รายงานการใช้งานระบบเครือข่ายคอมพิวเตอร์ มหาวิทยาลัยเทคโนโลยีสุรนารี

1 เมษายน – 30 เมษายน 2560

1. **<u>รายงานการดำเนินงานของฝ่ายเครือข่าย</u>**

1.1 สรุปการดำเนินการบนระบบเครือข่าย SUTnet

- แก้ไขปัญหาระบบเครือข่ายวันที่ 9 เมษายน 2560 โดยได้รับแจ้งจากนักศึกษาว่าไม่สามารถใช้งานเว็บไซต์ภายนอกมหาวิทยาลัยได้ จึงทำการตรวจสอบพบสาเหตุจาก software version ของ firewall ได้ทำการแก้ไข bug เรียบร้อยแล้ว
- monitor ระบบเครือข่าย ช่วงวันสงกรานต์ 13-17 เมษายน 2560 ให้อยู่ในสถานะปกติ
- แก้ไขปัญหาระบบเครือข่ายวันที่ 24 เมษายน 2560 ตรวจสอบพบการใช้งาน internet มีอาการหน่วงและทำงานช้าผิดปรกติ พบสาเหตุจากอุปกรณ์ Authen มีปัญหา ได้ทำการแก้ไข โดยการตั้งค่าอุปกรณ์ใหม่ จึงสามารถใช้งาน internet ได้ตามปกติ
- Uninet ได้เพิ่มความเร็ว internet ฝั่ง uninet จากเดิม 3 Gbps เป็น 4 Gbps วันที่ 28เมษายน 2560 แล้วเสร็จ
- นำ ups เปลี่ยนทดแทน ups ตัวเก่าที่ไม่สำรองไฟ ที่ห้อง network อาคารวิชาการ 1 ชั้น 2

1.2 สรุปการดำเนินการบนระบบเครือข่ายไร้สาย SUT-wifi

- นำ access point และ switch สำรองติดทดแทนอุปกรณ์ที่ได้รับความเสียหายจากพายุฤดูร้อน เมื่อช่วงค่ำของวันที่ 26 มีนาคม 2560 ที่ผ่านมา เนื่องจากเกิดไฟดับ-ไฟกระชาก ส่งผลให้อุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) ได้รับความเสียหาย รวมทั้งหมด 19 จุด ดังบริเวณต่อไปนี้
  - อาคารหอพักนักศึกษา (S9) ชำรุด 7 จุด และอุปกรณ์กระจายสัญญาณระบบเครือข่าย(Switch) 1 ตัว
  - อาคารหอพักนักศึกษา (S10) ชำรุด 9 จุด และอุปกรณ์ประจายสัญญาณระบบเครือข่าย(Switch)1 ตัว
  - อาคารเรียนรวม 1 ชำรุด 3 จุด
- ติดตั้ง Access Point ใหม่ รุ่น AIR-AP1832I-S-K9
  1. อาคารเรียนรวม 1 จำนวน 18 เครื่อง
  2. อาคารเรียนรวม 2 จำนวน 4 เครื่อง
  3. อาคารวิชาการ 1 จำนวน 1 เครื่อง
  4. อาคารบรรณสาร 1-2 จำนวน 5 เครื่อง
  5. อาคารสุรเริงไชย จำนวน 3 เครื่อง

6. ที่หอพักนักศึกษา จำนวน 55 เครื่อง ได้แก่

- 6.1 หอพักนักศึกษา 7 จำนวน 5 เครื่อง
- 6.2 หอพักนักศึกษา 8 จำนวน 7 เครื่อง
- 6.3 หอพักนักศึกษา 9 จำนวน 10 เครื่อง
- 6.4 หอพักนักศึกษา 10 จำนวน 13 เครื่อง
- 6.5 หอพักนักศึกษา 11 จำนวน 10 เครื่อง
- 6.6 หอพักนักศึกษา 12 จำนวน 10 เครื่อง

- เปลี่ยน Access Point จากรุ่นเดิม เป็นรุ่น AIR-AP1832I-S-K9 จำนวน 4 เครื่อง ที่ อาคารวิจัย

