รายงานการใช้งานระบบเครือข่ายคอมพิวเตอร์ มหาวิทยาลัยเทคโนโลยีสุรนารี

ประจำเดือน กันยายน 2561

รายงานการดำเนินงานของฝ่ายโครงสร้างฯ

1.1 สรุปการดำเนินการบนระบบเครือข่าย SUTnet

1.2 สรุปการดำเนินการบนระบบเครือข่ายไร้สาย

1.3 สรุปการดำเนินการบนระบบ Internet Data Center

1.4 สรุปการดำเนินการบนระบบโทรคมนาคม

1.5 สรุปการดำเนินการด้านงานบริการคอมพิวเตอร์

รายงานการใช้งานระบบเครือข่าย

2.1 รายงานจำนวนผู้ใช้งานผ่านระบบเครือข่าย (LAN) (ไม่รวมห้องปฏิบัติการคอมฯ)

2.2 รายงานจำนวนผู้ใช้งานผ่านระบบเครือข่ายไร้สาย

2.2.1 จำนวนผู้ใช้งานเครือข่ายไร้สาย @SUT-Wifi

2.2.2 จำนวนผู้ใช้งานเครือข่ายไร้สาย SUT-Wifi

2.2.3 จำนวนผู้ใช้งานเครือข่ายไร้สาย @SUT-Guest

2.2.4 จำนวนผู้ใช้งานเครือข่ายไร้สาย eduroam

2.2.5 จำนวนผู้ใช้งานเครือข่ายไร้สาย @SUT-IoT

2.2.6 จำนวนผู้ใช้งานผ่านระบบ AIS

2.2.7 สรุปสถิติจำนวนผู้ใช้งานผ่านระบบ wireless ทั้งหมด

ภัยคุกคามระบบเครือข่าย

สถานะการณ์ไวรัสและมัลแวร์ที่แพร่ระบาดในมหาวิทยาลัย

การยับยั้งการโจมตีบนระบบเครือข่าย โดย อุปกรณ์ Next Gen Firewall

การใช้งาน Application (Top20)

- **<u>รายงานการดำเนินงานของฝ่ายโครงสร้างฯ</u>**

1.1 สรุปการดำเนินการบนระบบเครือข่าย SUTnet

- (4ก.ย.61) ทำการ reboot firewall เมื่อเวลา 12.30-12.45 น. เนื่องจากระบบแจ้งเกี่ยวกับระบบ file system
- (14 ก.ย.61) ตรวจพบ traffic ไม่ออกฝั่ง AIS ตั้งแต่16.30 น. - ถึง 8.30 น. วันที่ 15 ก.ย. เจ้าหน้าที่ทำการ clear route ทำให้ traffic internet ออกทั้งสองช่องทางตามปกติ ทั้งนี้ไม่มีผลกระทบต่อผู้ใช้งาน
- (24 ก.ย.) ตรวจพบ traffic ไม่ออกฝั่ง AIS ตั้งแต่ช่วงกลางคืนของวันเสาร์ที่ 22ก.ย.- เวลา 8.30 น. วันที่ 24 ก.ย. เจ้าหน้าที่ทำการ clear route ทำให้ traffic internet ออกทั้งสองช่องทางตามปกติ ทั้งนี้ไม่มีผลกระทบต่อผู้ใช้งาน

- งานตามระบบแจ้งซ่อม

เลขที่ใบงาน	รายละเอียดงานซ่อมแซมระบบเครือข่าย	ผู้รับงาน
610903-11-1	สำนักงานไม่มีสัญญาณ / สัญญาณขาดหาย	ณัฐวัฒน์
610906-7-1	สำนักงานไม่มีสัญญาณ / สัญญาณขาดหาย	ณัฐวัฒน์
610906-13-1	สำนักงานไม่มีสัญญาณ / สัญญาณขาดหาย	ณัฐวัฒน์
610907-6-1	ซ่อมบำรุงสายสัญญาณ และขยายจุดบริการเครือข่าย	ณัฐวัฒน์
610912-3-1	สำนักงานไม่มีสัญญาณ / สัญญาณขาดหาย	ณัฐวัฒน์
610912-14-1	ตรวจสอบสัญญาณอินเทอร์เน็ต สำหรับการใช้ระบบ Video conference ทางไกล เพื่อสำหรับการเรียนการสอน	ณัฐวัฒน์
610912-20-1	สำนักงานไม่มีสัญญาณ / สัญญาณขาดหาย	สมบัติ
610905-3-1	ลง Windows	วัฒนา
610911-16-1	Activate Windows, ชี้ KMS Server	วัฒนา
610913-4-1	Repair OS windows	วัฒนา
610924-2-1	Activate Windows, ชี้ KMS Server	วัฒนา
610903-17-1	Set dot1x	วัฒนา
610904-5-1	โปรแกรมค้าง ไม่สามารถใช้งานได้	วัฒนา

1.2 สรุปการดำเนินการบนระบบเครือข่ายไร้สาย

- (21 ก.ย.61) ตรวจสอบพบ การใช้งาน internet ระบบเครือข่ายไร้สาย @SUT-Wifi มีอาการหน่วงเป็นระยะๆ พบปัญหา flapping ระหว่าง wireless controller ทั้งนี้แจ้งปัญหาให้ผู้เกี่ยวข้องทราบเพื่อหาแนวทางแก้ไขแล้ว
- งานตามระบบแจ้งซ่อม

เลขที่ใบงาน	รายละเอียดงานซ่อมแซมระบบเครือข่าย	ผู้รับงาน
610903-10-1	สำนักงานไม่มีสัญญาณ / สัญญาณขาดหาย	สมชาย/วสันต์

1.3 สรุปการดำเนินการบนระบบ Internet Data Center

- สืบเนื่องจากการ reboot firewall ทำให้ server ที่มีการ mapping storage ไม่สามารถมองเห็น storage ได้ ทำให้ server บางตัวหยุดทำงาน แก้ไขโดย restart server หลังจาก reboot firewall ทำให้สามารถใช้งานได้ตามปกติ
- Vmserver 7 ฟ้อง harddisk fail แก้ไขโดยเข้า maintenance mode และสั่ง reboot แบบcold boot ทำให้สามารถใช้งานได้ตามปกติ
- Vmserver 32 ขึ้น pink screen ไม่สามารถใช้งานได้ตามปกติ มีการแฮงค์ จึงทำการ ถอดปลั๊กและทำการ reboot ระบบใหม่ ส่งผลกระทบต่อ server กลุ่ม sutmail ประกอบไปด้วย cas3 mbx3 mbx4 ไม่สามารถใช้งานได้ ทั้งนี้ไม่มีผลกระทบต่อผู้ใช้งานเนื่องจากเป็นระบบ cluster มี virtual server ทำงานแทนตัวที่มีปญหา
- Vmserver12 แจ้งอาการพัดลมเสีย เจ้าหน้าที่ทำการเปลี่ยนอะไหล่พัดลมเรียบร้อยแล้ว
- Mainboard netapp storage เสีย แจ้งบริษัทเพื่อทำการเคลมเรียบร้อยแล้ว และได้รับการเปลี่ยน mainboard แล้ว ทั้งนี้ไม่ส่งผลกระทบผู้ใช้งาน
- ตรวจสอบพบการ hack เว็บไซต์ http://smart.sut.ac.th/green2017 พบการเปิด permission ไฟล์ไม่เหมาะสม จึงทำให้ hacker สามารถแก้ไขไฟล์ index ได้ ได้ทำการแก้ไข และแจ้งผู้เกี่ยวข้องแล้ว
- ตรวจสอบพบการ hack เว็บไซต์ http://its.sut.ac.th/log พบการเปิด permission 777 ที่ folder log จึงทำให้ hacker สามารถวางไฟล์แปลกปลอมในระบบได้ ได้ทำการแก้ไขเรียนร้อยแล้ว
- จัดสรร virtual server : transport.sut.ac.th สำหรับส่วนอาคารสถานที่ เพื่อพัฒนาระบบ application ระบบปฏิบัติการ windows server 2008R2 64 bit , cpu 4 vcpu, ram 8 Gb, Hdd C:80 Gb , ip : 203.158.3.20

