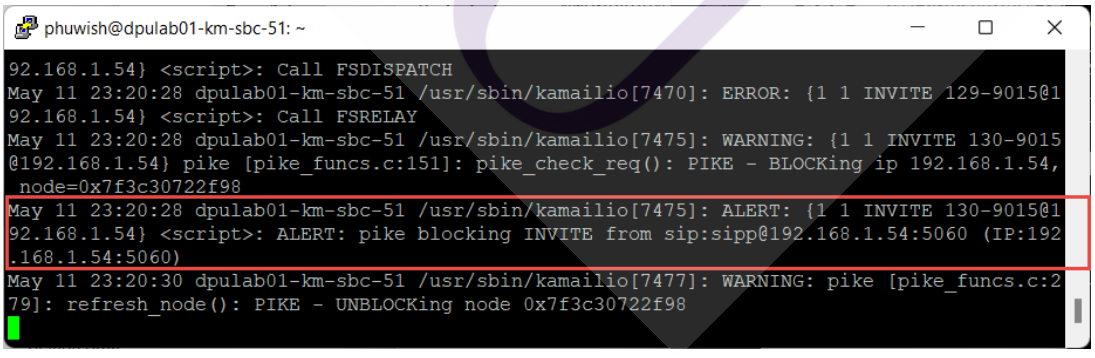
ภาพที่ 4.32 แสดงข้อมูลการใช้ทรัพยากรของ IPPBX SERVER แบบที่ 2 ครั้งที่ 3

ข้อมูลการใช้ทรัพยากรของ SIP PROXY SERVER

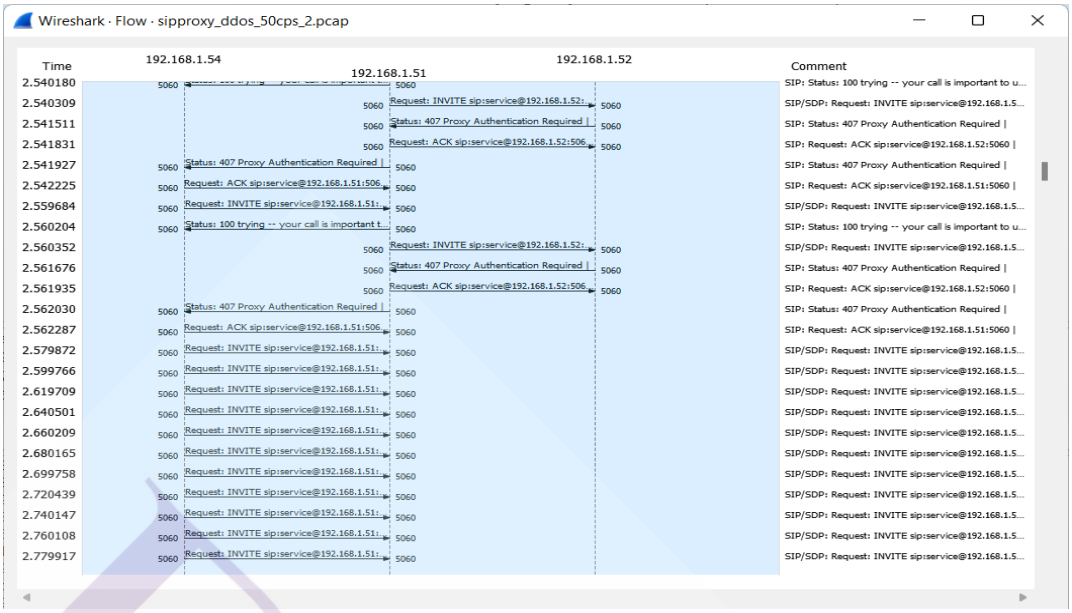
- หน่วยประมวลผลกลาง (CPU) จากโปรแซสทั้งหมด 0.60 เปอร์เซ็นต์(%)
- หน่วยความจำ (Memory) จากโปรแซสทั้งหมด 0.80 เปอร์เซ็นต์(%)
- อัตราการส่งข้อมูลของ SIP Protocol 150 กิโลบิตต่อวินาที (Kbps)
- การส่งคำสั่งเชื่อมต่อ (SIP INVITE) จากโปรแกรมทดสอบโจมตี SIPP ไปยัง IPPBX SERVER ผ่าน SIP PROXY SERVER ยังทำงานตามภาพที่ 4.35 ซึ่งจะมีช่วงที่ SIP PROXY SERVER ปฏิเสธการเชื่อมต่อจาก IP Address ตามภาพที่ 4.34 ทำให้เห็นว่ามีการหยุดส่งคำสั่ง ไปยัง IPPBX SERVER แล้วในขณะเดียวกันการเชื่อมต่อภายในของ IPPBX SERVER ยังทำงานได้ตามปกติโดยไม่มีผลกระทบดังภาพที่ 4.36 และ 4.37



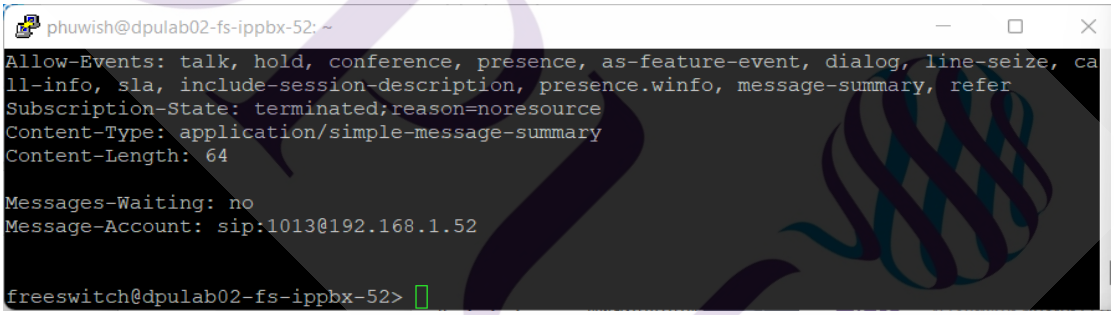
ภาพที่ 4.33 แสดงข้อมูลการใช้ทรัพยากร SIP PROXY SERVER แบบที่ 2 ครั้งที่ 3