1.3 สรุปการดำเนินการบนระบบ Internet Data Center

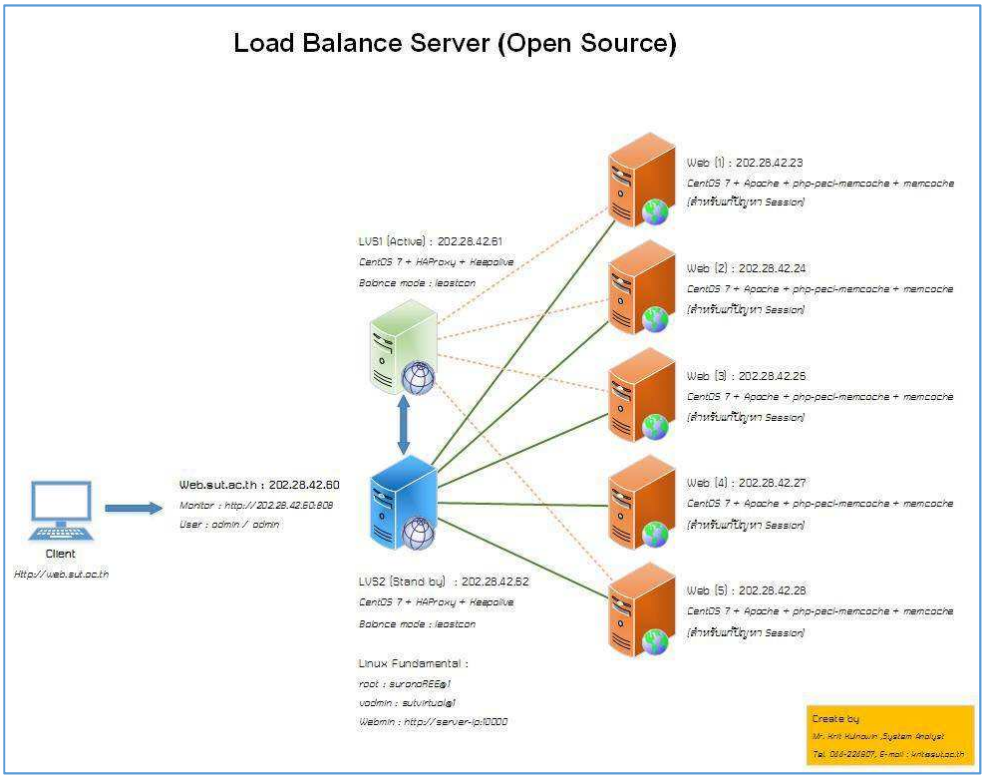
- แก้ไขปัญหาระบบจัดเก็บข้อมูลชนิด VSAN โดยระบบมี warning เกี่ยวกับความถูกต้องของข้อมูล metadata ที่จัดเก็บใน Disk group ของ Vmserver4 ไม่ถูกต้อง แก้ไขโดยสั่ง full migrate vmserver4 แล้วทำการปลด vmserver4 ออกจาก vsan cluster และทำการลบ disk group ของ vmsareve4 ออก แล้วแบ่ง diskgroup ใหม่ จากนั้น join กลับเข้า vsan cluster และสั่ง rebalance ข้อมูล ทำให้สามารถใช้งานได้ตามปกติ
- ต้อนรับนักศึกษาดูงานห้อง Internet Data Center จากสาขาวิชา IT จำนวน 40 คน เมื่อวันที่ 19 เมษายน 2560

1.4 สรุปการดำเนินการบนระบบโทรศัพท์

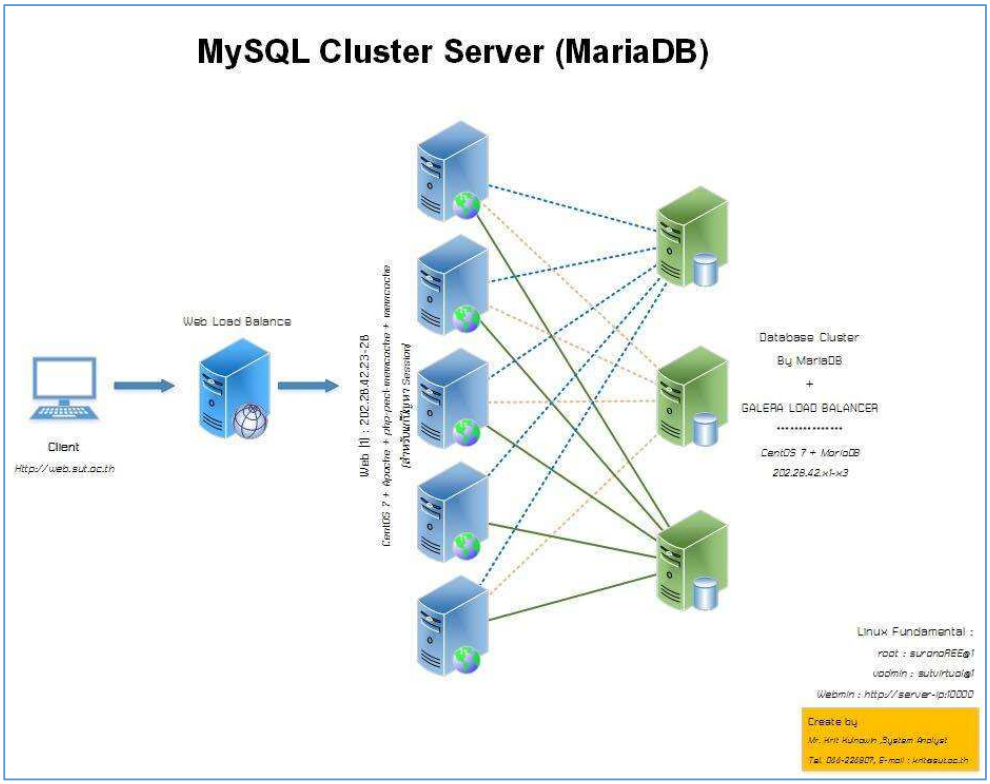
- ซ่อมบำรุงระบบโทรศัพท์อาคารวิชาการ 1 จากเหตุขัดข้องในการใช้งานโทรศัพท์เมื่อวันจันทร์ที่ 24 เมษายน 2560 โดยเกิดจากอุปกรณ์พักหรือกระจายสัญญาณระบบโทรศัพท์ที่ใช้งานมาตั้งแต่ก่อสร้างอาคารวิชาการ 1 ชำรุดและเกิดความเสียหายเนื่องจากแสงแดดและความร้อน ทำให้พลาสติกแผงกระจายกรอบ และเมื่อได้ตรวจสอบจึงจำเป็นต้องทำการรื้อสายทั้งหมดและพบว่าสายสัญญาณโทรศัพท์เกิดความเสียหายบางส่วนด้วย จึงทำให้ต้องมีการตัดต่อและรื้อสายสัญญาณโทรศัพท์ทั้งหมด 419 คู่สาย ทำให้สามารถใช้งานได้ตามปกติ
- ติดตั้งระบบโทรศัทพ์แบบ IP-Phone แทนระบบเก่า ณ หน่วยประสานงานมทส.-กทม. ให้เจ้าหน้าที่ จำนวน 12 เครื่อง / 12 เลขหมาย