- ☐ จัดสรร virtual server สำหรับสำนักทันตแพทยศาสตร์ 3 server ประกอบไปด้วย

  1. web-database server

  - ระบบปฏิบัติการ Ubuntu 18.04 lts 64 bit , cpu 4 vcpu, ram 8 Gb, Hdd 100 Gb

  - ip : 203.158.3.21 (static ip)

  2. media server

  - ระบบปฏิบัติการ Ubuntu 18.04 lts 64 bit , cpu 4 vcpu, ram 8 Gb, Hdd 200 Gb

  - ip : 203.158.3.22 (static ip)

  3. Test server

  - ระบบปฏิบัติการ Ubuntu 18.04 lts 64 bit , cpu 2 vcpu, ram 4 Gb, Hdd 50 Gb

  - ip : 203.158.3.23 (static ip)

- ☐ ติดตั้ง license โปรแกรม Joget workflow 70 license สำหรับใช้งานพัฒนา application ของศูนย์คอมพิวเตอร์
- ☐ แก้ไขปัญหา server : smart.sut.ac.th มีอาการไม่สามารถส่งเมลล์ได้ตามปกติ ตรวจสอบพบ service sendmail ไม่ทำงาน แก้ไขโดย start service และตั้งค่าให้ service สามารถ start ได้เองทุกครั้งที่การ reboot เครื่อง
- ☐ ตรวจสอบ virtual server : smart.sut.ac.th พบว่ามีการใช้งาน cpu สูงมากผิดปรกติจาก service mysql จึงทำการแจ้งหน่วยงานที่เกี่ยวข้อง (MIS) ให้ทำการตรวจสอบและแก้ไข
- ☐ แก้ไขปัญหา virtual server : it.sut.ac.th ไม่สามารถ remote desktop ได้ตามปกติ พบ password ของผู้ดูแลระบบถูกเปลี่ยนไปจากเดิม จึงทำการแก้ไขให้สามารถใช้งานได้ตามปกติ
- ☐ ตั้งค่าการใช้งาน ssl สำหรับเว็บไซต์ https://dorm.sut.ac.th
- ☐ สรุปจำนวนผู้ขอ account ระบบสารสนเทศแบบ online ดังนี้

  -internet account 62 account

  -email account (SUTMail) 14 account

  -google App account (@g.sut.ac.th) 83 account

  -vpn account 9 account

  -personal website 2 account

  -virtual application and desktop 2 account

☐ งานตามระบบแจ้งซ่อม

เลขที่ใบงาน	รายละเอียดงานซ่อมแซมระบบเครือข่าย	ผู้รับงาน
610904-14-1	ขอความอนุเคราะห์ติดตั้งระบบเครือข่าย Internet ประจำห้องปฏิบัติการกีฏวิทยา	กฤช
610907-9-1	ขอความอนุเคราะห์เครื่องโทรศัพท์พร้อมหมายเลขเพื่อติดต่อภายในและภายนอกมหาวิทยาลัยฯ และติดตั้งสายเครือข่ายอินเตอร์เน็ต (LAN)	กฤช
610913-6-1	ขอความอนุเคราะห์เปิดพอร์ต VPN	กฤช
610917-19-1	ขอความอนุเคราะห์เปิดเลขหมายโทรศัพท์เพิ่ม จำนวน 1 เลขหมาย	กฤช
610924-15-1	ขอความอนุเคราะห์พื้นที่ (Server) ในการจัดเก็บข้อมูลเวชระเบียนด้านสุขภาพช่องปาก	กฤช

1.4 สรุปการดำเนินการบนระบบโทรคมนาคม

☐ ดำเนินการเปลี่ยนระบบเชื่อมต่อสายนอกโทรศัพท์ของ AIS เดิมเป็นแบบ E1 เชื่อมต่อกับตู้สาขาโทรศัพท์ Alcatel มาใช้งานแบบใหม่เป็น SIP Trunk AIS เพื่อรองรับการใช้งานกับคู่สายจำนวนมากและรองรับการขยายเพิ่มได้ในเลขหมายเดิม เริ่มดำเนินการปรับปรุงตั้งแต่วันที่ 19 กันยายน 2561 แก้ไขระบบและทดสอบใช้งานจริง แล้วเสร็จเมื่อวันที่ 26 กันยายน 2561

☐ การโทรออกภายนอกทั้งกด 8 และ 9 ของระบบโทรศัพท์มหาวิทยาลัย จะโทรออกผ่าน SIP Trunk AIS เริ่มตั้งแต่วันที่ 1 ตุลาคม 2561 เป็นต้นไป

☐ เปลี่ยนเครื่องโทรศัพท์รับสายของโอเปอร์เรเตอร์ จากเครื่องโทรศัพท์แบบไอพี Alcatel เป็นเครื่องโทรศัพท์แบบไอพี Cisco และระบบเสียงตอบรับอัตโนมัติของมหาวิทยาลัยเบอร์กลางมาที่ระบบ Unified Communications System – Cisco เปิดใช้งานจริงเมื่อวันที่ 21 กันยายน 2561 และแก้ไขปัญหาการโอนสายต่อของโอเปอร์เรเตอร์ที่ไม่ได้ยินเสียงคู่สนทนา แล้วเสร็จ

☐ งานตามระบบแจ้งซ่อม

เลขที่ใบงาน	รายละเอียดงานซ่อมแซมระบบโทรคมนาคม	ผู้รับงาน
610903-2-1	โทรศัพท์ไม่มีสัญญาณและได้ทำการตรวจสอบในเบื้องต้นแล้วพบว่าโทรศัพท์ไม่ได้เสีย	ประสาน
610903-4-1	โทรศัพท์ไม่มีสัญญาณ หมายเลข 5203	ประสาน
610903-5-1	สัญญาณโทรศัพท์สำนักงานโซนหอพักชำรุด ไม่สามารถใช้งานได้	ประสาน
610905-8-1	โทรศัพท์ชำรุด ไม่สามารถใช้งานได้	ประสาน
610905-14-1	โทรศัพท์โทรได้เฉพาะภายในไม่สามารถโทรออกข้างนอกและโทรเข้ามือถือได้ หมายเลข 4096,4011,4012	ประสาน
610910-14-1	โทรศัพท์โทรเข้า-ออกไม่ได้	ประสาน
610910-13-1	โทรศัพท์โทรเข้า-ออกไม่ได้	ประสาน
610911-8-1	โทรศัพท์ใช้งานไม่ได้ หมายเลข 5023	ประสาน
610912-7-1	โทรศัพท์ไม่มีสัญญาณ หมายเลข 4930, 4932	ประสาน
610912-16-1	ขอเปลี่ยนโทรศัพท์ (ชำรุด เสียงเบามาก)	ประสาน
610913-19-1	แจ้งเปลี่ยนโทรศัพทสำนักงาน เสียงลำโพงแตก	ประสาน
610913-23-1	สัญญาณโทรศัพท์ใช้งานไม่ปกติ	ประสาน
610913-22-1	โทรศัพท์ชำรุด ไม่สามารถใช้งานได้	ประสาน
610914-8-1	โทรศัพท์มีสัญญาณไฟกระพริบรับสายได้ โทรออกได้ แต่เสียงเรียกไม่ดัง	ประสาน
610917-6-1	สายโทรศัพท์ขาด หมายเลข 3049	ประสาน
610920-1-1	โทรศัพท์ใช้งานไม่ปกติ ผู้รับได้ยินเสียงสัญญาณเบามาก	ประสาน
610920-7-1	โทรศัพท์ไม่มีสัญญาณ	ประสาน
610921-3-1	ขอความอนุเคราะห์เปลี่ยนโทรศัพท์เครื่องใหม่ให้คณบดี สวพย.	ประสาน
610905-10-1	ขอความอนุเคราะห์วิทยุสื่อสาร จำนวน 6 เครื่อง	ประสาน
610907-13-1	ขอโทรศัพท์ให้พนักงานสายปฏิบัติการ	ประสาน
610907-14-1	ขอโทรศัพท์ให้พนักงานสายปฏิบัติการ	ประสาน
610910-8-1	ขอยืมวิทยุสื่อสารพร้อมแท่นชาร์จ 20 เครื่อง	ประสาน
610911-13-1	ขอโทรศัพท์ให้พนักงานสายปฏิบัติการ	ประสาน
610912-19-1	โทรศัพท์ไม่สามารถใช้งานได้ หมายเลข 5953	ประสาน
610913-8-1	ขอยืมวิทยุสื่อสาร	ประสาน

