ต้นแบบระบบกำหนดการใช้งานอย่างยุติธรรมในโครงข่ายคอมพิวเตอร์ไร้สาย

ภาณุพงศ์ สายไพศรี

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมคอมพิวเตอร์และโทรคมนาคม คณะวิศวกรรมศาสตร์
มหาวิทยาลัยธุรกิจบัณฑิตย์
พ.ศ. 2556

Prototype of Fair Usage Policy in Wireless Computer Network

Panupong Saipaisri

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Engineering

Department of Computer and Telecommunication Engineering

Faculty of Engineering, Dhurakij Pundit University

2012

กิตติกรรมประกาศ

การจัดทำวิทยานิพนธ์ฉบับนี้สำเร็จสมบูรณ์ลงได้ ด้วยความเมตตากรุณาจาก อาจารย์ ดร.ชัยพร เขมะภาตะพันธ์ อาจารย์ที่ปรึกษาวิทยานิพนธ์ ที่ให้ข้อคิดเห็น คำแนะนำที่เป็นประโยชน์ต่องานวิจัย อาจารย์ ดร.ธนัญ จารุวิทยโกวิท อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม ที่สละเวลาอันมีค่าคอยให้คำแนะนำให้คำปรึกษา ตลอดจนแนวทางในการแก้ไขปัญหาต่างๆ และเอาใจใส่ข้าพเจ้ามาโดยตลอด ข้าพเจ้ารู้สึกซาบซึ้งเป็นอย่างยิ่ง จึงขอกราบขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

ขอขอบพระคุณ รศ.ดร.ไพบูลย์ พฤกษ์สุนันท์ ดร.ประศาสน์ จันทราทิพย์ กรรมการสอบ วิทยานิพนธ์ ซึ่งสละเวลาเพื่อเป็นกรรมการสอบวิทยานิพนธ์ และให้คำแนะนำที่เป็นประโยชน์ต่องานวิจัย และขอบคุณเจ้าหน้าที่ทุกท่านที่ช่วยดำเนินเรื่องต่างๆ ให้เป็นอย่างดี

ขอขอบพระคุณคณาจารย์ทุกท่านที่ได้ประสิทธิประสาทวิชาความรู้ จนข้าพเจ้าประสบความสำเร็จในการศึกษา ขอขอบพระคุณเพื่อนร่วมรุ่น พี่ๆ น้องๆ ทุกๆ คน รวมถึงคณะเจ้าหน้าที่ประจำหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต และคณะเจ้าหน้าที่บัณฑิตวิทยาลัย ทุกท่าน ซึ่งไม่อาจกล่าวนามได้ทั้งหมดในที่นี้ ที่ได้ให้กำลังใจและช่วยเหลือข้าพเจ้ามาโดยตลอด

สุดท้ายนี้ ขอขอบคุณ คุณพ่อ คุณแม่ ตลอดจนบุคคลในครอบครัวของผู้วิจัย ที่คอยให้กำลังใจ และสนับสนุนผู้วิจัยในทุกๆ ด้าน ตลอดระยะเวลาการศึกษาจวบจนสำเร็จการศึกษา

ภาณุพงศ์ สายไพศรี

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

สารบัญรูป

รูปที่ **หน้า**

หัวข้อวิทยานิพนธ์ ต้นแบบระบบกำหนดการใช้งานอย่างยุติธรรมในโครงข่ายคอมพิวเตอร์ไร้สาย
ชื่อผู้เขียน ภาณุพงศ์ สายไพศรี
อาจารย์ที่ปรึกษา อาจารย์ ดร.ชัยพร เขมะภาตะพันธ์
อาจารย์ที่ปรึกษาร่วม อาจารย์ ดร.ธนัญ จารุวิทยโกวิท
สาขาวิชา วิศวกรรมคอมพิวเตอร์และโทรคมนาคม
ปีการศึกษา 2555

บทคัดย่อ

วิทยานิพนธ์นี้ศึกษาหลักการของ Policy and Charging Rules Function (PCRF) ที่ใช้ในโครงข่ายโทรศัพท์เคลื่อนที่ 3G เพื่อนำมาพัฒนาและปรับใช้กับระบบโครงข่ายคอมพิวเตอร์ไร้สาย เพื่อควบคุมบริหารจัดการ การรับส่งข้อมูลของผู้ใช้งานแต่ละคน โดยยึดหลักพื้นฐานของการได้ใช้งานอย่างเท่าเทียมกัน (Fair Usage Policy)

การศึกษานี้ได้ประยุกต์ใช้อุปกรณ์ปล่อยสัญญาณโครงข่ายคอมพิวเตอร์ไร้สายยี่ห้อ Cisco รุ่น WRT54GL เพื่อทำการส่งผ่านข้อมูลผู้ใช้งานไปยังคอมพิวเตอร์เซิร์ฟเวอร์ที่มีการจัดเก็บข้อมูลต่างๆ รวมทั้งขนาดข้อมูลที่ใช้งานได้ ซึ่งคอมพิวเตอร์เซิร์ฟเวอร์จะทำการควบคุมบริหารจัดการ การรับส่งข้อมูลของผู้ใช้งานผ่านกรอบคำสั่ง DD-WRT version 24 ในลักษณะคำสั่งสคริปท์ผ่านการเชื่อมต่อแบบ Telnet โดยอัตโนมัติ ผลการทดสอบพบว่าระบบที่พัฒนาปรับปรุงขึ้นนี้ทำงานได้อย่างดี แต่อาจติดปัญหาเรื่องการตรวจสอบตัวตนผู้ใช้งานบ้าง

Thesis Title	Prototype of Fair Usage Policy in Wireless Computer Network
Author	Panupong Saipisri
Thesis Advisor	Chiyaporn Khemapatapan, Ph.D
Co-Thesis Advisor	Tanun Jaruvitayakovit, Dr.Eng
Department	Computer and Telecommunication Engineering
Academic Year	2012

ABSTRACT

This thesis studies the concept of Policy and Charging Rules Function (PCRF) that is used in the third generation mobile network in order to develop a prototype which deploy in Wireless Local Area Networks (WLANs). The prototype will control and manage data transitions of each user based on Fair Usage Policy (FUP).

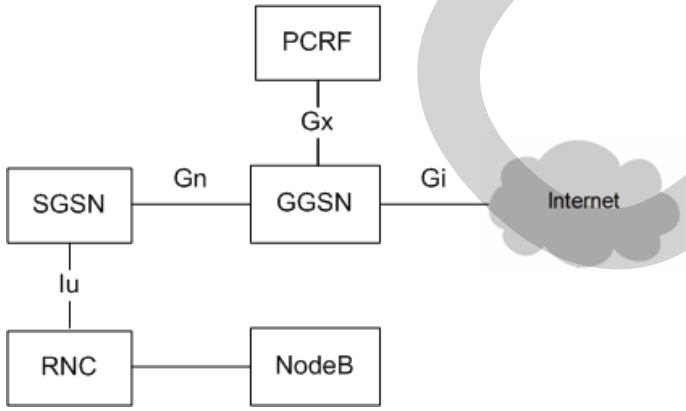
This study applies to use wireless local area network equipment, Cisco WRT54GL, for sending user information to a computer server for recording various data including user's traffic volume. The computer server will control and manage the user transmission with DD-WRT version 24 by scripts automatically via telnet protocol. From the testing results the system can work well. However, this thesis still has some limitations that are User Identification and Authentication.

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญของปัญหา

เทคโนโลยีในโทรคมนาคมในปัจจุบันนั้นมีความก้าวหน้าอย่างรวดเร็ว โดยปัจจุบันเทคโนโลยีใน 3G เป็นที่ได้รับความนิยมอย่างมาก โดยมีแนวโน้มของผู้ใช้บริการมากขึ้นเรื่อย ๆ นั้นเป็นเพราะเครือข่าย 3G ได้มีการพัฒนาความเร็วและความจุ (Capacity) จนได้ถึง 42 Mbps ด้วยเทคโนโลยี HSPA+ ทำให้การเชื่อมต่ออินเทอร์เน็ตผ่านมือถือได้รับความนิยมเป็นอย่างสูง และด้วยการคิดราคาแบบ Flat Rate ที่เหมาจ่ายราคาหนึ่ง และสามารถที่จะดาวน์โหลดปริมาณข้อมูลได้ตามแพ็คเกจ สิ่งต่างๆ เหล่านี้ทำให้บริการเครือข่าย 3G ประสบความสำเร็จเป็นอย่างสูง

โดยทั่วไปพฤติกรรมการใช้งานอินเทอร์เน็ตผ่านมือถือนั้น จะมีปริมาณการใช้ข้อมูลที่ไม่มาก แต่สามารถใช้งานได้ทุกที่ ที่มีสัญญาณโทรศัพท์ แต่มีผู้ใช้งานที่เป็นส่วนน้อย (ประมาณ 5%) นำโปรโมชั่นการใช้งานข้อมูลบนเครือข่าย 3G แบบไม่จำกัดไปใช้งานเพื่อวัตถุประสงค์อื่น เช่น การนำไปใช้งาน Bit Torrent โดยใช้โทรศัพท์มือถือต่อเป็นโมเด็ม หรือต่อผ่านแอร์การ์ด ซึ่งส่งผลกระทบต่อการใช้งานของผู้ใช้งานส่วนใหญ่ (ประมาณ 95%) ทำให้ประสิทธิภาพการใช้งาน 3G ลดลงเป็นอย่างมาก



รูปที่ 1.1 การใช้งาน PCRF ในเครือข่ายโมบายบรอดแบนด์[1]

[1] Data Offload ปัญหาใหม่สำหรับผู้ให้บริการ Mobile Broadband (ตอนที่ 2) , http://www.telecomjournal.net.

ด้วยเหตุดังกล่าวทำให้มาตรฐาน 3GPP (Release7 TS 23.060)[2] จึงได้มีการทำ Fair Usage Policy (FUP) เพื่อให้ผู้ใช้งานแต่ละคนสามารถใช้งานทรัพยากรต่าง ๆ ในระบบได้อย่างเท่าเทียมกัน ทำให้ช่วยลดภาระการทำงานของเครือข่ายอันเนื่องมาจากการใช้งานข้อมูลปริมาณมากของผู้ใช้งานบางคน ในมาตรฐาน 3GPP นั้นกำหนดให้ใช้อุปกรณ์ที่เรียกว่า Policy and Charging Rules Function (PCRF)[1] โดยอยู่บน Core Network และทำงานร่วมกับ Gateway GPRS Support Node (GGSN) ที่ทำหน้าที่เป็น gateway เชื่อมต่อระหว่างเครือข่าย GPRS กับ เครือข่ายข้อมูลทั่วไป ดังรูปที่ 1.1 โดย PCRF จะเป็นผู้บังคับใช้งาน Policy ต่างๆ ก็จะเข้าควบคุมการใช้งาน เช่น การลดแบนด์วิดท์ของทราฟฟิกบางชนิด หรือการที่จะลดปริมาณการใช้งาน เมื่อผู้ใช้งานดาวน์โหลดข้อมูลถึงปริมาณหนึ่งๆ เป็นต้น ซึ่งก็จะช่วยจัดการปริมาณ ทราฟฟิกที่จะเกิดขึ้นในเครือข่ายได้ดีขึ้น เพื่อให้เป็นตามหลักการของ นโยบายการใช้งานรับส่งข้อมูลอย่างเหมาะสม (Fair Usage Policy)

ปัญหา FUP นอกจากจะเกิดขึ้นกับเครือข่าย 3G แล้วยังเกิดกับระบบเครือข่ายไร้สายประเภท WiFi ซึ่งมักจะคิดค่าบริการของแพ็คเกจแบบใช้งานได้ไม่จำกัด Unlimited ทำให้มีปัญหาเรื่องของทราฟฟิกการใช้งานปริมาณมาก จากการค้นคว้าของผู้วิจัยยังไม่มีงานวิจัยใดนำแนวคิดการทำ Fair Usage Policy ในระบบ 3GPP มาแก้ปัญหาดังกล่าว บทความนี้มีวัตถุประสงค์เพื่อนำแนวความคิดการทำ Fair Usage Policy และการจำกัดปริมาณการใช้งานข้อมูลของ 3GPP มาประยุกต์ใช้กับระบบเครือข่าย WiFi

1.2 วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษา ออกแบบ และพัฒนาระบบการทำ Fair Usage Policy ในระบบ 3GPP มาใช้กับระบบเครือข่ายโครงข่ายไร้สายประเภท WiFi
2. เพื่อบริหารจัดการปริมาณทราฟฟิกในโครงข่ายไร้สายประเภท WiFi ให้มีประสิทธิภาพดีขึ้น
3. เพื่อให้ผู้ใช้งานในโครงข่าย WiFi ได้รับคุณภาพของการบริการอย่างเหมาะสม

1.3 ขอบเขตของการวิจัย

1. ออกแบบและพัฒนาระบบการทำ Fair Usage Policy ในระบบโครงข่ายไร้สาย WiFi โดยนำระบบ 3GPP มาเป็นต้นแบบในการพัฒนา

---

[2] 3rd Generation Partnership Project, http://www.3gpp .org.

2. ผู้ดูแลระบบสามารถกำหนดปริมาณของข้อมูลที่ผู้ใช้งาน แต่ละประเภทสามารถใช้งานได้ โดยสามารถกำหนดผู้ใช้งานได้อย่างน้อย 3 ระดับ โดยผู้ดูแลระบบสามารถกำหนดค่าต่าง ๆ ได้ผ่านทางหน้าเว็บเพจ

3. ก่อนการใช้งานในโครงข่าย WiFi ผู้ใช้งานต้องยืนยันตัวตนผ่านหน้าเว็บเพจโดยทำการกรอกข้อมูลชื่อผู้ใช้งานและรหัสผ่านของผู้ใช้ทุกครั้งก่อนใช้งาน

4. เครื่องคอมพิวเตอร์แม่ข่ายที่พัฒนาจะทำหน้าที่ตรวจสอบปริมาณ และ/หรือ เวลาการใช้งานข้อมูลของผู้ใช้งานแต่ละคนแบบ real-time กับอุปกรณ์ Wireless Access Point

5. เมื่อผู้ใช้งานมีการใช้งานในโครงข่าย WiFi จนถึงระดับที่กำหนดไว้ (ทั้งในแง่ของปริมาณการใช้ข้อมูล และเวลาการใช้ข้อมูล) อัตราการใช้งานข้อมูล (bit rate) ของผู้ใช้งานนั้นจะถูกลดค่าลงไปตามค่าที่ได้กำหนดไว้โดยผู้ใช้งาน

6. เมื่อครบรอบการใช้งานที่กำหนดในระบบ (ตัวอย่างเช่นการใช้งานแบบรายเดือน) ผู้ใช้งานแต่ละคนจะสามารถใช้งานได้ตามความเร็วสูงสุดที่กำหนดในระบบได้แบบอัตโนมัติ

7. การทำ Fair Usage Policy ในงานวิจัยนี้ครอบคลุมถึงกรณีที่ผู้ใช้งานมีการเคลื่อนที่ ทำให้มีการใช้งานภายใต้ Wireless Access Point มากกว่า 1 ตัว โดยระบบจะยังคงสามารถจำกัดความเร็วเมื่อผู้ใช้งานมีการใช้งานเกินปริมาณข้อมูล หรือเวลาที่กำหนดไว้ โดยระบบอาจจะมีความคลาดเคลื่อนของปริมาณข้อมูล หรือเวลาที่ใช้งาน ในระดับที่ยอมรับได้

8. อัตราการใช้งานข้อมูลที่จะถูกระบบที่พัฒนาจำกัดนั้น ครอบคลุมเฉพาะการใช้งานด้านขาลง (download) เท่านั้น

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1. ได้ต้นแบบระบบ Fair Usage Policy ในโครงข่ายคอมพิวเตอร์ไร้สาย WiFi

2. ผู้ใช้งานในโครงข่าย WiFi ได้รับคุณภาพของการบริการอย่างเหมาะสม

บทที่ 2
แนวคิด ทฤษฎี และผลงานวิจัยที่เกี่ยวข้อง

2.1 Gateway GPRS Support Node[1]

2.1.1 สถาปัตยกรรมเครือข่ายหลัก

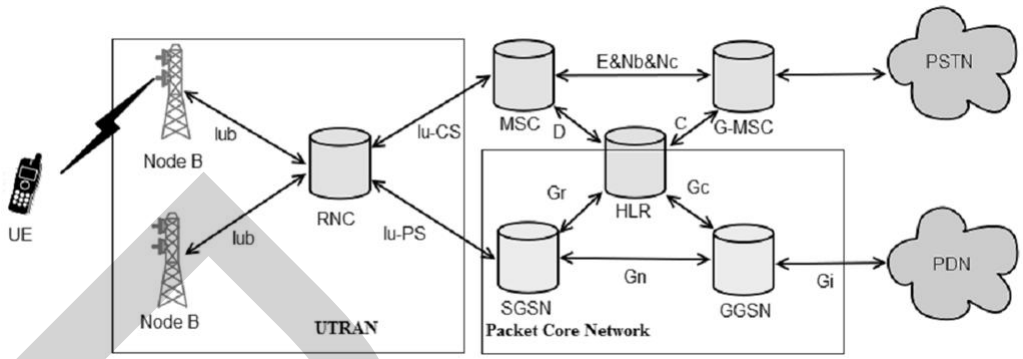
UMTS จะถูกกล่าวถึงในเทคโนโลยีและการบริการเครือข่ายโทรศัพท์มือถือยุคที่สาม (3G) UMTS core network เชื่อมต่อเครือข่ายในโทรศัพท์มือถือด้วย Packet Data Network (PDN) โดยโครงสร้าง Global System for Mobile Communications (GSM) ด้วยไอพีบนพื้นฐานของแพ็กเกจสวิทชิ่งด้วยการอัพเกรดนี้จะให้อัตราข้อมูลได้ถึง 144 kbit/s ในสภาพแวดล้อมที่มาโครเซลล์ลูล่า 384 kbit/s ในสภาพแวดล้อมที่เป็นไมโครเซลล์ลูล่าและ ถึง 2 Mbit/s ในสภาพแวดล้อมที่เป็นอินดอร์หรือที่เรียกว่าพิโคเซลล์ลูล่า นอกจากนี้ผู้ใช้หลายคนสามารถที่จะแบ่งปันทรัพยากรในแอร์อินเตอร์เฟซเดียวกันและทำให้ความเป็นไปได้ที่จะจัดสรรช่องสัญญาณใน อัพลิงค์และ ดาว์ลิงค์เป็นอิสระนำไปสู่การใช้งานมีประสิทธิภาพมากขึ้นของช่องสัญญาณวิทยุ

UMTS แต่ก่อน GPRS ถูกพัฒนาขึ้นที่ด้านบนของเครือข่าย GSM ที่มีอยู่ร่วมกันกับบางองค์ประกอบใหม่ของเครือข่าย อินเตอร์เฟซและโปรโตคอลที่จำเป็นในการจัดการทราฟฟิกของแพ็คเก็ต องค์ประกอบที่สำคัญที่สุดใน GPRS แบคโบนคือ SGSN และ GGSN โดยที่ SGSN อินเตอร์เฟซจะเชื่อมต่อไปยัง radio access network และ GGSN อินเตอร์เฟซไปยัง PDN UMTS สืบทอดโครงสร้างสถาปัตยกรรมเดียวกันจาก GPRS และจะใช้ W - CDMA ที่อยู่ภายใต้แอร์อินเตอร์เฟซ รูปที่ 2.1 แสดงองค์ประกอบสถาปัตยกรรมและการเชื่อมต่อของ UMTS

สถาปัตยกรรมจะถูกแบ่งออกเป็นสองส่วนคือส่วน เซอร์กิตสวิทช์ และแพ็กเก็จสวิทช์ โดยที่ในส่วน เซอร์กิตสวิทช์ เป็นส่วนที่เชื่อมต่อกับสายโทรศัพท์ไปยัง public switched telephone network (PSTN) ในส่วนที่เซอร์กิตสวิทช์จะประกอบด้วย Mobile Switching Center (MSC) และ Gateway-MSC (G - MSC) และส่วนที่สำคัญที่สุดของแพ็กเก็จสวิทช์ คือ SGSN และ GGSN โดยฐานข้อมูล Home Location Register (HLR) เป็นฐานข้อมูลร่วมกันสำหรับทั้ง เซอร์กิตสวิทช์ และแพ็กเก็จสวิทช์ สามารถดูได้จากในรูปที่ 2.1 UTRAN จะเชื่อมต่อกับ MSC ผ่านอินเตอร์เฟซ lu_CS และ SGSN ผ่านอินเตอร์เฟซ lu_PS.

---

[1] Fredrik Larsson & Azadeh Hosseinzad Amitkhizi, “Assessment of IxLoad in a GGSN environment”. Master thesis. University of Gothenburg. June 2010



รูปที่ 2.1 สถาปัตยกรรม UMTS

ที่มา: Fredrik Larsson and Azadeh Hosseinzad Amitkhizi. (2010, p. 16)

เมื่อผู้ใช้เปิดใช้งานอุปกรณ์ UMTS ของมันก็มักจะสแกนหาช่องทางที่มีอยู่และพยายามที่จะเชื่อมต่อกับเครือข่าย ผ่านโหนดและอินเตอร์เฟซต่างๆ ที่เห็นในรูปที่ 2.1 SGSN จะได้รับ"แนบคำขอ"จากอุปกรณ์และจะพยายามที่จะรับรองความถูกต้องของผู้ใช้โดยรายละเอียดข้อมูลของผู้ใช้ที่มาจาก HLR จากรายละเอียดของข้อมูลและข้อความร้องขอที่แนบมา SGSN ที่มาจาก Access Point Name (APN) ซึ่งการระบุ PDN และการตัดสินใจที่ถูกต้องของ GGSN ในการเลือกเส้นทางออกไป SGSN จะส่งข้อความ "บทความที่ถูกสร้าง" ต่อไปยัง GGSN ซึ่งจะเชื่อมโยงการให้บริการ SGSN กับผู้ใช้ GGSN จะกำหนดบทความและเส้นทางของแพ็คเก็ตที่ผู้ใช้ต้องการไปยัง PDN เมื่อทราฟฟิกกลับมาถึง GGSN มันจะมีไอพี แอดเดรสของผู้ใช้ที่เป็นปลายทาง เพื่อให้ GGSN ต้องการที่จะเชื่อมโยง SGSN กับผู้ใช้และเส้นทางที่กำหนดมา โดย SGSN จะส่งทราฟฟิกต่อยังสถานีฐานที่ผู้ใช้โทรศัพท์มือถือนั้นอยู่

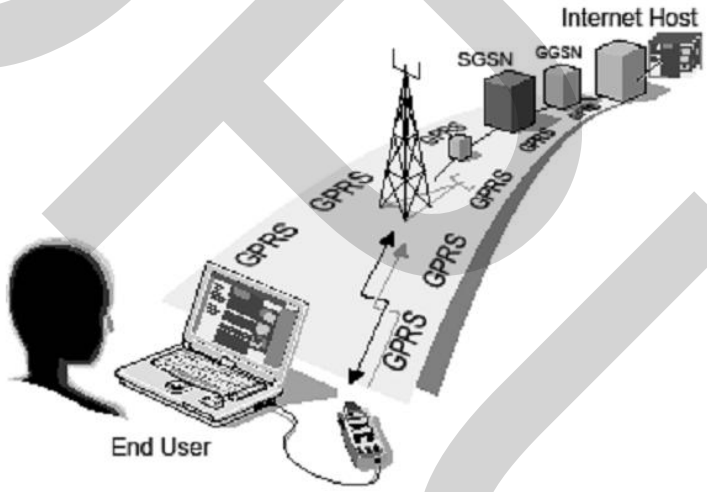
2.1.2 Serving GPRS Support Node

SGSN จะทำหน้าที่เป็นจุดของการเชื่อมต่อจากมือถือไปยังเครือข่ายหลัก โดนงานหลักคือเพื่อให้การเคลื่อนไหวของผู้ใช้ UMTS ที่เป็นไปได้ เมื่อผู้ใช้งานเชื่อมต่อกับเครือข่าย UMTS การเชื่อมต่อจะทำระหว่าง UE และ SGSN ที่เหมาะสม ซึ่งจะช่วยให้ผู้ใช้งานที่จะเดินทางระหว่างเซลล์ที่แตกต่างกันโดยไม่ถูกตัดการเชื่อมต่อ เมื่อผู้ใช้งานได้รับแพ็คเก็ตจาก PDN SGSN จะปรับปรุงมุมมองที่ Radio Network Controller (RNC) ให้พร้อมใช้งานได้ โดยที่มีลักษณะคล้ายกับไอพีเราเตอร์ปกติ แต่มีการเพิ่มฟังก์ชันการทำงานบางอย่างเพื่อการจัดการปัญหาเรดิโอเน็ตเวิร์คเช่น

- การควบคุมการส่งสัญญาณการโทรด้วย data services location registers
- การเชื่อมต่อ HLR, RNC และ GGSN

- การตรวจสอบและยืนยันตัวตนของผู้ใช้
- แปลงที่ทราฟฟิกของผู้ใช้จริงระหว่างคอร์เน็ตเวิร์คและเรดิโอเน็ตเวิร์ค

SGSN สามารถให้บริการโทรศัพท์มือถือเพียงในพื้นที่ที่จำกัด ซึ่งเป็นที่เรียกว่าพื้นที่ให้บริการ SGSN ที่สามารถประกอบด้วยหนึ่งหรือหลาย RNC อินเตอร์ SGSN จะสามารถทำได้เมื่อ UE มีการย้ายจากในพื้นที่ให้บริการของ SGSN ไปยัง SGSN อื่นๆ ในระหว่างการจัดส่งแพ็คเก็ตบัฟเฟอร์ใน SGSN เดิมที่อาจจะถูกลบและไม่พอใจโดยใช้ชั้นที่สูงกว่าของ IP สแต็ค เมื่อผู้ใช้งานทำการติดต่อกับเซิร์ฟเวอร์บนอินเทอร์เน็ตโดยมากการสูญเสียข้อมูลโดยทั่วไปจะใช้สถานที่ที่ผ่านเรดิโอลิงค์และการดูแลของการรีทรานสมิทชั่น กับโปรโตคอลชั้นสูงเช่น TCP จะช้าและไม่มีประสิทธิภาพ สำหรับเหตุผลที่โปรโตคอลรีทรานสมิทชั่นอย่างรวดเร็วได้รับการออกแบบที่ครอบคลุมเฉพาะส่วนที่ไร้สายและซ่อนการสูญเสียจากโปรโตคอลชั้นที่สูงขึ้น



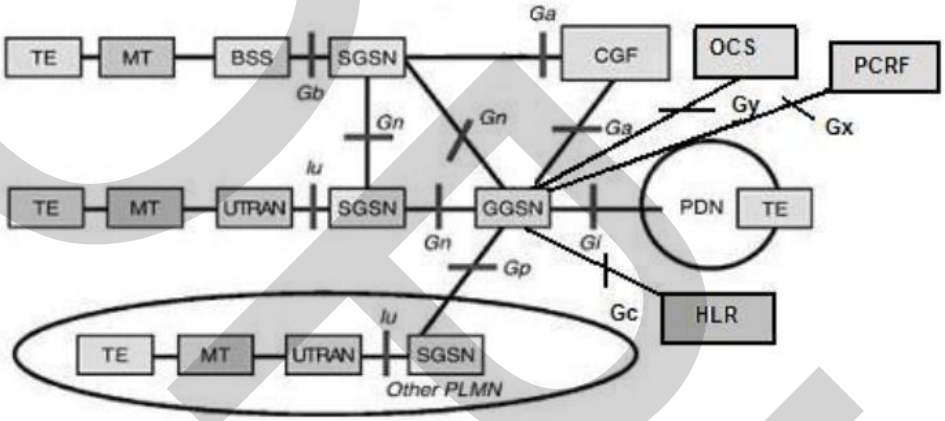
รูปที่ 2.2 เส้นทางจากผู้ใช้งานไปยังโฮสอินเทอร์เน็ต

ที่มา: Fredrik Larsson and Azadeh Hosseinzad Amitkhizi. (2010, p. 18)

2.1.3 Gateway GPRS Support Node

Gateway GPRS Support Node (GGSN) เป็นจุดของเครือข่ายหลักของการติดต่อกับ PDN ภายนอกเช่นอินเทอร์เน็ต GGSN จะเชื่อมโยงไป SGSN ตามไอพีแบคโบน ซึ่งจะส่งต่อแพ็กเก็ตจาก PDN ไปที่ MS จุดปัจจุบันของสิ่งที่แนบมา ซึ่งเป็น SGSN ที่มีข้อมูลเส้นทางของผู้ใช้ นอกจากนี้ยังมีเส้นทางที่แพ็กเก็ตไปยังปลายทาง PDN ภายนอก จากไอพีเน็ตเวอร์ภายนอก GGSN ถูกมองว่าเป็นเราเตอร์ทั่วไปซึ่งทำหน้าที่เป็นเกตเวย์ระหว่างเครือข่ายไร้สายและเครือข่ายข้อมูล

อินเตอร์เฟซของ GGSN จะแสดงไว้ในรูปที่ 2.3 อินเตอร์เฟซ Gi เป็นจุดเชื่อมต่อระหว่าง GGSN และ PDN ภายนอก Gn คือการติดต่อระหว่าง GGSN และ SGSN, GA คือการติดต่อระหว่าง GGSN และ Charging Gateway Function (CGF), Gp คือการติดต่อระหว่าง Home Public Land Mobile Network (HPLMN)ของ GGSN และ SGSN ใน Visited Public Land Mobile Network (VPLMN), Gc คือการติดต่อระหว่าง HLR และ GGSN ที่ Gx และ Gy คือการเชื่อมต่อระหว่าง GGSN ในด้านหนึ่งและ Policy and Charging Rules Function (PCRF) และ Charging System (OCS) ในด้านอื่นๆ