1.5การดำเนินการอื่นๆ

- จัดสร้าง ระบบ web load balance เพื่อแก้ไขปัญหา web server ล่มบ่อย



- ปรับปรุงระบบ MySQL Cluster โดยยกเลิกการให้บริการ MysQL Cluster ระบบเก่า ย้ายฐานข้อมูลสู่ Mysql Server ตัวใหม่ และอยู่ในระหว่างการจัดสร้างระบบ MySQL Cluster ระบบใหม่

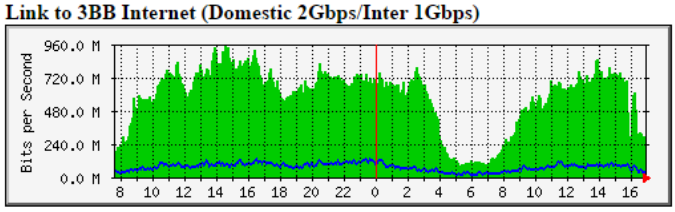


- สร้าง ftp server : webadmin.sut.ac.th สำหรับให้บริการ ftp โดยเฉพาะ สำหรับผู้ใช้งานบน server : web.sut.ac.th
- สร้างช่องทางการติดต่อสื่อสาร เพื่อกระจายข่าวสารเกี่ยวกับระบบเครือข่ายของมหาวิทยาลัย ผ่าน application Line เพื่อเป็นช่องทางหนึ่งสำหรับการแจ้งปัญหาการใช้งานอินเตอร์เน็ตของมหาวิทยาลัย ID : @sut.network
- จัดสรร internet account สำหรับงานอบรม ส่วนส่งเสริมวิชาการ 25 account
- เพิ่ม vpn account สำหรับสถานวิจัยแสงซินโครตรอน อีก 1 account เพื่อใช้งานทรัพยากรสารสนเทศออนไลน์จากภายนอก มทส.
- จัดสรรพื้นที่เว็บไซต์ http://bnct.sut.ac.th
- จัดสรร certificate สำหรับ server : tace.sut.ac.th
- จัดสรร certificate สำหรับ server : reg-sws.sut.ac.th

2.รายงานการใช้งานระบบเครือข่าย

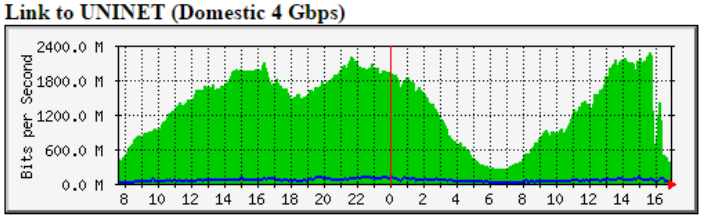
Internet Gateway Traffic

Link to 3BB Internet (Domestic 2Gbps/Inter 1Gbps)



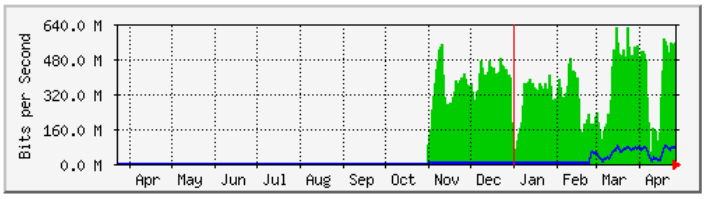
	Max	Average	Current
In	943.3 Mb/s (9.4%)	574.7 Mb/s (5.7%)	286.7 Mb/s (2.9%)
Out	131.8 Mb/s (1.3%)	70.9 Mb/s (0.7%)	30.6 Mb/s (0.3%)

Link to UNINET (Domestic 4 Gbps)



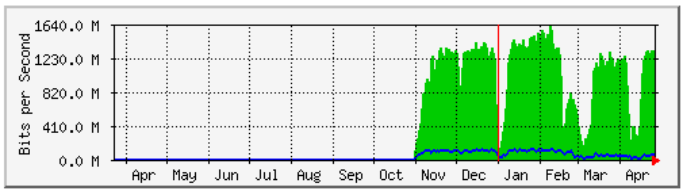
	Max	Average	Current
In	2262.4 Mb/s (22.6%)	1343.9 Mb/s (13.4%)	325.2 Mb/s (3.3%)
Out	118.1 Mb/s (1.2%)	54.0 Mb/s (0.5%)	42.4 Mb/s (0.4%)