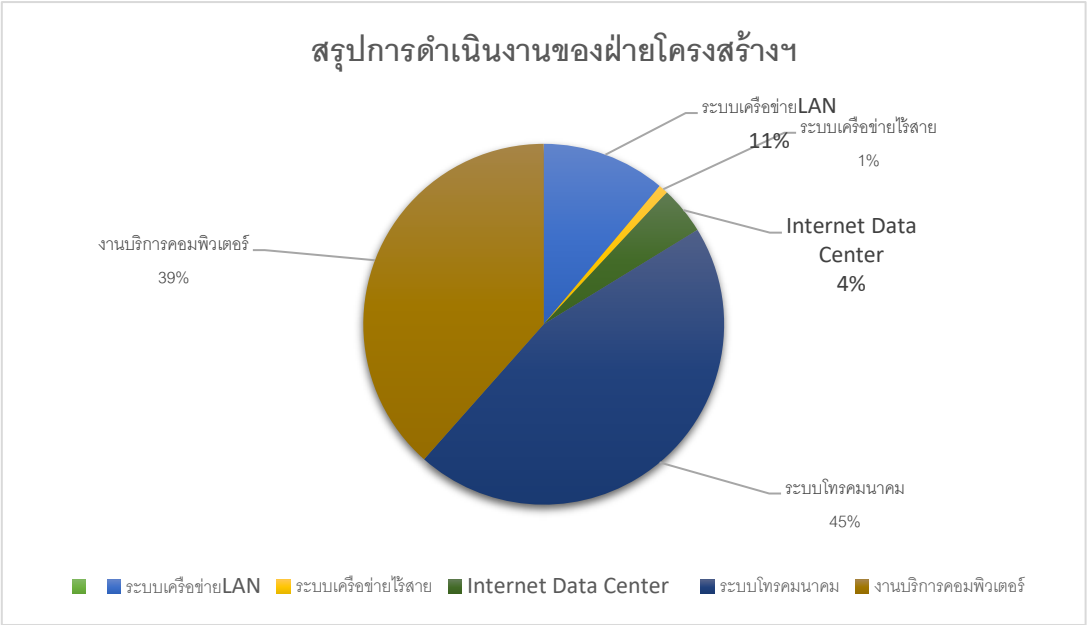
610914-11-1	ขอยืมวิทยุสื่อสารพร้อมแท่นชาร์จ 7 เครื่อง	ประสาน
610917-17-1	ขอยืมวิทยุสื่อสารพร้อมแท่นชาร์จ 15 เครื่อง	ประสาน
610917-18-1	ขอยืมวิทยุสื่อสารพร้อมแท่นชาร์จ 10 เครื่อง	ประสาน
610926-9-1	โทรศัพท์หมายเลข 5208 ไม่มีสัญญาณ	ประสาน
610910-6-1	โทรศัพท์โต๊ะ รปภ.หอพักสุรนิเวศ 1 ชำรุด	เสมา
610910-5-1	โทรศัพท์สัญญาณไม่ดี มีเสียงรบกวน และปลายสายไม่ได้ยินเสียง หมายเลข 5122	เสมา
610911-2-1	สายโทรศัพท์ชำรุด	เสมา
610911-9-1	โทรศัพท์ใช้งานไม่ได้ (ไม่ได้ยินเสียง)	เสมา
610913-20-1	แจ้งติดตั้งโทรศัพท์แบบแขวน ห้อง B1136	เสมา
610914-3-1	โทรศัพท์ไม่สามารถโทรเข้าและโทรออกได้	เสมา
610914-6-1	เครื่องรับโทรศัพท์สายด่วนแจ้งเหตุฉุกเฉินใช้งานไม่ปกติ ผู้รับสายไม่ได้ยินเสียงของผู้โทรเข้า	เสมา
610917-1-1	โทรศัพท์ใช้งานไม่ได้ หมายเลข 4954	เสมา
610920-3-1	โทรศัพท์มีเสียงสัญญาณแทรกดังเป็นบางเป็นครั้ง ขณะไม่ได้ใช้งาน	เสมา
610924-6-1	โทรศัพท์มีเสียงดังติ๊ดๆ ตลอดเวลา	เสมา
610926-5-1	สำนักงาน ไม่มีสัญญาณ / สัญญาณขาดหาย	เสมา
610926-13-1	โทรศัพท์หมายเลข 4945 ไม่มีสัญญาณ	เสมา
610906-12-1	ไม่สามารถใช้ Internet ที่บ้านพักบุคลากรได้	อำนาจ
610918-4-1	IP Phone หมายเลข 6617 ที่ตัวเครื่องขึ้นสัญญลักษณ์สัญญาณเน็ตเวิร์คใช้ไม่ได้	อำนาจ
610921-4-1	กล้องวงจรปิด อาคารเกษตรวิวัตน์ ใช้งานไม่ได้	อำนาจ
610912-18-1	ขอความอนุเคราะห์จัดสรรหมายเลขโทรศัพท์	อำนาจ
610913-5-1	ขอความอนุเคราะห์หมายเลขโทรศัพท์ จำนวน 1 หมายเลข	อำนาจ
610913-14-1	update สมุดโทรศัพท์, เรียกเก็บค่าใช้จ่าย	อำนาจ
610913-18-1	update สมุดโทรศัพท์, เรียกเก็บค่าใช้จ่าย	อำนาจ
610625-8-1	update สมุดโทรศัพท์, เรียกเก็บค่าใช้จ่าย	อำนาจ
610925-9-1	update สมุดโทรศัพท์, เรียกเก็บค่าใช้จ่าย	อำนาจ
610925-10-1	update สมุดโทรศัพท์, เรียกเก็บค่าใช้จ่าย	อำนาจ
610913-25-1	ไม่ได้ยินสัญญาณโทรศัพท์	สมพงษ์
610913-26-1	โทรศัพท์ไม่มีสัญญาณ	สมพงษ์

1.5 สรุปการดำเนินการด้านงานบริการคอมพิวเตอร์

☐ งานตามระบบแจ้งซ่อม

เลขที่ใบงาน	รายละเอียดงานซ่อมแซมระบบโทรคมนาคม	ผู้รับงาน
610904-4-1	Clear Tempory files, Optimized system, Update Windows	ศิริพงษ์
610904-16-1	KMS Office2016	ศิริพงษ์
610912-13-1	Activate Windows, ชี้ KMS Server	ศิริพงษ์
610913-2-1	Activate Windows, ชี้ KMS Server	ศิริพงษ์
610914-9-1	Activate Windows, ชี้ KMS Server	ศิริพงษ์
610919-3-1	ขอความอนุเคราะห์ปิดระบบ Windows Update ของ Windows 10 ในคอมพิวเตอร์ เนื่องจากอาจมีผลกระทบต่อโปรแกรมที่ใช้ในการทำงาน	ศิริพงษ์
610907-3-1	Activate Windows, ชี้ KMS Server	ศิริพงษ์
610918-6-1	ใช้งานพิมพ์ได้เป้นที่เรียบร้อย by Ricoh	ศิริพงษ์
610926-26-1	ใช้งานอยู่แล้วขึ้น Reload และ Send Feedback	ศิริพงษ์
610927-4-1	Windows ตอบสนองช้า ไม่สามารถทำงานได้	ศิริพงษ์
610904-7-1	เครื่องแฮงค์บ่อยเมื่อใช้งานผ่าน Browser พบอาการเช่นนี้ 2 เครื่อง	วัชรพล
610904-11-1	เครื่องแฮงค์บ่อยเมื่อใช้งานผ่าน Browser พบอาการเช่นนี้ 2 เครื่อง	วัชรพล
610914-7-1	Set Dot1x	วัชรพล
610920-4-1	MS Office ใช้งานไม่ได้	วัชรพล
610903-8-1	Set Dot1x	วัชรพล
610905-11-1	ตรวจสอบโปรแกรม Notebook อ.นพ.ลิขิต มาตระกูล เกษียณปี 2561	วัชรพล
610907-4-1	นำเครื่องสแกนกลับ ตรวจสอบการใช้งาน	วัชรพล
610911-10-1	Set Dot1x	วัชรพล
610912-19-1	มอบหมายงานโทรศัพท์	วัชรพล
610913-12-1	ขอส่งคืนครุภัณฑ์พร้อมคู่มือการใช้งาน	วัชรพล
610914-14-1	ไม่สามารถใช้ Wi-Fi ได้	วัชรพล
610921-1-1	ไม่สามารถใช้งานอินเตอร์เน็ตได้	วัชรพล