รูปที่ 2.3 การเชื่อมต่อของGGSN

ที่มา: Fredrik Larsson and Azadeh Hosseinzad Amitkhizi. (2010, p. 18)

อินเตอร์เฟซ Gi : แพ็คเก็ตข้อมูลที่ผู้ใช้จะถูกส่งจาก PDN ภายนอกไปยัง GGSN โดยผ่านอินเตอร์เฟซนี้ มาตรฐานที่ใช้สำหรับชั้นกายภาพและชั้นเชื่อมโยงข้อมูลที่สามารถถูกกำหนดโดยความตกลงร่วมกันระหว่างผู้ประกอบการและผู้ให้บริการอินเทอร์เน็ตภายนอก นอกจากนี้ยังมี Internet Engineering Task Force (IETF) เป็นการกำหนดเส้นทางโปรโตคอลมาตรฐานที่มีอยู่ใน GGSN โดยตัวกรองไม่มีรูปแบบโดยเฉพาะและนโยบายที่เจาะจงอาจจะนำมาใช้ในทราฟฟิกอินเตอร์เฟซ Gi โดยทั้ง IPv6 และ IPv4 นั้นรองรับใน Gi อินเตอร์เฟซ GGSN สามารถดำเนินการเอ็นแคบซูเลชั่นของทราฟฟิกผู้ใช้งานบนอินเตอร์เฟซ Gi ไปยังทันเน็ลลิ่ต่างๆ และโปรโตคอลรักษาความปลอดภัยเช่น Layer 2 Tunnelling Protocol (L2TP) และ IPSec ตั้งแต่ GGSN มีการทำงานไอพีเราเตอร์ก็ยังเป็นที่สามารถดำเนินการฟังก์ชันเราเตอร์ต่างๆ เช่น Ethernet Virtual Local Area Network, IPv6 tunnelling และ IP-over-IP-tunnelling

อินเตอร์เฟซ Gn จะการควบคุมการส่งสัญญาณสำหรับการจัดการระยะเวลาและการเคลื่อนที่เช่นเดียวกับทันเน็ลลิ่ของยูสเซอร์เพย์โหลดจะถูกดำเนินการผ่านการเชื่อมต่อระหว่าง GGSN โหนด GSN และ SGSN ก่อนที่โปรโตคอลข้อมูลผู้ใช้ที่สามารถทันเน็ลลิ่ไปยัง SGSN ผ่านอินเตอร์เฟซ Gn ก็ควรจะห่อหุ้มใน GPRS Tunnelling Protocol (GTP)

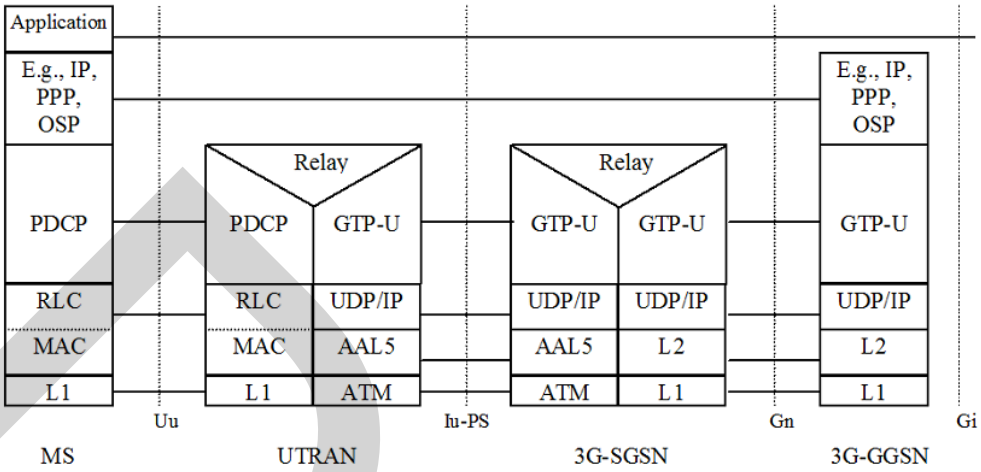
2.1.4 GPRS Tunneling Protocol

หนึ่งในปัจจัยพื้นฐานหลักของการทำงานของ GGSN คือการรองรับ GPRS Tunneling Protocol (GTP) ซึ่งมีทั้งการส่งสัญญาณ GTP (GTP - C) บนคอนโทรนเพลนและการถ่ายโอนข้อมูล (GTP - U) ไปยัง ทันเนิลยูเซอร์ดาต้าบนยูสเซอร์เพลน โดยส่วนเบี่ยงเบนของ GTP เป็น GTP' (GTP prime) ซึ่งใช้เหมือนกันกับรูปแบบข้อความ แต่จะใช้การเก็บข้อมูลที่เรียกเก็บระหว่าง GSNs และ charging gateway function (CGF)

GTP มีหน้าที่สำหรับการห่อหุ้มและส่งข้อมูล Protocol Data Units (PDUs) ระหว่าง SGSN และ GGSN เพื่อระบุช่องทาง PDU โดยเฉพาะ โดย GTP ใช้ Tunneling Endpoint ID (TEID) ในส่วนเฮดเดอร์ของมัน ซึ่งจะช่วยให้แพ็กเก็ตจาก UE เดียวกัน จะมัลติเพล็คและดีมัลติเพล็ค โดย GTP ระหว่าง GPRS support nodes ทั้งสอง

ค่า TEID จะถูกกำหนดในระหว่างการจัดตั้งแพ็คเก็ตดาต้าโปรโตคอล (PDP) ซึ่งเกิดขึ้นบน GTP คอนโทรนเพลน PDP จะเปิดใช้งาน ใบเจ็คทีฟ GTP ทัลเนิล ระหว่างคู่ GSN ในการถ่ายโอนแพ็คเก็ตห่อหุ้มข้อมูลระหว่างผู้ใช้งานและ PDN ภายนอก กระบวนการนี้ส่งผลให้การสร้างทัลเนิ่ลระหว่าง MS และ SGSN ผ่าน UTRAN ที่จะให้บริการ UE โดยการถ่ายโอนข้อมูล PDP ระหว่าง SGSN และ MS รูปที่ 2.4 แสดงให้เห็นถึงขั้นตอนการทัลเนิ่ลและโปรโตคอลภายใน UMTS แบล็คโบนและเรดิโอเน็ตเวิร์ค

เมื่อผู้ใช้มือถือเป็นการสื่อสารกับโฮสต์บน PDN ที่ยูสเซอร์ไอพีทราฟฟิกเป็นทัลเนิ่ลที่ด้านบนของเรดิโอเน็ตเวิร์คที่ผ่าน UTRAN ต่อไปยัง SGSN โดยที่ SGSN จะดีแคปซูเลตโปรโตคอลทัลเนิลลิ่ง และห่อหุ้มแพ็กเก็ตยูสเซอร์เพลนใน GTP เมสเซิจบนอินเตอร์เฟซ Gn เพื่อให้สามารถเสร้างเส้นทางมัลติโปรโตคอลแพ็กเกจไปยัง GGSN โดย GGSN จะดีแคปซูเลตยูเซอร์เพลนทราฟฟิกและแยกข้อมูลเส้นทางและขึ้นอยู่กับข้อมูล ที่ GGSN จะส่งต่อไปยัง PDN ที่ต้องการ



รูปที่ 2.4 UMTS transport protocol layer

ที่มา: Fredrik Larsson and Azadeh Hosseinzad Amitkhizi. (2010, p. 20)

2.1.5 Session Management

เมื่อ MS ต้องการที่จะแลกเปลี่ยนข้อมูลกับ PDN ภายนอก ในครั้งแรกความต้องการในการดำเนินการ GPRS ให้สำเร็จ แล้วต้องการที่จะประยุกต์กับไอพีแอดเดรสที่ใช้ในการค้นหา PDP โดยแอดเดรสจะอ้างอิงถึง PDP แอดเดรส โดย PDP คอนเท็คถูกสร้างขึ้นสำหรับแต่ละเซสชันแรก ซึ่งมีลักษณะที่ต้องการของเซสชั่นโดยเฉพาะที่รวมทั้งประเภท PDP (IPv4 หรือ IPv6) ความต้องการคุณภาพของการบริการ (QoS) กำหนด PDP แอดเดรสให้ MS และ GGSN แอดเดรสให้บริการเป็นเกจเวย์ไปสู่ PDN คอนเทคนี้จะถูกบันทึกไว้ใน GGSN, SGSN และ MS เมื่อ MS ที่ใช้ PDP คอนเทคสามารถใช้ต่อไปยัง PDN ภายนอกและสามารถที่จะส่งและรับข้อมูล โดย GGSN จะสามารถถ่ายโอนข้อมูลระหว่าง PDN และ MS เนื่องจากการแมพปิ้งที่ทำระหว่าง PDP แอดเดรส และ International Mobile Subscriber Identity (IMSI) ที่ได้รับจาก HLR โดย IMSI จะเป็นจำนวนเฉพาะที่สัมพันธ์กับแต่ละ GSM และ ผู้ใช้โทรศัพท์มือถือ UMTS ที่เก็บไว้ในซิมการ์ดที่อยู่ในโทรศัพท์

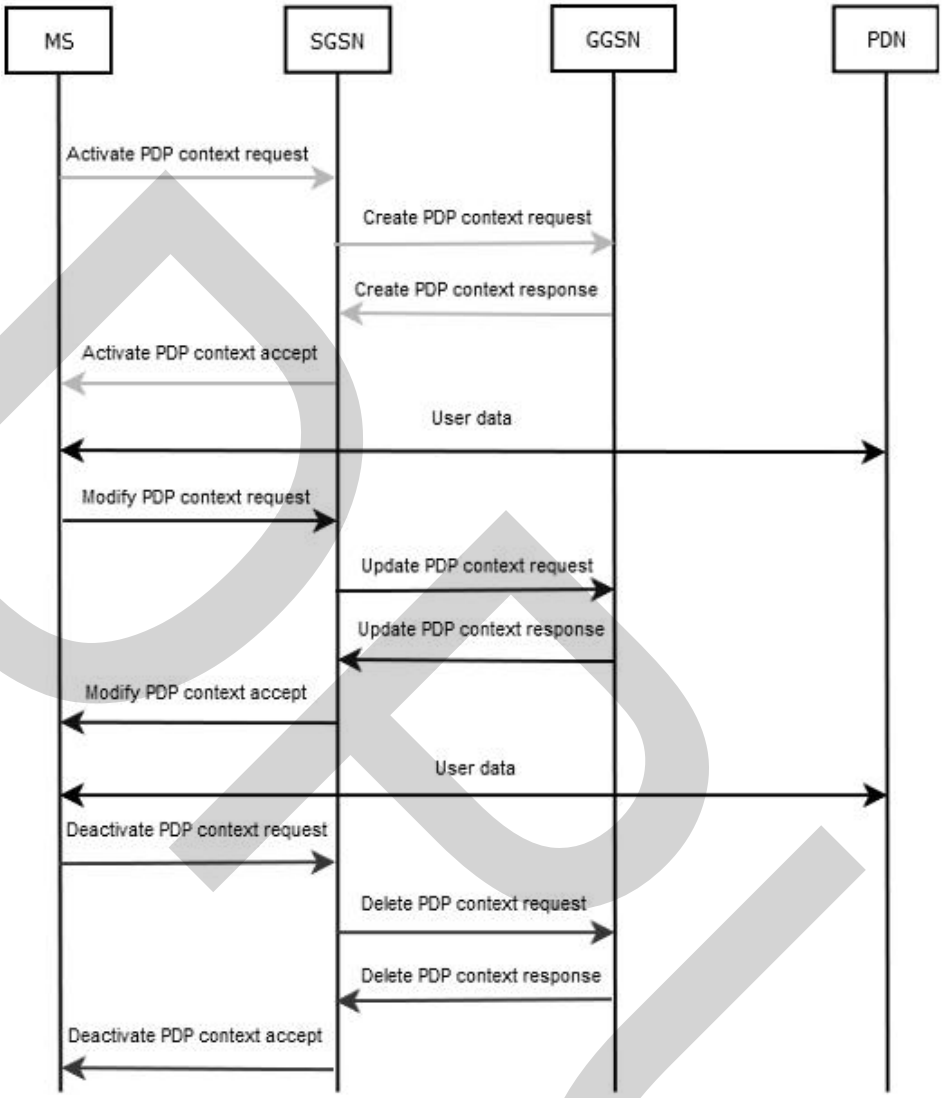
ผู้ใช้มือถือสามารถมี PDP คอนเท็คพร้อมกันหลายอย่างในช่วงเวลาเดียวกัน การจัดสรร PDP แอดเดรสสามารถเป็นได้ทั้งแบบสเตทิคหรือแบบไดนามิก สำหรับกรณีแรกที่ผู้ดูแลระบบเครือข่ายของ HPLMN ได้กำหนด PDP แอดเดรสอย่างถาวรไปยังผู้ใช้ สำหรับการจัดสรร PDP แอดเดรสแบบไดนามิก ที่PDP แอดเดรสสามารถกำหนดให้กับผู้ใช้เมื่อ “PDP context activation” มีการร้องขอ

รูปที่ 2.5 แสดงให้เห็นถึงขั้นตอนที่แตกต่างกันใน PDP คอนเทค เมื่อ MS ต้องการที่จะเชื่อมต่อกับ PDN ที่ต้องการจะส่ง “PDP context activation” ไปยัง SGSN เพื่อระบุ APN ที่ผ่านการเชื่อมต่อ ฟิลด์ PDP แอดเดรสควรจะเหลือที่ว่างเปล่าถ้าไดนามิก PDP แอดเดรสจัดสรรแบบที่ต้องการ โดย SGSN นั้นดำเนินงานปกติ เช่นการตรวจสอบและการอนุมัติของผู้ใช้ หากเข้าถึงได้ SGSN จะส่งข้อความ “Activate PDP context request” ไปยังเฉพาะ GGSN ที่ APN ต้องการเป็นปัจจุบัน ส่วนรายการใหม่ใน GGSN PDP แมพปิ้งเทเบิ้ลจะถูกสร้างขึ้น เพื่อให้ GGSN ความสามารถในการกำหนดเส้นทางการส่งข้อมูลระหว่าง SGSN และ PDN หลังจากขั้นตอนนี้ GGSN จะตอบด้วย “Create PDP context response” ไปยัง SGSN รวมถึง PDP แอดเดรส หากไดนามิก PDP แอดเดรสได้รับการร้องขอ

โดยการส่งข้อความ “Activate PDP context accept” SGSN จะอัพเดทมันใน PDP คอนเทคเทเบิลและอนุมัติการเปิดใช้งานของ PDP คอนเทคใหม่ไปยัง MS ในขั้นตอนนี้ PDP คอนเทคจะถูกสร้างขึ้นและทราฟฟิกของผู้ใช้อาจไหลได้อย่างอิสระระหว่าง MS และ PDN โดย GGSN อาจทำเครือข่ายได้รับการร้องขอการเปิดใช้งาน PDP คอนเทคเพื่อเปิดใช้งาน PDP คอนเทค เพื่อรองรับขั้นตอนที่ GGSN ต้องการที่จะมีข้อมูล PDP สเตติกเกี่ยวกับ PDP แอดเดรสรวมไปถึงข้อมูลเส้นทางที่ร้องขอไปยัง HLR

เมื่อ GTP - C “Create PDP context request” GGSN อาจตอบสนองทั้งที่มีการเปิดใช้งานที่ประสบความสำเร็จ รวมทั้งทำให้เกิดรหัส “รีเควสแอคเซพ” และรายละเอียดของ PDP คอนเทคหรือมันจะให้รหัสที่ระบุเหตุผลของความล้มเหลว รหัสสาเหตุต่างๆ ที่มีอยู่เช่น “No resources available” ที่สเตจนั้นเช่นว่ามีหน่วยความจำที่สามารถใช้ได้หรือว่าทั้งหมดของไดนามิก PDP แอดเดรสที่มีอยู่ “Missing or unknown APN” ซึ่งระบุว่า GGSN ไม่สนับสนุน APN ที่ระบุไว้และ “User authentication failed” ซึ่งบ่งชี้ว่า PDN ที่มีการปฏิเสธการบริการที่ร้องขอโดยผู้ใช้งาน

การปรับเปลี่ยน PDP คอนเทคพารามิเตอร์เช่น QoS เรดิโดไพออริทิหรือแพคเก็จโฟล ID ในระหว่างการแอคทีฟ PDP คอนเทค MS ที่สามารถส่งข้อความ “Modify PDP context request” ไปยัง SGSN ตามลำดับดังนี้ SGSN ส่งข้อความ “อัพเดต PDP คอนเทครีเควส” ไปที่ GGSN และถ้า GGSNและSGSN ทั้งสอง ทำตามการปรับปรุงทั้งสองจะตอบกลับด้วย “Update PDP context response”และ “Modify PDP context accept” กลับ



รูปที่ 2.5 PDP context activation/modification/deactivation

ที่มา: Fredrik Larsson and Azadeh Hosseinzad Amitkhizi. (2010, p. 21)

นอกจากนี้ “Update PDP Context Request” จะถูกส่งจาก SGSN ไปยัง GGSN เป็นส่วนหนึ่งของ GPRS Inter - SGSN ในขั้นตอนการปรับปรุงเส้นทางหรือจัดสรรคอนเทคใหม่เนื่องจากโหลดแชร์ริ่ง นอกจากนี้ก็จะต้องกล่าวว่าทั้ง GGSN และ SGSN สามารถที่จะเริ่มต้นการปรับเปลี่ยนของค่าพารามิเตอร์ โดย GGSN สามารถขอการแก้ไขโดยการส่ง “Update PDP Context Request” ไปยัง SGSN และ SGSN สามารถขอมันโดยการส่งข้อความ “Modify PDP Context Request” ไปที่ผู้ใช้งาน

PDP คอนเทคสามารถลบได้โดยการส่งข้อความ “Deactivate PDP context request” จากผู้ใช้งานไปยัง SGSN เป็นผลให้ SGSN จะส่งข้อความ “Delete PDP context request” ไปยัง GGSN และ GSN ทั้งสองโหนด จะยืนยันการลบ PDP คอนเทค ขั้นตอนการดีแอคทิเวทสามารถเริ่มโดย MS, SGSN และ GGSN

การที่จะได้รับที่ QoS แตกต่างกัน จากสิ่งที่มีให้ในคอนเทคหลักของมันก็ยังเป็นไปได้ที่จะเปิดใช้งาน PDP คอนเทครอง ที่ PDP แอดเดรสเดียวกันและ APN ตามที่ PDP คอนเทคหลักจะใช้สำหรับคอนเทคที่สอง โดย MS ที่จะกำหนดสิ่งที่ให้บริการจะต้องดำเนินการมากกว่าคอนเทคที่สองโดยการใช้ Traffic Flow Template (TFT) โดย TFT ถูกใช้โดย GGSN จำแนกความแต่กต่างในกลุ่ม PDP คอนเทคที่ใช้ร่วมกัน เป็นลิตส์ของแพ็คเก็ตฟิวล์เตอร์ที่ไม่ซ้ำกันสำหรับแต่ละ PDP คอนเทครวมทั้งพารามิเตอร์เช่น QoS, PDP คอนเทคและซิเคียวริตี้

โดย PDP แอดเดรสสามารถกำหนดโดยการดำเนินการของสมาชิก HPLMN หรือโดยการดำเนินการของ VPLMN ในกรณีที่เป็นไปได้อื่นๆ คือการกำหนด IP แอดเดรสที่ถาวรหรือแบบไดนามิกไปยัง MS โดยผู้ประกอบการ PDN ภายนอกหรือผู้ดูแลระบบ โดย GGSN มีหน้ารับผิดชอบในการจัดสรรที่อยู่และต่อด้วยการแอคทิเวทและดีแอคทิเวทของ PDP ในกรณีของการใช้ไดนามิกแอดเดรสจาก VPLMN หรือ HPLMN

ในระหว่างการจัดสรรที่อยู่ภายนอก PLMN อาจได้รับ PDP แอดเดรสจาก PDN และส่งมันไปยัง MS ในระหว่าง PDP คอนเทคแอคทิเวท นอกจากนี้ยังเป็นไปได้ว่าที่ MS แลกเปลี่ยน PDP แอดเดรสกับ PDN โดยตรงหลังจากเปิดใช้งาน PDP คอนเทค ในกรณีก่อนที่ PLMN จะให้ MS ที่มี PDP Address, GGSN และ PDN เป็นค่าใช้จ่ายของการกำหนดและปล่อยไดนามิกแอดเดรสโดยใช้ DHCP หรือโปรโตคอล RADIUS รวมทั้งการใช้โลเคิลพูล PDP แอดเดรสในการจัดสรร เมื่อใช้ DHCP, GGSN ทำหน้าที่เป็น DHCPไคลเอนต์ เมื่อใช้ RADIUS GGSN ทำหน้าที่เป็น RADIUS ไคลเอนต์และเมื่อใช้โลเคิลพูล GGSN ทำหน้าที่เป็น DHCP เซิร์ฟเวอร์ ในกรณีหลังนี้เมื่อ MS แลกเปลี่ยน PDP แอดเดรสโดยตรงกับ PDN ที่ MS และ PDN ที่มีค่าใช้จ่ายในการกำหนดและปล่อย PDP แอดเดรสโดยใช้ DHCP หรือ Mobile IP (MIP) โปรโตคอล เมื่อในการใช้ DHCP GGSN ทำหน้าที่เป็น DHCP รีเรย์เอเจินและเมื่อในการใช้งาน MIP GGSN ใช้เป็นฟอร์รินเอเจิน

การจัดสรร IPv6 ไดนามิกแอดเดรสมีขั้นตอนที่แตกต่างกันเมื่อเทียบกับการจัดสรร IPv4แอดเดรสในขั้นตอนนี้มีสองวิธีที่แตกต่างกันของการจัดสรรที่อยู่ การตั้งค่าอัตโนมัติแบบสเททลิสและสเททฟูล ในการกำหนดค่าอัตโนมัติแบบสเททฟูล DHCP เซิร์ฟเวอร์จำเป็นต้องมีการกำหนดที่อยู่สำหรับ IPv6 MS กระบวนการสเททลิสเป็นเพียงเล็กน้อยแต่ซับซ้อนมากขึ้นเนื่องจาก

MS มีการใช้งานในกระบวนการมากขึ้น ในขณะที่ข้อดีจากการตั้งค่าอัตโนมัติแบบสเททลีสที่มีคือไม่มีความต้องการสำหรับองค์กรภายนอกเช่น DHCP เซิร์ฟเวอร์และ RADIUS เซิร์ฟเวอร์

2.1.6 ฟังก์ชันการทำงาน GGSN

ในทุกธุรกิจจำเป็นต้องมีรายได้อยู่เสมอ ในโลกของ GPRS นี้มาจากการเรียกเก็บเงิน และ GGSN สามารถในการระบุทราฟฟิคโดยการดำเนินการตรวจสอบแพ็คเก็ตและการจำแนกการบริการและการรายงานผลไปยังระบบที่เรียกเก็บเงิน ผู้ใช้งานมีให้บริการจำนวนมหาศาลในการให้บริการในพื้นที่นี้และขึ้นอยู่กับผู้ประกอบการที่จะเกิดขึ้นด้วยวิธีที่แตกต่างกันของการเรียกเก็บเงินผู้ใช้สำหรับการใช้บริการของพวกเขา บางส่วนของฟังก์ชันการทำงานหลักของ GGSN สามารถแบ่งออกเป็นดังต่อไปนี้

- การเชื่อมต่อไปยังเครือข่ายภายนอก
- การเรียกเก็บเงิน
- การจัดการ QoS และ QoE
- ทราฟฟิคเชปปิ้ง
- การตรวจสอบแพ็คเก็ตและการจำแนกประเภทการให้บริการ
- ไดเรคท์ทัลเนิล
- เลเยอร์ 2 ทันเนิลลิ่งโปรโตคอล

โดยรายละเอียดของแต่ละฟังก์ชันการทำงานของ GGSN จะกล่าวในภาคผนวก ก

2.2 Policy and Charging Rules Function (PCRF)[2]

Policy and Charging Rules Function คืออุปกรณ์ที่เชื่อมต่อกับ GGSN ที่เริ่มนำเข้าใช้ใน 3GPP Rel.7 และทำหน้าที่จัดการนโยบายการให้บริการ ของแต่ละผู้ใช้งาน โดย PCRF จะรวมฟังก์ชันการทำงานระหว่าง The Policy Decision Function (PDF) และ The Charging Rules Function (CRF) โดย PDF จะมีหน้าที่คอยตัดสินใจในนโยบายที่จะปฏิบัติ และ CRF คือส่วนที่ให้ผู้ประกอบการกำหนดกฎระเบียบที่บังคับใช้โดย CRF จะเลือกกฎระเบียบที่เกี่ยวข้องการเรียกเก็บเงินตามข้อมูลที่ได้

PCRF ครอบคลุมการตัดสินใจการควบคุมนโยบายและโฟลตามฟังก์ชันการควบคุมการเรียกเก็บเงิน

---

[2] 3GPP TS 23.203 V7.9.0, http://www.quintillion.co.jp/3GPP/Specs/23203-790.pdf

PCRF ให้การควบคุมเครือข่ายที่เกี่ยวกับบริการ การตรวจจับโฟลข้อมูล แกสติ่ง QoS และโฟลไหนการเก็บเงิน (ยกเว้นการจัดการแบบเครดิต) ไปยัง PCEF

PCRF จะใช้วิธีการรักษาความปลอดภัยตามที่กำหนดโดยผู้ประกอบการก่อนที่จะรับบริการข้อมูลจาก AF

PCRF ต้องตัดสินใจเลือกวิธีการให้บริการการดาต้าโฟลบางอย่างจะต้องได้รับการพิจารณาใน PCEF และให้แน่ใจว่า PCEF ยูสเซอร์แพลนทราฟฟิค แมพปิ้งและทริปเมนท์เป็นไปตามรายละเอียดการสมัครของผู้ใช้

PCRF ควรจะใช้สำหรับ IP-CAN เซสชั่นได้รับมาจาก ข้อจำกัดเฉพาะของ IP-CAN นโยบายดำเนินการและ SPR ดาต้า รายชื่อของผู้ที่ได้รับอนุญาต QoS ระบุคลาสและที่เกี่ยวข้องข้อจำกัด GBR และ MBR สำหรับ IP-CAN เซสชั่น

PCRF สามารถตรวจสอบว่าข้อมูลที่ให้บริการที่มีให้โดย AF มีความสอดคล้องกับทั้งกฎระเบียบการกำหนดนโยบายของผู้ประกอบและเกี่ยวข้องกับข้อมูลของสมาชิกที่ได้รับจาก SPR ระหว่าง IP-CAN เซสชั่นจัดตั้งก่อนที่จะเก็บข้อมูลการให้บริการ การบริการข้อมูลจะถูกใช้เพื่อนให้ได้ QoS สำหรับบริการ PCRF อาจปฏิเสธคำขอที่ได้รับจาก AF เมื่อข้อมูลการบริการไม่สอดคล้องกับทั้งข้อมูลสมาชิกที่เกี่ยวข้องหรือผู้ประกอบการกำหนดกฎระเบียบนโยบายและเป็นผล PCRF ต้องแสดงให้เห็นว่าข้อมูลบริการนี้จะไม่ครอบคลุมข้อมูลของสมาชิกหรือโดยผู้ประกอบการกำหนดนโยบายและกฎระเบียบที่อาจบ่งชี้ในการตอบสนองไปยัง AF ข้อมูลการบริการที่สามารถยอมรับจาก PCRF (เช่นแบนด์วิดธ์ที่ยอมรับ) ในกรณีที่ไม่มีกลไกการควบคุมนโยบายอื่นๆ ที่อยู่นอกขอบเขตของ PCC จะแนะนำว่า PCRF รวมข้อมูลนี้ในการตอบสนอง

ในรุ่นนี้ PCRF สนับสนุนเพียงจุดอ้างอิงซิงเกิล Rx คือมีหนึ่ง AF สำหรับแต่ละเซสชั่น AF

PCRF ให้สิทธิข้อมูล QoS โดย PCRF ใช้บริการข้อมูลที่ได้รับจาก AF (เช่นข้อมูลSDP หรือข้อมูลโปรแกรมที่มีอื่นๆ) และ/หรือข้อมูลการเป็นสมาชิกที่ได้รับจาก SPR ในการคำนวณการอนุมัติ QoS ที่เหมาะสม (ระดับตัวบ่งชี้ QoS บิทเรท) PCRF อาจคำนึงถึงการร้องขอ QoS ที่ได้รับจาก PCEF ผ่านอินเตอร์เฟซ Gx

หมายเหตุ: PCRF จะให้ค่าสูงสุดสำหรับ QoS ได้รับอนุญาต แม้ว่าร้องขอ QoS ต่ำกว่าสิ่งที่สามารถได้รับอนุญาต

การอนุญาตของ QoS แหล่งข้อมูลจะต้องขึ้นอยู่กับข้อมูลบริการที่สมบูรณ์เว้นแต่ PCRF จะต้องดำเนินการอนุมัติจากแหล่งข้อมูล QoS บนพื้นฐานของข้อมูลบริการที่ไม่สมบูรณ์ หลังจากที่ PCRF ได้รับข้อมูลการบริการที่สมบูรณ์ และอับเดทกฎระเบียบ PCC ได้รับผลกระทบตามไปด้วย

PCRF อาจใช้ข้อมูลการสมัครเป็นพื้นฐานสำหรับการกำหนดนโยบายและการตัดสินใจการควบคุม การเรียกเก็บเงิน ข้อมูลสมาชิกอาจใช้สำหรับทั้งบริการที่ใช้เซสชันและไม่ใช้เซสชั่น