`Yearly' Graph (1 Day Average)



	Max	Average	Current
In	623.9 Mb/s (6.2%)	345.7 Mb/s (3.5%)	552.8 Mb/s (5.5%)
Out	83.1 Mb/s (0.8%)	17.9 Mb/s (0.2%)	72.6 Mb/s (0.7%)

`Yearly' Graph (1 Day Average)



	Max	Average	Current
In	1609.6 Mb/s (16.1%)	1036.5 Mb/s (10.4%)	1314.5 Mb/s (13.1%)
Out	126.6 Mb/s (1.3%)	74.9 Mb/s (0.7%)	51.3 Mb/s (0.5%)

*ทางออก Uninet 4Gbps / 3BB Domestic 2 Gbps,Inter 1 Gbps) ข้อมูลเมื่อวันที่ 28 เม.ย. 60

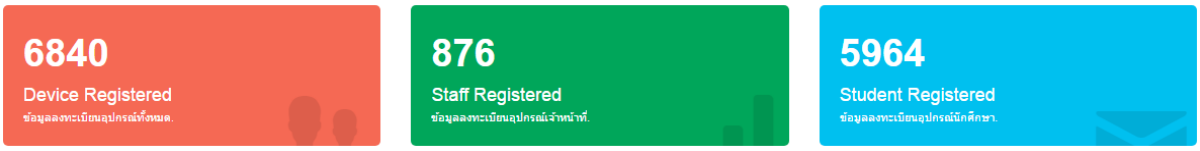
2.1 รายงานจำนวนผู้ใช้งานผ่านระบบเครือข่าย (LAN) (ไม่รวมห้องปฏิบัติการคอมฯ)

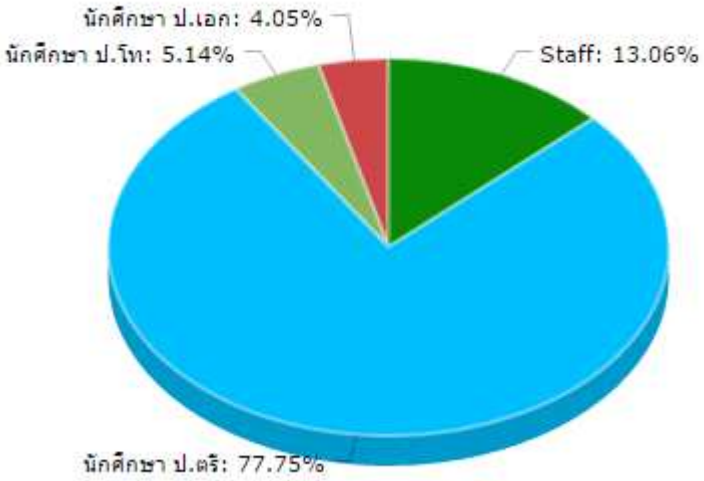
(ข้อมูลวันที่ 28 เม.ย 60)

วิธีการ	จำนวน
วิธีการแบบ NAC In-Band	307 คน
วิธีการแบบ ISE	1304 คน
รวมทั้งหมด	**1,611 คน**

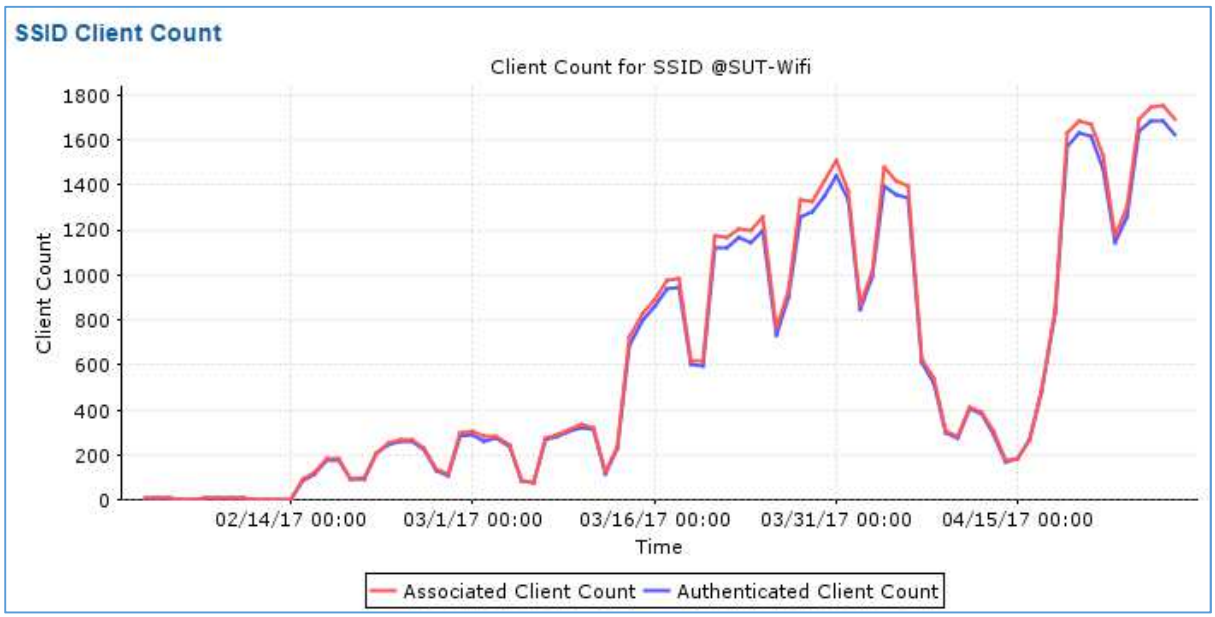
2.2 รายงานจำนวนผู้ใช้งานผ่านระบบเครือข่ายไร้สาย