610926-7-1	ขอความอนุเคราะห์จัดสรรเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง	วัชรพล
610926-9-1	ตรวจสอบโปรแกรมคอมพิวเตอร์ เครื่องคอมพิวเตอร์เช่า ปี 2560	วัชรพล
610904-13-1	ไม่สามารถ บูธเครื่องได้	เอกภาวี
610906-2-1	เม้าส์ กล้องวงจรปิดเครื่องคอมพิวเตอร์ ชำรุด	เอกภาวี
610912-2-1	ดำเนินการปิด process บางโปรแกรม, ปรับ virtual memory, update windows, ลบ temp	เอกภาวี
610913-21-1	Activate windows และชี้ Server KMS	เอกภาวี
610919-7-1	ติดตั้ง offices และโปรแกรมพื้นฐานอื่นๆ	เอกภาวี
610919-11-1	set @SUT-Wifi และ Dot1x	เอกภาวี
610920-5-1	เคลียร์ temp, ปิด process และ starup ที่แปลกๆ หรือไม่ได้ใช้งาน, ปรับ virtual mamory, update windows	เอกภาวี
610903-14-1	ขอยืมคอมพิวเตอร์ Notebook 1 เครื่อง	เอกภาวี
610906-10-1	ขอยืมคอมพิวเตอร์ Notebook และหูฟัง 1 ชุด	เอกภาวี
610907-16-1	ขอยืมคอมพิวเตอร์ Notebook 1 เครื่อง	เอกภาวี
610910-12-1	ขอยืมคอมพิวเตอร์ Notebook 7 เครื่อง	เอกภาวี
610911-11-1	Set @SUT-Wifi และ Dot1x	เอกภาวี
610912-17-1	ขอยืมคอมพิวเตอร์ Notebook 5 เครื่อง	เอกภาวี
610914-13-1	ขอยืมคอมพิวเตอร์ Notebook 3 เครื่อง	เอกภาวี
610924-14-1	ขอยืมคอมพิวเตอร์ Notebook 10 เครื่อง	เอกภาวี
610926-3-1	ขอยืมคอมพิวเตอร์ Notebook	เอกภาวี
610926-6-1	ขอความอนุเคราะห์ยืมคอมพิวเตอร์ชนิดพกพา Notebook	เอกภาวี
610927-3-1	ขอยืมคอมพิวเตอร์ Notebook 1 เครื่อง	เอกภาวี
610911-15-1	ค้นหาสัญญาน wifi ไม่ได้	โกเมณ
610917-3-1	ส่งคืนเครื่องพิมพ์ รุ่น EPSON LQ-2080i	โกเมณ
610919-9-1	ขอยืมคอมพิวเตอร์ Notebook 1 เครื่อง	โกเมณ