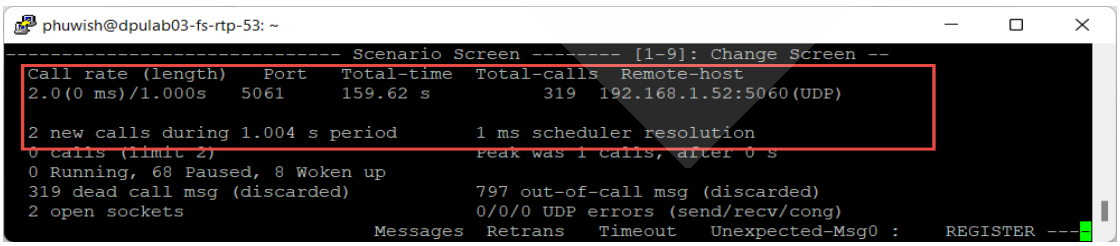
ภาพที่ 4.34 แสดงข้อมูลการใช้ทรัพยากร SIP PROXY SERVER แบบที่ 2 ครั้งที่ 3



ภาพที่ 4.35 แสดงข้อมูลการเชื่อมต่อสัญญาณระหว่างโปรแกรมทดสอบการโจมตีกับ IPPBX SERVER และ SIP PROXY SERVER แบบที่ 2 ครั้งที่ 3



ภาพที่ 4.36 แสดงข้อมูลการทำงาน IPPBX SERVER ในการทดสอบแบบที่ 2 ครั้งที่ 3



ภาพที่ 4.37 แสดงข้อมูลสถานะการทดสอบคำสั่งลงทะเบียน(SIP REGISTER) IPPBX SERVER ในการทดสอบแบบที่ 2 ครั้งที่ 3

4.2.2 สรุปข้อมูลการใช้ทรัพยากรของระบบในการทดสอบ

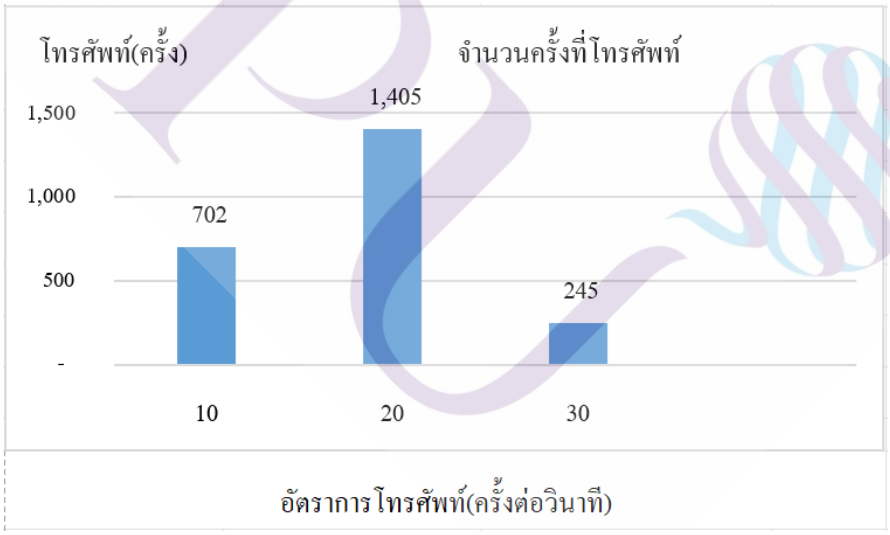
4.2.2.1 การทดสอบแบบที่ 1 กำหนดให้โมดูล Pike มีการตั้งค่าดังนี้

- Sampling time unit 2 วินาที
- Reqs_density_per_unit 100 ครั้ง
- Remove_latency 120 วินาที

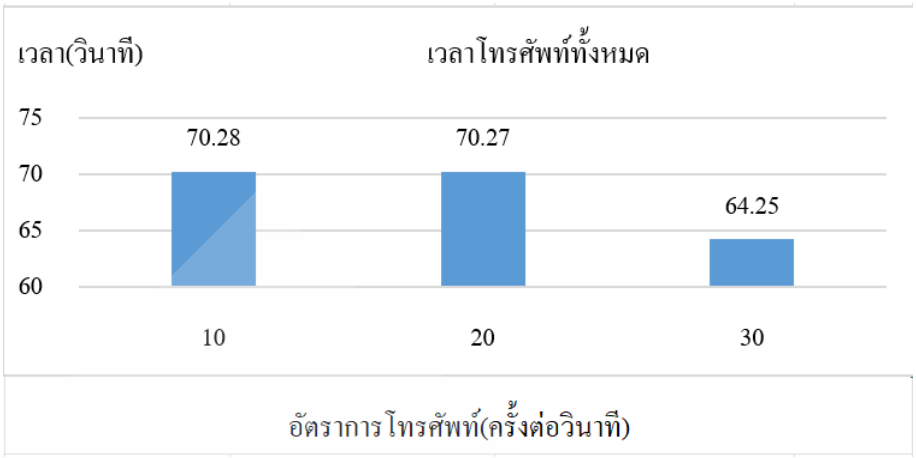
ข้อมูลการใช้ทรัพยากรของ IPPBX SERVER

ตารางที่ 4.2 แสดงขข้อมูลทรัพยากรขของ IPPBX SERVER ในการทดสอบแบบที่ 1

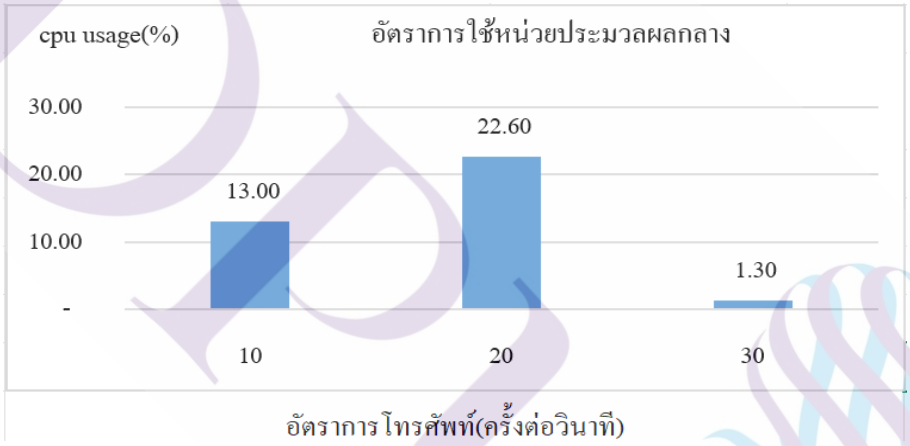
อัตราการโทรศัพท์ (ครั้งต่อวินาที)	โทรศัพท์ (ครั้ง)	ทั้งหมด (วินาที)	หน่วยประมวลผลกลาง (%)	หน่วยความจำหลัก (%)	ของ SIP Protocol (กิโลบิต/วินาที)
10	702	70.28	13.00	16.40	221
20	1,405	70.27	22.60	16.40	347
30	245	64.25	1.30	16.30	117