2.2.1 จำนวนผู้ใช้งานเครือข่ายไร้สาย @SUT-Wifi

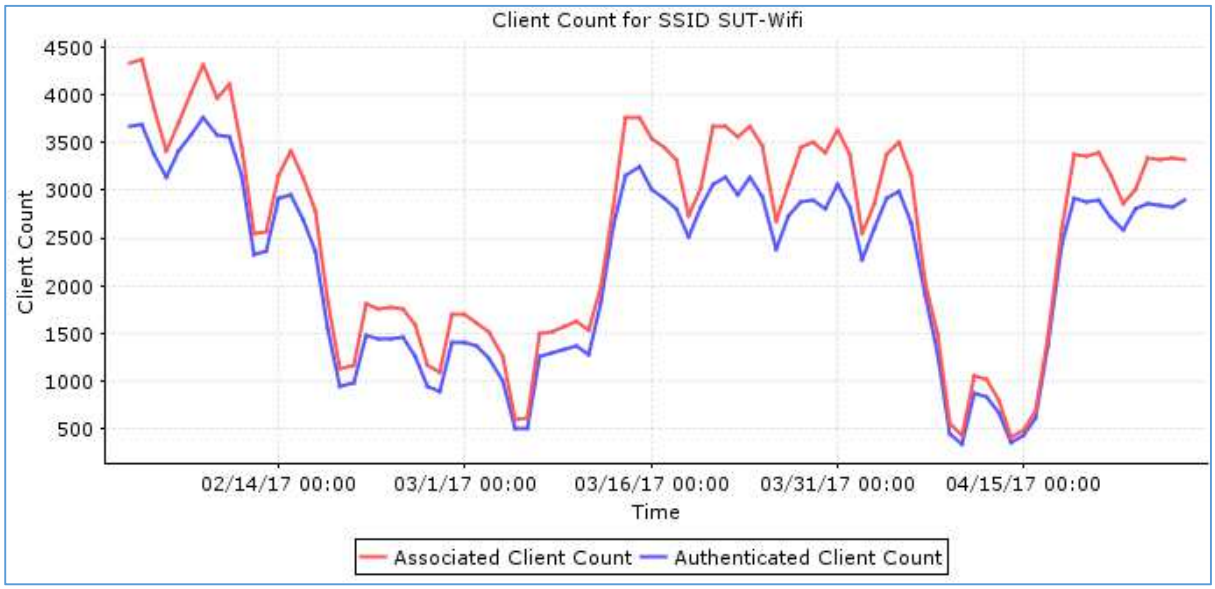




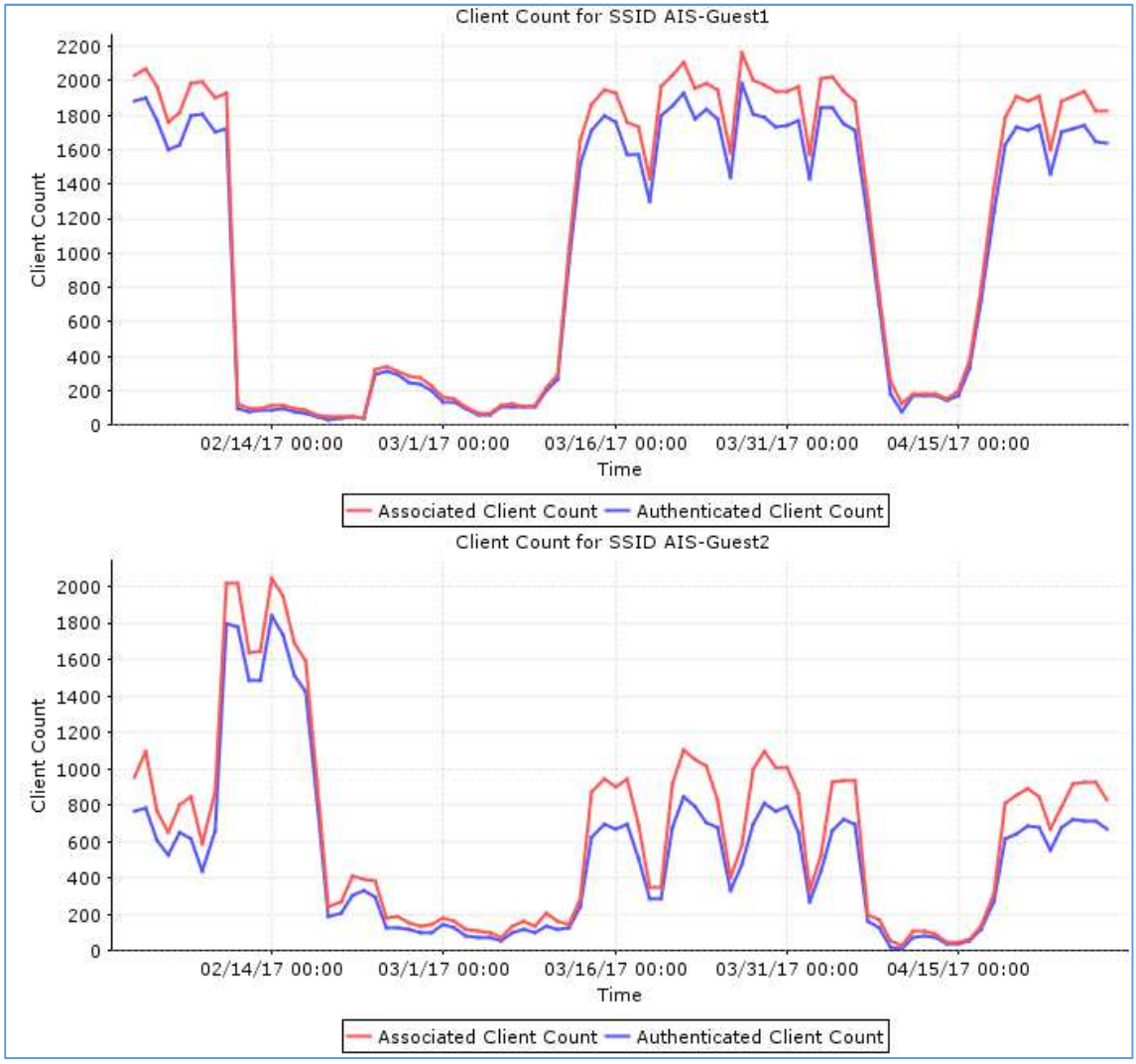