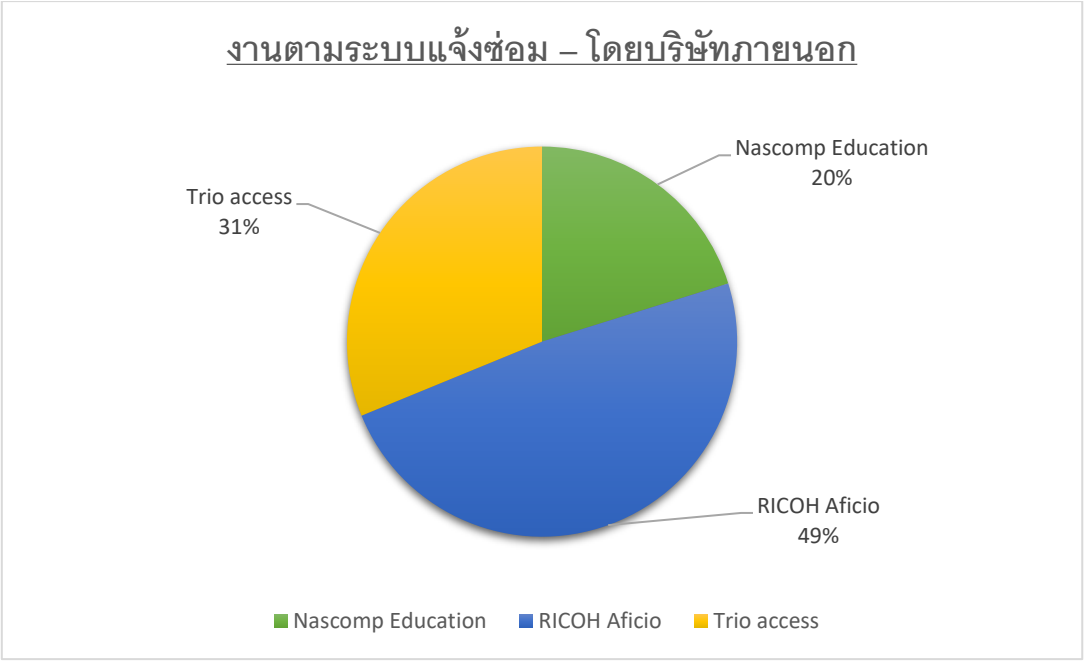


งานตามระบบแจ้งซ่อม – โดยบริษัทภายนอก

รายงานสรุปการให้บริการแยกตามฝ่ายงาน ฝ่ายบริการงานคอมพิวเตอร์

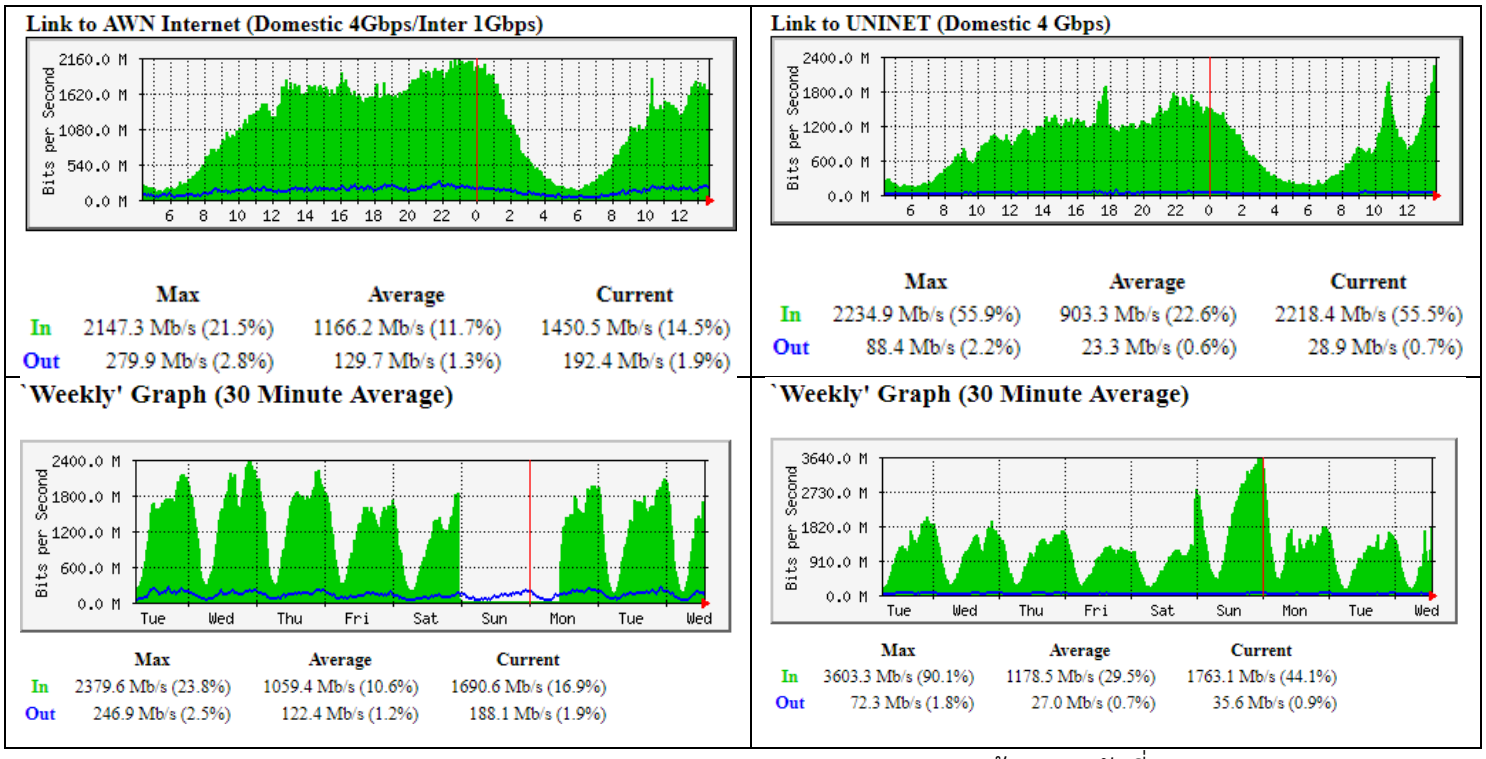
ใบงานแจ้งวันที่ 61/09/01 ถึง 61/09/30

ชื่อเจ้าหน้าที่	งานบริการ	งานซ่อมบำรุง	รวม	จ. ยังไม่ดำเนินการ	กำลังดำเนินการ	แล้วเสร็จ
Nascomp Education (ฝ่ายบริการงานคอมพิวเตอร์)	5	17	22	0	0	16
RICOH Aficio (ฝ่ายบริการงานคอมพิวเตอร์)	6	47	53	0	7	36
Trio access (ฝ่ายบริการงานคอมพิวเตอร์)	4	30	34	0	3	31
สรุปรวม	15	94	109	0	10	83



2.รายงานการใช้งานระบบเครือข่าย

Internet Gateway Traffic



*ทางออก AWN Domestic 4 Gbps,Inter 1 Gbps) / Uninet 4Gbps / ข้อมูล ณ วันที่ 26 ก.ย. 61

ที่มา http://mrtg.sut.ac.th

2.1 รายงานจำนวนผู้ใช้งานผ่านระบบเครือข่าย (LAN) (ไม่รวมห้องปฏิบัติการคอมฯ)

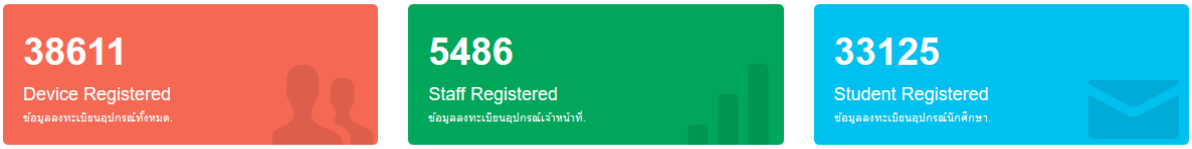
(ข้อมูล ณ วันที่ 26 ก.ย. 61)

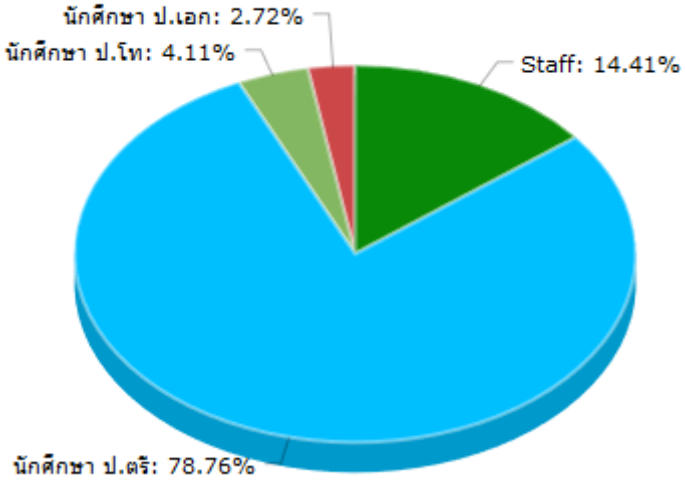
วิธีการ	จำนวน
วิธีการแบบ NAC In-Band	219 คน
วิธีการแบบ ISE (802.1x)	538 คน
รวมทั้งหมด	**757 คน**

ที่มา (nac) https://203.158.4.213 / (ise) https://203.158.4.207

2.2 รายงานจำนวนผู้ใช้งานผ่านระบบเครือข่ายไร้สาย

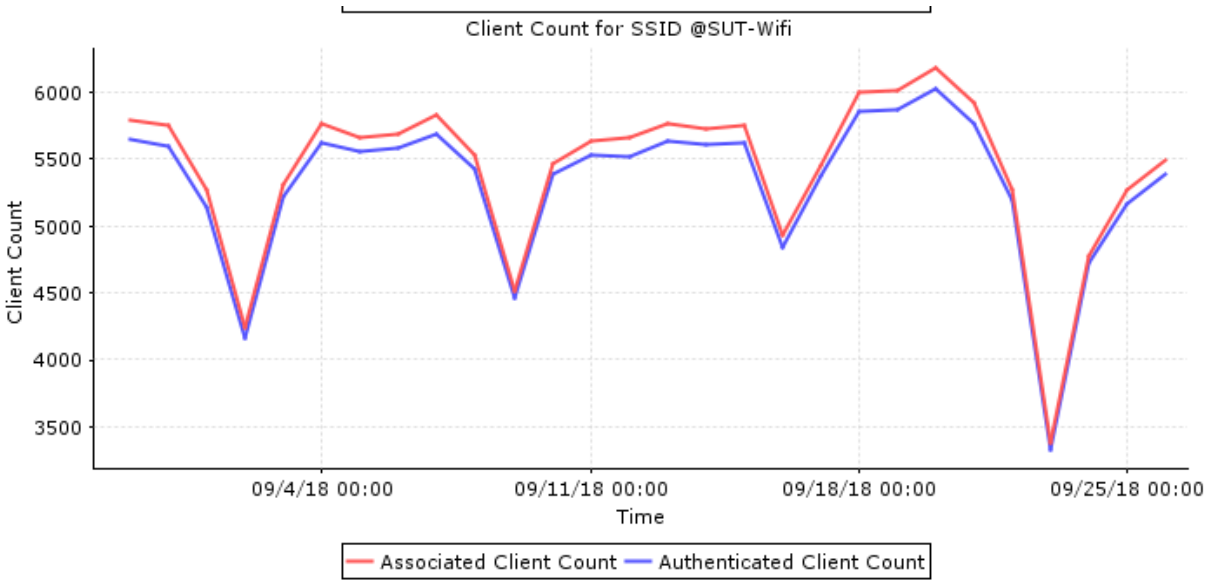
2.2.1 จำนวนผู้ใช้งานเครือข่ายไร้สาย @SUT-Wifi