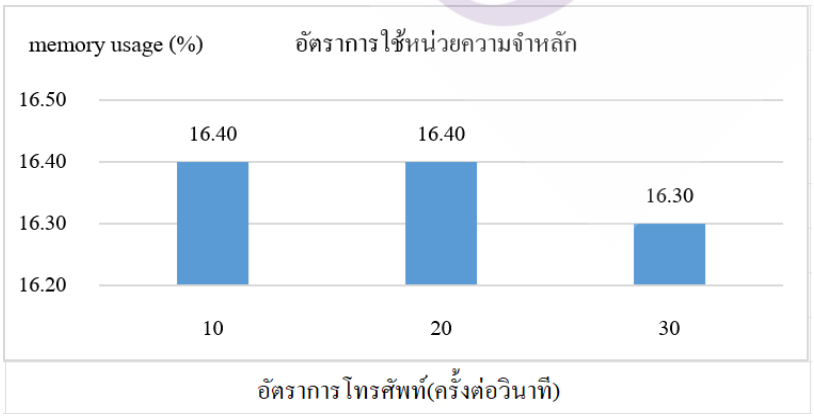
ภาพที่ 4.38 กราฟแสดงจำนวนครั้งที่โทรศัพท์ในการทดสอบแบบที่ 1



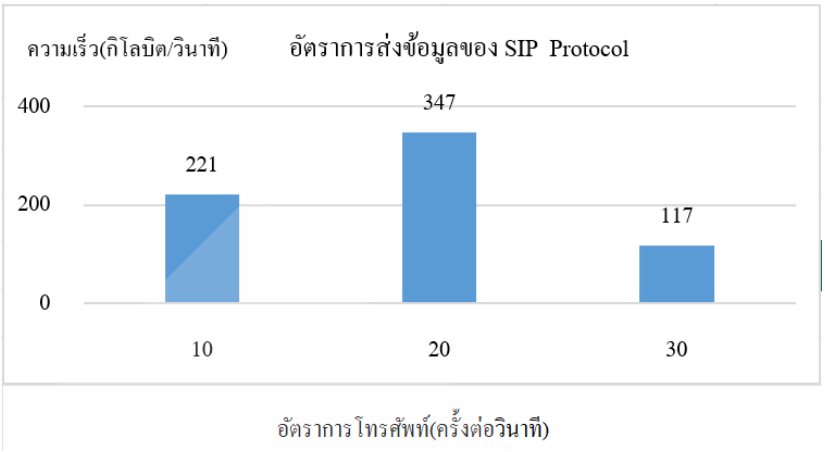
ภาพที่ 4.39 กราฟแสดงเวลาที่โทรศัพท์ทั้งหมดในการทดสอบแบบที่ 1



ภาพที่ 4.40 กราฟแสดงอัตราการใช้หน่วยประมวลผลกลางในการทดสอบแบบที่ 1



ภาพที่ 4.41 กราฟแสดงอัตราการใช้หน่วยความจำหลักในการทดสอบแบบที่ 1

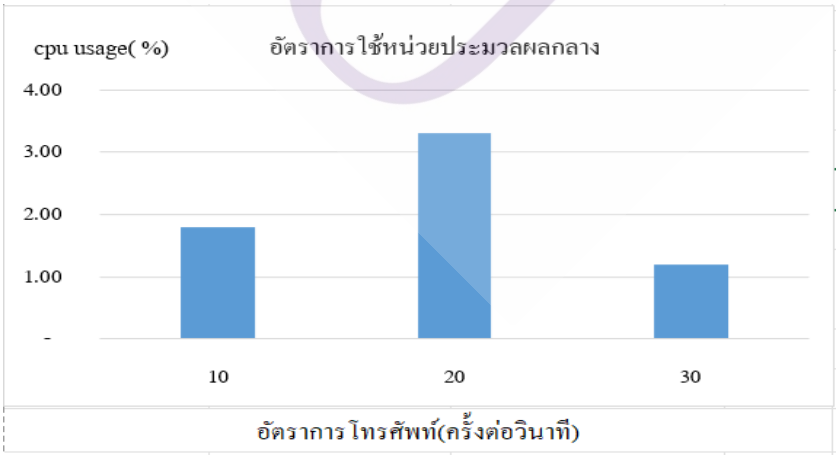


ภาพที่ 4.42 กราฟแสดงอัตราการส่งข้อมูลของ SIP Protocol ในการทดสอบแบบที่ 1

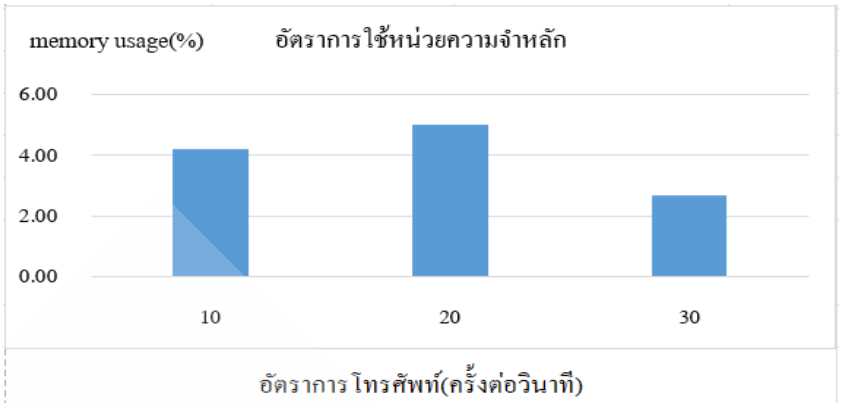
ข้อมูลการใช้ทรัพยากรของ SIP PROXY SERVER