หาก AF ร้องขอ PCRF เพื่อรายงานเกี่ยวกับสถานะของเส้นทางการส่งสัญญาณสำหรับ AF เซสชั่น PCRF ต้องบ่งชี้ของการสูญเสียทรัพยากรจาก PCEF สำหรับกฎ PCC ที่สอดคล้องกับอัตราการทราฟฟิคของการส่งสัญญาณแจ้งให้ทราบเกี่ยวกับ AF เปลี่ยนแปลงสถานะเส้นทางการส่งสัญญาณ PCRF ต้องมีความรู้เกี่ยวกับกฎ PCC ที่ระบุสัญญาณทราฟฟิค

2.3 ระบบเครือข่ายไร้สาย (Wireless LAN)

2.3.1 เครือข่ายไร้สาย[3]

เครือข่ายไร้สาย เป็นเทคโนโลยีเครือข่ายไร้สาย ซึ่งทำให้เกิดการเปลี่ยนแปลงแนวคิดและวิธีการจัดการทางด้านเครือข่ายคอมพิวเตอร์ขององค์กรต่างๆ ทั้งในองค์กรเดิมที่มีเครือข่ายคอมพิวเตอร์อยู่แล้วและองค์กรที่เกิดขึ้นใหม่ที่ก าลังวางแผนติดตั้งระบบเครือข่ายคอมพิวเตอร์ ซึ่ง Wireless LAN (WLAN) ไม่ใช่เทคโนโลยีเครือข่ายคอมพิวเตอร์ที่มาทดแทนเครือข่ายแบบใช้สัญญาณ (Wired Network) แต่เป็นเทคโนโลยีที่สามารถขยายเครือข่ายแบบใช้สัญญาณได้ นอกจากนั้นยังถูกไปใช้ในบริเวณที่การติดตั้งสายสัญญาณมีอุปสรรคทางด้านภูมิศาสตร์หรือในบริเวณที่ต้องการความรวดเร็วในการติดตั้งเครือข่ายใหม่สำหรับการทำงานแบบชั่วคราว ซึ่ง WLAN มีความสะดวก รวดเร็วในการติดตั้งและรวดเร็วในการเคลื่อนย้ายอุปกรณ์เครือข่ายในปัจจุบันเครือข่าย WLAN ได้มีการพัฒนามาตรฐานมาหลายมาตรฐาน และมาตรฐานที่ได้รับความนิยมใช้มากที่สุด คือ มาตรฐาน IEEE 802.11

IEEE ได้กำหนดคุณสมบัติสำหรับ WLAN มาตรฐาน IEEE 802.11 ซึ่งครอบคลุมทั้ง Physical Layer (PHY) และ Media Access Control (MAC) มาตรฐาน IEEE 802.11 มีการใช้งานครั้งแรกตั้งแต่ปี 1987 โดยเป็นส่วนหนึ่งของมาตรฐาน IEEE 802.11 (Token Bus) และท างานอยู่ภายใต้กลุ่มที่เรียกว่า IEEE 802.4L ซึ่งการนำ WLAN มาใช้งานครั้งแรกนั้นเป็นการใช้ภายในโรงงานอุตสาหกรรมการผลิตรถยนต์สำหรับการควบคุมและการติดต่อสื่อสารระหว่างเครื่องมือในปี 1990 กลุ่ม IEEE 802.4L WLAN ได้เปลี่ยนชื่อเป็น IEEE 802.11 และเป็นมาตรฐานอิสระของ IEEE 802 ที่กำหนดระดับ PHY และ MAC สำหรับ WLAN โดยมาตรฐานแรกของ IEEE 802.11 ใช้อัตราส่ง 1Mbps และ 2Mbps ได้เสร็จสมบูรณ์ตั้งแต่ปี 1997 โดยมีระดับของ PHY เป็นแบบ DSSS, FHSS และ Diffused Infrared (DFIR) เมื่อมาตรฐานแรกเสร็จสมบูรณ์แล้วหลังจากนั้นได้มี

---

[3] เครือข่ายไร้สาย, http://www.bc.msu.ac.th/project_file/6%288%29.pdf

การกำหนดให้มี PHY ใหม่ที่รองรับอัตราส่ง 11 Mbps โดยใช้การเข้ารหัสแบบ CCK เรียกว่า IEEE 802.11b และอัตราส่ง 54 Mbps โดยใช้ PHY แบบ OFDM เรียกว่า IEEE 802.11a และทั้งสามรุ่นมีการทำงานในระบบ MAC ที่เหมือนกัน คือ การใช้กลไกของ Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) ในการใช้ช่องสัญญาณสำหรับการติดต่อสื่อสาร

2.3.2 รูปแบบการเชื่อมต่อของระบบเครือข่ายไร้สาย

2.3.2.1 Peer-to-Peer (ad hoc mode)

รูปแบบการเชื่อมต่อแลนไร้สายแบบ Peer to Peer เป็นการเชื่อมต่อแบบโครงข่ายโดยตรงระหว่างเครื่องคอมพิวเตอร์ โดยเครื่องคอมพิวเตอร์แต่ละเครื่องนั้นจะมีความเท่าเทียมกัน สามารถทำงานของตนเองได้ และขอใช้บริการเครื่องอื่นได้ จึงเหมาะสำหรับนำมาใช้งานเพื่อจุดประสงค์ด้านความรวดเร็ว หรือติดตั้งได้โดยง่ายเมื่อไม่มีโครงสร้างพื้นฐานที่จะรองรับ ตัวอย่างเช่น ในศูนย์ประชุมหรือการประชุมที่จัดนอกสถานที่

2.3.2.2 Client/Server (Infrastructure mode)

ระบบเครือข่ายไร้สายแบบ Client/Server (Infrastructure mode) มีลักษณะการรับส่งข้อมูลโดยอาศัย Access Point (AP) หรือเรียกว่า "Hot Spot" ทำหน้าที่เป็นสะพานเชื่อมต่อระหว่างระบบเครือข่ายแบบใช้สาย กับคอมพิวเตอร์ลูกข่าย (Client) โดยจะกระจายสัญญาณคลื่นวิทยุเพื่อรับ -ส่งข้อมูลเป็นรัศมีโดยรอบ ซึ่ง AP 1 จุด สามารถให้บริการเครื่องลูกข่ายได้ถึง 15-50 อุปกรณ์ เหมาะส าหรับการนำไปขยายเครือข่าย หรือใช้ร่วมกับระบบเครือข่ายแบบใช้สายเดิมใน Office ห้องสมุด หรือในห้องประชุม เพื่อเพิ่มประสิทธิภาพในการทำงานให้มากขึ้น

2.3.2.3 Multiple access points and roaming

เป็นการเพิ่มจุดการติดตั้ง AP ให้มากขึ้น เพื่อให้การรับส่งสัญญาณในบริเวณของเครือข่ายขนาดใหญ่เป็นไปอย่างครอบคลุมทั่วถึง

2.3.2.4 Use of an Extension Point

มีคุณสมบัติเหมือนกับ Access Point แต่ไม่ต้องผูกติดไว้กับเครือข่ายไร้สาย

2.3.2.5 The Use of Directional Antennas

ระบบแลนไร้สายแบบนี้เป็นแบบใช้เสาอากาศในการรับส่งสัญญาณระหว่างอาคารที่อยู่ห่างกัน โดยการติดตั้งเสาอากาศที่แต่ละอาคาร เพื่อส่งและรับสัญญาณระหว่างกัน

2.3.3 เฟริมแวร์ DD-WRT[4]

DD-WRT เป็น Third partyในการพัฒนาเฟิร์มแวร์ภายใต้เงื่อนไขของ GPL ที่สำหรับเราเตอร์ไร้สาย ieee802.11a/b/g/h/n อยู่บนพื้นฐานอ้างอิงการออกแบบชิปของ Broadcom หรือ Atheros

โดยเฟิร์มแวร์จะดูแลโดย BrainSlayer และโฮสต์ที่ dd-wrt.com รุ่นแรกของ DD - WRT ได้อยู่บนพื้นฐานของแอลชิมิสเฟิร์มแวร์จาก Sveasoft Inc ซึ่งในการเปิดตามเดิม GPL'd Linksys เฟิร์มแวร์และจำนวนอื่นๆ ของโครงการโอเพ่นซอร์ช DD-WRT ถูกสร้างขึ้นโดยตรงจากการตัดสินใจของซอฟต์แวร์

ในปัจจุบันที่ DD - WRT สามารถใช้ได้ฟรีถึงแม้ว่ารูปแบบธุรกิจที่แตกต่างกันจะถูกเกณฑ์โดย BrainSlayer เพื่อจ่ายเงินเดือนของเขาเช่นนี้เป็นเวลางานของเขาเต็ม

ตารางที่ 2.1 ข้อมูลอุปกรณ์ที่สามารถติดตั้งเฟิร์มแวร์ DD-WRT

ยี่ห้อ	รุ่น
Buffalo	WCR-GN, WHR-G125, WHR-G300N, WHR-HP-G300N, WHR-AMG54, WHR-HP-GN, WHR3-AG54, WLA-G54C, WLI-TX1-G54, WLI-TX4-G54HP, WZR-G54, WZR-G300N
Cisco Linksys (Wireless a/b/g)	WRE54G, WRH54G, WRT54G, WRT54G, WRT54GL, WRT54GS, WRTSL54GS
Cisco Linksys (Wireless a/b/g/n)	WRT150N, WRT160N, WRT300N, WRT310N, WRT350N, WRT600N
D-Link	DIR-300, DIR-320, DIR-330, DIR-400, DIR-600, DIR-601, DIR-615, DIR-825, DSM-G600
TP-Link	WA901N(D), WR740N, WR741N(D), WR741ND, WR841N(D), WR940N, WR941N(D), WR1043N(D)

ที่มา: Firmware DD-WRT v23 SP2 [online] : เข้าถึง 6 ก.ค. 2554. http://www.dd-wrt.com

[4] Firmware DD-WRT v23 SP2, http://www.dd-wrt.com.

รุ่นใหม่ของ DD-WRT (v24) เป็นโครงการใหม่ที่สมบูรณ์ DD-WRT มีคุณลักษณะขั้นสูงจำนวนมากที่ไม่พบใน firmwares OEM ของอุปกรณ์เหล่านี้หรือแม้กระทั่งเฟิร์มพร้อมสำหรับการซื้อจาก Sveasoft นอกจากนี้ยังเป็นอิสระจากการเปิดใช้งานผลิตภัณฑ์หรือการติดตามที่พบในเฟิร์มแวร์ Sveasoft

โดยอุปกรณ์ที่สามารถติดตั้งเฟิร์มแวร์ DD-WRT ในการใช้งานได้ ดังตารางที่ 2.1

2.3.4 การใช้ RFlow Collector และ MySQL เพื่อรวบรวมข้อมูลทราฟฟิค[5]

เราเตอร์ DD - WRT ของคุณสามารถส่งข้อมูลการจราจรไปยังเครื่องคอมพิวเตอร์ในเครือข่ายของคุณแล้วเก็บข้อมูลในฐานข้อมูล MySQL ที่คุณสามารถค้นหานั้นสามารถบอกคุณเกี่ยวกับทราฟฟิคบนเครือข่ายของเรา กระบวนการนี้เกี่ยวข้องกับหลายขั้นตอน

ส่วนที่ 1 การตั้งค่าเราเตอร์ของคุณเพื่อส่งข้อมูลการจราจรไปยังเครื่องคอมพิวเตอร์

ส่วนที่ 2 การตั้งค่า RFlowCollector

ส่วนที่ 3 การตั้งค่า MySQL

โดยรายละเอียดของแต่ละส่วนจะกล่าวในภาคผนวก ก

2.4 งานวิจัยที่เกี่ยวข้อง

2.4.1 บริดจ์วอเตอร์โพลิซีคอนโทรล[6]

บริดจ์วอเตอร์ โพลิซีคอนโทรลเป็นโพลิซีเซิร์ฟเวอร์ที่มีความยืดหยุ่นสูงซึ่งออกแบบโดยเฉพาะเพื่อช่วยให้ผู้ให้บริการการจัดการผลกระทบของการเติบโตของข้อมูลบนเครือข่ายโทรศัพท์มือถือของพวกเขาและสร้างรายได้จากบริการส่วนบุคคล

การรวมความสามารถในการวัดที่มีความซับซ้อประสบการณ์มากที่มีกำหนดกฎทางธุรกิจสูง โพลิซีคอนโทรลสามารถนำไปใช้ที่หลากหลายเช่นอินเทอริเจ้น การควบคุมแบบเรียลไทม์รวมถึงการจัดการคุณภาพของการให้บริการ (QoS) ที่เปลี่ยนแปลง เพิ่มประสิทธิภาพแบนด์วิดธ์ทราฟฟิกให้สูงและการบังคับใช้โควต้าการใช้งาน การควบคุมเหล่านี้สามารถถูกใช้เพื่อสนับสนุนการตั้งค่าที่กว้างขวางของการใช้งานสำหรับทั้งการเพิ่มประสิทธิภาพเครือข่ายและ เซอร์วิทอีนาเบิลเม็นท์ การรวมบริการที่เป็นชั้น โปรแกรมความซื่อสัตย์ของลูกค้า การเพิ่มประสิทธิภาพวิดีโอและอื่นๆ

---

[5] RFlow Collector, http://www.dd-wrt.com/wiki/index.php/RFlow_Collector.

[6] Data Sheet: Bridgewater Policy Controller, http://www.bridgewatersystems.com/Policy-Controller.aspx

โพลิซีคอนโทรลที่สอดคล้องกับ Third Generation Partnership Project (3GPP) Release 7, 8 และ 9 มาตรฐานสำหรับ and Charging Rules Function (PCRF) และสามารถใช้งานในเครือข่าย HSPA, EVDO, WiMAX และ LTE เป็นส่วนหนึ่งของ evolved packet core (EPC) ภายในสภาพแวดล้อมเหล่านี้จะสามารถใช้งานได้อย่างรวดเร็วได้หลายประเภทของการบังคับใช้นโยบายจุดดังกล่าวเป็นแอคเซทเกตเวย์ DPIs และการเพิ่มประสิทธิภาพการแก้ปัญหาขึ้นอยู่กับกรณีการใช้งานจะต้องสนับสนุน

2.4.1.1 วิธีการที่สมาร์ทในโพลิซีคอนโทรล

บริดจ์วอเตอร์ได้มีการพัฒนาวิธีการใหม่ในการกำหนดนโยบายที่ช่วยให้ผู้ให้บริการครอบคลุมการควบคุมเพื่อเพิ่มประสิทธิภาพเครือข่าย 3G และ 4G และการดำเนินการที่หลากหลายของบริการส่วนบุคคลสำหรับลูกค้า วิธีการสมาร์ทของบริดจ์วอเตอร์ประกอบด้วยความสามารถที่สำคัญ 4 สิ่งในการรองรับบริดจ์วอเตอร์โพลิซีคอนโทรล

สมาร์ทคอนโทรล ช่วยให้การควบคุมการให้บริการเพื่อจัดลำดับความสำคัญการใช้ทรัพยากรเครือข่ายสำหรับเว็บไซต์ของแต่ละเซลล์และสำหรับสมาชิกแต่ละคน สมาร์ทคอนโทรลใช้ประโยชน์จากมีมุมมองของผู้ใช้บริการรวมถึงการเชื่อมต่อและข้อมูลสถานที่ ได้รับสิทธิและโปรไฟล์การให้บริการและเซลล์ในสภาวะแบบไดนามิกเพื่อตัดสินใจอย่างชาญฉลาดที่จัดลำดับความสำคัญโดยเฉพาะกลุ่มผู้ใช้บริการในชีวิตจริง

สมาร์ทแคป มีความยืดหยุ่นและเป็นวิธีการแบบเรียลไทม์เพื่อครอบแบนด์วิดธ์ที่ช่วยให้ผู้ประกอบการใช้การควบคุมที่แตกต่างกันแบบไดนามิกขึ้นอยู่กับจำนวนของปัจจัยต่างๆ เช่นการบริการรูปแบบชั้น รูปแบบการใช้งานและเวลาของวัน สมาร์ทแคปปรับปรุง ROI โดยการลบความจำเป็นในการอัพเกรดที่มีราคาแพงเพื่อบรรเทาความแออัดที่เกิดจากผู้ใช้จำนวนมาก พวกเขายังเพิ่มประสิทธิภาพการจัดสรรแบนด์วิดธ์ที่มีอยู่ทั่วทั้งสมาชิกเพิ่มขึ้น เป็นธรรมในการเข้าถึงเครือข่ายและการปรับปรุงประสบการณ์ของผู้ใช้

สมาร์ทแอป ให้การควบคุมประสบการณ์ของผู้ใช้ที่ช่วยให้ผู้ประกอบการและสมาชิกที่จะตัดต่อประสบการณ์บนพื้นฐานของความต้องการใช้ (เช่นสตรีมมิ่ง เกม ดาวน์โหลด อีเมล์) ในขณะที่ยังคงคำนึงถึงความจริง การตั้งค่าของผู้ใช้บริการและพฤติกรรมแบบเรียวทาม

สมาร์ทไคล์แอนท์ มีความสามารถที่ช่วยให้ผู้ประกอบการที่จะขยายความโปร่งใสและการควบคุมส่วนบุคคลให้กับสมาชิกโดยใช้โปรแกรมของลูกค้าที่สะดวกและง่ายสำหรับมาร์ทโฟนและแล็ปท็อปจึงวางการควบคุมที่มันอยู่ในมือของลูกค้าและความโปร่งใสในการปรับปรุง

2.4.1.2 คุณลักษณะและคุณประโยชน์

1) การวัดแบบเรียลไทม์

ดำเนินการมาตรฐาน 3GPP อินเตอร์เฟซ Gx สำหรับการดำเนินการวัดแบบเรียลไทม์ รวมถึงการวัดทราฟฟิคโฟลที่แตกต่างกันภายในระยะเวลาที่แต่ละผู้ใช้ ระบบวัดจะขึ้นอยู่กับเวลาปริมาณ แอฟพิเคชั่น หรือการรวมกันทั้งสามให้การสนับสนุนสำหรับบริการที่ชั้นแตกต่างกัน

2) ใช้ซัพพอร์ตเคชอย่างกว้างขวาง

รองรับการตั้งค่าที่กว้างที่สุดของกรณีใช้ในอุตสาหกรรมเพื่อช่วยให้ผู้ประกอบการจัดการประสิทธิภาพของเครือข่ายและความสามารถอย่างชาญฉลาดและสนับสนุนการให้บริการที่สร้างรายได้ใหม่

3) การบังคับใช้พอยท์ซัพพอร์ท

ช่วยให้กฎระเบียบนโยบายที่จะดำเนินการในหลายจุดที่แตกต่างกันบังคับใช้รวมถึงแอคเซตเกตเวย์ DPIs, Content optimization servers และอุปกรณ์ของสมาชิก นี้จะช่วยให้ผู้ให้บริการจะนำไปใช้กับกฎระเบียบนโยบายตลอดทั้งเครือข่าย จากอุปกรณ์ radio access network (RAN) ไปยังคอร์เน็ตเวอร์และการสนับสนุนความหลากหลายของกรณีการใช้งาน

4) การตระหนักซับสคริปเบอร์คอนเท็ค

ทำให้ผู้ให้บริการจะนำไปใช้การควบคุมอย่างอัจฉริยะอยู่บนพื้นฐานของข้อมูลแบบเรียลไทม์เกี่ยวกับเครือข่ายที่ใช้บริการและการประยุกต์ใช้เช่น แผนสถานะบริการ สถานะการโรมมิ่ง ความแออัดของเครือข่ายและประเภทของทราฟฟิค

5) การปรับเปลี่ยนช่วงกลางแบบไดนามิก

ให้การควบคุมที่ละเอียดมากกว่าการใช้งานแบนด์วิดธ์และช่วยให้การปรับเปลี่ยนที่จะริเริ่มโดยสมาชิกหรือบุคลากรการบริการลูกค้า เนื่องจากการควบคุมนโยบายที่สามารถจัดการข้อมูลการใช้งานแบบเรียลไทม์ต่อเซสชั่นและต่อพื้นฐานสมาชิก มันลดค่าใช้จ่ายที่เกี่ยวข้องกับการวิเคราะห์ที่ไม่ใช่เรียลไทม์ของการใช้บริการและการจัดเตรียมของวงเงินการใช้งานและช่วยลดการโทรในการดูแลลูกค้าจากลูกค้าไม่พอใจ

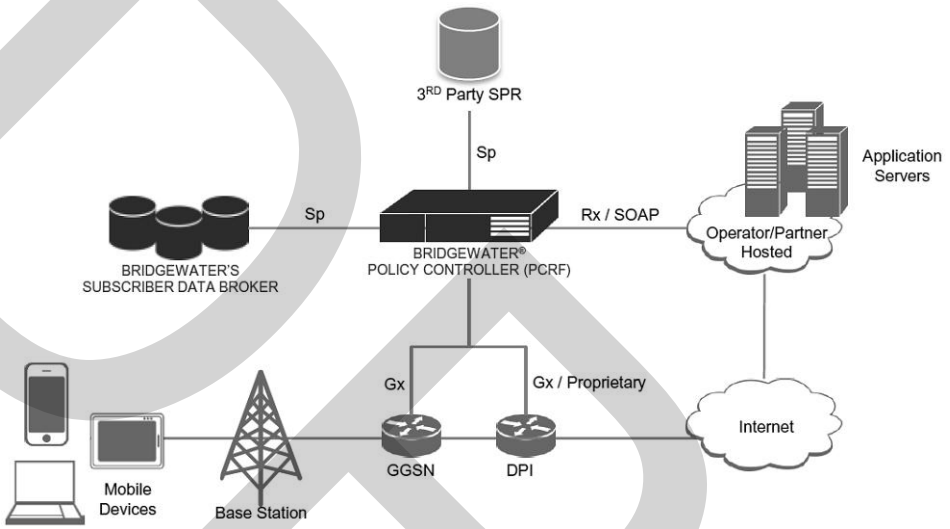
6) ความโปร่งใสของสมาชิก

ให้แจ้งเตือนผู้ใช้บริการแบบเรียลไทม์ผ่านทาง SMS, e-mail หรือเปลี่ยนเส้นทางไปยังพอร์ทัลลูกค้า การแจ้งเตือนจะถูกเรียกโดยเหตุการณ์แบบ real-time เช่นเกินเกณฑ์การใช้งานสำหรับการใช้งานที่เฉพาะเจาะจง ให้บริการโรมมิ่งกับเครือข่ายอื่นหรือเทียบเท่าสำหรับโปรแกรมความภักดีของลูกค้า ความโปร่งใสที่ดีขึ้นจะช่วยลดต้นทุนการดำเนินงานและเพิ่มความพึงพอใจของผู้ใช้บริการ

7) การทำงานร่วมกันหลายผู้ผลิตในวงกว้างและมาตรฐานการสนับสนุน

สอดคล้องกับมาตรฐาน 3GPP ที่มีการเชื่อมต่อและความต้องการด้านประสิทธิภาพการออกแบบและทดสอบสำหรับสภาพแวดล้อมหลายผู้ผลิต

8) ตัวอย่างการใช้งาน



รูปที่ 2.6 PCRF Network Deployment (3GPP R7)

ที่มา: Data Sheet: Bridgewater Policy Controller [online] : เข้าถึง 12 ต.ค. 2554. http://www.bridgewatersystems.com/Policy-Controller.aspx

2.4.2 Personalized Policy & Charging Solution (Telcordia)[7]

ลูกค้าที่มีความปราณาที่ไม่เพียงพอสำหรับการให้บริการใหม่และอุปกรณ์มีมากขึ้นจะมีประสบการณ์ที่ดีที่สุดโดยไม่คำนึงถึงเครือข่าย ประสิทธิภาพ มูลค่า ที่ดีที่สุด Telcordia จะช่วยให้ผู้ให้บริการด้านการสื่อสาร (CSPs) สร้างรายได้จากเครือข่ายบรอดแบนด์ดีโดยการย้ายจากเพียงการขาย"ไบต์"เป็นการให้บริการแทนการขาย ซึ่งมีมูลค่าที่แท้จริงที่สูงขึ้นให้กับลูกค้า Telcordia นโยบายส่วนบุคคลและการแก้ปัญหาการคิดเงิน สำเร็จนี้โดยการทำการรวมชาร์จและการจัดการ

[7] Personalized Policy & Charging Solution, http://www.telcordia.com/collateral/brochures/personalized-policy-charging-brief.pdf

นโยบายอย่างใกล้ชิด ทำให้ CSPs มีความง่ายขึ้นในการให้บริการแพคเกจ แอดออน และแรงกระตุ้นในการซื้อ

ด้วยเครือข่ายบรอดแบนด์ทราฟฟิคเป็นที่นิยม ความท้าทายสำหรับผู้ให้บริการเพื่อสร้างรายได้เพิ่มสูงขึ้นจากทราฟฟิค และความต้องการเหล่านี้เป็นเพียงจำนวนที่เพิ่มขึ้นของอุปกรณ์ที่เติบโตแบบเอ็คโปเน็นเชียว แบบเครื่องต่อเครื่องและอุปกรณ์อิเล็กทรอนิกส์ยังจุดเริ่มต้นที่จะใช้ข้อมูลเครือข่าย ตามที่ Marson กล่าวว่า “ดาต้าทราฟฟิคแบบไร้สายในประเทศที่พัฒนาจะเพิ่มขึ้นเป็นสิบเท่าระหว่างปี 2008 และปี 2015 และเจ็ดเท่าในตลาดเกิดใหม่ในช่วงเวลาเดียวกัน รายได้ต่อเมกะไบต์จะยังคงแย่อยู่ ขับเคลื่อนลงแข่งขันที่เพิ่มขึ้นและการกำหนดราคาแบบแฟลทเรท” ต่อด้วย “ไม่ได้เป็นรูปแบบธุรกิจที่ยั่งยืนและ CSPs รู้ว่าพวกเขาจะต้อง ... ใช้เครือข่ายที่ชาญฉลาด”

ระบบไดนามิก รวมกับความต้องการของการกำกับดูแลการคุ้มครองผู้บริโภคจำเป็นต้องมีผู้ให้บริการในการปรับใช้นโยบายการควบคุมที่ซับซ้อนมากขึ้นและประดิษฐ์วิธีใหม่ในบรรจุภัณฑ์และการตลาดในการให้บริการบรอดแบนด์ของพวกเขา การรวมกันของบริการตามนโยบายการจัดการและการเรียกเก็บเงินเรียลไทม์ที่สามารถช่วยให้ CSPs ใช้ประโยชน์อย่างเต็มที่จากการนิยมของบรอดแบนด์นี้

2.4.2.1 การควบคุมและความแตกต่างของบรอดแบนด์ของคุณ

นโยบายส่วนบุคคลและการแก้ปัญหาการเรียกเก็บเงินของ Telcordia ทำให้ผู้ให้บริการที่จะแนะนำแผนและเพื่อเสนอแพคเกจและโปรโมชั่นสำหรับข้อมูล เนื้อหาและบริการที่เพิ่มมูลค่าให้กับรายได้เพิ่มขึ้นบนเครือข่าย Telcordia หาทางออกที่จะช่วยให้ผู้ประกอบการมีความยืดหยุ่นและจำเป็นที่ควบคุมในการสร้างการนำเสนอแบบไดนามิกสำหรับการกำหนดนโยบายและการเรียกเก็บเงินเพื่อช่วยในการแยกความแตกต่างของตราสินค้าในตลาด-และจะยังคงทำเช่นนี้อย่างต่อเนื่องและอย่างรวดเร็ว วิธีการแก้ปัญหาการจัดการนโยบายและการเรียกเก็บเงินแบบเรียลไทม์ สามารถใช้ได้กับการใช้งานบรอดแบนด์ของทั้งแบบรายเดือนและลูกค้าแบบเติมเงิน เพราะในสภาพแวดล้อมนี้ ที่ประสบการณ์ของผู้ใช้เช่น สิ่งที่สำคัญ ค่าการเข้าถึงขั้นพื้นฐานหรือแผนแบบคงที่ มีไม่เพียงพอ

2.4.2.2 สร้างโอกาสรายได้เพิ่มขึ้น

นโยบายส่วนบุคคลและการแก้ปัญหาการเรียกเก็บเงินของ Telcordia จะช่วยให้คุณหาวิธีสร้างรายได้จากโครงสร้างพื้นฐานบรอดแบนด์ของคุณ ตัวอย่างง่ายๆ ของการบริการรูปแบบใหม่ที่เป็นผลกระทบของการแออัดของเครือข่าย สมาชิกที่มีคุณภาพของประสบการณ์เมื่อมีการใช้สตรีมมิ่งวิดีโอ ด้วยนโยบายและการควบคุมการเรียกเก็บเงินแบบเรียลไทม์ ผู้ให้บริการสามารถสร้างบริการแบบไดนามิกแบบ “turbo boot” ซึ่งผู้ใช้สามารถเพิ่มโปรไฟล์ของตน

2.4.2.3 ความเชื่อถือตามมาตรฐาน OCS และ PCRF INTEGRATION

สร้างรายได้ที่ดีกว่าของเครือข่ายบรอดแบนด์ของคุณ ไม่ควรหมายถึงการสูญเสียการควบคุมหรือล็อคลงไปในวิถีทางที่เป็นกรรมสิทธิ์เฉพาะ มันเริ่มต้นด้วยการควบคุมแบบเรียลไทม์สำหรับทั้ง นโยบายและการเรียกเก็บเงิน (ระบบเรียกเก็บเงิน ออนไลน์หรือโอซีเอและนโยบายและการทำงานกฎการเรียกเก็บเงิน หรือ PCRF) อีกหนึ่งองค์ประกอบที่สำคัญคือ เรียลไทม์ ในหน่วยความจำ ฐานข้อมูลสมาชิกที่ว่างสูง (พื้นที่เก็บข้อมูลรายละเอียดสมาชิกหรือ SPR)