- จำนวนผู้ใช้งาน



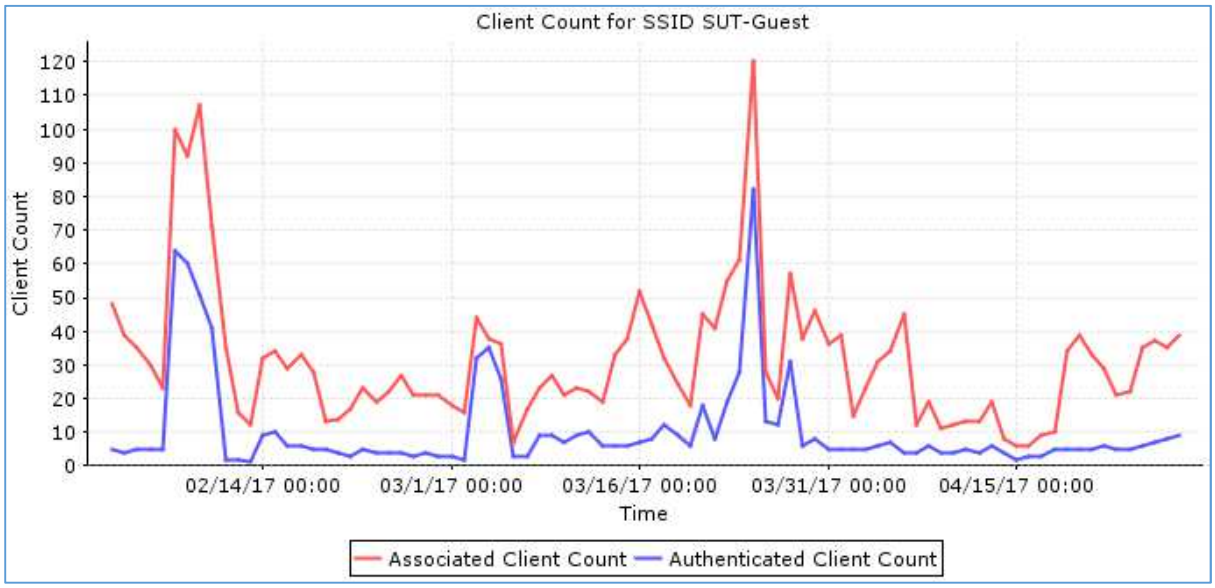
2.2.2 จำนวนผู้ใช้งานเครือข่ายไร้สาย SUT-Wifi