ตารางที่ 4.3 แสดงข้อมูลทรัพยากรของ SIP PROXY SERVER ในการทดสอบแบบที่ 1

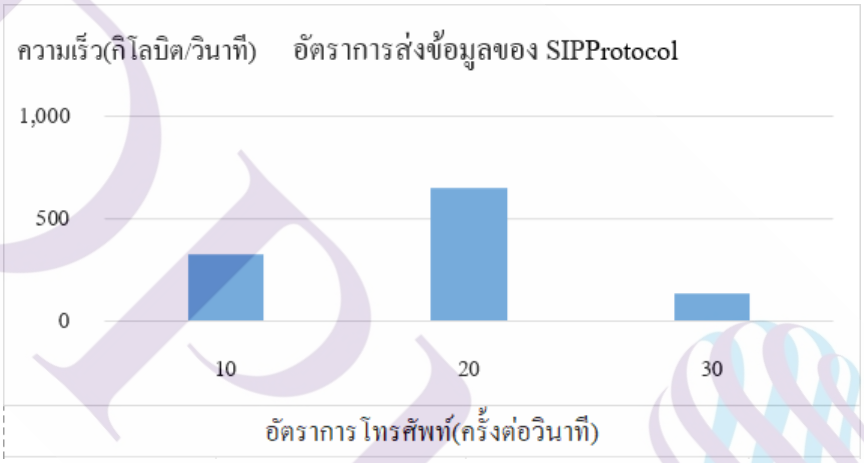
อัตราการโทรศัพท์ (ครั้งต่อวินาที)	อัตราการใช้หน่วยประมวลผลกลาง (%)	อัตราการใช้หน่วยความจำหลัก (%)	อัตราการส่งข้อมูลของ SIP Protocol (กิโลบิต/วินาที)
10	1.80	4.20	324
20	3.30	5.00	650
30	1.20	2.70	132



ภาพที่ 4.43 กราฟแสดงอัตราการใช้หน่วยประมวลผลกลางในการทดสอบแบบที่ 1



ภาพที่ 4.44 กราฟแสดงอัตราการใช้หน่วยความจำหลักในการทดสอบแบบที่ 1



ภาพที่ 4.45 กราฟแสดงอัตราการส่งข้อมูลของ SIP Protocol ในการทดสอบแบบที่ 1

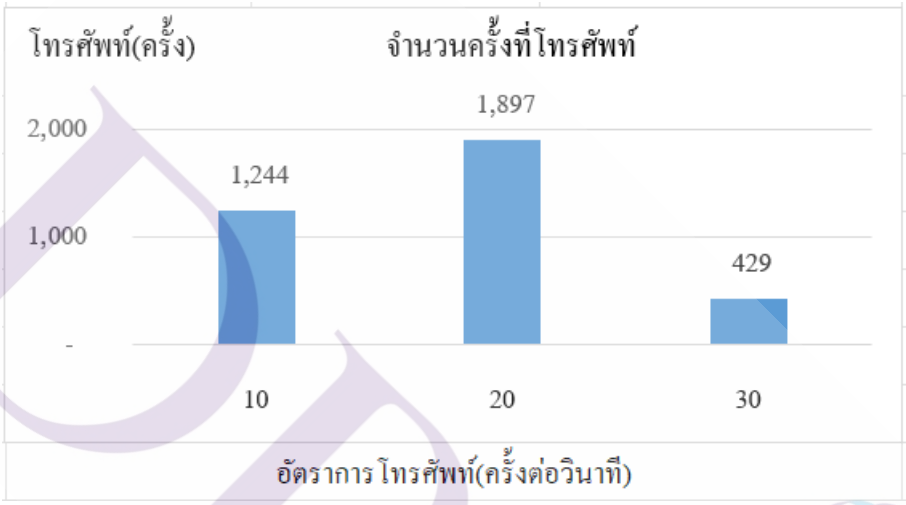
4.2.2.2 การทดสอบแบบที่ 2 กำหนดให้โมดูล Pike มีการตั้งค่าดังนี้

- Sampling time unit 2 วินาที
- Reqs_density_per_unit 200 ครั้ง
- Remove_latency 120 วินาที

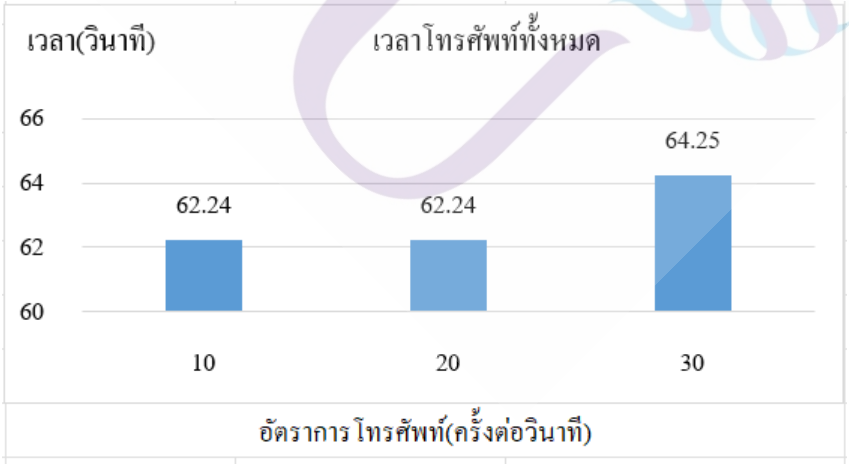
ข้อมูลการใช้ทรัพยากรของ IPPBX SERVER

ตารางที่ 4.4 แสดงข้อมูลทรัพยากรของ IPPBX SERVER ในการทดสอบแบบที่ 2

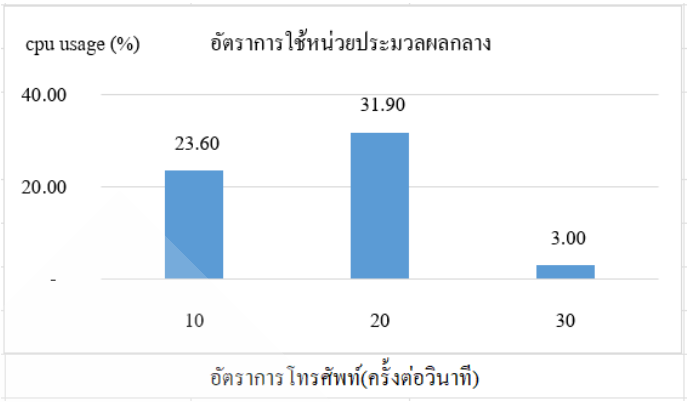
อัตราการโทรศัพท์ (ครั้งต่อวินาที)	จำนวนครั้งที่โทรศัพท์ (ครั้ง)	เวลาโทรศัพท์ทั้งหมด (วินาที)	อัตราการใช้หน่วยประมวลผลกลาง (%)	อัตราการใช้หน่วยความจำหลัก (%)	อัตราการส่งข้อมูลของ SIP Protocol (กิโลบิต/วินาที)
10	702	70.28	13.00	16.40	221
20	1,405	70.27	22.60	16.40	347
30	245	64.25	1.30	16.30	117