การรวมเข้าด้วยกันของเครือข่ายระหว่าง OCS / PCRF และองค์ประกอบของเครือข่ายจะถูกกำหนดโดยมาตรฐาน 3GPP แต่การรวมเข้าด้วยกัน ระหว่างระบบ OCS และ PCRF จะไม่ได้พูดอย่างชัดเจนตามมาตรฐานโดยเฉพาะอย่างยิ่งสำหรับการบริการและการวางแผนสร้างงาน - ซึ่งมีความจำเป็นสำหรับนวัตกรรมบริการอินเทอร์เน็ตความเร็วสูงและใช้เวลาอย่างรวดเร็วในตลาด Personalized Policy & Charging solution integrates Telcordia®, Broadband Charging and Telcordia® และการจัดการแบนด์วิดท์ ให้ผู้ประกอบการมีเครื่องมือที่จำเป็นเพื่อให้ง่ายต่อการกำหนดและปรับใช้บริการใหม่ในเครือข่าย

2.4.2.4 การอัพเกรดในการขาย

ให้ผู้ใช้อัพเกรดในขณะที่เมื่อพวกเขากำลังพยายามที่จะทำสิ่งที่ได้รับประโยชน์จากการอัพเกรด ตัวอย่างเช่นหากผู้ใช้ต้องการในการเข้าถึงวิดีโอ HD คุณสามารถให้ผู้ใช้อัพเกรดถาวรหรือชั่วคราวให้กับผู้สมัครเป็นสมาชิกของพวกเขาหรือโปร่งใสโดยบริการอัพเกรดในการจัดส่งเนื้อหา (ผู้ใช้เพียงแค่จ่ายสำหรับเนื้อหาและบอกเนื้อหาเซิร์ฟเวอร์ที่เครือข่ายเพื่อให้แบนด์วิดธ์ที่จำเป็น) ซึ่งประเภทของที่คุณนำเสนอให้ขึ้นอยู่กับการแบ่งส่วนตลาดและประเภทของข้อตกลงที่คุณมีของคุณกับคู่ของเนื้อหา

2.4.2.5 การป้องกัน BILL SHOCK

การตรวจสอบการใช้จ่ายในเวลาจริงสำหรับข้อมูลและการทำธุรกรรมอื่นๆ และใช้กฎและเกณฑ์ที่กำหนดไว้โดย CSP และผู้ใช้ การดำเนินการสามารถรวมไปถึงการแจ้งเตือนของการใช้และเกณฑ์ให้กับผู้ใช้หรือบุคคลที่สาม ป้องกันการทำธุรกรรมและการเข้าถึงอีกเส้นทางไปยังหน้าเว็บ

2.4.2.6 โปรโมชั่น off–peak

เสนอโปรโมชั่นพิเศษสำหรับการใช้งานในช่วงเวลาการใช้งานต่ำหรือในภายใต้การใช้เซลล์ บริการตามกฎระเบียบนโยบาย อนุญาตให้มีการโปรโมชั่นของการบริการ (ตัวอย่างเช่นวิดีโอสตรีมมิ่ง) เวลาและสถานที่ซึ่งจะมีผลเพียงเล็กน้อยบนเครือข่าย ทั้งสองนี้สามารถส่งเสริมการใช้งานและยังเพิ่มผลกำไรสำหรับผู้ใช้ทั้งแบบเติมเงินและแบบรายเดือน

2.4.2.7 การเพิ่มและแรงกระตุ้นซื้อ

การสร้างและนำเสนอคุณสมบัติหรือบริการเพิ่มเติมที่ผู้ใช้ทันทีที่สามารถเพิ่มไปยังบัญชีของพวกเขา (ทั้งถาวรหรือสำหรับระยะเวลาที่จำกัด) ตัวอย่างเช่นอาจจะเข้าสู่การแข่งขันโดยเฉพาะผ่านทางเนื้อหาของพาทเนอร์ที่เฉพาะเจาะจงสำหรับราคาคงที่ กับการเข้าถึงข้อมูลที่เกี่ยวข้องต่อการไม่นับโควต้าและมีแบนด์วิดธ์ให้ได้ตามความจำเป็น นี้จะสามารถนำเสนอผ่านการเชื่อมโยงจากการโฆษณา (ในทางเข้าเว็บหรือใน SMS) หรือเป็นส่วนหนึ่งของลูกค้าปกติของการดูแลและสามารถส่งเสริมให้ผู้ใช้ทั้งหมดทั้งเติมเงินหรือแบบรายเดือน

2.4.2.8 ควบคุมโดยผู้ปกครอง/ธุรกิจ/ครัวเรือน

อนุญาตให้ผู้ปกครองและธุรกิจขนาดเล็กหรือหัวหน้าครัวเรือนจัดการการใช้งานโดยครอบครัวหรือพนักงาน เจ้าของบัญชีกำหนดข้อจำกัดในการใช้งานและยังสามารถตั้งค่ากฎระเบียบเพื่อควบคุมเมื่อได้ให้บริการที่อาจถูกใช้ (ตัวอย่างเช่นเพื่อป้องกันการใช้ในช่วงเวลาที่โรงเรียน) มีการเปลี่ยนแปลงได้อย่างง่ายดาย (ตัวอย่างเช่นเพื่อให้รางวัลแก่พฤติกรรมที่ดีหรือส่งเสริมให้มีความจงรักภักดีของพนักงาน)

2.4.2.9 การทดลองให้บริการ

อนุญาตให้จำกัดทดลองที่การให้บริการสำหรับค่าใช้จ่ายที่ต่ำมาก ส่งเสริมให้ผู้ใช้ได้ลองความสามารถใหม่ๆ การทดลองสามารถรวมวงเงินค่าใช้จ่ายหรือการใช้งานที่จำกัด (ให้ทั้ง CSP และความเชื่อมั่นของผู้ใช้ที่ค่าใช้จ่ายของมีจำนวนจำกัด) รวมทั้งการควบคุมคาปาซิตี้ (จำกัดการใช้งาน) ผู้ใช้ยังสามารถอัพเกรดทันทีให้บริการเต็มรูปแบบได้ตามที่เขาต้องการ

2.4.2.10 บริการตามขั้นและการใช้ความยุติธรรม

การสร้างและเสนอขั้นไม่ได้ขึ้นอยู่เพียงแค่ในโควต้าหรือแบนด์วิดธ์ แต่เกี่ยวกับการบริการ รวมถึงการเข้าถึง (มีหรือไม่มีข้อจำกัดในการใช้งานยุติธรรม) โดยเฉพาะอย่างยิ่งการให้บริการหรือเว็บไซต์ (เช่นเว็บไซต์เครือข่ายสังคมที่นิยม) ในขณะที่การไม่อนุญาตหรือจำกัดการเข้าถึงผู้อื่นโดยที่อยู่เว็บไซต์ โดยโปรโตคอลหรือโดยการใช้คุณลักษณะที่มีประสิทธิภาพของระบบ DPI อนุญาตให้ผู้ใช้สามารถอัพเกรดได้ตลอดเวลาอย่างใดอย่างหนึ่งอย่างถาวรหรือสำหรับระยะเวลาที่จำกัด เช่นหนึ่งชั่วโมงวันหนึ่ง ฯลฯ

2.4.2.11 สร้างรายได้ของอุปกรณ์

สร้างบริการที่สามารถให้บริการฟรีค่าใช้จ่ายเพื่อดึงดูดผู้ใช้อุปกรณ์เฉพาะเช่นสมาร์ทโฟนยอดนิยม แท็บเล็ต ปุ๊ครีดเดอร์ที่สามารถอัพเกรดได้ง่ายโดยผู้ใช้บริการชำระเงินสำหรับตัวอย่างเช่นมีซิมการ์ดสำหรับแท็บเล็ตใหม่ที่มีการเข้าถึงเว็บไซต์ของCSPและฟรีบางเนื้อหา – รวมการแอฟสำหรับ “one-touch” การอัพเกรดเพื่อให้สามารถเรียกดูอีเมลและเว็บและการอัพเกรด

ต่อไปในการเข้าถึงบริการวิดีโอและอื่นๆ ราคาที่สามารถตั้งค่าเพื่อให้การรวมกันของค่าใช้จ่ายที่เดียว ค่าใช้จ่ายที่เกิดขึ้นและค่าใช้จ่ายการใช้งานใดๆ

2.4.3 SERVICE AWARE CHARGING AND CONTROL(ERICSSON)[8]

2.4.3.1 การตระหนักถึงเครือข่าย – การแสดงผลและการควบคุม

ตระหนักถึงการบริการโซลูชั่นการควบคุมและการเรียกเก็บเงินของอีริคสันกำหนดการตรวจสอบแพ็คเก็ตที่ลึกและฟังก์ชันการทำงานการจดจำรูปแบบที่จำเป็นในการระบุทราฟฟิคที่ดำเนินการผ่านเครือข่าย โดนพัฒนาอย่างต่อเนื่องของการแก้ปัญหาเพื่อให้มั่นใจว่าการใช้งานใหม่ (เช่น Voice over IP และ โปรแกรมแบบ peer-to-peer อื่นๆ) สามารถตรวจพบและการบริหารจัดการสอดคล้องกับนโยบายที่ต้องการสำหรับการรักษาความปลอดภัย เส้นทางและการเรียกเก็บเงิน ในระยะสั้นทุกอย่างเกี่ยวกับการแสดงผลและการควบคุม

2.4.3.2 พฤติกรรมผู้ใช้บริการ

ในธุรกิจสื่อสารการแข่งขันมากขึ้นมันสำคัญที่จะรับกับแนวโน้มใหม่ในช่วงเริ่มต้น ส่วนการวิเคราะห์ทราฟฟิคของโซลูชั่นการควบคุมและการเรียกเก็บเงินของอีริคสันเป็นเครื่องมือสำหรับวัตถุประสงค์นี้ โดยการวิเคราะห์พฤติกรรมผู้ใช้บริการและประเภทของการใช้งานที่ใช้การตัดสินใจที่มีผลกำไร สามารถทำแผนเกี่ยวกับการเรียกเก็บเงินและการเปิดตัวบริการใหม่

2.4.3.3 การรักษาความปลอดภัยที่มีคุณภาพของการใช้งาน

ที่คาดการณ์ไว้การยอมรับอย่างกว้างขวางและเจริญเติบโตอย่างรวดเร็วของการให้บริการข้อมูลบนมือถือไม่เพียงแต่เป็นตัวแทนของโอกาสทางธุรกิจที่สำคัญ ผู้ใช้งานส่วนน้อยใช้โปรแกรม peer-to-peer ซึ่งใช้ทรัพยากรเครือข่ายจำนวนมากและมีผลกระทบในการใช้งานกับสมาชิกคนอื่นๆ เพื่อป้องกันไม่ให้ปัญหานี้เกิดขึ้น ยากในการจัดการแบนด์วิดธ์ที่มีอยู่ในวิธีที่ชาญฉลาด คุณสมบัติสำหรับการจัดการแบนด์วิดธ์และการควบคุมคุณภาพในการบริการโซลูชั่นการควบคุมและการเรียกเก็บเงินของอีริคสันทำให้เป็นไปได้ แบนด์วิดธ์ที่จัดสรรเพื่อการใช้งานบางอย่างที่สามารถถูกจำกัดในขณะที่ให้ความสำคัญกับโปรแกรมการโต้ตอบและอ่อนไหวต่อดีเลย์ การแก้ปัญหาจะใช้เพื่อป้องกันทราฟฟิคหรือผู้ใช้ที่เป็นอันตรายที่ละเมิดข้อกำหนดและเงื่อนไขของการสมัครของพวกเขา เพื่อที่จะได้เครือข่ายที่มีประสิทธิภาพและเหมาะสมในการใช้ประโยชน์จากทรัพยากรที่มีอยู่ ขณะที่การรักษาความพึงพอใจของสมาชิก

---

[8] Service Aware Charging and Control, http://archive.ericsson.net/service/internet/picov/get?DocNo=34/28701-FGB101268&Lang=EN&HighestFree=Y

2.4.3.4 บริการที่แตกต่าง

แม้ว่าคุณภาพของประสบการณ์ที่เป็นไปตามความคาดหวัง สมาชิกจะไม่พอใจอย่างมาก จนกว่าพวกเขาจะได้รับสิ่งที่คุ้มค่ากับเงิน

ทุกวันนี้การเรียกเก็บเงินโดยปกติจะขึ้นอยู่กับปริมาณของข้อมูลที่ใช้ แพ็คเก็ตที่มีการตรวจสอบและจำแนกความสามารถในการให้บริการของการบริการ โซลูชั่นการควบคุมและการเรียกเก็บเงินของอีริคสัน เนื้อหา เหตุการณ์และเวลาการใช้งานที่มีประสิทธิภาพนอกจากนี้ยังสามารถนำมาพิจารณาผลในการประเมินแบบไดนามิกอย่างแท้จริง

การแก้ปัญหาจะช่วยให้รูปแบบการกำหนดราคาที่มีมานานแล้วและปัจจุบันปัจจัยสำคัญที่มีผลต่อการเจริญเติบโตในการใช้ทราฟฟิคข้อมูลของมือถือ ตอนนี้ไปได้ที่จะคิดค่าใช้จ่ายสำหรับการบริการในทางที่ทำให้รู้สึกถึงและเป็นที่เข้าใจได้ง่าย โดยส่วนสมาชิกที่แตกต่างกัน นอกจากนี้ยังมีความยืดหยุ่นของการแก้ปัญหาที่ทำให้มันเป็นไปได้ในการตอบสนองอย่างรวดเร็วต่อการเปลี่ยนแปลงในสภาพแวดล้อมการแข่งขัน เป็นโมเดลธุรกิจใหม่รวมทั้งคู่ค้าและผู้ให้บริการอื่นๆ บนอินเทอร์เน็ตที่มียังอำนวยความสะดวกโดยการใช้กลไกในการอนุมัติให้บริการเรียกเก็บเงินตามเวลาจริงและการแบ่งปันรายได้

จากการศึกษาการใช้งานผลงานวิจัยและผลิตภัณฑ์ที่เกี่ยวข้องกับวิทยานิพนธ์ที่นำเสนอสามารถเปรียบเทียบคุณสมบัติได้ดังตารางที่ 2.2

ตารางที่ 2.2 แสดงการเปรียบเทียบคุณสมบัติของผลิตภัณฑ์ที่เกี่ยวข้องกับงานวิจัยที่นำเสนอ

คุณสมบัติ	Bridgwater systems	Telcordia	Ericsson	งานวิจัยที่นำเสนอ
จัดเก็บข้อมูลทราฟฟิค	✓	✓	✓	✓
จำกัดอัตราการรับส่งข้อมูล	✓	✓	✓	✓
การควบคุมแบบเรียวไทม์	✓	✓	✓	✓
ปฏิบัติตามหลักของ 3GPP	✓	✓	✓	×
สามารถตรวจสอบข้อมูลการใช้งาน	✓	✓	N/A	✓
ระบบแจ้งเตือนผ่าน sms, e-mail	✓	✓	×	×
อัพเกรดการใช้งานได้ทันที	×	✓	×	×
ควบคุมการใช้งานจากผู้ปกครอง	×	✓	×	×
การควบคุมด้านดาวน์โหลด	✓	✓	✓	✓

ตารางที่ 2.2 (ต่อ)

คุณสมบัติ	Bridgwater systems	Telcordia	Ericsson	งานวิจัยที่นำเสนอ
การควบคุมด้านอัพโหลด	✓	✓	✓	✗
การประยุกต์ใช้งานกับ WiFi	✗	✗	✗	✓
การรองรับโมบิลลิตี้	✓	✓	✓	✓
รองรับการใช้งานแบบ volumn based	✓	✓	✓	✓

บทที่ 3
ระเบียบวิธีวิจัย

3.1 แนวทางการวิจัยและพัฒนา

งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษา ออกแบบ และพัฒนาระบบการทำ Fair Usage Policy ในระบบเครือข่ายไร้สายประเภท WiFi โดยใช้มาตรฐานของระบบโทรศัพท์เคลื่อนที่ซึ่งกำหนดโดย 3GPP เป็นต้นแบบในการพัฒนา เพื่อให้ผู้ใช้งานได้รับคุณภาพของการบริการได้อย่างเหมาะสม โดยมีแนวทางในการวิจัยและพัฒนาดังนี้

3.1.1 ศึกษาและรวบรวมข้อมูล

3.1.1.1 ศึกษาการทำงานของ GGSN และ PCRF

3.1.1.2 ศึกษาหลักการและคุณสมบัติของ Wireless Router Linksys WRT54GL

3.1.1.3 ศึกษาเพิ่มเติมการใช้งานภาษา Visual Basic, PHP, Apache และ MySQL

3.1.1.4 ศึกษาเพิ่มเติมการใช้งานโปรแกรม Radius Server

3.1.1.5 ศึกษาเพิ่มเติมเกี่ยวกับการทำงานของระบบเครือข่ายไร้สาย

3.1.2 การออกแบบระบบงาน

ออกแบบระบบการทำ Fair Usage Policy ในระบบเครือข่ายไร้สาย ที่ใช้พัฒนาอย่างละเอียด

3.1.3 พัฒนาระบบงาน

ทำการพัฒนาระบบให้สามารถทำงานได้ตามวัตถุประสงค์ที่ตั้งไว้ มีการทดสอบย่อยเพื่อหาข้อผิดพลาดต่างๆ ภายในระบบแล้วทำการแก้ไข

3.1.4 ทดสอบการใช้งาน

มีการทดสอบการใช้งานกับผู้ใช้บริการอินเทอร์เน็ตความเร็วสูง เพื่อดูประสิทธิภาพของทั้งระบบ และการเกิดข้อผิดพลาดในการทำงาน โดยการทดสอบจะทำการจำลองสถานการณ์การใช้งานอินเทอร์เน็ตแล้วถูกจำกัดความเร็วในการใช้งานในระดับต่างๆที่กำหนด

3.1.5 สรุปผลการพัฒนา

นำข้อมูลที่ได้ในการจำลองสถานการณ์มาสรุปผล เพื่อใช้ในการวิเคราะห์การทำงานและประเมินประสิทธิภาพของระบบ

3.2 เครื่องมือที่ใช้

3.2.1 เครื่องคอมพิวเตอร์ส่วนบุคคล CPU แบบ Intel Pentium M 735A ความเร็วสัญญาณนาฬิกา 1.7 GHz ทำหน้าที่เป็นเครื่องแม่ข่าย PCRF

3.2.2 เครื่องคอมพิวเตอร์ส่วนบุคคล CPU แบบ Intel Core i5 ความเร็วสัญญาณนาฬิกา 2.4 GHz ทำหน้าที่เป็นเครื่องแม่ข่าย RADIUS

3.2.3 Wireless Router Linksys WRT54GL ซึ่งทำหน้าที่เป็น PCEF (Policy and Charging Enforcement Function)

3.2.4 ซอฟแวร์โปรแกรม APPSERV เวอร์ชั่น 2.5.4a, Microsoft visual basic 2008, โปรแกรม Radius Server, เฟริมแวร์ DD-WRT.v24 และโปรแกรม RFlow Collector

3.3 แผนการดำเนินงาน

3.3.1 รวบรวมข้อมูลที่เกี่ยวข้องกับระบบ Fair Usage Policy ในระบบ 3GPP และระบบเครือข่ายไร้สาย พร้อมทั้งศึกษา ขอบเขต ข้อจำกัดของระบบ ซึ่งจะทำให้การออกแบบระบบ Fair Usage Policy ในระบบเครือข่ายไร้สายมีความเหมาะสมในการใช้งานมากขึ้น

3.3.2 ศึกษาทฤษฎีและหลักการทำงานของ PCRF เพื่อนำมาประยุกต์ใช้งานกับระบบเครือข่ายไร้สายได้

3.3.3 ศึกษาทฤษฎีและหลักการทำงานของอุปกรณ์เครือข่ายไร้สาย ประเภทและยี่ห้อต่างๆ ว่าอุปกรณ์ใดบ้างที่สามารถทำหน้าที่ได้เสมือนอุปกรณ์ GGSN

3.3.4 ออกแบบระบบ Fair Usage Policy ในระบบเครือข่ายไร้สาย โดยศึกษาเครื่องมือและอุปกรณ์ที่ใช้พัฒนาอย่างละเอียดพร้อมทั้งรวบรวมอุปกรณ์ในการพัฒนาระบบให้พร้อมที่สุด

3.3.5 หลังจากเตรียมความพร้อมมาทั้งหมดแล้วก็ทำการพัฒนาระบบให้สามารถทำงานได้ตามวัตถุประสงค์ที่ตั้งไว้ มีการพัฒนาระบบไประยะหนึ่ง จะเริ่มทำการทดสอบย่อยเพื่อหาข้อผิดพลาดต่างๆ ภายในระบบ แล้วทำการแก้ไข

3.3.6 เมื่อแก้ไขการทำงานต่างๆของระบบเป็นที่เรียบร้อยแล้ว จะนำไปสู่การทดสอบเพื่อดูประสิทธิภาพของทั้งระบบ และการเกิดข้อผิดพลาดในการทำงาน โดยการทดสอบจะทำการจำลองสถานการณ์การใช้งานอินเทอร์เน็ตแล้วถูกจำกัดความเร็วในการใช้งานในระดับต่างๆที่กำหนด

3.3.7 นำข้อมูลที่ได้ในการจำลองสถานการณ์มาสรุปผล เพื่อใช้ในการวิเคราะห์การทำงานและประเมินประสิทธิภาพของระบบ เพื่อใช้เป็นข้อมูลในการจัดทำวิทยานิพนธ์ดังแสดงในตารางที่ 3.1

ตารางที่ 3.1 แผนการดำเนินงาน

งาน \ เดือน	มิ.ย. ก.ค. 54	ส.ค. ก.ย. 54	ต.ค. พ.ย. 54	ธ.ค. 54 ม.ค. 55	ก.พ. มี.ค. 55	เม.ย พ.ค. 55	มิ.ย. ก.ค. 55	ส.ค. ก.ย. 55	ต.ค. พ.ย. 55	ธ.ค. 55 ม.ค. 56
รวบรวมข้อมูลระบบ Fair Usage Policy										
ศึกษาหลักการทำงานของ PCRF										
ศึกษาการหลักการทำงานของอุปกรณ์เครือข่ายไร้สาย										
ออกแบบระบบงานและรวบรวมอุปกรณ์ที่จำเป็นต้องใช้ในระบบ										
พัฒนาระบบ										
ทดสอบการใช้งาน										
สรุปผลการพัฒนา และประโยชน์ที่จะได้รับของระบบ										

3.4 ขั้นตอนและวิธีดำเนินงาน

3.4.1 แนวคิดการทำงานของโปรแกรม

ระบบ Fair Usage Policy ในระบบเครือข่ายคอมพิวเตอร์ไร้สายที่พัฒนาขึ้นในวิทยานิพนธ์ฉบับนี้นำระบบ Fair Usage Policy ในระบบ 3GPP มาเป็นต้นแบบในการพัฒนาเพื่อให้ผู้ใช้งานในเครือข่ายคอมพิวเตอร์ไร้สายสามารถใช้งานปริมาณข้อมูลได้อย่างเท่าเทียมกัน โดยมีขั้นตอนการทำงาน ดังนี้

3.4.1.1 ใช้หลักการของ GGSN ที่ทำหน้าที่เก็บและส่งข้อมูลการใช้งานของผู้ใช้งานอินเทอร์เน็ต

3.4.1.2 ใช้หลักการของ PCRF ทำหน้าที่ตรวจสอบ และกำหนดการใช้งานให้เป็นไปตามเงื่อนไขที่กำหนดไว้

3.4.1.3 ใช้ RADIUS Server ในการยืนยันตัวตนของผู้ใช้งาน เพื่อความปลอดภัยในการเข้าใช้งานอินเทอร์เน็ต

3.4.1.4 ผู้ใช้งานสามารถเข้าตรวจเช็คปริมาณข้อมูลและจำนวนวันที่ได้ใช้งาน โดยผ่านเว็บบราว์เซอร์ที่เชื่อมโยงเข้ากับระบบ

3.4.2 การออกแบบระบบ

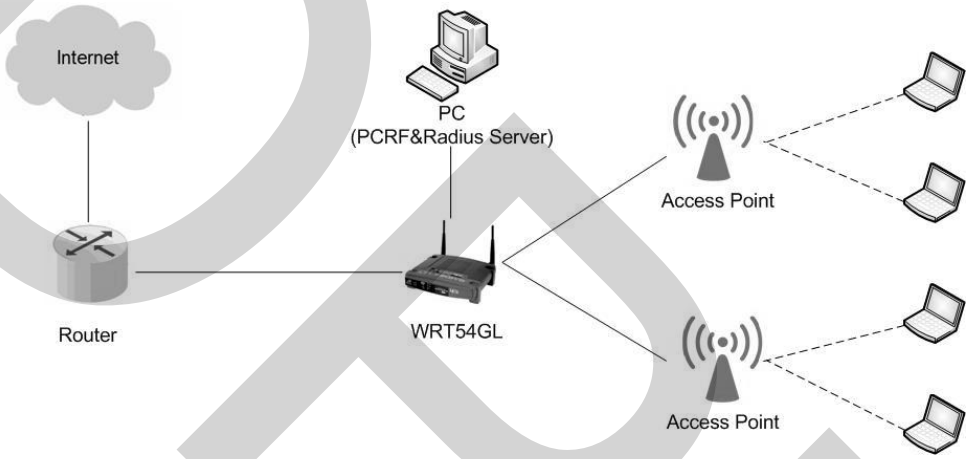
การทำงานของระบบจะนำรูปแบบการทำงานของโครงข่าย 3G (Release7) ดังรูปที่ 1.1 มาประยุกต์กับระบบเครือข่ายคอมพิวเตอร์ไร้สาย (Wireless LAN) โดยโดยนำคอมพิวเตอร์มาจำลองเป็นอุปกรณ์ PCRF และใช้ Wireless Router Linksys WRT54GL แทน GGSN ดังรูปที่ 3.1

ตารางที่ 3.2 ตารางเปรียบเทียบอุปกรณ์ระหว่าง โครงข่าย 3G กับระบบเครือข่ายคอมพิวเตอร์ไร้สาย

โครงข่าย 3G	ระบบเครือข่ายคอมพิวเตอร์ไร้สาย
GGSN	Router Linksys WRT54GL
PCRF	คอมพิวเตอร์แม่ข่าย
AAA Server	RADIUS Server
Node-B	Access Point

จากตารางที่ 3.2 Wireless Router Linksys WRT54GL ทำหน้าที่เปรียบได้กับ GGSN โดยผู้วิจัยได้ติดตั้ง Firmware DD-WRT v23 SP2 [6] เพื่อให้มีความสามารถในการจำกัดแบนด์วิดท์ของแต่ละผู้ใช้งานได้ โดยจะจำกัดแบนด์วิดท์โดยอ้างอิงจาก MAC Address ของแต่ละผู้ใช้งานและ

สามารถส่งปริมาณของทราฟฟิกการใช้งาน [7] ของผู้ใช้งานไปยังคอมพิวเตอร์ โดยคอมพิวเตอร์ทำหน้าที่เหมือนกับอุปกรณ์ PCRF โดยจะมีลักษณะการทำงานคือ นำทราฟฟิกที่ได้รับมาของแต่ละผู้ใช้งานมาคำนวณว่าปริมาณทราฟฟิกที่มีการใช้งาน ครบตามเงื่อนไขของแต่ละผู้ใช้งานได้รับแล้วหรือไม่ โดยข้อมูลของผู้ใช้งานนั้น จะถูกระบุในฐานข้อมูลไว้อยู่แล้ว และมีหน้าที่ส่ง IP Address ของผู้ใช้งานที่ใช้งานครบที่กำหนดไว้ไปยัง Wireless Router Linksys WRT54GL เพื่อทำการจำกัดแบนด์วิดท์ตามเงื่อนไขที่กำหนด



รูปที่ 3.1 ภาพรวมการทำงานของระบบ

3.4.1.1 กระบวนการทำงานจะทำการโต้ตอบโดยการส่งข้อมูลหากันระหว่างคอมพิวเตอร์แม่ข่าย (PCRF) และอุปกรณ์ WRT54GL โดย หลักการทำงานของระบบจะแบ่งหน้าที่ออกเป็น 2 ส่วนดังนี้

1) WRT54GL

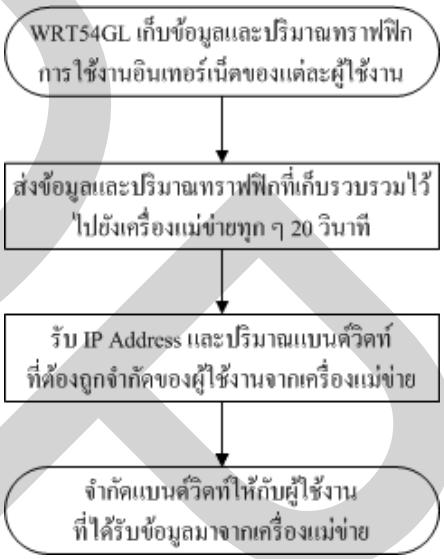
จากรูปที่ 3.2 หลักการทำงานของระบบ WRT54GL สามารถอธิบายได้ดังนี้

1.1) อุปกรณ์ WRT54GL นั้นจะเก็บข้อมูลของผู้ใช้งานซึ่งประกอบด้วย IP Address, MAC Address และปริมาณทราฟฟิกการใช้งานอินเทอร์เน็ตล่าสุดของแต่ละผู้ใช้งาน

1.2) อุปกรณ์ WRT54GL จะทำการส่งข้อมูลทั้งหมดที่เก็บไว้ได้ไปยังเครื่องคอมพิวเตอร์แม่ข่ายทุกๆ 20 วินาที ซึ่งเป็นค่าที่ถูกกำหนดแบบตายตัวในซอฟแวร์ rflow collector เพื่อลดการใช้ทรัพยากรของตัวอุปกรณ์ที่มีอยู่อย่างจำกัด