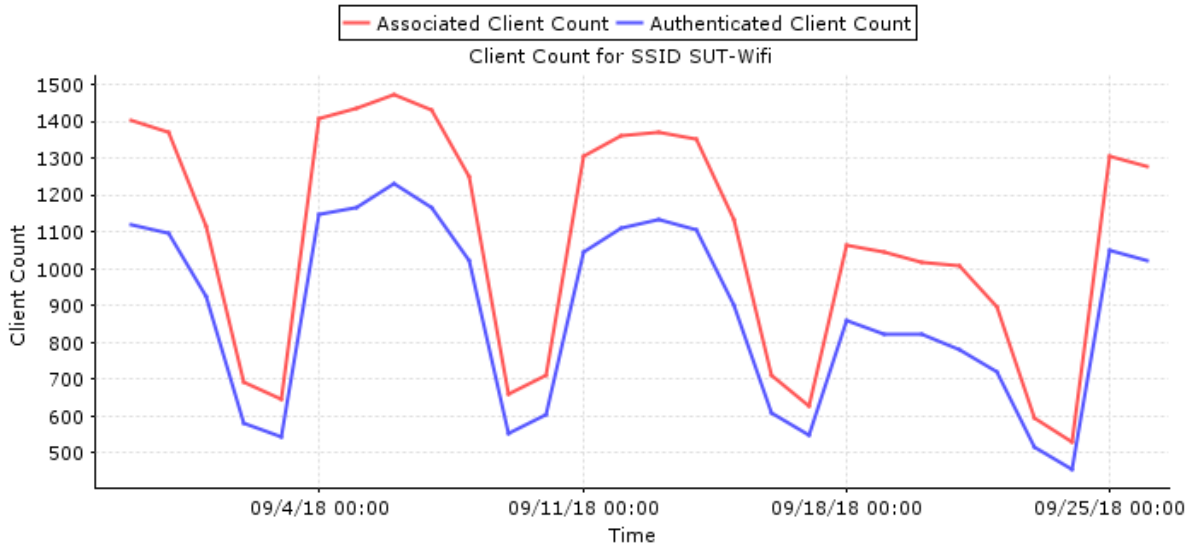


*ที่มา http://idm.sut.ac.th/admin

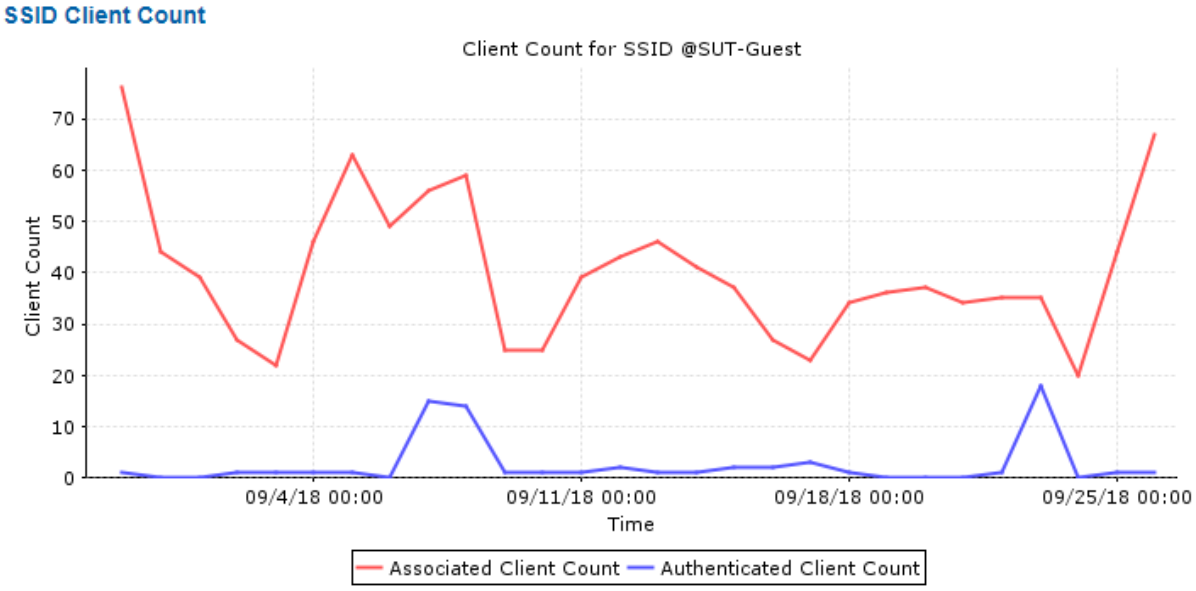
-จำนวนผู้ใช้งานเครือข่ายไร้สาย @SUT-Wifi (ที่มา https://203.158.4.211) (ข้อมูล 1 เดือนย้อนหลัง)



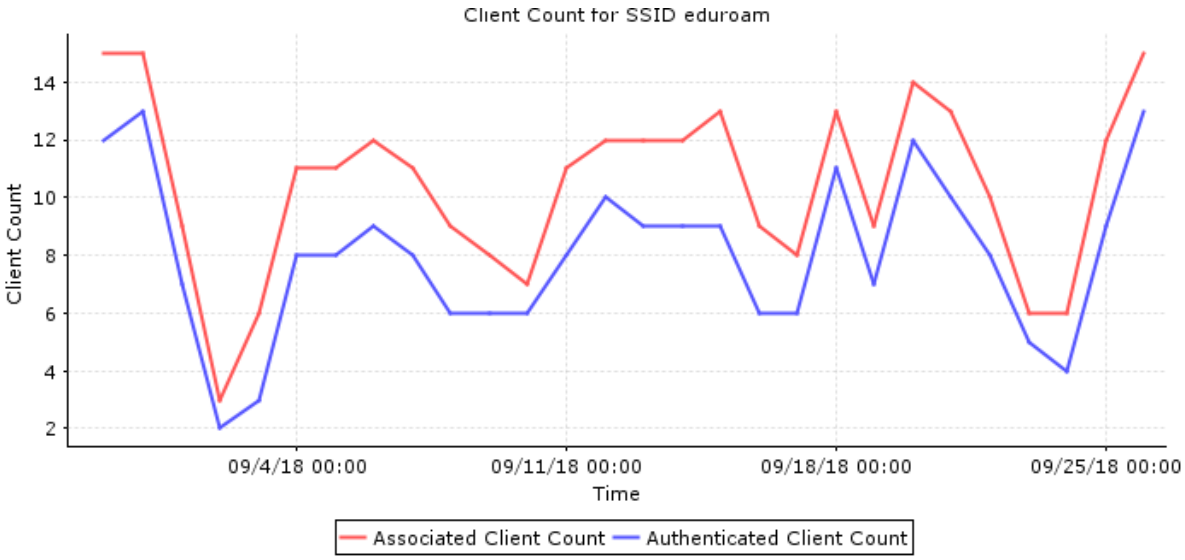
2.2.2 จำนวนผู้ใช้งานเครือข่ายไร้สาย SUT-Wifi



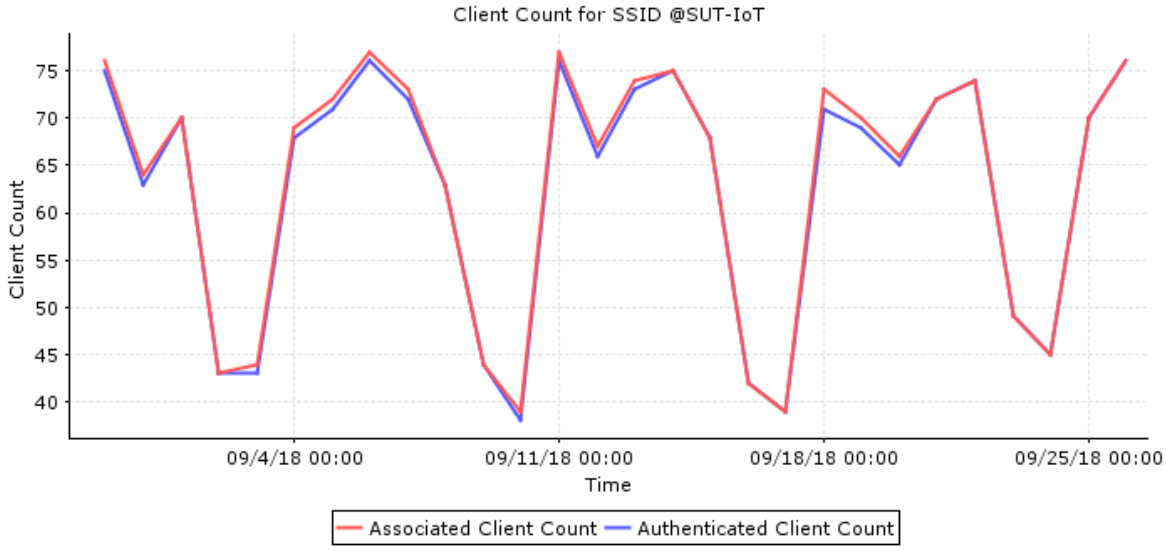
2.2.3 จำนวนผู้ใช้งานเครือข่ายไร้สาย @SUT-Guest