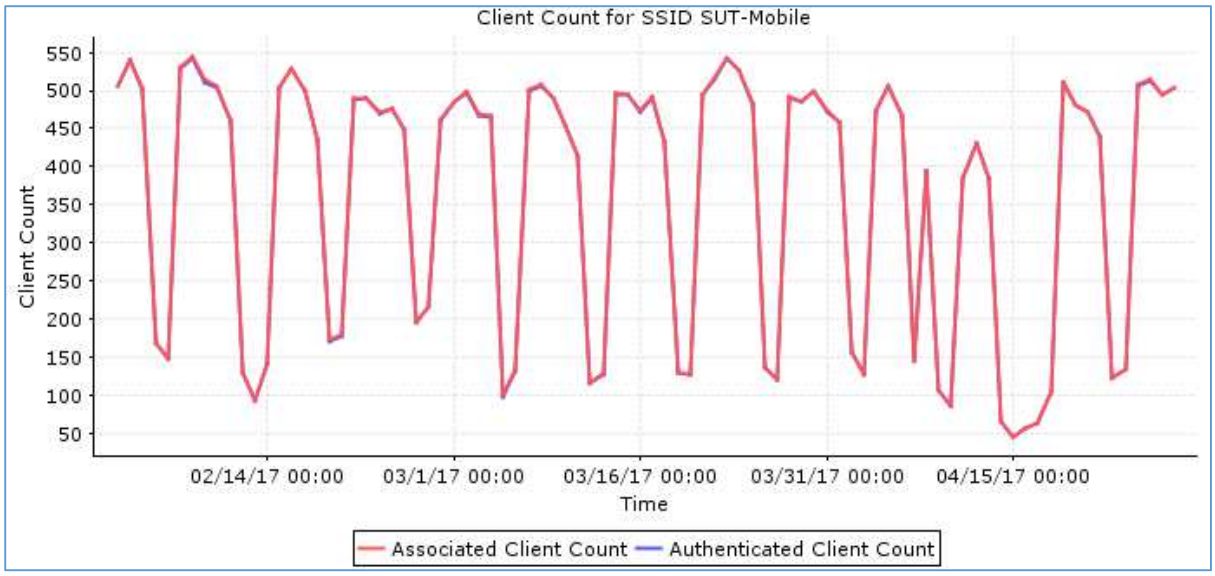
2.2.3 จำนวนผู้ใช้งานเครือข่ายไร้สาย SUT-AIS



2.2.4 จำนวนผู้ใช้งานเครือข่ายไร้สาย SUT-Guest



2.2.5 จำนวนผู้ใช้งานเครือข่ายไร้สาย SUT-Mobile



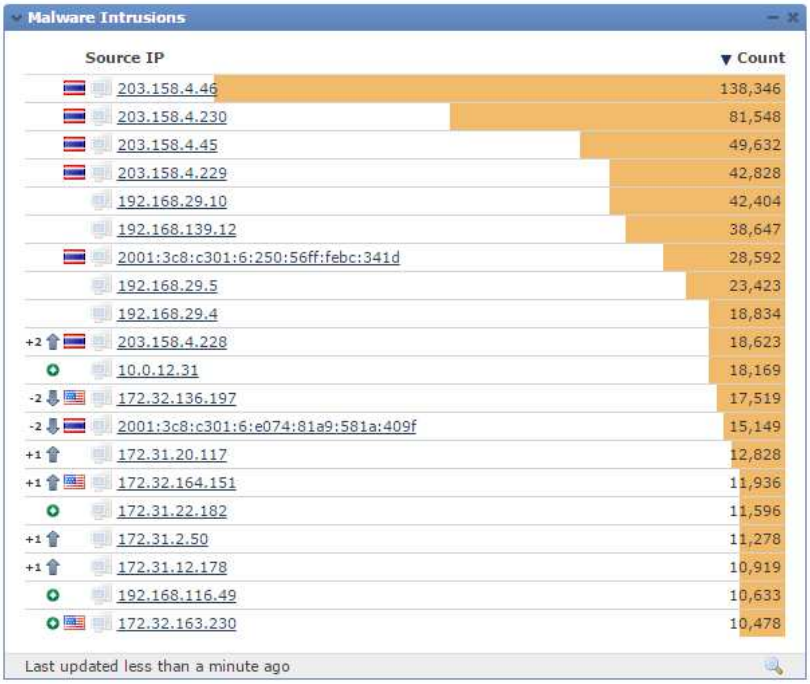
2.2.6 สรุปสถิติจำนวนผู้ใช้งานผ่านระบบ wireless ทั้งหมด

- ผู้ใช้งานผ่านระบบ wireless สูงสุด 6,601 คน/วัน
- ผู้ใช้งานผ่านระบบ wireless ต่ำสุด 735 คน/วัน
- ผู้ใช้งานผ่านระบบ wireless เฉลี่ย 4,279 คน/วัน

3. ภัยคุกคามระบบเครือข่าย

- **สถานะการณ์ไวรัสและมัลแวร์ที่แพร่ระบาดในมหาวิทยาลัย** (ข้อมูลย้อนหลัง 90วัน)

  (ที่มา : Sourcefire 203.158.4.43)



Malware Intrusions

	Source IP	▼ Count
	203.158.4.46	138,346
	203.158.4.230	81,548
	203.158.4.45	49,632
	203.158.4.229	42,828
	192.168.29.10	42,404
	192.168.139.12	38,647
	2001:3c8:c301:6:250:56ff:febc:341d	28,592
	192.168.29.5	23,423
	192.168.29.4	18,834
+2	203.158.4.228	18,623
	10.0.12.31	18,169
-2	172.32.136.197	17,519
-2	2001:3c8:c301:6:e074:81a9:581a:409f	15,149
+1	172.31.20.117	12,828
+1	172.32.164.151	11,936
	172.31.22.182	11,596
+1	172.31.2.50	11,278
+1	172.31.12.178	10,919
	192.168.116.49	10,633
	172.32.163.230	10,478