1.3) หลังจากที่ส่งข้อมูลไปยังเครื่องแม่ข่ายแล้ว WRT54GL จะรอรับข้อมูลจากเครื่องคอมพิวเตอร์แม่ข่ายโดยข้อมูลที่ได้รับมาจะประกอบด้วย IP Address และปริมาณแบนด์วิดท์ที่จะต้องจำกัดให้กับผู้ใช้งาน

1.4) WRT54GL จะจำกัดแบนด์วิดท์ให้กับผู้ใช้งาน ตามที่ได้รับข้อมูลมาจากเครื่องคอมพิวเตอร์แม่ข่าย



รูปที่ 3.2 หลักการทำงานของระบบ WRT54GL

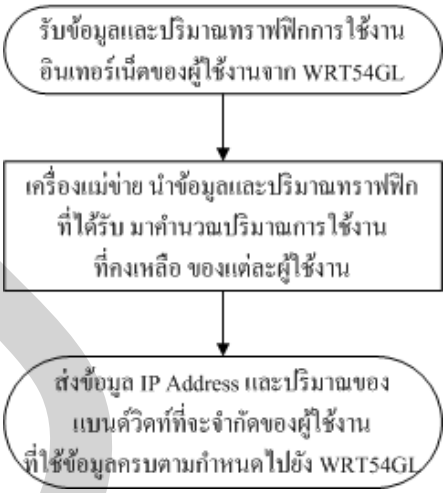
2) เครื่องแม่ข่าย PCRF

จากรูปที่ 3.3 หลักการทำงานของเครื่องแม่ข่าย PCRF สามารถอธิบายได้ดังนี้

2.1) คอมพิวเตอร์แม่ข่ายจะรับข้อมูลและปริมาณทราฟฟิกของแต่ละผู้ใช้งานจาก WRT54GL โดยอ้างอิงผู้ใช้งานจาก IP Address ของแต่ละเครื่อง

2.2) เมื่อคอมพิวเตอร์แม่ข่ายเก็บบัญทึกข้อมูลของแต่ละผู้ใช้งานตาม IP Address ลงฐานข้อมูล แล้วตรวจสอบปริมาณการใช้งานที่คงเหลือ โดยนำปริมาณ ทราฟฟิกที่ได้รับจาก WRT54GL มาหักล้างออกจากประมาณข้อมูลของผู้ใช้งานที่ได้รับ (เพื่อที่สามารถนำไปประยุกต์ใช้ได้ทั้งกับระบบ Postpaid และPrepaid)

2.3) เมื่อคอมพิวเตอร์แม่ข่าย ตรวจพบว่าปริมาณการใช้ข้อมูลของผู้ใช้งานครบตามที่ผู้ใช้งานได้รับแล้วคอมพิวเตอร์แม่ข่าย จะส่ง IP Address และปริมาณแบนด์วิดท์ที่ต้องจำกัด ส่งไปยัง WRT54GL เพื่อให้จำกัดแบนด์วิดท์ให้กับผู้ใช้งานต่อไป



รูปที่ 3.3 หลักการทำงานของเครื่องแม่ข่าย PCRF

3.4.1.2 ขั้นตอนการออกแบบการทำงาน ในการใช้งานอินเทอร์เน็ตในระบบเครือข่ายคอมพิวเตอร์ไร้สาย

1) โดยขั้นตอนการทำงานในการใช้งานอินเทอร์เน็ตในระบบเครือข่ายคอมพิวเตอร์ไร้สายเมื่อใช้ปริมาณข้อมูลมากกว่ากำหนด ดังรูปที่ 3.4

โดยขั้นตอนในการใช้งานอินเทอร์เน็ตในระบบเครือข่ายไร้สายจะขออธิบายตามขั้นตอนการออกแบบดังต่อไปนี้คือ

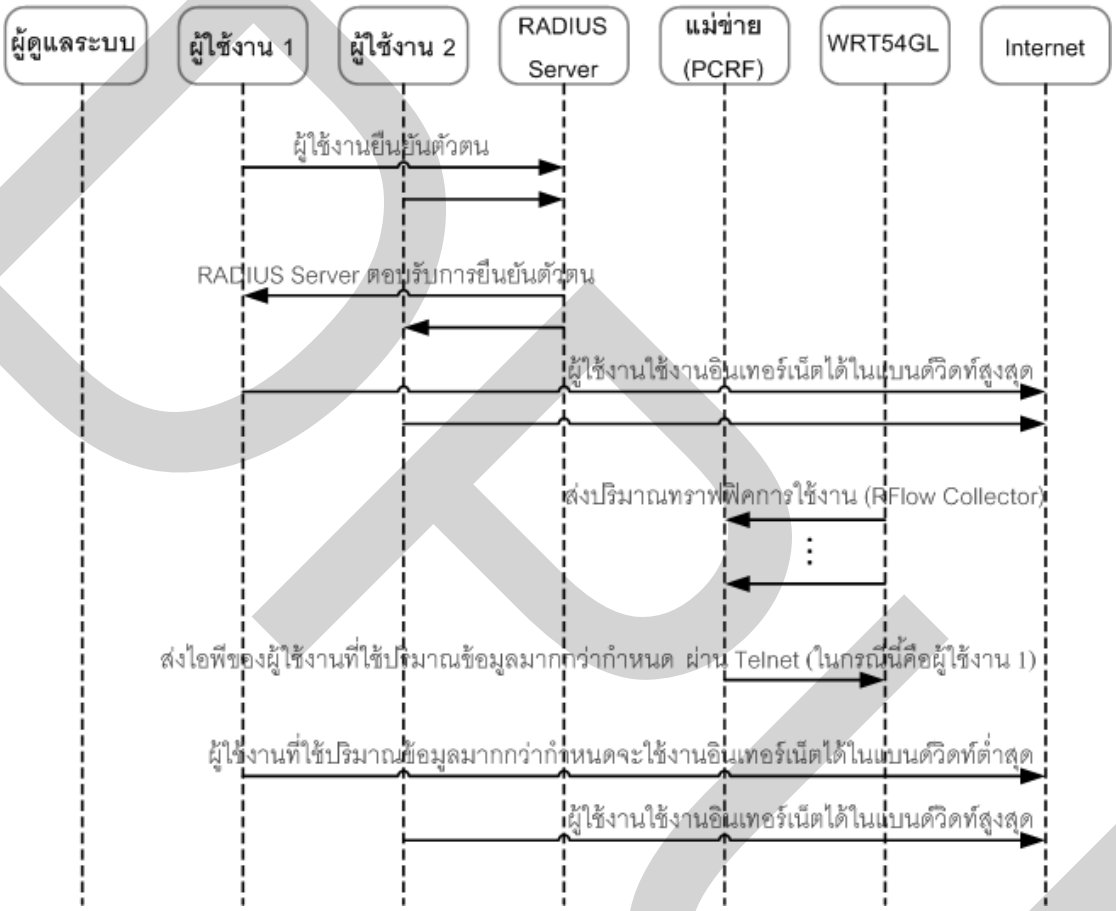
1.1) ขั้นตอนแรกเมื่อผู้ใช้งานทำการใช้งานอินเทอร์เน็ต ในครั้งแรกจะต้องทำการยืนยันตัวตนในการใช้งานกับ RADIUS Server ว่ามีสิทธิ์ในการใช้งานหรือไม่ โดย RADIUS Server จะมีการตอบกลับผ่านหน้าเว็บเพจว่ายืนยันตัวสำเร็จ

1.2) เมื่อยืนยันตัวตนสำเร็จผู้ใช้งานจะสามารถใช้งานอินเทอร์เน็ตได้ในระดับแบนด์วิดท์ที่สูงสุดที่ระบบสามารถรองรับได้หรือตามแพ็คเกจที่ใช้

1.3) ระหว่างการใช้อินเทอร์เน็ตของผู้ใช้งาน อุปกรณ์ WRT54GL จะทำการส่งปริมาณทราฟฟิกการใช้งานอินเทอร์เน็ตของแต่ละผู้ใช้งานที่เก็บไว้ได้ส่งไปยังเครื่องคอมพิวเตอร์แม่ข่ายทุก ๆ 20 วินาที

1.4) เครื่องคอมพิวเตอร์แม่ข่ายจะทำการตรวจสอบปริมาณการใช้งานของผู้ใช้จากปริมาณทราฟฟิกที่ได้รับ เมื่อพบว่าผู้ใช้งานใดมีการใช้ข้อมูลเกินกว่าที่ได้รับ จะทำการส่งไอพีแอดเดรสและปริมาณแบนด์วิดท์ที่ต้องจำกัด ส่งไปยัง WRT54GL เพื่อให้จำกัดแบนด์วิดท์ให้กับผู้ใช้งานนั้นๆ

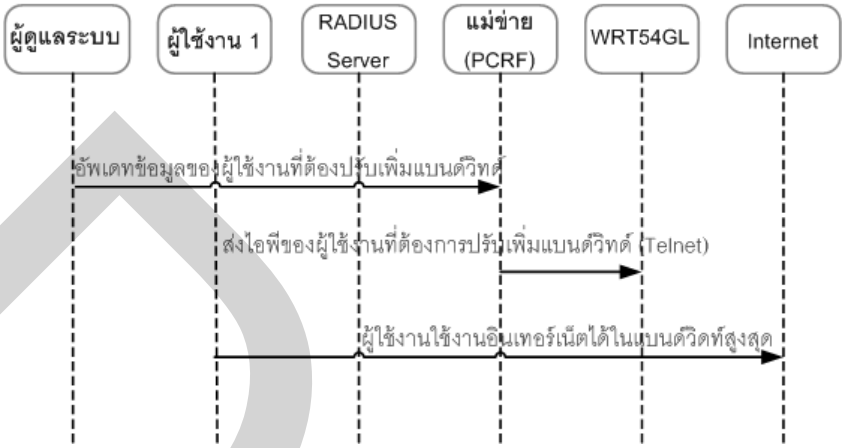
1.5) อุปกรณ์ WRT54GL จะทำการกำหนดแบนด์วิดท์ให้กับผู้ใช้งานนั้นๆ ตามที่เครื่องคอมพิวเตอร์แม่ข่ายส่งมา ส่งผลให้ผู้ใช้งานนั้นๆ ใช้งานอินเทอร์เน็ตด้วยแบนด์วิดท์ที่ถูกกำหนด แต่ผู้ใช้งานอื่นจะใช้งานอินเทอร์เน็ตได้ในระดับแบนด์วิดท์ที่สูงสุดได้ตามปกติ



รูปที่ 3.4 หลักการการใช้งานอินเทอร์เน็ตในระบบเครือข่ายคอมพิวเตอร์ไร้สาย

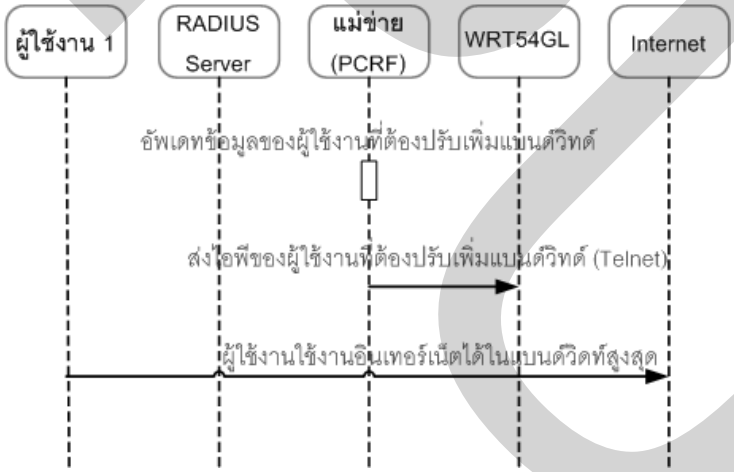
2) ขั้นตอนการทำงาน เมื่อมีการอัพเดทข้อมูลการใช้งานของผู้ใช้งาน (แบบเติมเงิน)

จากรูปที่ 3.5 ผู้ดูแลระบบจะสามารถอัพเดทข้อมูลของผู้ใช้งานเมื่อผู้ใช้งานมีความต้องการที่จะใช้ปริมาณแบนด์วิทด์ที่สูงเท่าเดิม โดยจะทำการแก้ไขที่เครื่องคอมพิวเตอร์แม่ข่ายโดยผ่านหน้าเว็บเพจ หลังจากนั้นเครื่องคอมพิวเตอร์แม่ข่ายจะการส่งไอพีแอดเดรสของผู้ใช้งานนั้นๆ ไปยังเราเตอร์ WRT54GL ทำให้ผู้ใช้งานนั้นๆ สามารถที่จะได้รับแบนด์วิทด์สูงสุดที่กำหนดไว้เช่นเดิม



รูปที่ 3.5 หลักการทำงานเมื่อมีการอัพเดทข้อมูลการใช้งานของผู้ใช้งาน (แบบเติมเงิน)

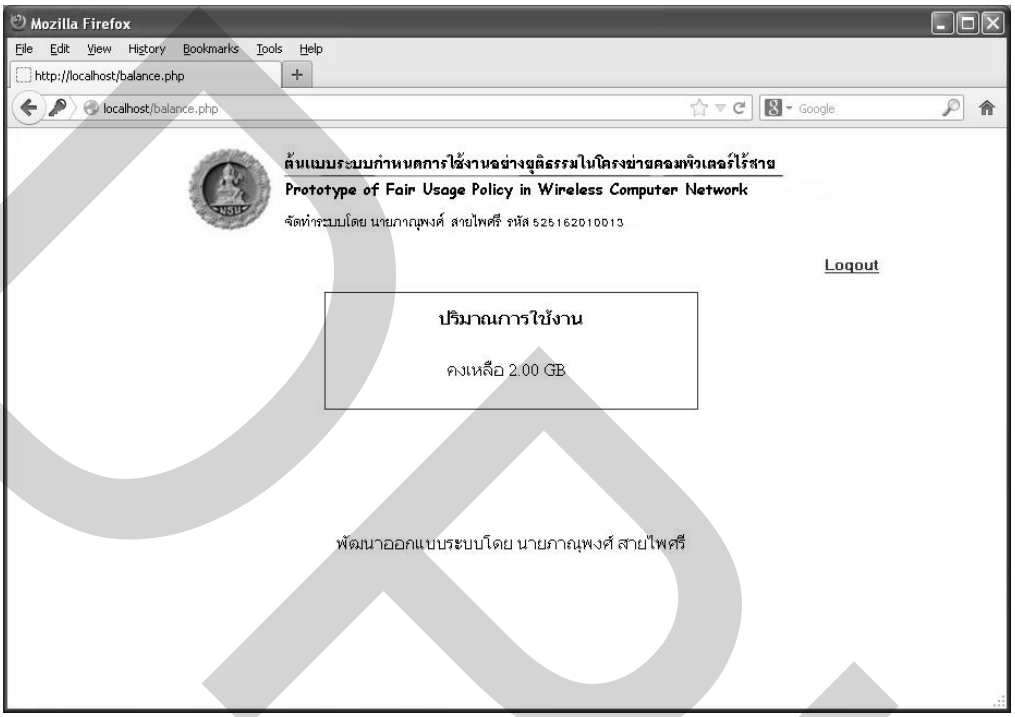
3) ขั้นตอนการทำงาน เมื่อผู้ใช้งานครบรอบการใช้งานที่กำหนดในระบบ (แบบรายเดือน)



รูปที่ 3.6 หลักการทำงานเมื่อมีการอัพเดทข้อมูลการใช้งานของผู้ใช้งาน (แบบรายเดือน)

เมื่อผู้ใช้งานถึงวันครบกำหนดการใช้งานในระบบ (แบบรายเดือน) ยกตัวอย่างเช่น 24.00 น. ของวันสิ้นเดือน เครื่องแม่ข่ายจะปรับแบนด์วิทด์ให้กับผู้ใช้งานและส่งไอพีแอดเดรสของผู้ใช้งานนั้นๆ ไปยังเราเตอร์ WRT54GL ทำให้ผู้ใช้งานนั้นๆ สามารถที่จะได้รับแบนด์วิทด์สูงสุดที่กำหนดไว้เช่นเดิมได้แบบอัตโนมัติ ดังรูปที่ 3.6

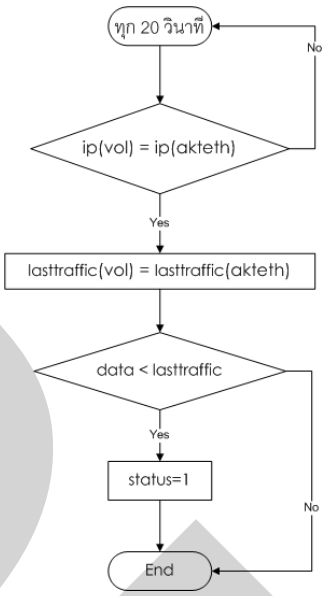
3.2.1.3 ผู้ใช้งานสามารถเข้าตรวจเช็คปริมาณข้อมูลและเวลาที่ได้ใช้งานคงเหลือ โดยผ่านเว็บบราว์เซอร์ที่เชื่อมโยงเข้ากับระบบของเครื่องคอมพิวเตอร์แม่ข่าย



รูปที่ 3.7 หน้าเว็บเพจในการเช็คปริมาณการใช้งานคงเหลือ

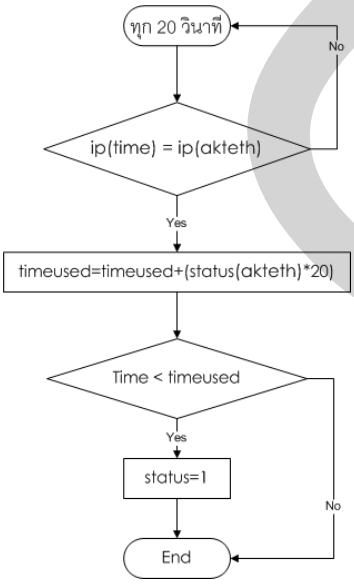
3.2.1.4 ขั้นตอนการออกแบบการทำงานภายในของระบบคอมพิวเตอร์แม่ข่ายเมื่อรับปริมาณทราฟฟิกมา เราเตอร์ WRT54GL สามารถแบ่งออกได้ดังต่อไปนี้

1) ในส่วนของผู้ใช้งานในแบบประเภทปริมาณการใช้งาน ทุกๆ 20 วินาที จะอัพเดตทราฟฟิกการใช้งานจากเทเบิล akteth ไปยังเทเบิลที่เก็บข้อมูลผู้ใช้งานไว้ หลังจากนั้นจะทำการตรวจเช็คว่าปริมาณข้อมูลที่ใช้ไปเกินกว่าปริมาณที่ได้รับหรือไม่ ถ้าใช้ปริมาณข้อมูลมากกว่าที่ได้รับ ระบบจะทำการอัพเดทสถานะเป็น 1 เพื่อบ่งบอกว่าผู้ใช้งานนั้นๆ ใช้งานอินเทอร์เน็ตในปริมาณที่มากกว่ากำหนด ดังรูปที่ 3.8



รูปที่ 3.8 ขั้นตอนการทำงานของระบบในส่วนของการใช้งานแบบปริมาณข้อมูล

2) ในส่วนของผู้ใช้งานในแบบเวลาการใช้งาน ทุกๆ 20 วินาที จะทำการอัพเดทสถานะการใช้งาน ถ้ามีการใช้งานเวลาการใช้งานก็จะถูกบวกเพิ่ม 20 วินาที และเมื่อมีการใช้เวลามากกว่าที่ได้รับ ระบบจะทำการอัพเดทสถานะเป็น 1 เพื่อบ่งบอกว่าผู้ใช้งานนั้นๆ ใช้งานอินเทอร์เน็ตในเวลาที่มากกว่ากำหนด ดังรูปที่ 3.9



รูปที่ 3.9 ขั้นตอนการทำงานของระบบในส่วนของการใช้งานแบบเวลา

3) ในส่วนของเมื่อผู้ใช้งาน ใช้งานเกินกว่าปริมาณที่ได้รับทั้งแบบปริมาณข้อมูล หรือแบบเวลา เครื่องแม่ข่ายจะส่งสคริปท์ไปยังเราเตอร์ WRT54GL เพื่อแจ้งให้กับทราบว่าผู้ใช้งานใดบ้างต้องถูกลดแบนด์วิดท์ลงโดยภายในสคริปท์จะประกอบไปด้วยไอพี แอดเดรส และปริมาณแบนด์วิดท์ของแต่ละผู้ใช้งาน ซึ่งการส่งสคริปท์ดังกล่าวสามารถปรับค่าในการส่งออกไปตั้งแต่ 30 วินาทีเป็นต้นไป เนื่องจากโปรแกรมที่ใช้ในการสร้างสคริปท์และส่งสคริปท์นั้นต้องใช้เวลาในการทำงาน แต่ในงานวิทยานิพนธ์นี้ ได้กำหนดค่าถูกส่งออกไปทุกๆ 30 วินาที เหตุเพราะเป็นช่วงเวลาที่เหมาะสมในการใช้งานและไม่เป็นการสร้างปัญหาด้านทราฟฟิกและการใช้ทรัพยากรที่มากจนเกินไป โดยตัวอย่างสคริปท์ในการ Telnet ไปยังเราเตอร์เพื่อลดแบนด์วิทด์จะแสดงดังต่อไปนี้

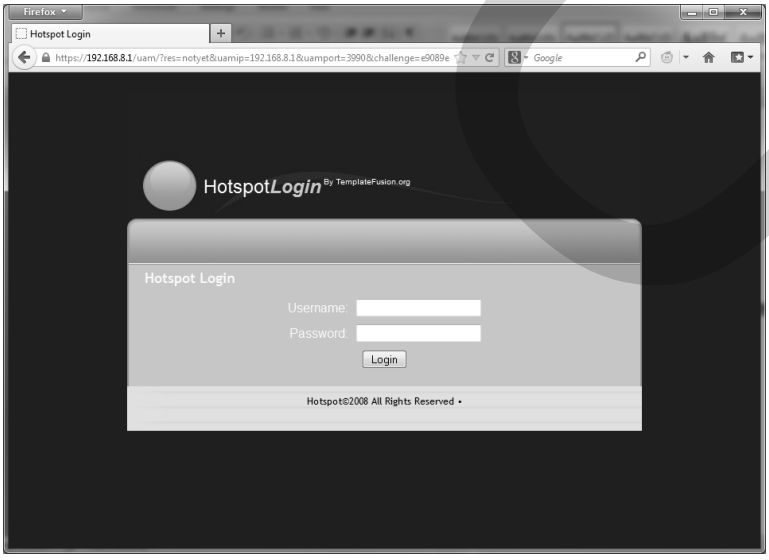
```
TCA="tc class add dev br0"
TFA="tc filter add dev br0"
TQA="tc qdisc add dev br0"
SFQ="sfq perturb 10"
tc qdisc del dev br0 root
tc qdisc add dev br0 root handle 1: htb
// ตั้งค่าอัตราการรับข้อมูลสูงสุดที่ระบบรองรับ
tc class add dev br0 parent 1: classid 1:1 htb rate 10240kbit
// ตั้งค่าอัตราการรับข้อมูลโดยอ้างอิงจากไอดี โดยค่าจะเริ่มที่ 10
$TCA parent 1:1 classid 1:10 htb rate 2048kbit ceil 2048kbit prio 2
$TCA parent 1:1 classid 1:11 htb rate 1024kbit ceil 1024kbit prio 2
$TQA parent 1:10 handle 10: $SFQ
$TQA parent 1:11 handle 11: $SFQ
// ตั้งค่าความสำคัญโดยค่าปกติมีค่าเท่ากับ 2
$TFA parent 1:0 prio 2 protocol ip handle 10 fw flowid 1:10
$TFA parent 1:0 prio 2 protocol ip handle 11 fw flowid 1:11
// กำหนดค่าไอพี แอดเดรส ว่ามีค่าไอดีเท่ากับเท่าไร
iptables -t mangle -A POSTROUTING -d 192.168.8.32 -j MARK --set-mark 10
iptables -t mangle -A POSTROUTING -d 192.168.8.31 -j MARK --set-mark 11
```

บทที่ 4
การทดสอบระบบ

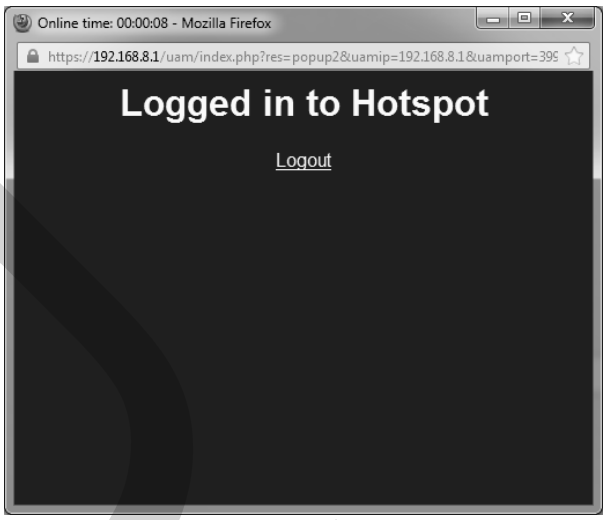
ในการทดสอบในต้นแบบระบบกำหนดการใช้งานอย่างยุติธรรมในโครงข่ายคอมพิวเตอร์ไร้สายได้ทดสอบโดยเริ่มตั้งแต่การเข้าใช้งานอินเทอร์เน็ตโดยผ่านการยืนยันตัวตันผ่าน RADIUS Server ตลอดจนการใช้อินเทอร์เน็ตของแต่ละประเภทการใช้งานทั้งระบบ Postpaid และ Prepaid โดยจะทำการทดสอบว่าเมื่อมีการใช้งานอินเทอร์เน็ตเกินว่าที่ได้รับจะทำงานลดแบนด์วิทด์ลงตามเพ็คเกจที่ได้รับหรือไม่ และเมื่อครบวันที่กำหนดของการใช้งาน ผู้ใช้งานสามารถใช้แบนด์วิทด์ที่สูงสุดเท่าเดิมหรือไม่ ซึ่งทางผู้วิจัยได้แบ่งการทดสอบออกเป็น 8 หัวข้อ ดังต่อไปนี้

1) การทดสอบการยืนยันตัวขอผู้ใช้งานผ่าน RADIUS Server เมื่อใช้งานอินเทอร์เน็ต

การทดสอบนี้จะเป็นการยืนยันตัวตนของผู้ใช้งานโดยเมื่อผู้ใช้งานเปิดเว็บบราว์เซอร์เพื่อทำการเข้าใช้งานอินเทอร์เน็ต ระบบจะทำการเปิดหน้าเว็บเพจที่ไว้ทำการยืนยันตัวตนโดยอัตโนมัติดังรูปที่ 4.1 โดยจะต้องกรอกยูสเซอร์เนม และพาสเวิร์ดเพื่อทำการยืนยันตัวตนถ้ากรอก ถ้ากรอกข้อมูลไม่ถูกต้องจะแสดงหน้าเพื่อกรอกยูสเซอร์เนม และพาสเวิร์ดใหม่อีกครั้ง ถ้ากรอกยูสเซอร์เนม และพาสเวิร์ดถูกต้องก็จะมีหน้าเว็บเพจแสดงว่ากรอกยูสเซอร์เนม และพาสเวิร์ดของผู้ใช้งานถูกต้องดังรูปที่ 4.2



รูปที่ 4.1 หน้าเว็บเพจในการกรอกข้อมูลเพื่อยืนยันตัวตน



รูปที่ 4.2 หน้าเว็บเพจเมื่อมีการยืนยันตัวตนถูกต้อง

การทดสอบการยืนยันตัวขอผู้ใช้งานผ่าน RADIUS Server ได้ทำการกรอกข้อมูลผู้ใช้งานถูกต้องจำนวน 30 ครั้ง และไม่ถูกต้องจำนวน 30 ครั้ง ได้ผลแสดงในตารางที่ 4.1

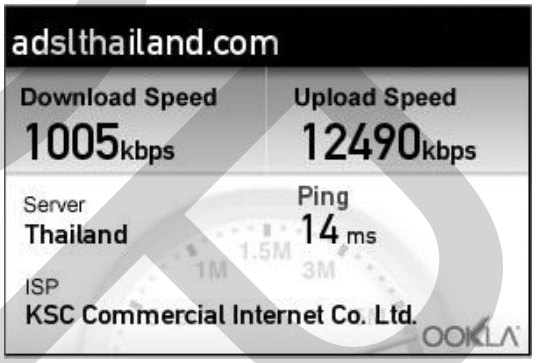
ตารางที่ 4.1 ตารางผลการยืนยันตัวตนผ่าน RADIUS Server

รายการ	ยืนยันตัวตนสำเร็จ (ครั้ง)	ยืนยันตัวตนไม่สำเร็จ (ครั้ง)	ความถูกต้องคิดเป็น %
กรอกข้อมูลถูกต้อง	30	0	100 %
กรอกข้อมูลไม่ถูกต้อง	0	30	100 %

2) การทดสอบการใช้งานอินเทอร์เน็ตเมื่อใช้งานเกินกว่าปริมาณที่กำหนดในระบบจ่ายก่อนใช้ (Prepaid) แบบปริมาณข้อมูล

การทดสอบนี้จะเป็นการใช้งานอินเทอร์เน็ตเมื่อใช้งานปริมาณข้อมูลเกินกว่าปริมาณข้อมูลที่ผู้ใช้ได้รับ โดยจะทำการทดสอบอัตรารับส่งข้อมูลขณะใช้งานปกติดังรูปที่ 4.3 และจะทำการทดสอบอัตรารับส่งข้อมูลอีกครั้งเมื่อผู้ใช้งานใช้ปริมาณข้อมูลเกินกว่าปริมาณข้อมูลที่ได้รับดังรูปที่ 4.4