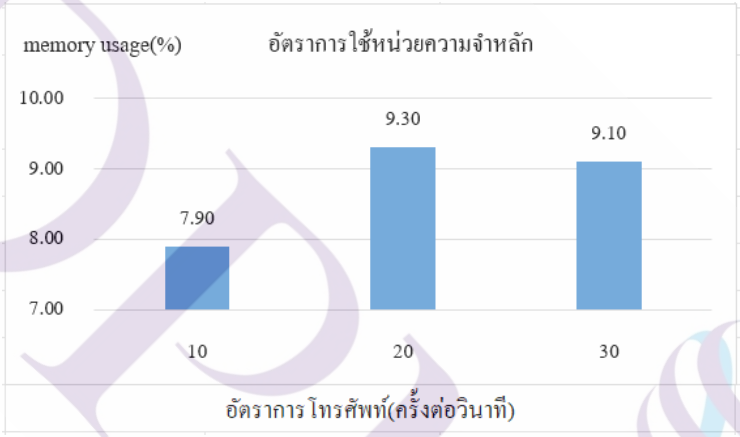
ภาพที่ 4.46 กราฟแสดงจำนวนครั้งที่โทรศัพท์ในการทดสอบแบบที่ 2



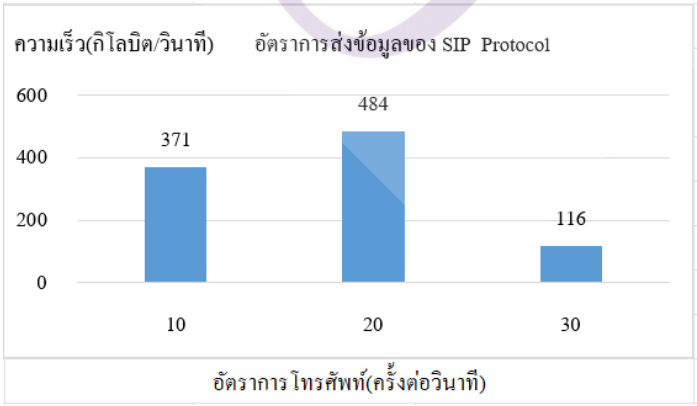
ภาพที่ 4.47 กราฟแสดงเวลาที่โทรศัพท์ทั้งหมดในการทดสอบแบบที่ 2



ภาพที่ 4.48 กราฟแสดงอัตราการใช้หน่วยประมวลผลกลางในการทดสอบแบบที่ 2



ภาพที่ 4.49 กราฟแสดงอัตราการใช้หน่วยความจำหลักในการทดสอบแบบที่ 2

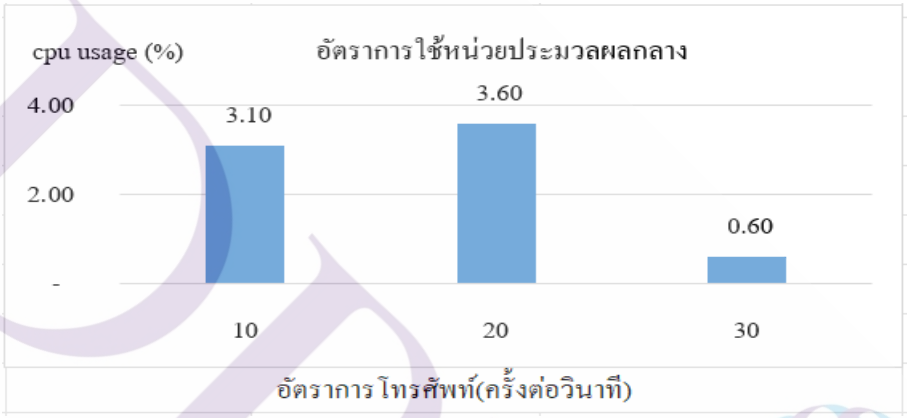


ภาพที่ 4.50 กราฟแสดงอัตราการส่งข้อมูลของ SIP Protocol ในการทดสอบแบบที่ 2

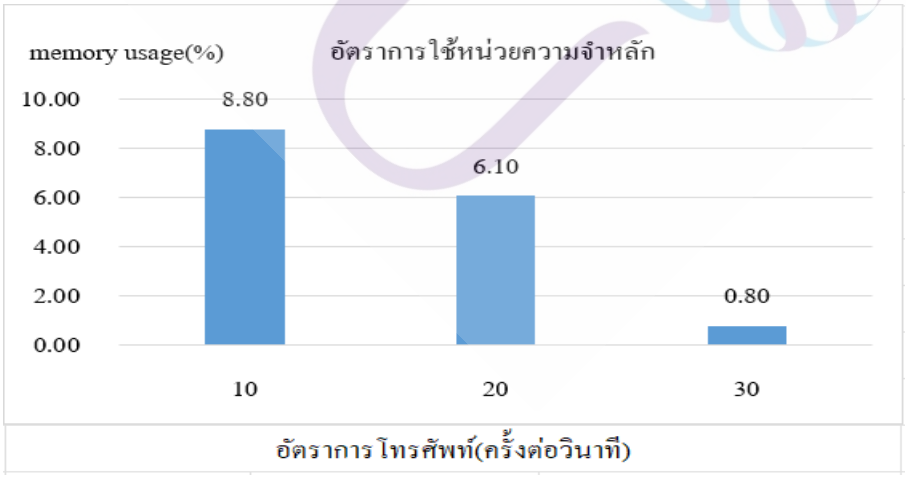
ข้อมูลการใช้ทรัพยากรของ SIP PROXY SERVER