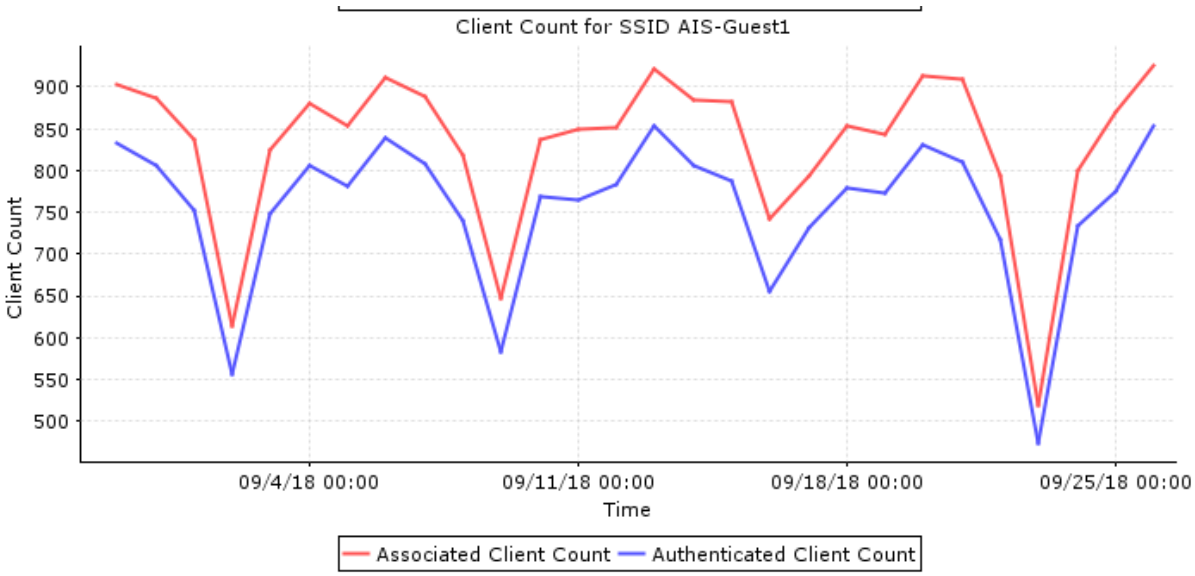
2.2.4 จำนวนผู้ใช้งานเครือข่ายไร้สาย eduroam

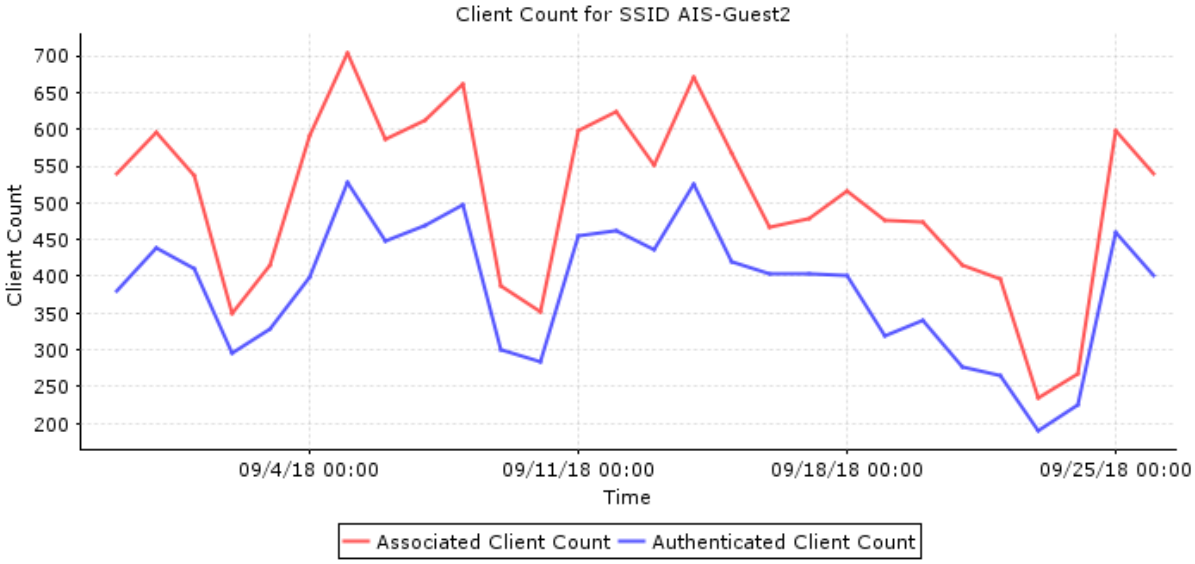


2.2.5 จำนวนผู้ใช้งานเครือข่ายไร้สาย @SUT-IoT

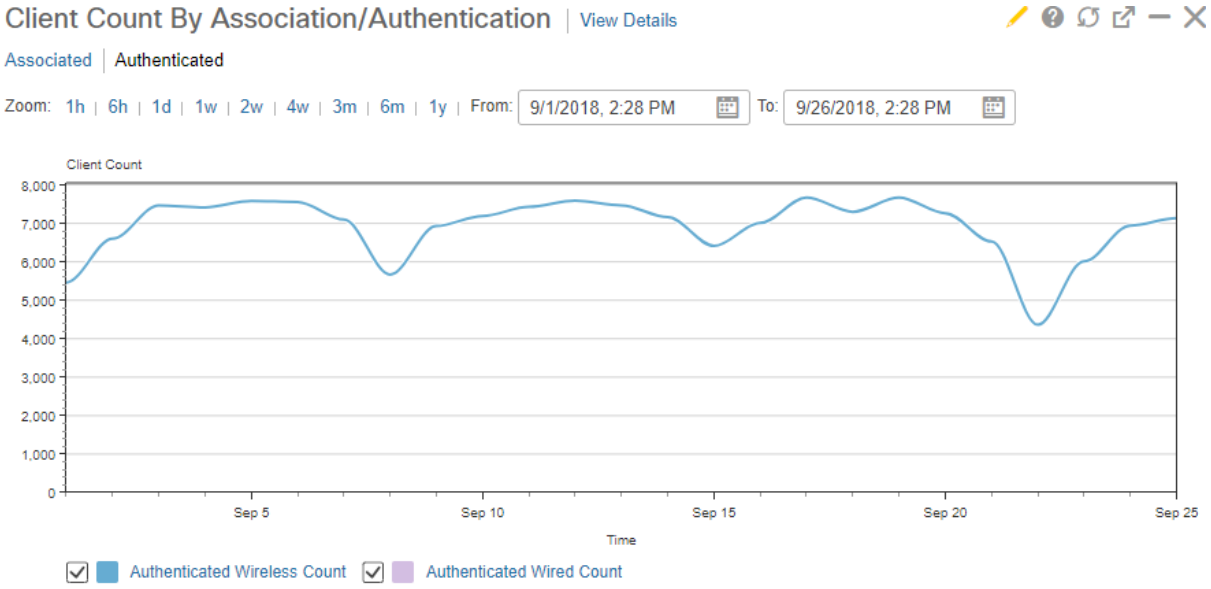


2.2.6 จำนวนผู้ใช้งานผ่านระบบ AIS





2.2.7 สรุปสถิติจำนวนผู้ใช้งานผ่านระบบ wireless ทั้งหมด



- ☐ ผู้ใช้งานผ่านระบบ wireless สูงสุด 7,670 คน/วัน
- ☐ ผู้ใช้งานผ่านระบบ wireless ต่ำสุด 4,362 คน/วัน
- ☐ ผู้ใช้งานผ่านระบบ wireless เฉลี่ย 6,917 คน/วัน

3. ภัยคุกคามระบบเครือข่าย

☐ **สถานะการณ์ไวรัสและมัลแวร์ที่แพร่ระบาดในมหาวิทยาลัย** (ข้อมูล 1 เดือนย้อนหลัง)

(ที่มา : Sourcefire https://203.158.4.43)