รูปที่ 4.3 ตัวอย่างการทดสอบอัตรารับส่งข้อมูลขณะใช้งานปกติ



รูปที่ 4.4 ตัวอย่างอัตราความเร็วเมื่อถูกจำกัดของแพ็กเกจโกลด์

การทดสอบการใช้งานอินเทอร์เน็ตเมื่อใช้งานปริมาณข้อมูลเกินกว่าปริมาณข้อมูลที่ผู้ใช้ได้รับ ได้ทำการทดสอบจำนวน 30 ครั้ง โดยจำกัดอัตราการรับข้อมูลเป็นแพ็กเก็จ แพลทินัม โกลด์ และซิลเวอร์คือ 2048, 1024 และ 512 kbps ตามลำดับ แบ่งเป็นแพ็กเก็จละ 10 ครั้ง ได้ผลแสดงในตารางที่ 4.2

ตารางที่ 4.2 ตารางผลทดสอบระบบจ่ายก่อนใช้ (Prepaid) แบบปริมาณข้อมูล

รายการ	จำกัดอัตราการรับข้อมูล		ความถูกต้องคิดเป็น %
	สำเร็จ (ครั้ง)	ไม่สำเร็จ (ครั้ง)	
แพลตินัม	10	0	100 %
โกลด์	10	0	100 %
ซิลเวอร์	10	0	100 %

3) การทดสอบการใช้งานอินเทอร์เน็ตเมื่อใช้งานเกินกว่าปริมาณที่กำหนดในระบบจ่ายก่อนใช้ (Prepaid) แบบปริมาณเวลา

การทดสอบนี้จะเป็นการใช้งานอินเทอร์เน็ตเมื่อใช้งานปริมาณเวลาเกินกว่าปริมาณเวลาที่ผู้ใช้ได้รับ โดยจะทำการทดสอบอัตรารับส่งข้อมูลขณะใช้งานปกติ และจะทำการทดสอบอัตรารับส่งข้อมูลอีกครั้งเมื่อผู้ใช้งานใช้ปริมาณเวลาเกินกว่าปริมาณเวลาที่ได้รับ

การทดสอบการใช้งานอินเทอร์เน็ตเมื่อใช้งานปริมาณเวลาเกินกว่าปริมาณเวลาที่ผู้ใช้ได้รับ ได้ทำการทดสอบจำนวน 30 ครั้ง โดยจำกัดอัตราการรับข้อมูลเป็นแพ็กเก็จ แพลทินัม โกลด์ และซิลเวอร์คือ 2048, 1024 และ 512 kbps ตามลำดับ แบ่งเป็นแพ็กเก็จละ 10 ครั้ง ได้ผลแสดงในตารางที่ 4.3

ตารางที่ 4.3 ตารางผลทดสอบระบบจ่ายก่อนใช้ (Prepaid) แบบปริมาณเวลา

รายการ	จำกัดอัตราการรับข้อมูล		ความถูกต้องคิดเป็น %
	สำเร็จ (ครั้ง)	ไม่สำเร็จ (ครั้ง)	
แพลตินัม	10	0	100 %
โกลด์	10	0	100 %
ซิลเวอร์	10	0	100 %

4) การทดสอบการใช้งานอินเทอร์เน็ตเมื่อใช้งานเกินกว่าปริมาณที่กำหนดในระบบใช้ก่อนจ่ายที่หลัง (Postpaid) แบบปริมาณข้อมูล

การทดสอบนี้จะเป็นการใช้งานอินเทอร์เน็ตเมื่อใช้งานปริมาณข้อมูลเกินกว่าปริมาณข้อมูลที่ผู้ใช้ได้รับ โดยจะทำการทดสอบอัตรารับส่งข้อมูลขณะใช้งานปกติ และจะทำการทดสอบอัตรารับส่งข้อมูลอีกครั้งเมื่อผู้ใช้งานใช้ปริมาณข้อมูลเกินกว่าปริมาณข้อมูลที่ได้รับ

การทดสอบการใช้งานอินเทอร์เน็ตเมื่อใช้งานปริมาณข้อมูลเกินกว่าปริมาณข้อมูลที่ผู้ใช้ได้รับ ได้ทำการทดสอบจำนวน 30 ครั้ง โดยจำกัดอัตราการรับข้อมูลเป็นแพ็กเก็จ แพลทินัม โกลด์ และซิลเวอร์คือ 2048, 1024 และ 512 kbps ตามลำดับ แบ่งเป็นแพ็กเก็จละ 10 ครั้ง ได้ผลแสดงในตารางที่ 4.4

ตารางที่ 4.4 ตารางผลทดสอบระบบใช้ก่อนจ่ายที่หลัง (Postpaid) แบบปริมาณข้อมูล

รายการ	จำกัดอัตราการรับข้อมูล		ความถูกต้องคิดเป็น %
	สำเร็จ (ครั้ง)	ไม่สำเร็จ (ครั้ง)	
แพลตินัม	10	0	100 %
โกลด์	10	0	100 %
ซิลเวอร์	10	0	100 %

5) การทดสอบการใช้งานอินเทอร์เน็ตเมื่อใช้งานเกินกว่าปริมาณที่กำหนดในระบบใช้ก่อนจ่ายที่หลัง (Postpaid) แบบปริมาณเวลา

การทดสอบนี้จะเป็นการใช้งานอินเทอร์เน็ตเมื่อใช้งานปริมาณเวลาเกินกว่าปริมาณเวลาที่ผู้ใช้ได้รับ โดยจะทำการทดสอบอัตรารับส่งข้อมูลขณะใช้งานปกติ และจะทำการทดสอบอัตรารับส่งข้อมูลอีกครั้งเมื่อผู้ใช้งานใช้ปริมาณเวลาเกินกว่าปริมาณเวลาที่ได้รับ

การทดสอบการใช้งานอินเทอร์เน็ตเมื่อใช้งานปริมาณเวลาเกินกว่าปริมาณเวลาที่ผู้ใช้ได้รับ ได้ทำการทดสอบจำนวน 30 ครั้ง โดยจำกัดอัตราการรับข้อมูลเป็นแพ็กเก็จ แพลทินัม โกลด์ และซิลเวอร์คือ 2048, 1024 และ 512 kbps ตามลำดับ แบ่งเป็นแพ็กเก็จละ 10 ครั้ง ได้ผลแสดงในตารางที่ 4.5

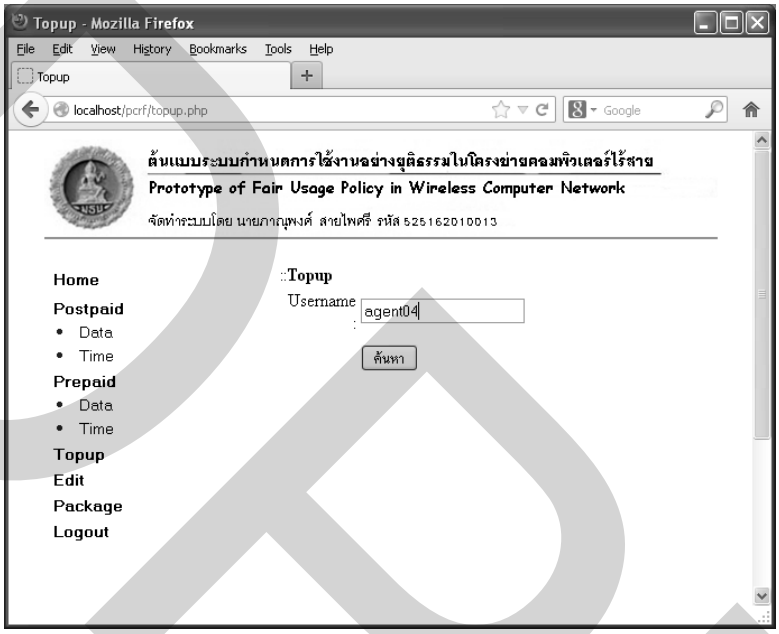
ตารางที่ 4.5 ตารางผลทดสอบระบบใช้ก่อนจ่ายที่หลัง (Postpaid) แบบปริมาณเวลา

รายการ	จำกัดอัตราการรับข้อมูล		ความถูกต้องคิดเป็น %
	สำเร็จ (ครั้ง)	ไม่สำเร็จ (ครั้ง)	
แพลตินัม	10	0	100 %
โกลด์	10	0	100 %
ซิลเวอร์	10	0	100 %

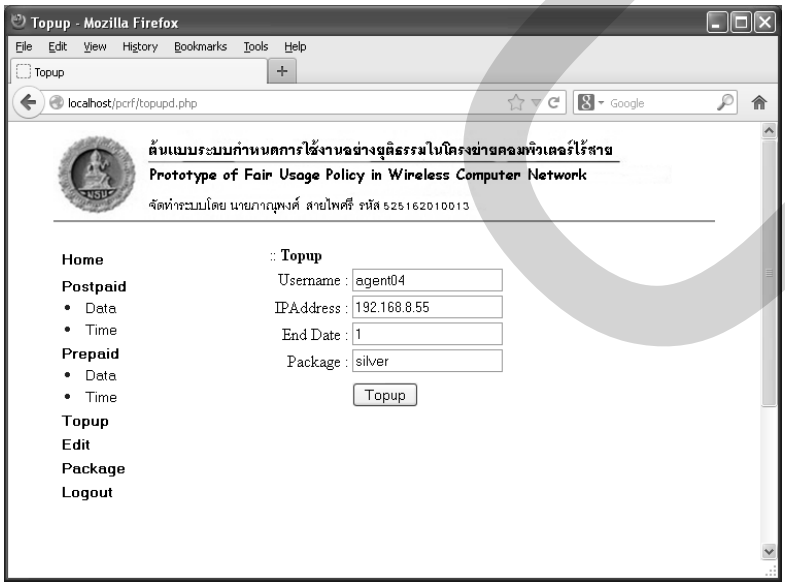
6) การทดสอบการปรับแบนด์วิดท์ให้กลับมาใช้ในอัตราสูงสุดของระบบจ่ายก่อนใช้ (Prepaid)

การทดสอบนี้จะเป็นปรับแบนด์วิดท์ให้กลับมาใช้ในอัตราสูงสุดเมื่อครบรอบของวันการใช้งาน ซึ่งผู้ดูแลระบบจะทำการกรอกยูสเซอร์เนมของผู้ใช้งานโดยผ่านหน้าเว็บเพจดังรูปที่ 4.5

เพื่อทำการตรวจสอบข้อมูลดังรูปที่ 4.6 หลังจากนั้นจะทำการปรับแบนด์วิดท์ให้กับผู้ใช้งาน หลังจากนั้นจะทำการทดสอบอัตรารับส่งข้อมูลเพื่อเป็นการยืนยันว่าผู้ใช้งานนั้นๆ สามารถใช้อินเทอร์เน็ตได้ในระดับแบนด์วิดท์ที่อัตราสูงสุดได้อีกครั้ง



รูปที่ 4.5 หน้าเว็บเพจในการกรอกยูสเซอร์เนมของผู้ใช้งาน



รูปที่ 4.6 หน้าเว็บเพจในการตรวจสอบข้อมูลผู้ใช้งาน

การปรับแบนด์วิดท์ให้กลับมาใช้ในอัตราสูงสุดจะทำการทำสอบแบบปริมาณข้อมูล จำนวน 30 ครั้ง และปริมาณเวลา 30 ครั้ง ซึ่งได้ผลแสดงในตารางที่ 4.6

ตารางที่ 4.6 ตารางผลทดสอบการปรับแบนด์วิดท์ของระบบจ่ายก่อนใช้ (Prepaid) ทั้งแบบปริมาณข้อมูลและเวลา

รายการ	สำเร็จ (ครั้ง)	ไม่สำเร็จ (ครั้ง)	ความถูกต้องคิดเป็น %
ปริมาณข้อมูล	30	0	100 %
ปริมาณเวลา	30	0	100 %

7) การทดสอบการปรับแบนด์วิดท์ให้กลับมาใช้ในอัตราสูงสุดของระบบใช้ก่อนจ่ายที่หลัง (Postpaid)

การทดสอบนี้จะเป็นปรับแบนด์วิดท์ให้กลับมาใช้ในอัตราสูงสุดเมื่อครบรอบของวันการใช้งาน ซึ่งการทดสอบจะทำการรันโปรแกรมที่เครื่องแม่ข่ายเพื่อตรวจสอบวันที่ครบกำหนดการใช้งานว่าตรงกันวันที่ปัจจุบันหรือไม่ ซึ่งถ้าข้อมูลตรงกันจะทำการปรับแบนด์วิดท์ให้กับผู้ใช้งานนั้นๆ และหลังจากนั้นจะทำการทดสอบอัตรารับส่งข้อมูลเพื่อเป็นการยืนยันว่าผู้ใช้งานนั้นๆ สามารถใช้อินเทอร์เน็ตได้ในระดับแบนด์วิดท์ที่อัตราสูงสุดได้อีกครั้ง

การปรับแบนด์วิดท์ให้กลับมาใช้ในอัตราสูงสุดจะทำการทำสอบแบบปริมาณข้อมูล จำนวน 30 ครั้ง และปริมาณเวลา 30 ครั้ง ซึ่งได้ผลแสดงในตารางที่ 4.7

ตารางที่ 4.7 ตารางผลทดสอบการปรับแบนด์วิดท์ของระบบใช้ก่อนจ่ายที่หลัง (Postpaid) ทั้งแบบปริมาณข้อมูลและเวลา

รายการ	สำเร็จ (ครั้ง)	ไม่สำเร็จ (ครั้ง)	ความถูกต้องคิดเป็น %
ปริมาณข้อมูล	30	0	100 %
ปริมาณเวลา	30	0	100 %

8) การทดสอบการอัตราการรับข้อมูลของแต่ละแพ็กเกจ

ในการทดสอบนี้ได้กำหนดแพ็กเจผู้ใช้งาน ได้แก่ แพลทินัม โกลด์ และซิลเวอร์ ซึ่งมีค่าอัตราการรับข้อมูลเมื่อใช้งานเกินที่กำหนดเป็น 2048, 1024 และ 512 kbps ตามลำดับ ซึ่งจะทดลอง

การใช้งานของแต่ละแพ็กเกจการใช้งาน เมื่อจำกัดปริมาณแบนด์วิดท์แล้วใช้โปรแกรมสำหรับทดสอบทดสอบอัตรารับส่งข้อมูลของอินเทอร์เน็ต แบ่งเป็นแพ็กเกจละ 30 ครั้ง ซึ่งผลอัตราการรับข้อมูลที่ได้จะแสดงในตารางที่ 4.8

ตารางที่ 4.8 ผลการทดสอบความของอัตราการรับข้อมูล

แพ็กเกจ	แพลตินัม (kbps)	โกลด์ (kbps)	ซิลเวอร์ (kbps)
อัตราการรับข้อมูล	2048	1024	512
ค่าสูงสุด	2005	1005	500
ค่าต่ำสุด	1988	995	495
ค่าเฉลี่ย	1999	999	497
ส่วนเบี่ยงเบนมาตรฐาน	4.92	3.44	1.76

บทที่ 5
บทสรุปผลและข้อเสนอแนะ

5.1 สรุปผลการศึกษาตามขอบเขตงานวิจัย

5.1.1 สามารถพัฒนาระบบการทำ Fair Usage Policy ในระบบโครงข่ายไร้สาย WiFi โดยนำระบบ 3GPP มาเป็นต้นแบบในการพัฒนา โดยเมื่อผู้ใช้งานมีการใช้งานในโครงข่าย WiFi จนถึงระดับที่กำหนดไว้ (ทั้งในแง่ของปริมาณการใช้ข้อมูล และเวลาการใช้ข้อมูล) อัตราการใช้งานข้อมูล (bit rate) ในด้านขาลง (download) ของผู้ใช้งานนั้นจะถูกลดค่าลงไปตามค่าที่ได้กำหนดไว้โดยผู้ดูแลระบบ โดยเมื่อครบรอบการใช้งานที่กำหนดในระบบ (ตัวอย่างเช่นการใช้งานแบบรายเดือน) ผู้ใช้งานแต่ละคนจะสามารถใช้งานได้ตามความเร็วสูงสุดที่กำหนดในระบบได้แบบอัตโนมัติ

5.1.2 เครื่องคอมพิวเตอร์แม่ข่ายที่พัฒนาสามารถตรวจสอบปริมาณ และ/หรือ เวลาการใช้งานข้อมูลของผู้ใช้งานแต่ละคนแบบทันทีทันใดกับอุปกรณ์ Wireless Access Point ได้ โดยผู้ดูแลระบบสามารถกำหนดปริมาณของข้อมูลที่ผู้ใช้งานแต่ละประเภทสามารถใช้งานได้ โดยสามารถกำหนดผู้ใช้งานได้ 3 ระดับ ได้แก่ แพลทินัม โกล์ด และซิลเวอร์ โดยผู้ดูแลระบบสามารถกำหนดค่าต่าง ๆ ได้ผ่านทางหน้าเว็บเพจได้ ซึ่งก่อนการใช้งานในโครงข่าย WiFi ผู้ใช้งานต้องยืนยันตัวตนผ่านหน้าเว็บเพจโดยกรอกข้อมูลชื่อผู้ใช้งานและรหัสผ่านของผู้ใช้ทุกครั้งก่อนใช้งาน

5.1.3 การทำ Fair Usage Policy ในงานวิจัยนี้ครอบคลุมถึงกรณีที่ผู้ใช้งานมีการเคลื่อนที่ ทำให้มีการใช้งานภายใต้ Wireless Access Point มากกว่า 1 ตัว โดยระบบจะยังคงสามารถจำกัดความเร็วเมื่อผู้ใช้งานมีการใช้งานเกินปริมาณข้อมูล หรือเวลาที่กำหนดไว้

5.2 ข้อจำกัดของระบบ

ข้อจำกัดของต้นแบบระบบกำหนดการใช้งานอย่างยุติธรรมในโครงข่ายคอมพิวเตอร์ไร้สายสามารถแยกข้อจำกัดออกเป็นข้อๆได้ดังต่อไปนี้คือ

5.2.1 อุปกรณ์เราเตอร์ WRT54GL สามารถลดอัตราแบนด์วิดท์ได้เฉพาะขาลงเท่านั้น

5.2.2 ในการใช้งาน แต่ละผู้ใช้งานจำเป็นต้องมีไอพี แอดเดรสเป็นเฉพาะของผู้ใช้งานนั้นๆ

5.2.3 สถานะในการแสดงว่าผู้ใช้งานนั้นใช้งานอินเทอร์เน็ตอยู่หรือไม่ ของแต่ละผู้ใช้งานที่ WRT54GL ส่งมายังเครื่องแม่ข่ายนั้น จะส่งค่ามาว่าผู้ใช้งานนั้นยังใช้งานอยู่ แม้ว่าผู้ใช้งานนั้นจะเลิก

ใช้งานไปแล้วก็ตาม โดยจะส่งค่าว่าผู้ใช้งานนั้นเลิกใช้งานก็ต่อเมื่อผู้ใช้งานนั้นเลิกใช้งานไปแล้วเป็นเวลาโดยเฉลี่ย 7 นาที

5.2.4 ระบบที่ได้ออกแบบรองรับเฉพาะเครือข่ายขนาดเล็กเท่านั้น เนื่องจาก ขนาดของหน่วยความจำของอุปกรณ์เราเตอร์ WRT54GL ที่มีอย่างจำกัด

5.3 ข้อเสนอแนะ

ข้อเสนอแนะของต้นแบบระบบกำหนดการใช้งานอย่างยุติธรรมในโครงข่ายคอมพิวเตอร์ไร้สายสามารถแยกข้อเสนอแนะออกเป็นข้อๆได้ดังต่อไปนี้คือ

5.3.1 ควรเพิ่มความสามารถในการจำกัดแบนด์วิดท์ให้กับขาขึ้น

5.3.2 ในอนาคตสามารถปรับปรุงและเขียนโปรแกรมเพื่อให้เครื่องคอมพิวเตอร์แม่ข่าย PCRF นั้นมีความสามารถและมีประสิทธิภาพที่ดีขึ้นไป

5.3.3 ควรใช้อุปกรณ์เราเตอร์ในรุ่นที่มีประสิทธิภาพที่ดีมากขึ้น เพื่อรองรับเครือข่ายที่มีขนาดใหญ่

บรรณานุกรม

บรรณานุกรม

ภาษาไทย

สารสนเทศจากสื่ออิเล็กทรอนิกส์

เทเลคอม เจอร์นัล, (2554). *Data Offload ปัญหาใหม่สำหรับผู้ให้บริการ Mobile Broadband (ตอนที่ 2).* สืบค้นเมื่อ 20 มิถุนายน 2554 จาก http://www.telecomjournal.net

มหาวิทยาลัยมหาสารคาม, (2554). *เครือข่ายไร้สาย.* สืบค้นเมื่อ 20 มิถุนายน 2554 จาก http://www.bc.msu.ac.th/project_file/6%288%29.pdf

ภาษาต่างประเทศ

ARTICLE

Fredrik Larsson and Azadeh Hosseinzad Amitkhizi. (2010, June). *Assessment of IxLoad in a GGSN environment.* University of Gothenburg.

ELECTRINIC SOURCES

3rd Generation Partnership Project, (2011). *Standard 3GPP.* Retrieved August 9 2011. form http://www.3gpp .org

Bridgewater Systems, (2011). *Data Sheet: Bridgewater Policy Controller.* Retrieved October 12 2011. form http://www.bridgewatersystems.com/Policy-Controller.aspx

DD-WRT, (2011). *Firmware DD-WRT v23 SP2.* Retrieved July 6 2011. form http://www.dd-wrt.com

DD-WRT, (2011). *RFlow Collector.* Retrieved July 6 2011. form http://www.dd-wrt.com/wiki/index.php/RFlow_Collector

Ericsson, (2011). *Service Aware Charging and Control.* Retrieved October 12 2011. form http://archive.ericsson.net/service/internet/picov/get?DocNo=34/28701-FGB101268&Lang=EN&HighestFree=Y

Quintillion Technologies, (2011). *3GPP TS 23.203 V7.9.0.* Retrieved June 20 2011. form http://www.quintillion.co.jp/3GPP/Specs/23203-790.pdf

Telcordia, (2011). *Personalized Policy & Charging Solution.* Retrieved October 12 2011. form http://www.telcordia.com/collateral/brochures/personalized-policy-charging-brief.pdf

ภาคผนวก

ฟังก์ชันการทำงาน GGSN

1) การเชื่อมต่อไปยังเครือข่ายภายนอก

GGSN ดำเนินการส่งสัญญาณสำหรับการสร้าง, การปรับเปลี่ยนและลบ PDP คอนเทค ไปที่แพ็คเก็ตของเครือข่ายหลัก นอกจากนี้ยังดำเนินการส่งสัญญาณการกำหนดค่า PDP คอนเทคไป ยัง PDN ตัวอย่างเช่นในการจัดสรร IP แอดเดรสสำหรับผู้ใช้งาน โดยปกติการส่งสัญญาณนี้เกิดขึ้น หลังจากการสร้าง PDP คอนเทค

2) การเรียกเก็บเงิน

จากกล่าวถึงในส่วนแรก GGSN จะต้องสามารถในการวิเคราะห์ทราฟฟิคของผู้ใช้งาน และรายงานการใช้งานที่วัดได้ให้ระบบการเรียกเก็บเงิน สำหรับการรายงาน GGSN มีการรองรับ มาตรฐานของกลไกการเรียกเก็บเงินทั้งออนไลน์และออฟไลน์

2.1) การเรียกเก็บเงินออฟไลน์

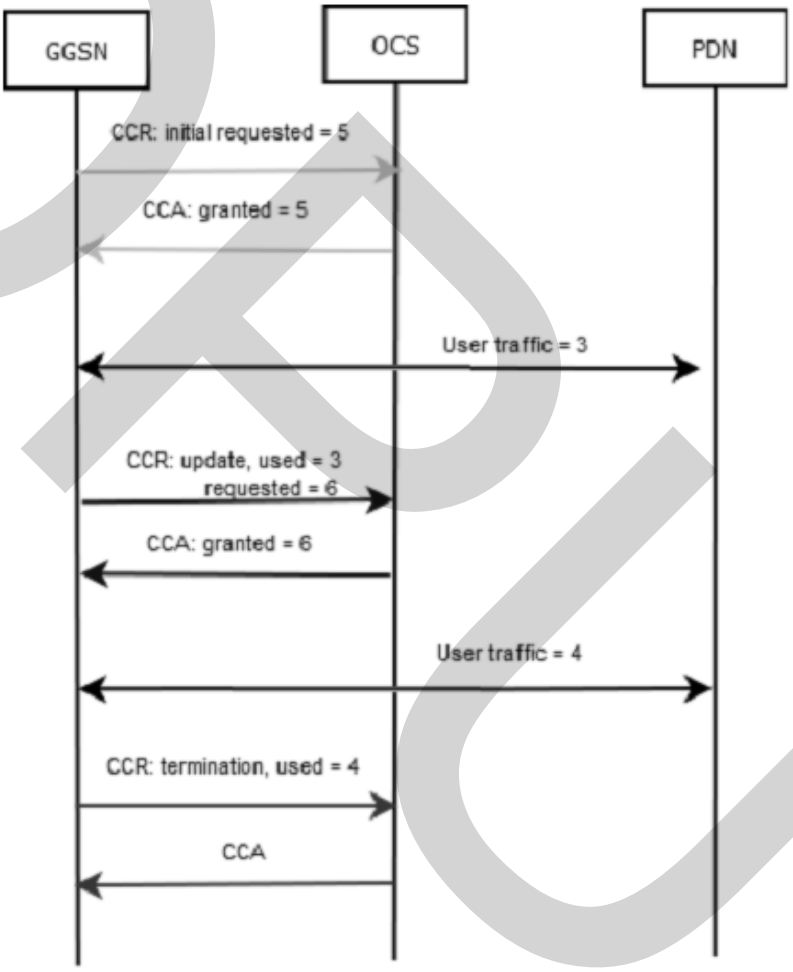
สำหรับข้อมูลการคิดเงินระบบโทรศัพท์มือถือมีหน่วยพื้นฐานที่เรียกว่าชาร์จจิ่งดาต้าเร็ค คอส (CDR) โดย CDR อาจรวมเขตข้อมูลที่ระบุผู้ใช้บริการและข้อมูลเกี่ยวกับทรัพยากรของ เครือข่ายและบริการที่ใช้ในช่วงของสมาชิกโดยเฉพาะอย่างยิ่งปริมาณจำนวนที่โอนจากดาว์นลิงค์ และอัปลิงค์ยูสเซอร์ทราฟฟิค และระยะเวลาของ PDP คอนเทค

ด้วยการเรียกเก็บเงินแบบออฟไลน์ การเก็บรวบรวมข้อมูลการเรียกเก็บเงินที่จะทำ ควบคู่กันไปกับการใช้งานทรัพยากรเครือข่าย ข้อมูลนี้จะถูกถ่ายโอนไปยัง CDR ที่จะถูกโอนไปยัง บิลลิ่งโดเมน (BD) ของผู้ประกอบการเครือข่าย โดย BDs มีวัตถุประสงค์คือการจัดการกับการเรียก เก็บเงินสมาชิก หรือบัญชีระหว่างผู้ประกอบการ นอกจากนี้ยังเป็นไปได้สำหรับผู้ประกอบการใน การเก็บรวบรวมสถิติจาก BD โปรโตคอลทรานสพอร์ตที่ใช้เมื่อมีการส่ง CDRs ที่มีแหล่งที่มาจาก GTP เรียกว่า GTP'(GTP ไพรม) มันเป็นโปรโตคอลที่แยกกันอยู่บนพื้นฐานของ GTP - C โดยการ นำโครงสร้างข้อความเดียวกัน แต่ GTP' รวมถึงโปรโตคอลที่ทำข้อมูลให้ตรงกันเพื่อไม่ให้สูญเสีย หรือซ้ำกันของ CDRs โดยมันถูกใช้ในอินเตอร์เฟซ Ga ระหว่าง GSN และ CGF โดยในส่วน ออฟไลน์ชาร์จจิ่งหมายความว่าข้อมูลการเรียกเก็บเงินไม่ได้มีอิทธิพลต่อผู้ใช้หรือบริการจนกว่าถึง รอบบิล วิธีการนี้จะเรียกว่าโพสเพด

2.2) การเรียกเก็บเงินออนไลน์

สมาชิกพรีเพดต้องการวิธีที่มากกว่าการเรียกเก็บเงินแบบออฟไลน์ซึ่งในข้อมูลการเรียก เก็บเงินไม่สามารถมีอิทธิพลในการให้บริการ การเรียกเก็บเงินออนไลน์เป็นกุญแจสำคัญสำหรับ การแก้ปัญหานี้ ในโซลูชั่นระบบการเรียกเก็บเงินออนไลน์ (OCS) รับผิดชอบในการควบคุมสินเชื่อ ที่จะติดต่อสื่อสารกับ GGSN ในอินเตอร์เฟซ Gy ที่ผ่านไดแอมมิเตอร์เครดิตคอนโทรลแอพลิเคชัน

(DCCA) ที่มีสองไดแอมมิเตอร์คือ CCR (เครดิตคอนโทรลรีเควส) และ CCA (เครดิตคอลโทรลอันเซอร์) ตัวชี้วัดที่เครดิตแบ่งออกเป็นปริมาณ,เวลาหรือเป็นหน่วยที่กำหนดไว้เป็นพิเศษที่แสดงถึงการใช้งาน สำหรับการจัดการโควต้า GGSN จะส่ง CCR ไปที่หน่วยการขอใช้บริการ OCS โดยเซิร์ฟเวอร์ที่ยอมให้ยูนิตและค่าใช้จ่ายในบัญชีสมาชิก นอกจากนี้ยังเป็นไปได้ที่จะสอบถามรายละเอียดราคาที่ GGSN จะถาม OCS ราคาต้นทุนต่อหน่วยที่เฉพาะเจาะจง ตัวอย่างของการใช้การควบคุมสินเชื่อแบบดั้งเดิมจะถูกแสดงในรูปที่ ก1