ตารางที่ 4.5 แสดงข้อมูลทรัพยากรของ SIP PROXY SERVER ในการทดสอบแบบที่ 2

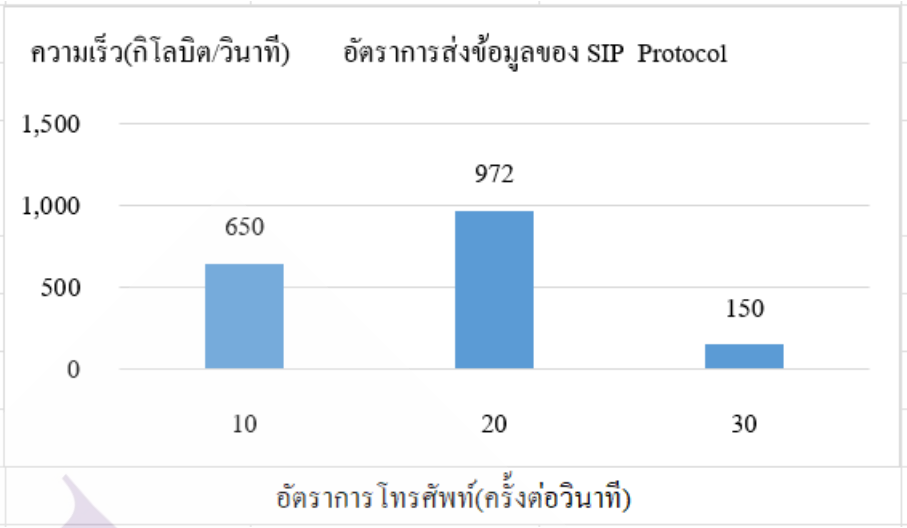
อัตราการโทรศัพท์ (ครั้งต่อวินาที)	อัตราการใช้หน่วยประมวลผลกลาง (%)	อัตราการใช้หน่วยความจำหลัก (%)	อัตราการส่งข้อมูลของ SIP Protocol (กิโลบิต/วินาที)
10	3.10	8.80	650
20	3.60	6.10	972
30	0.60	0.80	150



ภาพที่ 4.51 กราฟแสดงอัตราการใช้หน่วยประมวลผลกลางในการทดสอบแบบที่ 2



ภาพที่ 4.52 กราฟแสดงอัตราการใช้หน่วยความจำหลักในการทดสอบแบบที่ 2



ภาพที่ 4.53 กราฟแสดงอัตราการส่งข้อมูลของ SIP Protocol ในการทดสอบแบบที่ 2

จากข้อมูลในตารางที่ 4.2 ถึง 4.5 และภาพที่ 4.38 ถึง 4.53 จะเห็นได้ว่า มีการใช้ทรัพยากรเครื่องคอมพิวเตอร์แม่ข่ายของ IPPBX SERVER และ SIP PROXY SERVER มีอัตราสูงขึ้นตามอัตราการโทรศัพท์ (Call rate) และจำนวนครั้งที่โทรศัพท์ (Total call) ที่เพิ่มขึ้นโดยมีระยะเวลาในการโทรศัพท์ทั้งหมด(Total time) ใกล้เคียงกัน โดยเฉพาะการใช้หน่วยประมวลผลกลาง (CPU) ,หน่วยความจำ (Memory) และอัตราการส่งข้อมูลของ SIP Protocol มีอัตราการใช้งานเพิ่มขึ้นอย่างเป็นอัตราส่วนที่สอดคล้องกันจนถึงการทดสอบแบบที่ 1 ครั้งที่ 3 จำนวนอัตราการโทรศัพท์(Call rate) มีจำนวนเกินที่กำหนดในโมดูล Pike ของ SIP PROXY SERVER สถานการณ์เชื่อมต่อของ IP ADDRESS จะถูกเปลี่ยนเป็นปฏิเสธการเชื่อมต่อทำให้ทรัพยากรเครื่องคอมพิวเตอร์แม่ข่ายของ IPPBX SERVER และ SIP PROXY SERVER ลดลง และในการทดสอบแบบที่ 2 ครั้งที่ 3 จะเห็นได้ว่าโปรแกรมทดสอบการลงทะเบียนเลขหมาย(SIP REGISTER) ยังสามารถทำงานตามปกติ IPPBX SERVER ในขณะที่คำสั่ง SIP INVITE จาก SIP PROXY SERVER ที่ส่งไปยัง IPPBX SERVER ได้หยุดส่งแล้ว

4.3 อภิปลายผลทดลองและเปรียบเทียบประสิทธิภาพ

สรุปข้อมูลผลการทดสอบเพื่อเปรียบเทียบประสิทธิภาดังตารางที่ 4.6 นี้

ตารางที่ 4.6 แสดงข้อมูลเปรียบเทียบผลการทดสอบในแต่ละแบบ

รูปแบบการทดสอบ	จำนวนครั้งที่โทรศัพท์ทดสอบต่อวินาที	สถานะระบบ SIP PROXY SERVER	สภานะระบบ IPPBX SERVER	การใช้งานโทรศัพท์ผ่านอินเตอร์เน็ต (Softphone) และอุปกรณ์โทรศัพท์	การลงทะเบียนบัญชีหมายเลขโทรศัพท์(SIP Register)
การทดสอบโจมตี IPPBX SERVER	0	ปกติ	ปกติ	โทรศัพท์ระหว่างเครื่องภายในได้	สำเร็จ
	100	ปกติ	ไม่ตอบสนองต่อคำสั่งเชื่อมต่อ (Invite)	ไม่สามารถโทรศัพท์ระหว่างเครื่องภายในได้	ล้มเหลว
	500	ปกติ	ไม่ตอบสนองต่อคำสั่งเชื่อมต่อ (Invite)	ไม่สามารถโทรศัพท์ระหว่างเครื่องภายในได้	ล้มเหลว
	1,000	ปกติ	ไม่ตอบสนองต่อคำสั่งเชื่อมต่อ (Invite)	ไม่สามารถโทรศัพท์ระหว่างเครื่องภายในได้	ล้มเหลว
	5,000	ปกติ	ไม่ตอบสนองต่อคำสั่งเชื่อมต่อ (Invite)	ไม่สามารถโทรศัพท์ระหว่างเครื่องภายในได้	ล้มเหลว
	10,000	ปกติ	ไม่ตอบสนองต่อคำสั่งเชื่อมต่อ (Invite)	ไม่สามารถโทรศัพท์ระหว่างเครื่องภายในได้	ล้มเหลว
การทดสอบโจมตีโดยผ่าน SIP PROXY SERVER กำหนดค่าโมดูล Pike Sampling time unit 2 วินาที Reqs_density_per_unit 100 ครั้ง Remove_latency 120 วินาที	10	ปกติ	ปกติ	โทรศัพท์ระหว่างเครื่องภายในได้	สำเร็จ
	20	ปกติ	ปกติ	โทรศัพท์ระหว่างเครื่องภายในได้	สำเร็จ
	30	ปฏิเสธการคำสั่งเชื่อมต่อ (Invite)	ปกติ	โทรศัพท์ระหว่างเครื่องภายในได้	สำเร็จ
การทดสอบโจมตีโดยผ่าน SIP PROXY SERVER กำหนดค่าโมดูล Pike Sampling time unit 2 วินาที Reqs_density_per_unit 200 ครั้ง Remove_latency 120 วินาที	20	ปกติ	ปกติ	โทรศัพท์ระหว่างเครื่องภายในได้	สำเร็จ
	30	ปกติ	ปกติ	โทรศัพท์ระหว่างเครื่องภายในได้	สำเร็จ
	50	ปฏิเสธการคำสั่งเชื่อมต่อ (Invite)	ไม่ตอบสนองต่อคำสั่งเชื่อมต่อ (Invite)	ไม่สามารถโทรศัพท์ระหว่างเครื่องภายในได้	ล้มเหลว
** หมายเหตุ ระบบ IPPBX SERVER สามารถรองรับการเชื่อมต่อได้ 30 คำสั่งต่อวินาที					