Malware Intrusions

Message	Count
MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35030:1)	202,263
MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35549:1)	139,869
MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35746:1)	109,236
MALWARE-CNC Win.Trojan.Glupteba.M initial outbound connection (1:30288:2)	89,831
MALWARE-CNC Win.Trojan.Nvbpass variant outbound connection (1:19864:5)	78,192
MALWARE-CNC Win.Trojan.Zbot variant in.php outbound connection (1:26023:3)	24,628
MALWARE-CNC Win.Trojan.Andromeda variant outbound connection (1:33496:1)	13,437
MALWARE-CNC Win.Trojan.Nvbpass variant outbound connection (1:19864:6)	11,633
MALWARE-CNC DNS suspicious .bit dns query (1:41083:3)	8,363
MALWARE-CNC Win.Trojan.Ramnit variant outbound detected (1:33600:3)	3,827
MALWARE-CNC Win.Ransomware.GandCrab outbound connection (1:47766:1)	3,059
MALWARE-CNC DNS suspicious .bit dns query (1:41083:4)	2,620
MALWARE-CNC Win.Trojan.Pmabot outbound connection (1:37213:3)	2,403
MALWARE-CNC Win.Worm.Brontok user-agent outbound connection (1:20021:6)	2,198
MALWARE-CNC User-Agent known malicious user-agent string - Virut (1:40870:2)	1,624
MALWARE-CNC Win.Rootkit.Necurs outbound connection (1:31070:2)	1,457
MALWARE-CNC Win.Trojan.Fareit variant outbound connection (1:27775:4)	782
MALWARE-CNC Win.Trojan.Graftor variant HTTP Response (1:34997:1)	490
MALWARE-CNC Torpig bot sinkhole server DNS lookup (1:16693:7)	299
MALWARE-CNC Win.Trojan.Kuluoz variant download request (1:30773:1)	259

Last updated 11 hours, 57 minutes ago

Malware Intrusions

	Source IP	Count
	203.158.4.230	174,036
	203.158.4.227	36,793
	172.32.234.69	18,163
	172.32.225.181	17,651
+1	192.168.29.9	17,556
-1	203.158.4.228	17,342
	192.168.29.10	15,200
	192.168.140.24	13,226
	203.158.4.226	12,763
	10.0.71.231	10,346
+1	172.31.10.167	9,354
+1	192.168.140.157	9,339
-2	10.0.46.55	9,256
	10.0.15.2	8,564
+1	192.168.29.5	8,331
-1	172.31.0.249	8,318
	172.32.65.65	7,750
	10.0.33.28	7,204
	10.0.85.129	6,417
	10.0.33.208	6,218

Last updated 11 hours, 57 minutes ago

Top Attackers (High Impact Events)

	Source IP	Count
	203.158.4.230	162,262
	203.158.4.227	39,111
+1	192.168.29.9	18,039
-1	172.32.234.69	17,936
	192.168.29.10	15,651
	203.158.4.228	15,055
	192.168.140.24	13,226
	203.158.4.226	12,311
+1	192.168.140.157	9,964
-1	172.31.10.167	9,354
	10.0.46.55	8,803
	192.168.29.5	8,674
	10.0.85.185	5,494
+1	192.168.29.62	5,331
-1	172.31.1.124	5,177
	10.0.149.91	4,754
	10.0.10.16	4,263
	10.0.28.236	4,189
+1	192.168.124.18	3,807
-1	10.0.41.76	3,752

Last updated 2 minutes ago

Dropped Intrusion Events

Classification	Count
A Network Trojan was Detected	700,131
Potential Corporate Policy Violation	419,339
Misc Attack	38,237
Attempted Administrator Privilege Gain	1,135
Web Application Attack	238
Misc Activity	210
Attempted User Privilege Gain	105
Attempted Information Leak	8

Last updated 2 minutes ago

☐ **การยับยั้งการโจมตีบนระบบเครือข่าย โดย อุปกรณ์ Next Gen Firewall:** fortinet (ข้อมูล 1 เดือนย้อนหลัง) ที่มา https://203.158.4.195

-thread (top 20) ที่แพร่ระบาดภายในมหาวิทยาลัย และ block โดย อุปกรณ์ firewall next gen

#	Threat	Category	Threat Level	Threat Score(Blocked/ Allowed)
1	ip_dst_session	IPS	Critical	2,462,550
2	udp_dst_session	IPS	Critical	2,459,800
3	ip_src_session	IPS	Critical	2,394,750
4	udp_src_session	IPS	Critical	2,386,150
5	Netcore.Netis.Devices.Hardcoded.Password.Sec...	IPS	Critical	132,750
6	tcp_src_session	IPS	Critical	126,300
7	tcp_dst_session	IPS	Critical	59,000
8	Dasan.GPON.Remote.Code.Execution	IPS	Critical	39,000
9	MS.IIS.WebDAV.PROPFIND.ScStoragePathFrom...	IPS: CVE-2017-7269	Critical	11,400
10	tcp_port_scan	IPS	Critical	6,000
11	icmp_src_session	IPS	Critical	4,200
12	D-Link.DSL-2750B.CLI.OS.Command.Injection	IPS	Critical	3,500
13	Zivif.PR115-204-P-RS.Web.Cameras.Hardcoded.Password	IPS	Critical	3,000
14	Drupal.Core.Form.Rendering.Component.Remote...	IPS	Critical	2,450
15	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	IPS	Critical	1,150
16	OpenSSL.Heartbleed.Attack	IPS: CVE-2014-0160	Critical	950
17	udp_flood	IPS	Critical	850
18	WordPress.Multiple.Plugins.CMS.Software.Arbitr...	IPS	Critical	600
19	Adware/Generic	Malware	Critical	500
20	WordPress.Plugin.Userpro.Authentication.Bypass	IPS	Critical	300

-การใช้งาน Application (Top20)

#	Application	Category	Risk	# of Clients	Sessions(Blocked/ Allowed)
1	Proxy.HTTP	Proxy	Critical	1	1,522
2	Hotspot.Shield	Proxy	Critical	5	1,174
3	Hola.Unblocker	Proxy	Critical	1	4
4	RDP	Not.Scanned	High	13	25,143
5	BitTorrent	P2P	High	4	146
6	TeamViewer	Remote.Access	High	4	4
7	PPStream	P2P	High	1	2
8	HTTPS.BROWSER	Web.Client	Medium	8382	1,682,615
9	Facebook	Social.Media	Medium	10373	1,587,616
10	Microsoft.Outlook	Email	Medium	339	46,645
11	IMAPS	Email	Medium	518	40,832
12	Amazon.AWS	Cloud.IT	Medium	459	21,458
13	iCloud	Storage.Backup	Medium	749	13,895
14	4shared	Storage.Backup	Medium	47	13,585
15	Dropbox	Storage.Backup	Medium	145	11,186
16	Microsoft.Office.Online	Collaboration	Medium	393	8,544
17	HTTP.BROWSER	Web.Client	Medium	66	8,227
18	Google.Drive	Storage.Backup	Medium	276	5,565
19	Gmail	Email	Medium	183	2,349
20	Yahoo.Mail	Email	Medium	14	2,218

Top source

Top 20 destination

#	Destination	Applications	▼Sessions(Blocked/ Allowed)
1	8.8.8.8	DNS, HTTP, Ping	9,423,858
2	202.28.42.11	DNS, FTP, HTTP, HTTPS, PING, SNMP	6,540,271
3	8.8.4.4	DNS, Ping	5,298,721
4	203.158.4.45	DNS	1,182,705
5	192.5.6.30	DNS	244,437
6	203.158.4.51	DNS, Internet-Locator-Service, LDAP, PING, SMB, tcp, tc...	207,216
7	192.33.14.30	DNS	207,034
8	49.231.52.96	Facebook, HTTPS	204,929
9	192.26.92.30	DNS	181,590
10	192.31.80.30	DNS	170,598
11	202.28.42.51	HTTP, HTTPS, MySQL	149,427
12	192.12.94.30	DNS	139,115
13	31.13.78.17	Facebook, HTTP, HTTPS, HTTPS.BROWSER, SSL	131,465
14	157.240.13.35	Facebook, HTTP, HTTPS, HTTPS.BROWSER	127,042
15	49.231.63.97	Facebook, HTTPS	118,377
16	202.28.85.204	Google.Services, HTTP, HTTPS, HTTPS.BROWSER, SS...	111,541
17	157.240.13.14	Facebook, HTTP, HTTPS, HTTPS.BROWSER, SSL	108,750
18	202.28.85.205	Google.Services, HTTP, HTTPS, HTTPS.BROWSER, SS...	105,418
19	202.28.85.206	Google.Services, HTTP, HTTPS, HTTPS.BROWSER, SS...	101,849
20	203.158.4.46	DNS	101,741