รูปที่ ก1 Credit control message overview

เมื่อผู้ใช้เสร็จสิ้นขั้นตอนการเปิดใช้งาน PDP และต้องการที่จะเข้าถึงบริการ GGSN ต้องขอโควต้าจาก OCS ก่อนที่จะได้รับการเข้าถึง โดย OCS ควบคุมการส่งมอบบริการโดยสำรองจำนวนเครดิตที่สามารถใช้ได้ของผู้ใช้งานและการอนุญาตให้ GGSN โควต้าของปริมาณ,เวลาหรือ

ยูนิต หากผู้ใช้จะต้องมียอดเงินคงเหลือไม่เพียงพอในบัญชีของเขา, OCS อาจจำกัดหรือปฏิเสธมันอย่างสมบูรณ์ เมื่อผู้ใช้บริการเกี่ยวกับการใช้หน่วยที่ได้รับทั้งหมดของ GGSN อาจส่งการอัพเดตที่มีไปยัง OCS เช่นถ้าโควต้าที่ได้รับหมดหรือถึงระดับเกณฑ์ที่เวลาที่ได้รับหมดลง PDP คอนเทคได้รับการอัพเดท ฯลฯ OCS ประเมินผลของผู้ใช้อีกครั้งและหากมีเงินคงเหลือพอที่จะมอบโควต้าที่ร้องขอไป เมื่อผู้ใช้ทราฟฟิคเสร็จสิ้นมันจะส่ง PDP คอนเทคลบรีเควสไปยัง GGSN ซึ่งเริ่มต้นการลบคอนเทคและส่ง CCR สิ้นสุดไปยัง OSC เพื่อรายงานหน่วยที่ใช้ล่าสุด

หากผู้ใช้ไม่มีเงินคงเหลือพอ OCS อาจร้องขอสำหรับการเปลี่ยนเส้นทางของผู้ใช้ ตัวอย่างเช่นหากผู้ใช้จะใช้ HTTP, OCS อาจเปลี่ยนเส้นทางผู้ใช้ไปยังเว็บไซต์ของผู้ประกอบการ ที่สมาชิกอาจเลือกไปที่จะเติมเงินในบัญชีของตน

มันเป็นไปได้ที่จะมาพร้อมกับการเรียกเก็บเงินออนไลน์ด้วยวิธีออฟไลน์เพื่อที่จะสร้าง CDRs สำหรับสมาชิกเรียกเก็บเงินออนไลน์ ให้สำรองข้อมูลต่าง ๆ ที่เป็นไปได้ถ้าส่วนต่าง ๆ ของระบบล้มเหลว

3) QoS, QoE และ ทราฟฟิคเชพปิ้ง

เป็นที่รู้จักกันดีว่า ทราฟฟิคบนอินเทอร์เน็ตที่จะดำเนินการด้วยความพยายามที่ดีที่สุด ซึ่งหมายความว่าจะไม่มีการรับประกันว่าแพ็กเก็ตทั้งหมดจะถูกส่งผ่านเครือข่าย การสูญเสียแพ็คเก็ตที่อาจเกิดขึ้นได้จากหลายสาเหตุเช่นโดยการแออัดของเครือข่ายหรืออุปกรณ์ที่มากเกินไป การเพิ่มความจุของแบนด์วิดธ์อาจจะเป็นแก้ปัญหาที่ง่าย แต่โปรโตคอลที่ทำให้เกิดความแออัดอาจกินแบนด์วิดธ์เพิ่มขึ้นและปัญหาก็จะเกิดขึ้นอีกครั้ง

บริการที่แตกต่างและโปรโตคอลที่มีความต้องการและคุณสมบัติที่แตกต่างกัน เช่น FTP ที่เป็นตัวอย่างหนึ่งที่ไม่ได้รับผลกระทบมากเกินไปโดย จิทเทอะ, แพ็คเกจลอสหรือดีเลย์ ถึงแม้ว่าจะจำกัดแบนด์วิดธ์ที่อาจมีผลกระทบต่อระยะเวลาของการดาวน์โหลดไฟล์ แต่ผลสุดท้ายจะไม่สามารถเปลี่ยนแปลง ในขณะที่บริการการสนทนาแบบเรียวทาม เช่นวิดีโอและเสียงที่มีความไวต่อการทำงานของเครือข่าย การสนทนาที่อาจจะมีเสียงขาด ๆ หาย ๆ และการเปลี่ยนแปลงเมื่อวอยซแพ็กเก็ตมีดีเลย์มากกว่า 150-200 ms

นอกจากนี้ยังเป็นสิ่งสำคัญที่จะทราบว่าผู้ใช้ที่แตกต่างกันจำเป็นต้องมีคุณภาพที่แตกต่างกันและด้วยเหตุนั้น มันเป็นส่วนใหญ่มีแนวโน้มที่ลูกค้าบางคนยินดีที่จะจ่ายมากขึ้นเพื่อที่จะได้รับบริการที่ดีกว่าเพื่อให้ได้รับความผิดพลาดในการส่งและการหลุดการเชื่อมต่อน้อยลงในขณะที่ลูกค้าอื่น ๆ ที่ต้องการจ่ายน้อย ในกรณีดังกล่าวเป็นแนวคิด QoS สามารถใช้เพื่อเสนอการรับประกันการใช้บริการโทรศัพท์มือถือ

บริการที่ทำให้แตกต่าง (DiffServ) เป็นส่วนหนึ่งของวิธีการที่ดีขึ้นสำหรับการเปิดใช้แนวคิด QoS ในเครือข่ายไอพี DiffServ เป็นกลไก QoS อาศัยกับการกำหนดค่าคงที่ของทรัพยากรที่ส่งต่อ DiffServ เครือข่ายแบ่งออกเป็นแพ็กเก็ตจำนวนเล็ก ๆ ของโฟลรวมหรือ “คลาส” อยู่บนพื้นฐานของ DiffServ Code Point (DSCP) ในส่วนหัวของ IP ของแพ็กเก็ต ประเภทนี้เพื่อให้รู้ประเภทของการปฏิบัติ วิธีก็คือการจัดเตรียมที่มากกว่าเพื่อที่จะให้แบนด์วิดธ์เพียงพอที่จะหลีกเลี่ยงความแออัด ในกรณีส่วนใหญ่การแก้ปัญหามากกว่าการจัดเตรียมตอบสนองความต้องการ QoS สำหรับทราฟฟิคที่ทนต่อดีเลย์ เช่นการดาวน์โหลดไฟล์และการท่องเว็บ แม้ว่าโซลูชั่นที่สูงขึ้นเช่นบริการที่แตกต่างมีความจำเป็นเมื่อโหลดของเครือข่ายจะสูงขึ้นหรือการรับรองการบริการที่นำเสนอโดยผู้ประกอบการ

สถาปัตยกรรมQoS มีองค์ประกอบอยู่สองวิธีคือ Internet Engineering Task Force (IETF) การพัฒนา QoS สำหรับเครือข่ายที่ฟิกไอพี และ 3rd Generation Partnership Project (3GPP) โดยออกแบบสถาปัตยกรรม QoS สำหรับการใช้ทรัพยากรที่ขาดแคลนอย่างมีประสิทธิภาพ

ประเภทของ QoS ยังเรียกว่าประเภทการจราจรที่กำหนดไว้ในมาตรฐาน 3GPP “คุณภาพของแนวคิดการให้บริการและโครงสร้างสถาปัตยกรรมแบบ” TS 23107 โดยแบ่ง QoS ออกเป็น 4 ประเภท ดังต่อไปนี้

- การสนทนา

มีไว้สำหรับการพูดโทรศัพท์, วอยส์โอเวอร์ไอพี (VoIP), และวิดีโอคอนเฟอเรนท์

- สตรีมมิ่ง

มีไว้สำหรับเรียวทามออดิโอและแอปพิเคชั่นวิดีโอสตรีมมิ่ง

- อินเตอร์แอคทีฟ

ไว้สำหรับโปรแกรมประยุกต์แบบโต้ตอบเช่นอีเมล์โต้ตอบหรือการท่องเว็บแบบโต้ตอบ, เทลเน็ต และผู้ที่ต้องการการตอบสนองต่อการร้องขอ

- แบคกราวน์

มีไว้สำหรับแบคกราวน์ทราฟฟิคตัวอย่างเช่น อีเมลและดาวน์โหลดไฟล์, บริการข้อความสั้น (SMS), ถ่ายโอนไฟล์และการบริการดังกล่าวที่ไม่จำเป็นต้องจัดส่งภายในระยะเวลาหนึ่ง

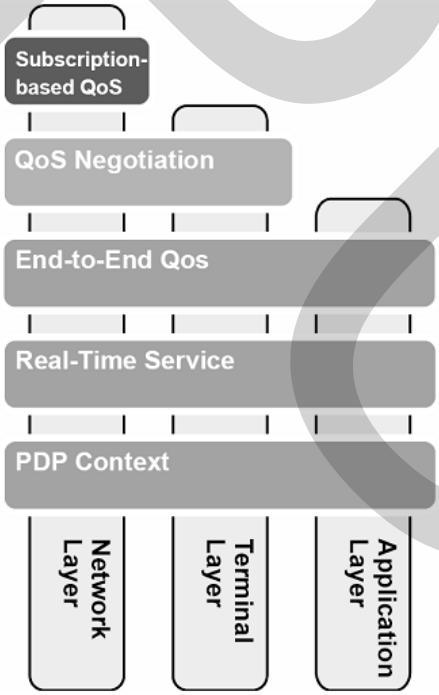
ที่ระดับการสนทนามีไว้สำหรับทราฟฟิคที่มีความอ่อนไหวต่อดีเลย์มากที่สุดและระดับของแบคกราวน์มีไว้สำหรับทราฟฟิคที่มีความอ่อนไหวน้อย ระดับอินเตอร์แอคทีฟและแบคกราวน์ควรจะให้อัตราความผิดพลาดที่ต่ำ โดยใช้วิธีการเข้ารหัสช่องทางและ รีทรานสมิทชั่นในเซลแนลเรดิโอเมื่อเทียบกับระดับการสนทนาและสตรีมมิ่งเนื่องจากการที่ต้องการความทนทานต่อดีเลย์ที่

แตกต่างกัน ทราฟฟิคในระดับอินเตอร์แอคทีควรจะมีความสำคัญสูงในการตั้งเวลากว่าทราฟฟิคระดับแบคกราวน์ ซึ่งเป็นสิ่งสำคัญในสภาพแวดล้อมไร้สายที่แบนด์วิดธ์ที่ต่ำ

อินทิเกรดติ่ง ดิฟเซฟ ใน GGSN มีความสำคัญสำหรับมันเพื่อให้สามารถในการดูแลของแพ็กเก็ตไอพี ที่เกี่ยวกับระดับทราฟฟิกหรือในช่วงระยะเวลาของความแออัด ผู้ใช้งานต้องการ QoS เพื่อต่อรองเพื่อให้มั่นใจความสมบูรณ์ของ GGSN และโหนดที่อยู่ติดกัน

โดย GGSNs ขั้นตอนการ QoS จะถูกเรียกจากข้อความที่ส่งสัญญาณจาก UE, SGSN หรือสำรองที่ไม่พึงประสงค์จากเซิร์ฟเวอร์ของการควบคุมนโยบายภายนอกเช่นนโยบายและการทำงานกฎชาร์จ (PCRF) โดยเฉพาะที่กระบวนงาน QoS ขึ้นอยู่กับความสามารถใน GSNs เช่นเดียวกับความสามารถใน UEs QoS ซึ่งถูกระบุไว้ในมาตรฐาน 3GPP TS 23207, GGSN เป็นสิ่งจำเป็นเพื่อสนับสนุนการทำงานอย่างน้อยของฟังก์ชันดิฟเซฟ นอกจากนี้ยังอาจซัพพอร์ท รีซอร์ท รีเซอร์เวชั่นโปรโตคอล (RSVP) และพอลลิซีเอ็นฟอชเม็นท์ฟังก์ชัน

โมเดลในรูปที่ ก2 แสดงให้เห็นถึงมุมมองแบบตั้งแต่ต้นจนจบของ QoS ที่นำเสนอโดยเครือข่ายรวมถึงสาม เลเยอร์ที่แตกต่างกันคือเน็ตเวิร์ค, เทอมิเนิล และแอพลิเคชันเลเยอร์



รูปที่ ก2 QoS Layer Model

เน็ตเวิร์คเลเยอร์นี้จะจัดการกับซับสคริปชั่นเบส QoS, ที่เกี่ยวข้องกับเรดิโอและเน็ตเวิร์คแบคโบน ต้องที่การโหนดเน็ตเวิร์ค, RNCs, NodeBs และ GSNs ที่เจรจา QoS พารามิเตอร์กับอื่น ๆ และส่งแพ็กเก็ตต่อไปตามนั้น ซับสคริปชั่นเบส QoS สามารถควบคุมได้โดยประกอบการเครือข่าย

เทอมินิลเลเยอร์ที่เกี่ยวข้องกับซับสคริปเบอร์ ของ MS ในการจัดเตรียม QoS โมบายสเตชั่นที่มีการรองรับ QoS ที่สามารถส่งแพ็กเก็ตไปยัง QoS นิโกชิเอท ตัวอย่างเช่นแพ็คเก็ตนี้จะทำเครื่องหมายและการกำหนดเวลา

แอพลิเคชันเลเยอร์ที่เกี่ยวข้องกับแอพลิเคชันที่ทำงานบน MS ที่ซึ่งทำให้มันเป็นไปได้สำหรับแอพลิเคชันที่คล่องตัวมีส่วนร่วมใน QoS นิโกชิเอเชินและให้เครือข่ายที่มีข้อมูลเกี่ยวกับการต้องการ QoS ที่เฉพาะ แอพลิเคชันจะตระหนักถึงสิ่งที่ QoS ได้รับจากเครือข่ายและอาจพยายามที่รีนิโกชิเอเชิน

สำหรับผู้ประกอบการก็เป็นสิ่งจำเป็นที่จะมีการควบคุมที่เพิ่มขึ้นกว่า QoS ที่นำเสนอมากกว่าคอร์และเรดิโนเน็ตเวิรค์รีซอท มีคุณภาพที่เหมาะสมสำหรับผู้ใช้โดยไม่ต้องจัดสรรทรัพยากรที่ไม่จำเป็นเป็นสิ่งจำเป็นสำหรับการรักษามีค่าใช้จ่ายที่ต่ำที่ถูกผูกไว้ ผ่านอินเตอร์เฟซ GX, แอพพลิเคชันเซิร์ฟเวอร์ของผู้ประกอบการได้รับอนุญาตให้มีส่วนร่วมมากขึ้นใน QoS นิโกชิเอเชิน ที่ PDP คอนเท็กแอคทีฟและการปรับเปลี่ยน นี้จะเปิดใช้งานโดยการใช้งานของ PCRF ที่ให้บริการการอนุมัติและการควบคุมนโยบายสำหรับการบริการที่เข้าถึงได้ผ่านทาง GGSN โดย GGSN และ PCRF ใช้ในการสื่อสารแบบ ไคลเอิน-เซิร์ฟเวอร์มากกว่าอินเตอร์เฟซ Gx โดย PCRF จะสนับสนุน GGSN กับกฎการเรียกเก็บเงินที่แตกต่างกันที่ระบุว่าบริการที่ได้รับอนุญาตและที่ไม่ได้ กฎระเบียบที่ชัดเจนอาจจะบอก GGSN วิธีการจำแนกประเภทผู้ใช้บริการดาต้าโฟล นอกจากนี้ PCRF ยังสามารถรับผิดชอบสำหรับการประเมินที่เรียกเก็บเงินจากกฎที่จะใช้สำหรับผู้ใช้บริการขึ้นอยู่กับการสมัครสมาชิกประเภทที่รายละเอียดของผู้ใช้ถ้า MS จะโรมมิ่งหรือขึ้นอยู่กับเวลาและวันที่ ขึ้นอยู่กับการกำหนดค่า GGSN อาจเปลี่ยนเส้นทางผู้ใช้ขึ้นอยู่กับการตอบสนองจาก PCRF

อีกปัญหาที่สำคัญที่ผู้ประกอบการที่ต้องเน้นคือความพึงพอใจการบริการของสมาชิก สาเหตุของความพึงพอใจนี้ไม่ได้เป็นเพียงการติดต่อกับผู้ประกอบการ แต่ยังมีประสบการณ์การบริการที่ดี การท่องอินเทอร์เน็ตให้ส่งวิดีโอหรือภาพถ่ายและดาวน์โหลดเสียงเรียกเข้า ตัวอย่างเช่น ส่วนของประสบการณ์การให้บริการของสมาชิก วิธีการวัดของที่ดีของสมาชิกเกี่ยวกับความพึงพอใจของบริการที่ได้รับเรียกว่า"ประสบการณ์ของคุณภาพ"(QoE)

ในทางตรงกันข้ามกับ QoS ซึ่งเป็นแนวคิดที่ดีที่กำหนดไว้ในวิศวกรรมซอฟต์แวร์ QoE เป็นเรื่องเกี่ยวกับความพึงพอใจของมนุษย์และความพึงพอใจเมื่อใช้บริการที่ จากอธิบายไว้ข้างต้น

QoS วิเคราะห์ของสภาพการทำงานของเครือข่ายเช่นจิสเตอร์, แพ็คเก็จลอสหรือนอยซ ในขณะที่ QoE เป็นการวิเคราะห์ของความพึงพอใจในปัจจุบันของผู้ใช้จากแอฟพิเคชันและเซอร์วิท ถึงแม้ว่า QoS และ QoE เป็นสองแนวคิดที่แตกต่างกันแต่ทั้งสองเกี่ยวข้องอย่างแน่นอนเนื่องจากคุณภาพของการบริการเป็นหนึ่งในรายการที่มีผลต่อความพึงพอใจของผู้ใช้บริการ แต่มีระดับ QoS สูงไม่จำเป็นต้องนำไปสู่การ QoE ระดับสูง ตัวอย่างเช่นผู้ประกอบการที่อาจจะให้บริการข้อมูลที่มี QoS สูง แต่สมาชิกที่ไม่พอใจกับเนื้อหาที่นำไปสู่การได้ QoE ที่ต่ำ

ทราฟฟิกเชฟปิ้งเป็นวิธีการที่จะปรับปรุงและรับประกันการทำงานและการควบคุมทราฟฟิกบนเครือข่ายตัวอย่างเช่นการเพิ่มแบนด์วิดธ์ใช้งานได้โดยดีเลย์เซอร์เทนแพ็กเก็ตหรือการควบคุมปริมาณการถูกส่งไปยังเครือข่ายหรือการกระทำอื่น ๆ เกี่ยวกับโฟลในเครือข่าย ทราฟฟิกเชฟปิ้งเป็นวิธีที่จะรับประกันได้ว่าให้เครือข่ายอยู่ในระดับที่คาดว่าจะได้ QoE และความพึงพอใจของผู้ใช้ วันนี้มีความต้องการที่เพิ่มขึ้นสำหรับ ทราฟฟิคเชฟปิ้งเพราะการเพิ่มขึ้นของปริมาณข้อมูลที่ถ่ายโอนผ่านเรดิโอเน็ตเวิร์คและด้านโครงสร้างพื้นฐานของผู้ประกอบการ อาจจะไม่สามารถที่จะรับมือได้ จะบังคับให้พวกเขาปรับคาปาซิตี้ของพวกเขาโดยไม่มีรายได้ที่สอดคล้องกัน ในสถานการณ์เหล่านี้ทราฟฟิคบางอย่างจำเป็นต้องได้รับการบีบเพื่อปกป้องโครงสร้างพื้นฐาน หากทราฟฟิกเชฟปิ้งจะถูกนำไปใช้ประสบความสำเร็จก็จะให้ลำดับทราฟฟิคสำคัญและมีความอดทนต่ำการบริหารจัดการของการบริโภคการบริการข้อมูลเพื่อให้แน่ใจว่าผู้ใช้บางรายไม่โอเวอร์โหลดของระบบ นอกจากนี้ยังจะให้แน่ใจว่าอัตราทราฟฟิคโลโทเลอเรนท์ จะมีคุณลักษณะทราฟฟิกที่ดีเช่นแบนด์วิดธ์ที่ดีพอ, โลจิทเทอร์, ดีเลย์และแพ็คเก็ตลอส

การแก้ปัญหาด้วยคอนเวอร์เจนซ์ออลไอพีเบส ความหลากหลายของการจำแนกโฟลและการจองทรัพยากรที่นำเสนอโดยดิฟเซฟอาจจะไม่เพียงพอ เพื่อตอบสนองความคาดหวังการส่งมอบบริการของสมาชิกเครือข่ายหลักที่ต้องการเพื่อให้สามารถแยกแยะความแตกต่างระหว่างประเภทของบริการและยังแยกความแตกต่างระหว่างประเภทต่างๆของการใช้งานเฉพาะ ในที่นี้บริการตาม QoS ผู้รับต้องการที่จะมีปฏิสัมพันธ์กับเครือข่ายหลัก ข้อมูลผู้ใช้ที่ยังเป็นความสำคัญตั้งแต่การให้บริการจะขึ้นอยู่กับสิ่งที่ผู้ใช้สมัครได้และสิ่งที่ผู้ใช้บริการมีสิทธิพิเศษได้รับ ซึ่งจะส่งผลในการเกี่ยวข้องกับ PCRF มากขึ้นเนื่องจาก PCRF เป็นผู้รับผิดชอบต่อการบังคับใช้รายละเอียดของผู้ใช้ โดยแจ้ง GGSN เกี่ยวกับสิทธิ์ของผู้ใช้

4) การตรวจสอบแพ็คเกจและการจำแนกประเภทการบริการ

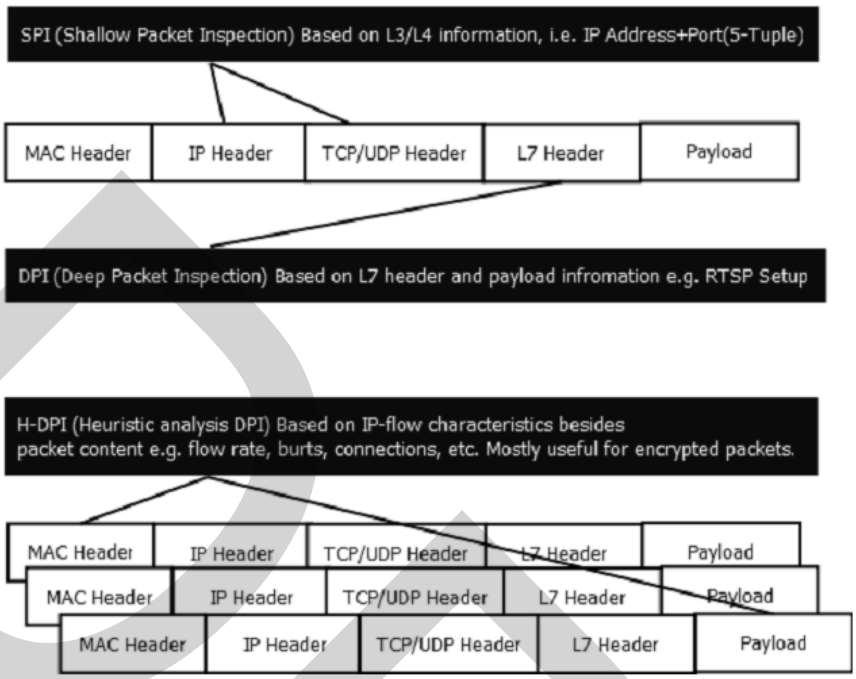
การตรวจสอบแพ็คเก็ตและการวิเคราะห์ทราฟฟิคของยูสเซอร์แพลนทราฟฟิคที่เป็นหนึ่งในฟังก์ชันการทำงานที่สำคัญใน GGSN ปกติยูสเซอร์แพลนทราฟฟิครวมถึง Hypertext Transfer Protocol (HTTP), Wireless Application Protocol (WAP), Multimedia Messaging Service

(MMS), อีเมลและการสตรีมเสียงหรือภาพที่มี Session Initiation Protocol (SIP) และ Real-Time Streaming Protocol (RTSP) โดยสามารถที่จะรู้ว่าสิ่งที่กำลังทำงานอยู่บนเครือข่ายที่มีความจำเป็นสำหรับผู้ประกอบการในการแสวงหาของพวกเขาสำหรับการเสนอบริการใหม่ที่แตกต่างให้กับลูกค้าของพวกเขาเป็นความสามารถในการรับประกัน QoS ของพวกเขา

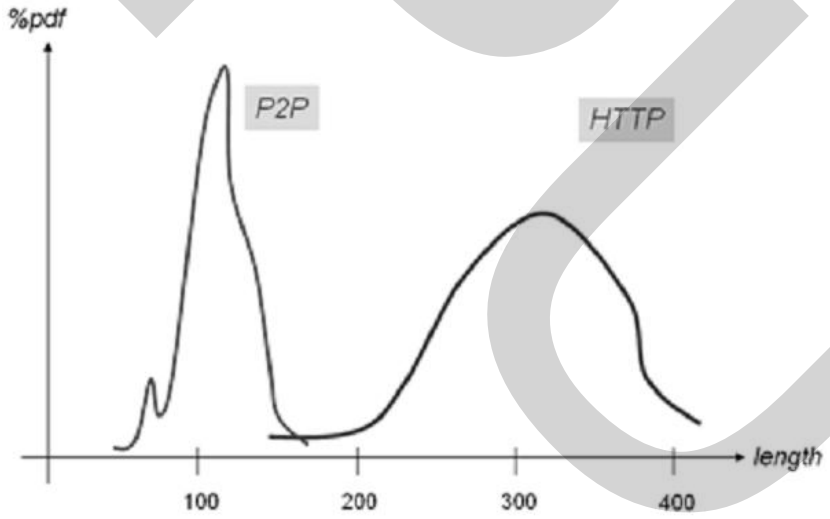
การกรองและการตรวจสอบของแพ็กเก็ตที่ได้รับการพัฒนาอย่างต่อเนื่อง รูปที่ ก3 แสดงให้เห็นถึงการวิเคราะห์แพ็คเก็ตที่สามารถแบ่งออกเป็น 3 ระดับที่แตกต่างกันคือ Shallow Packet Inspection (SPI), Deep Packet Inspection (DPI) และ Heuristic analysis Deep Packet Inspection (H-DPI) SPI ใช้ข้อมูลส่วนหัวเช่นไอพีแอดเดรสของต้นทางและปลายทาง พอร์ตและทราสพอร์ทโปรโตคอลสำหรับการวิเคราะห์และการตรวจสอบของแพ็กเก็ตในขณะที่ DPI ตรวจสอบส่วนหัวของแพ็กเก็ตที่เช่นเดียวกับส่วนที่เก็บข้อมูลโดยใช้การวิเคราะห์โปรโตคอลขึ้นอยู่กับเลเยอร์ 7 เช่นการค้นหาสิ่งที่ผู้ใช้เว็บไซต์ คือการเรียกดูได้โดยดูที่ HTTP ร้องขอ URL ใน HTTP GET เมสเซจ จะให้แอฟพิเคชันรับรู้ความสามารถในการวิเคราะห์การใช้งานเครือข่ายและการปรับปรุงประสิทธิภาพของเครือข่าย โดย James Crashaw นักวิเคราะห์การวิจัยกล่าวไว้ว่า “DPI จะช่วยให้การดำเนินการปรับปรุงประสิทธิภาพของโปรแกรมประยุกต์เชิงโต้ตอบ การป้องกันทราฟฟิคแอพลิเคชันบางอย่างจากรีซอทฮอคกินมากเกินไปและเอื้อต่อการแออัด นอกจากนี้ยังช่วยลดผลกระทบของการโจมตีเครือข่ายซึ่งจะช่วยลดคาเป็คและโอเป็ค ขณะที่การเพิ่มความพึงพอใจของผู้ใช้บริการนำไปสู่การลดลง”

H-DPI ทำหน้าที่ตรวจสอบทรานแซคชั่นแพ็คเก็ตขึ้นอยู่กับการดีเท็ครูปแบบพฤติกรรมจะทำให้มันเป็นไปได้ที่จะวิเคราะห์ทราฟฟิคที่ได้รับการเข้ารหัส รูปแบบพฤติกรรมจะถูกเก็บไว้ในฐานข้อมูลซึ่งจะใช้สำหรับการจับคู่กับแพ็คเก็ตโฟลและมีข้อสังเกตจากโฟลเรต ของความยาวปกติของแพ็คเก็ต, อัตราแพ็คเก็ตอัพโหลด/ดาว์โหลด, การเชื่อมต่อแบบขนานเป็นต้น

การจัดการและการตรวจสอบแบบ peer-to-peer (P2P) ทราฟฟิคมีความซับซ้อนมากขึ้น DPI อาจจะไม่เพียงพอสำหรับการใช้โปรโตคอลเช่น P2P เป็นผลมาจากลักษณะบางอย่างเช่นการใช้งานพอร์ตแบบไดนามิก การเข้ารหัสตั้งแต่ต้นจนจบ และอื่น ๆ รูปที่ ก4 แสดงการเปรียบเทียบระหว่างทราฟฟิค P2P และ HTTP



รูปที่ ก3 ระดับการวิเคราห์แพ็กเกจ



รูปที่ ก4 การเปรียบเทียบรูปแบบระหว่างทราฟฟิค P2P และ HTTP

ถ้า packet length histogram flow (PDF) คือการตรวจสอบเป็นที่ชัดเจนว่าการควบคุมแพ็กเก็ต P2P มีแนวโน้มที่จะสั้นกว่าแพ็คเก็ต HTTP โดยเฉพาะในช่วงเวลาการติดตั้ง หากมีการวิเคราะห์ในการเลือกทางที่ดีที่สุดที่มีความรู้ดังกล่าวข้างต้นถูกนำไปใช้ในตัวอย่างที่มี P2P