จากตารางที่ 4.6 ผลการทดสอบโจมตีจากกากำหนดรูปแบบการทดสอบเป็น 3 แบบ เพื่อจะสามารถเปรียบเทียบผลลัพท์จากการทดสอบได้ดังนี้

- แบบที่ 1 การทดสอบโจมตี IPPBX SERVER กำหนดจำนวนครั้งที่โทรศัพท์ทดสอบต่อวินาที เป็น 100, 500, 1,000 ,5,000 และ 10,000 ครั้งต่อวินาที มีผลให้ IPPBX SERVER มีผลให้การใช้งานโทรศัพท์ผ่านอินเตอร์เน็ต (Softphone) และอุปกรณ์โทรศัพท์ รวมถึงการลงทะเบียนบัญชีหมายเลขโทรศัพท์ (SIP Register) ไม่สามารถทำงานได้และล้มเหลว ซึ่งจำนวนคำสั่ง SIP

INVITE ที่ถูกส่งไปยัง IPPBX SERVER จะเกินความสามารถในการรองรับคำสั่งไม่เกิน 30 คำสั่งต่อวินาที

- แบบที่ 2 การทดสอบโจมตีโดยผ่าน SIP PROXY SERVER กำหนดค่าพารามิเตอร์บนโมดูล Pike Sampling time unit 2 วินาที ,Reqs_density_per_unit 100 ครั้ง, Remove_latency 120 วินาที กำหนดจำนวนครั้งที่โทรศัพท์ทดสอบต่อวินาที เป็น 10,20 และ 30 ครั้งต่อวินาที มีผลให้ IPPBX SERVER มีผลให้การใช้งานโทรศัพท์ผ่านอินเตอร์เน็ต (Softphone) และอุปกรณ์โทรศัพท์ รวมถึงการลงทะเบียนบัญชีหมายเลขโทรศัพท์ (SIP Register) สามารถทำงานได้ตามปกติ ทั้งนี้ในการทดสอบส่งคำสั่ง 30 ครั้งต่อวินาที SIP PROXY SERVER จะหยุดส่งคำสั่งไปยัง IPPBX SERVER ตามเงื่อนไขที่กำหนดบน SIP PROXY SERVER เพื่อเป็นการจำกัดการส่งคำสั่ง SIP INVITE และมีผลให้ IPPBX SERVER ยังคงทำงานได้ตามปกติ

- แบบที่ 3 การทดสอบโจมตีโดยผ่าน SIP PROXY SERVER กำหนดค่าพารามิเตอร์บนโมดูล Pike Sampling time unit 2 วินาที,Reqs_density_per_unit 200 ครั้ง,Remove_latency 120 วินาที เพื่อสามารถรับคำสั่ง SIP INVITE และส่งไปยัง IPPBX SERVER เกินกว่าความสามารถในการรองรับคำสั่ง จะเห็นได้ว่า จำนวนครั้งที่โทรศัพท์ทดสอบต่อวินาที เป็น 20 และ 30 ครั้งต่อวินาที การใช้งานโทรศัพท์ผ่านอินเตอร์เน็ต(Softphone) และ อุปกรณ์โทรศัพท์ รวมถึงการลงทะเบียนบัญชีหมายเลขโทรศัพท์ (SIP Register) บน IPPBX SERVER สามารถทำงานได้ตามปกติ แต่ในการคำสั่ง SIP INVITE 50 ครั้งต่อวินาที จะทำให้ผลการทำงานคำสั่งภายในที่ทดสอบ IPPBX SERVER ทำงานไม่สามารถทำงานได้และล้มเหลว ซึ่งเป็นผลจาก SIP PROXY SERVER ส่งคำสั่ง SIP INVITE ไปยัง IPPBX SERVER เกินความสามารถในการรองรับคำสั่งได้

จากข้อมูลข้างต้นจะเห็นได้ว่าการกำหนดค่าพารามิเตอร์ของโมดูล Pike บน SIP PROXY SERVER จะมีผลต่อการตอบสนองต่อการส่งคำสั่งจาก SIP PROXY SERVER ไปยัง IPPBX SERVER การกำหนดค่าให้อยู่ในช่วงค่าความสามารถในการรองรับคำสั่งต่อวินาทีของ IPPBX SERVER ก็จะมีผลทำให้ SIP PROXY SERVER หยุดส่งคำสั่งไปยัง IPPBX SERVER ตามเงื่อนไขที่กำหนดได้ หากกำหนดไว้มากกว่าก็จะมีผลทำให้ IPPBX SERVER ทำงานล้มเหลวต่อการทำงานคำสั่งภายใน ทั้งนี้การทดสอบโจมตีไปยัง IPPBX SERVER โดยตรงทำให้ระบบทำงานล้มเหลว กรณีคำสั่ง SIP INVITE มีจำนวนเกินความสามารถในการรองรับคำสั่งต่อวินาทีของ IPPBX SERVER