Last updated less than a minute ago

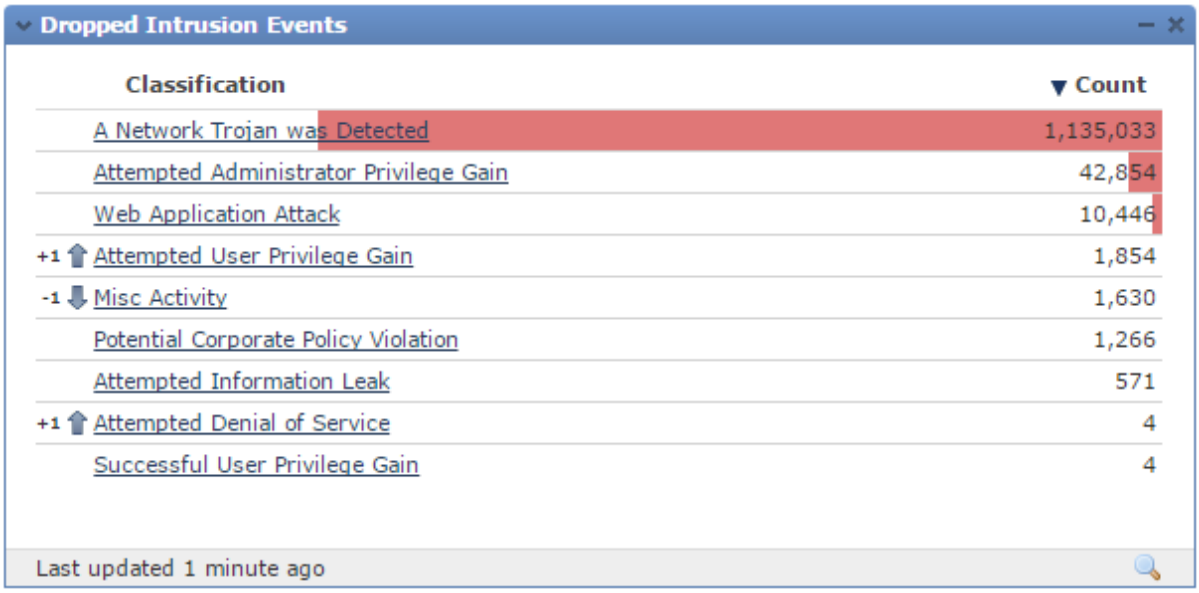
Malware Intrusions

	Message	▼ Count
	MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35030:1)	219,853
	MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35549:1)	207,474
	BLACKLIST suspicious .bit dns query (1:41083:1)	118,758
	MALWARE-CNC Win.Trojan.Andromeda variant outbound connection (1:33496:1)	70,860
+4	MALWARE-CNC Win.Trojan.Nirat variant outbound connection (1:25100:5)	51,949
-1	MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35746:1)	50,884
-1	BLACKLIST DNS request for known malware domain rvbwtbeitwjeitv.com (1:28060:1)	48,340
-1	BLACKLIST DNS request for known malware domain rterybrstutnrsbberve.com	47,499
-1	BLACKLIST DNS request for known malware domain erwbtkidthetcwerc.com (1:28058:1)	46,804
+2	MALWARE-CNC Win.Trojan.Glupteba.M initial outbound connection (1:30288:2)	33,069
+2	MALWARE-CNC Win.Trojan.Nvbpass variant outbound connection (1:19864:5)	32,889
+3	MALWARE-CNC Torpig bot sinkhole server DNS lookup (1:16693:5)	27,886
-2	BLACKLIST DNS request for known malware domain xa.yessearches.com -	26,307
+3	MALWARE-CNC Win.Trojan.Zbot variant in.php outbound connection (1:26023:3)	23,775
+4	MALWARE-CNC Win.Trojan.Pmabot outbound connection (1:37213:3)	21,583
-6	MALWARE-CNC Win.Trojan.Fareit variant outbound connection (1:27775:4)	17,550
	MALWARE-CNC Win.Trojan.Jenxcus outbound connection attempt with unique User-Agent	11,616
+7	MALWARE-CNC Win.Trojan.Jaktinier outbound connection (1:31459:3)	9,881
+2	BLACKLIST User-Agent known malicious user-agent string RookIE/1.0 (1:18388:10)	8,541
-6	BLACKLIST DNS request for known malware domain ltc.give-me-coins.com (1:31660:1)	7,901

Last updated less than a minute ago

- **การยับยั้งการโจมตีบนระบบเครือข่าย โดย อุปกรณ์ IPS** (ข้อมูลย้อนหลัง 90วัน)

  (ที่มา : Sourcefire 203.158.4.43)



- **การยับยั้งการโจมตีบนระบบเครือข่าย โดย อุปกรณ์ Firewall** (ข้อมูลย้อนหลัง 30วัน)

  (ที่มา Paloalto:203.158.4.110)