แอฟพิเคชั่นใช้พอร์ต 80 ซึ่งทั่วไปเกี่ยวข้องกับ HTTP ที่มันจะสามารถตรวจสอบความยาวของแพ็กเกจในกราฟและกำหนดว่าพอร์ต 80 ดำเนินการ ทราฟฟิค HTTP อย่างเดียวหรือเกี่ยวข้องกับทราฟฟิค P2P

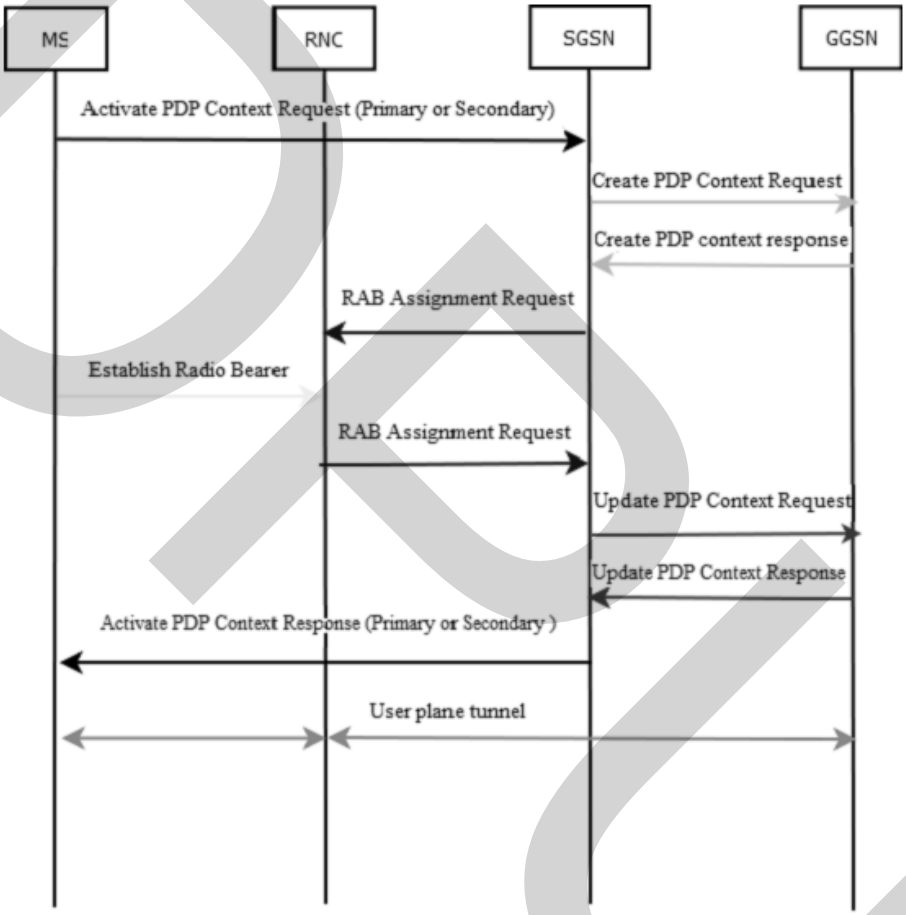
GGSN ดำเนินการตรวจสอบแพ็คเก็ตและการวิเคราะห์แพ็กเก็ตในทั้งหมด 3 ระดับที่แตกต่างที่ได้รับการกล่าวถึง มันสามารถระบุประเภทของทราฟฟิคที่แตกต่างกันซึ่งใช้ได้สำหรับทราฟฟิคเชปปิ้งภายใต้เงื่อนไขโหลดเครือข่ายที่แตกต่างกัน ฟังก์ชันการทำงานที่ GGSN DPI จะเริ่มต้นตรวจสอบและวิเคราะห์ทราฟฟิคจากเน็ตเวอร์เลเยอร์ขึ้นไปแอปพิเคชั่นเลเยอร์ เป็นข้อมูลที่ถูกจับในเวลาจริงทั้งเนื้อหาและแพ็กเก็ตในเลเยอร์ 3 จะได้รับการตรวจสอบโดยกฎของ DPI GGSN ในวิธีนี้ผู้ประกอบการที่มีความสามารถในการเก็บรวบรวมข้อมูลเกี่ยวกับสิ่งที่สมาชิกกำลังประสบเกี่ยวกับการให้บริการที่มี ความสามารถดังกล่าวช่วยเพิ่มระดับของ QoE และจะนำไปสู่ความพึงพอใจมากขึ้นเช่นกันเป็นผลกำไรที่เพิ่มขึ้นด้วย

5) ไดเรคท์ทัลเนิล

ในสถาปัตยกรรมหลักแพ็คเก็ต 3G, SGSN จะรับผิดชอบในการขุดเจาะอุโมงค์ส่งสัญญาณทราฟฟิคและยูสเซอร์แพลนทราฟฟิคจากเรดิโอเน็ตเวอร์ไปยัง GGSN ทรากฟิคที่ห่อหุ้มนี้เป็นครั้งแรกระหว่างตัวเรดิโดเน็ตเวิร์คคอนโทรลเลอร์ (RNC) และ SGSN ซึ่งที่ SGSN ความต้องการที่จะยุติการแยกยูเซอร์แพลนทราฟฟิคและใส่ลงท่อที่ต่อไปยัง GGSN ขั้นตอนนี้ต้องใช้พลังงานทั้งเวลาและการประมวลผล ในช่วงนี้สถานการณ์ส่วนใหญ่ไม่จำเป็นจริงๆ เนื่องจากทั้ง GGSN และ RNC ที่มี IP เราเตอร์ปกติซึ่งสามารถที่จะสื่อสารโดยตรงกับส่วนอื่น ๆ วิธีการหนึ่งที่เป็นมาตรฐานของไดเร็คทัลเนิลฟังก์ชัน ซึ่งจะช่วยให้ SGSN สร้างไดเรคยูสเซอร์แพลนทัลเนิลระหว่าง RNC และ GGSN จึงกำจัดตัวเองจากยูเซอร์แพลนทราฟฟิค อย่างไรก็ตามการจัดการการเคลื่อนที่ยังคงอยู่ใน SGSN ซึ่งหมายความว่ามันยังคงเป็นผู้รับผิดชอบในการแก้ไขทัลเนิล ถ้า UE จะโรมมิ่งไปยังพื้นที่ที่ให้บริการโดย RNC อื่น

ในวิธีนี้ 3G เพย์โหลดทราฟฟิคจะอ้อมไปยัง SGSN ที่ตอนนี้ทำงานเป็นซิกเนลลิ่งเซิร์ฟเวอร์เท่านั้น ซึ่งหมายความว่าขนาดของตัวชี้วัดสำหรับ SGSN เป็นซิงแนลลิ่งโหลดและไม่ใช่ยูซเซอร์แพลนทราฟฟิค มีข้อ จำกัดบางอย่างสำหรับคุณลักษณะนี้ ตัวอย่างเช่นโรมมิ่งระหว่างประเทศไม่ทำงานถ้า SGSN จะต้องมีการเกี่ยวข้องในการนับจำนวนทราฟฟิคสำหรับการเรียกเก็บเงินระหว่างผู้ประกอบการ กรณีที่เพิ่มเติมคือเมื่อ SGSN อยู่ในโฟลค่าใช้จ่ายของการนับทราฟฟิค แต่ในทางปฏิบัติมันเป็นไปได้เพื่อหลีกเลี่ยงข้อจำกัด ดังกล่าวด้วยการใช้ OCS ที่สามารถเห็นได้ในรูปที่ ก5 เมื่อเริ่มต้น DTI ทัลเนิล MS ที่เปิดใช้งานส่ง PDP คอนเท็ครีเควสไปยัง SGSN และปกติจะสร้าง PDP คอนเท็กโพรซิเจอะที่มีอยู่ โดย SGSN ส่งคำขอการกำหนด RAB เพื่อให้มั่นใจว่า RNC

และ MS ทราบว่าทัลเนิลเป็นเรื่องเกี่ยวกับที่จะสร้าง หลังจาก RAB ขั้นตอนการกำหนด SGSN จะแจ้ง GGSN โดยการส่งอัพเดท PDP คอนเท็กรีเควสรวมถึงแจ้งข้อมูลที่ DTI ซึ่ง RNC จะไปส่งยูซเซอร์แพลนทราฟฟิกไปยัง GGSN หลังจากที่ GGSN มีการตอบสนองต่อ SGSN ที่แอคทีฟ PDP คอนเท็กรีสปอนถูกส่งไปยัง MS ที่จึงทำให้ MS เพื่อเริ่มต้นการส่ง payload



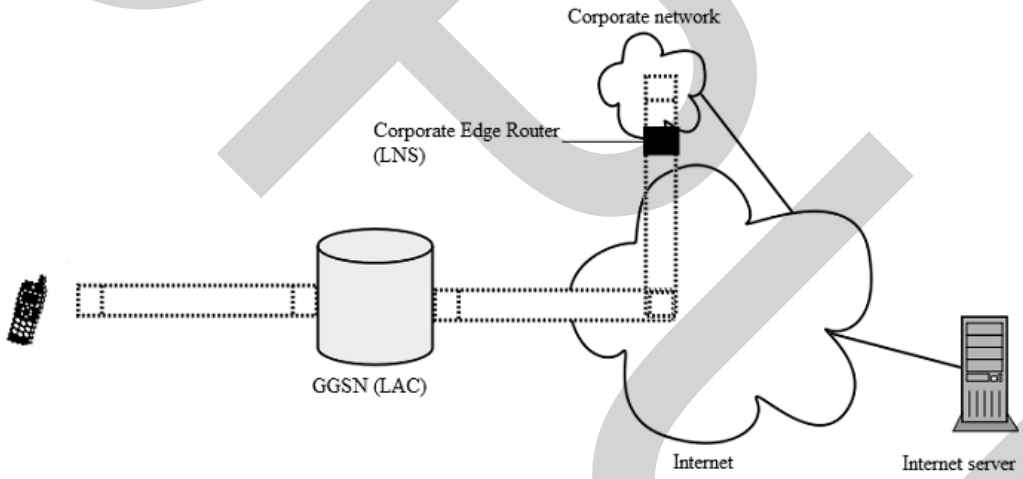
รูปที่ ก5 DTI PDP context activation procedure

6) เลเยอร์ 2 ทันเน็ลลิ่งโปรโตคอล

เลเยอร์ 2 ทันเน็ลลิ่งโปรโตคอล (L2TP) จะถูกใช้เพื่อทัลเนิลยูสเซอร์ทราฟฟิคผ่านเครือข่ายที่ไม่ปลอดภัยตัวอย่างเช่น ใช้อินเทอร์เน็ตรีโมทไปยังเครือข่ายท้องถิ่นหรือเครือข่ายขององค์กร โดยมีวัตถุประสงค์หลักสำหรับการเริ่มต้น L2TP ทัลเนิลใน GGSN ที่มีสภาพแวดล้อมที่เชื่อมต่อจุดต่อจุดระหว่าง UEs และ LAC ผ่านเครือข่ายที่ไม่ปลอดภัย มาตรฐาน L2TP (RFC 2661) ที่พัฒนามาจากการโปรโตคอลที่เจ้าของแตกต่างกันเช่น เลเยอร์ 2 ฟอร์เวิร์ดดิ่ง(L2F) และพอยท์ทู

พอยท์ทันเน็ลลิ่งโปรโตคอล (PPTP) ที่รองรับเซสชัน PPP, ที่ด้านบนของ UDP หรือด้านบนของโปรโตคอลลิงค์เลเยอร์เช่น Frame Relay (FR) และ ATM การดำเนินงาน L2TP มีการสนับสนุนใน GRPS และ UMTS คอร์เน็ตเวิร์คโดยมาตรฐาน รีลีส98 และ รีลีส99 ดังนั้น GGSN ต้องรอรับ PPP – PDP คอนเท็ก

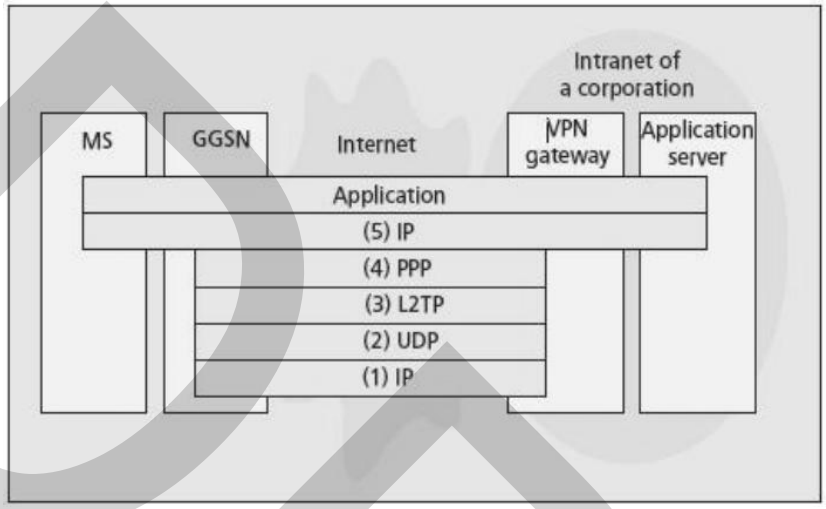
L2TP ทัลเนิลจะเริ่มระหว่าง GGSN และเราเตอร์อื่น โดยปกติขอบเราเตอร์ที่ทำงานร่วมกันสามารถเห็นได้ในรูปที่ ก6 ในระหว่างสถานการณ์ที่ L2TP, ผู้ใช้มือถือกำลังเชื่อมต่อกับ APN ซึ่งระบุไว้สำหรับ GGSN คือการสร้างเซสชัน PPP ยูซเซอร์แพ็คเก็ตจะห่อหุ้มและส่งผ่านเซสชันเหล่านี้ GGSN จะทำหน้าที่เป็น L2TP แอคเซสคอนเซนเทเตอร์ (LAC) ทันทีที่ PDP คอนเท็คเปิดใช้งาน แล้ว GGSN จะแบ่งออกลง GTP ทัลเนิล และใช้ L2TP เพื่อขนส่งแพ็คเก็ต PPP ไปยังคอร์เพอเรจ L2TP เน็ตเวิร์คเซิร์ฟเวอร์ (LNS) โดย LNS จะดำเนินการตรวจสอบและจะกำหนดคอร์เพอเรจ IP แอดเดรสไปยังผู้ใช้โทรศัพท์มือถือ



รูปที่ ก6 L2TP-functionality in a packet core network

หนึ่งในข้อดีที่สำคัญของการใช้ L2TP ในเครือข่าย UMTS / GPRS ที่เป็นผู้ประกอบการเครือข่ายสามารถที่จะส่งทราฟฟิค UMTS / GPRS ผ่านเครือข่าย IP ให้กับลูกค้าของพวกเขาเพื่อให้มั่นใจว่าข้อมูลจะถูกเก็บไว้บนมือถือนอกเหนือจากการจราจรอื่น ๆ ที่อยู่บน PDN ขอดีอื่น ๆ ในการใช้ L2TP ก็คือว่าเราเตอร์ในด้านอื่น ๆ ของทัลเนิ่ลเครือข่ายลูกค้าที่รองรับการจัดสรรไอพีแอสเดรสและตรวจสอบผู้ใช้สำหรับโมบายทัลมิเนิลแทน GGSN ซึ่งอยู่ในเครือข่ายผู้ประกอบการ ในวิธีนี้เครือข่ายภายนอกที่ต้องการที่จะรักษาความปลอดภัยจะได้ไม่ต้องไว้วางใจบุคคลที่สามสำหรับยูซเซอร์ของพวกเขาในเรื่องการยืนยันตัวตนและการจัดสรรไอพีแอสเดรส หมายความว่าผู้ใช้มือถือ

เป็นขององค์กรธุรกิจอาจได้รับไอพีแอสเดรสจากเครือข่ายขององค์กรแทนไอพีแอสเดรสที่ให้โดย GGSN



รูปที่ ก7 L2TP tunnelling

แม้ว่า L2TP สามารถนำเสนอการรักษาความปลอดภัยของการตรวจสอบการเชื่อมโยง CHAP ของการควบคุมการเชื่อมต่อ L2TP, มันเป็นไปไม่ได้อย่างเต็มที่รักษาความปลอดภัยตั้งแต่ทัลเนิ่นไฮแจ็คยังคงเป็นไป IPSec สามารถใช้ที่ด้านบนของ L2TP ในการสั่งเพื่อให้เป็นทัลเนิลที่ปลอดภัยอย่างเต็มที่

L2TP ไม่ได้เป็นวิธีการทัลเนิลลิ่งเท่านั้น IP-in-IP ทัลเนิลลิ่งและ Generic Routing Encapsulation (GRE) ทัลเนิลลิ่งคือสองวิธีที่สามารถใช้สำหรับการทัลเนิลลิ่งใน UMTS สำหรับ IP-in-IP ของผู้ใช้ไอพีแพ็กเก็ต ที่ห่อหุ้มในทัลเนิลไอพีแพ็กเก็ตและสำหรับ GRE ทัลเนิลลิ่งแพ็คเก็ตสามารถบรรจุแพ็คเก็ตของผู้ใช้ด้วยโปรโตคอลที่แตกต่างกันเช่น IP หรือ PPP ตารางที่ ก1 แสดงให้เห็นถึงคุณสมบัติของวิธีการทัลเนิ่ลลิ่งทั้งสามที่เป็นไปได้ ทั้งหมดสามวิธีที่ใช้งานสำหรับ MS ที่สนับสนุนทั้ง PPP และ IP นอกจากนี้หากผู้ใช้โปรแกรมเท่านั้นที่สนับสนุน PPP, GRE ทัลเนิ่ลลิ่งเป็นตัวเลือกที่ดีที่สุด แต่ถ้าโปรโตคอลลิงค์เลเยอร์เป็น FR หรือ ATM แล้ว L2TP จะต้องเลือก แต่เป็นผลมาจากในระยะสั้นโปรโตคอลโอเวอร์เฮด IP-in-IP ทัลเนิลลิ่งที่มีประสิทธิภาพที่ดีขึ้น

ตารางที่ ก1 Tunneling methods

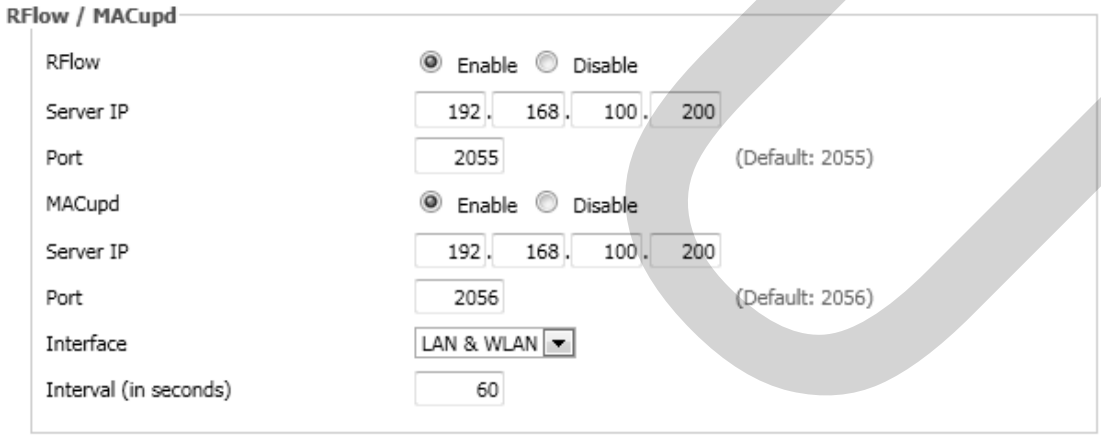
Tunnelling method	Overhead	Transport network protocol support	MS protocol support
IP-in-IP	Low	IP	IP
GRE	Medium	IP	PPP
L2TP	High	IP/UDP, FR, ATM	IP

การใช้ RFlow Collector และ MySQL ในการจัดเก็บข้อมูลทราฟฟิค

เราสามารถใช้เราเตอร์ที่มีเฟริมแวร์ DD-WRT ส่งข้อมูลทราฟฟิคไปยังเครื่องพีซีที่อยู่ในเน็ตเวิร์คและเก็บข้อมูลทราฟฟิคลงฐานข้อมูล MySQL โดยมีขั้นตอนก่อนติดตั้งดังต่อไปนี้

1) ตั้งค่าเราเตอร์ให้ส่งข้อมูลทราฟฟิคไปยังเครื่องพีซี

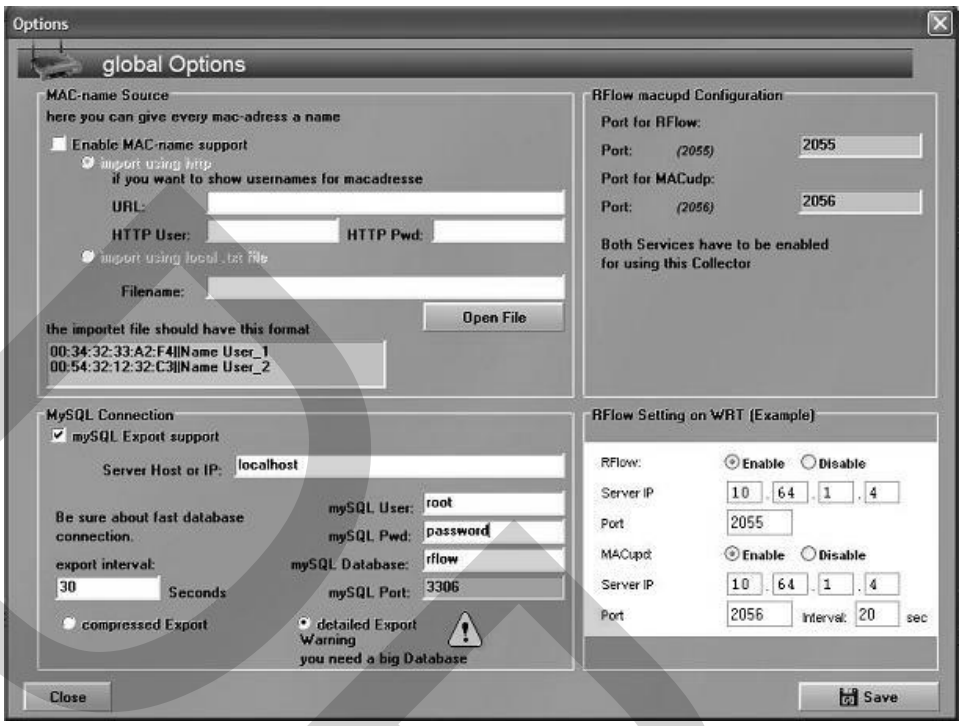
เริ่มต้นโดยการล๊อกอินเข้าไปยังเราเตอร์แล้วไปที่เมนู “Services” แล้วไปที่ “RFlow / MACupd” โดยทำการเปิดการใช้งาน RFlow / MACupd โดยที่ตั้งค่า Server IP คือเครื่องคอมพิวเตอร์ที่ Run โปรแกรม RFlowCollector ดังรูปที่ ก8 หลังจากนั้นกดปุ่ม “Save Settings” ที่อยู่ด้านล่าง



รูปที่ ก8 RFlow/MACupd

2) ตั้งค่าโปรแกรม RFlowCollector

เปิดโปรแกรม RFlowCollector แล้วทำการกำหนดค่า My SQL Connection เพื่อกำหนดค่าฐานข้อมูล เพื่อให้มีการ Export ข้อมูลไปยัง mySQL ที่เราติดตั้งไว้ดังรูปที่ ก9



รูปที่ ก9 หน้าต่าง RFlowCollector

3) ตั้งค่า MySOL

ใช้โปรแกรม phpMyAdmin สร้างฐานข้อมูลใหม่ชื่อว่า rflow ต่อจากนั้น Table ตาม script ต่อไปนี้

```
CREATE TABLE akteth (
ID int(11) NOT NULL auto_increment,
ip varchar(17) NOT NULL default ,
mac varchar(17) NOT NULL default ,
status char(1) NOT NULL default ,
lasttraffic int(11) NOT NULL default '0',
name varchar(100) NOT NULL default ,
device varchar(10) NOT NULL default ,
PRIMARY KEY (ID)
)

CREATE TABLE aktrouter (
ID int(11) NOT NULL auto_increment,
```

```
ip varchar(17) NOT NULL default ,
flowsequenz int(11) NOT NULL default '0',
lastflow varchar(7) NOT NULL default '0',
ploss int(11) NOT NULL default '0',
PRIMARY KEY (ID)
)
```

การติดตั้งเฟริม์แวร์ DD-WRT กับอุปกรณ์ Linksys WRT54GL

การติดตั้ง DD-WRT ซึ่งเป็น Linux-based firmware ของอุปกรณ์ประเภท Wireless AP หรือ Router เพื่อเพิ่มประสิทธิภาพการทำงาน และมีคุณสมบัติอื่นๆ มากกว่าที่มีใน firmware ที่ติดตั้งมาพร้อมกับอุปกรณ์มีขั้นตอนดังต่อไปนี้

1. ทำการรีเซตเราเตอร์ด้วยวิธี Hard reset 30/30/30 เพื่อป้องกันปัญหาที่เกิดขึ้น ก่อนและหลังการติดตั้งหรือ upgrade เพื่อเคลียร์ NVRAM ของอุปกรณ์ โดยมีขั้นตอนดังนี้

เปิดอุปกรณ์ไว้ซักพัก จนกว่าอุปกรณ์ใช้งานได้ตามปกติ

1.1 ในระหว่างที่อุปกรณ์เปิดอยู่ กดปุ่ม reset ค้างไว้ 30 วินาที

1.2 ดึงสายหม้อแปลง power ออก โดยที่ยังกดปุ่ม reset ค้างไว้อีก 30 วินาที

1.3 ต่อสายหม้อแปลง power กลับ โดยที่ยังกดปุ่ม reset ค้างไว้อีก 30 วินาที แล้วปล่อย

โดยหลังจากการทำ Hard reset อุปกรณ์จะเปลี่ยนคอนฟิกกลับไปเป็นค่าดีฟอลต์โดยมีไอพี แอดเดรสเป็น 192.168.1.1 ชื่อผู้ใช้งานและรหัสผ่านมีค่าเป็น Admin

2. อัพเกรดเฟริมแวร์โดยผ่านหน้าเว็บล๊อกอินไปยังเราเตอร์โดยทำตามขั้นตอนดังต่อไปนี้

2.1 คลิกที่เมนู Administration

2.2 คลิกเลือกเมนูย่อย Firmware Upgrade

2.3 เลือก Browse และเลือกไฟล์ที่ต้องการอัพเกรดเฟิร์มแวร์ที่ดาวน์โหลดมา

2.4 กดปุ่ม Upgrade

2.5 เราเตอร์จะใช้เวลาในการอัพโหลดไฟล์และทำการแฟลชเฟริมแวร์สักครู่

2.6 หลังจากโหลดเสร็จจะขึ้นข้อความ Upgrade is successful

3.ทำการรีเซตอีกรอบด้วยการ กดปุ่ม Reset ทางด้านหลังอุปกรณ์ค้างไว้ประมาณ 30 วินาที เพื่อให้ระบบคืนค่าเฟริมเวร์ให้เป็นแบบ Factory Defaults ของระบบเดิม

คุณลักษณะของเฟริมแวร์ DD-WRT ของแต่ละเวอร์ชั่น

ตารางที่ ก2 คุณลักษณะของเฟริมแวร์แต่ละเวอร์ชั่น

Features	Micro (2 MB)	Mini	Nokaid	Standard	STD Nokaid
Access restrictions	Yes	Yes	Yes	Yes	Yes
AnchorFree	Yes	Yes	Yes	Yes	Yes
Bandwidth monitoring	Yes	Yes	Yes	Yes	Yes
ChilliSpot			Yes	Yes	
Dynamic DNS	Yes	Yes	Yes	Yes	Yes
HTTPS option for web management			Yes	Yes	Yes
IPv6			Yes		Yes
JFFS2		Yes	Yes		Yes
XLink Kai (kaid)				Yes	
MMC/SD card support			Yes	Yes	Yes
NoCat			Yes	Yes	Yes
OpenVPN					
PPTP Client/Server		Yes	Yes	Yes	Yes
Quality of service	Yes	Yes	Yes	Yes	Yes
radvd			Yes	Yes	Yes
repeater	Yes	Yes	Yes	Yes	Yes
RFlow			Yes	Yes	Yes
Samba/CIFS client			Yes	Yes	Yes
SNMP			Yes	Yes	Yes
SPI firewall/IPtables	Yes	Yes	Yes	Yes	Yes
SSH		Yes	Yes	Yes	Yes

ตารางที่ ก2 (ต่อ)

Features	Micro (2 MB)	Mini	Nokaid	Standard	STD Nokaid
Telnet	Yes	Yes	Yes	Yes	Yes
Transmit (Tx) power adjustment	Yes	Yes	Yes	Yes	Yes
UPnP	Yes	Yes	Yes	Yes	Yes
Wake-on-LAN	Yes	Yes	Yes	Yes	Yes
WPA/WPA2 personal/enterprise	Yes	Yes	Yes	Yes	Yes
Wiviz		Yes	Yes	Yes	Yes
Access restrictions	Yes	Yes	Yes	Yes	Yes

ประวัติผู้เขียน

ชื่อ-นามสกุล	นาย ภาณุพงศ์ สายไพศรี
วัน เดือน ปีเกิด	20 มกราคม 2526
ประวัติการศึกษา	สำเร็จการศึกษาระดับปริญญาตรี วิทยาศาสตรบัณฑิต สาขาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยราชภัฏเทพสตรี ปีการศึกษา 2552
ตำแหน่งและสถานที่ทำงานปัจจุบัน	วิศวกรระบบ บริษัท แวสว็อกซ์ จำกัด 98 อาคารสาธรสแควร์ ถนนสาธรเหนือ แขวงสีลม เขตบางบางรัก กรุงเทพมหานครฯ 10500