ดังนั้นการป้องกันการโจมตี IPPBX SERVER จากคำสั่ง SIP INVITE ด้วยวิธีแบบ Denial of Service (DoS) ด้วยโมดูล Pike บน SIP PROXY SERVER นั้นจะต้องปรับค่าอัตราการรับคำสั่งต่อวินาที ให้เหมาะสมกับค่าความสามารถในการรองรับคำสั่งต่อวินาที ของ IPPBX SERVER

บทที่ 5
สรุปผลการวิจัยและข้อเสนอแนะ

5.1 สรุปผลการวิจัย

งานวิจัยนี้เป็นการประเมินผลกระทบการโจมตีระบบโทรศัพท์ผ่านอินเตอร์เน็ตจากการปฏิเสธการให้บริการด้วยการยิงข้อความ SIP INVITE ไปยัง IPPBX SERVER จากเครือข่ายอินเตอร์เน็ตท้องถิ่น ซึ่งเป็นการปฏิเสธให้บริการบน IPPBX SERVER การส่งคำสั่ง SIP INVITE จะมีผลต่อการใช้ทรัพยากรของ IPPBX SERVER เพิ่มขึ้นอย่างเป็นสัดส่วนต่ออัตราคำสั่งต่อวินาทีที่ถูกส่งจากโปรแกรมจำลองการโจมตี จะเห็นได้ว่ามีผลทำให้ IPPBX SERVER มีการทำงานล้มเหลวไม่ตอบสนองต่อคำสั่งการทำงานภายในของ IPPBX SERVER และไม่สามารถให้บริการได้

โดยการเปรียบเทียบกับการทดสอบโจมตี IPPBX SERVER ผ่าน SIP PROXY SERVER ที่กำหนดค่าความสามารถในการรองรับคำสั่งต่อวินาทีบน IPPBX SERVER และ SIP PROXY SERVER มีค่าเท่ากัน มีผลทำให้ SIP PROXY SERVER ปฏิเสธการให้บริการด้วยการหยุดส่งคำสั่ง SIP INVITE ไปยัง IPPBX SERVER กรณีอัตราคำสั่งต่อวินาทีเกินที่กำหนด ทำให้ IPPBX SERVER สามารถทำงานตอบสนองต่อคำสั่งภายในระบบโดยไม่มีผลกระทบต่อบริการ ทั้งนี้ในการทดสอบโดยใช้คำสั่งการโจมตีด้วยคำสั่ง อื่น เช่น OPTION,NOTIFY,CANCEL จะมีผลต่อการใช้ทรัพยากรของ IPPBX SERVER ในปริมาณที่แตกต่างกันตามรูปแบบของการตอบสนองต่อคำสั่งของ IPPBX SERVER

จากข้อสรุปการวิจัยนี้พบว่าผลกระทบการโจมตี IPPBX SERVER จากการปฏิเสธการให้บริการด้วยการยิงข้อความ SIP INVITE จะทำให้ IPPBX SERVER ทำงานล้มเหลว และ SIP PROXY SERVER สามารถป้องกันการโจมตีจากการปฏิเสธการให้บริการได้

5.2 ข้อจำกัดของการวิจัย

ในการศึกษาวิจัยครั้งนี้ได้กำหนดกรอบการทดสอบเฉพาะเครือข่ายอินเตอร์เน็ตท้องถิ่นเท่านั้น และการติดตั้งโปรแกรมรวมถึงระบบที่ใช้ในการทดสอบถูกติดตั้งบนเครื่องคอมพิวเตอร์เสมือนที่ทำงานบนเครื่องคอมพิวเตอร์แม่ข่ายเครื่องเดียวกัน ทำให้การตอบสนองต่อคำสั่งที่ใช้ทดสอบไม่ได้ถูกประเมินจากสภาวะแวดล้อมที่มีปัจจัยในด้านเครือข่ายสารข้อมูลเข้ามาเกี่ยวข้อง

เช่น อัตราความล่าช้าของการส่งข้อมูลต่อหน่วยเวลา (Delay) ค่าความแปรปรวนของความล่าช้าของการรับส่งข้อมูล (Jitter) และรูปการโจมตีจากผู้บุกรุกจากเครือข่ายสาธารณะที่มีรูปแบบการโจมตีที่ซับซ้อนและไม่สามารถกำหนดรูปแบบได้ ซึ่งการเพิ่มปัจจัยในการทดสอบดังกล่าวจะทำให้บันทึกข้อมูลการโจมตี การใช้ทรัพยากรของระบบ และมีข้อมูลที่หลากหลายในการประเมินเปรียบเทียบการโจมตีในสถานะการณ์ที่แตกต่างกันมากขึ้น

5.3 ข้อเสนอแนะ

เพื่อให้การศึกษาวิจัยครอบด้านความปลอดภัยระบบโทรศัพท์ผ่านอินเตอร์เน็ต(IPPBX SERVER) หัวข้อที่ต้องศึกษาเพิ่มเติมดังเช่น

5.3.1 การป้องกันโจมตีโดยใช้รหัสผู้ใช้งานและรหัสผ่านแบบคาดเดาไม่คำนึงถึงรูปแบบ (Brute force user name / password) , การโจมตีด้วยเบอร์โทรศัพท์ที่คาดเดาไม่คำนึงถึงรูปแบบ (Brute force numbering /prefix)

5.3.2 การตรวจสอบหมายเลขประจำเครื่องคอมพิวเตอร์ (IP Address) ที่เห็นว่าเป็นเครื่องที่โจมตีจากผู้ไม่หวังดีแล้วทำการปิดการเชื่อมต่อโดยถาวร (IP Banned / Blocking)

5.3.3 การเพิ่มการแจ้งเตือนแบบต่อผู้ดูแลระบบเพื่อเป็นการรับมือต่อการโจมตีได้อย่างมีประสิทธิภาพและแก้ไขปัญหาหรือผลกระทบที่เกิดขึ้นได้ทันท่วงที

5.3.4 การปกปิดโครงสร้างของระบบเครือข่าย (Network topology hiding)

5.3.5 การควบคุมและจำกัดการลงทะเบียน (Registration rate throttling)

5.3.6 กำหนดสถาพแวดล้อมการทดสอบบนเครือข่ายสาธารณะ

5.3.7 กำหนดให้ระบบ IPPBX SERVER ,SIP PROXY SERVER ,SIPP ที่ทดสอบติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายแยกเฉพาะเครื่อง