โครงการประกวดแนวปฏิบัติที่ดี (Good Practices)

การบูรณาการการจัดการความรู้สู่ชุมชนและประชาคมอาเซียน ระดับอุดมศึกษา

⊗ การบรูณาการการจัดการเรียนการสอน ○ การบูรณาการวิจัย/งานสร้างสรรค์

○ การบูรณาการการบริการวิชาการแก่สังคม ○ การบูรณาการการทำนุบำรุงศิลปวัฒนธรรม

ชื่อเรื่อง/แนวปฏิบัติที่ดี Remote access point

ชื่อ-นามสกุลผู้นำเสนอ นายสรศิษฏ์ พุ่มฉัตร

ชื่อสถาบันอุดมศึกษา มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

หน่วยงาน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

เบอร์โทรศัพท์ 02-6653-777 ต่อ 6765

E-mail address sorasit.p@rmutp.ac.th

บทสรุปผู้บริหาร

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ (สวส.) ได้มีการพัฒนาและทดสอบการใช้งานระบบเครือข่ายไร้สายให้มีสะดวกมากขึ้นครอบคลุมทุกสถานที่ เพื่อให้บุคลากรและนักศึกษาสามารถเข้าใช้งานทรัพยากรเครือข่ายของมหาวิทยาลัยจากภายนอกได้ โดยนำอุปกรณ์กระจายสัญญาณ Wi-Fi (Access Point) มาใช้เทคนิคที่เรียกว่า Remote ap เป็นการนำ Access Point มาตั้งค่าให้อยู่ในโหมด Remote access point แล้วนำไปติดตั้งกับระบบเครือข่ายภายนอก ซึ่งจะทำให้ Access Point กระจายสัญญาณที่มี SSID เดียวกับภายในมหาวิทยาลัย เปรียบเหมือนได้ใช้งานเครือข่ายของมหาวิทยาลัยจากนอกสถานที่ ซึ่งจะคล้ายกับการใช้เทคนิค SSLVPN แต่จะมีความสะดวกมากกว่า เนื่องจากผู้ใช้งานไม่จำเป็นที่จะต้องลงแอพพลิเคชั่นเพิ่ม ไม่ต้องล็อกอินเข้าระบบใหม่และไม่มีข้อจำกัดของอุปกรณ์ที่ใช้งาน

ประวัติหน่วยงาน

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ เริ่มดำเนินการจัดตั้งเป็นโครงการจัดตั้งสำนักวิทยบริการและเทคโนโลยีสารสนเทศ เมื่อวันที่ 1 ตุลาคม พ.ศ. 2548 โดยมีผู้ช่วยศาสตราจารย์นิวัตร จารุวาระกูล เป็นประธานโครงการจัดตั้งสำนักวิทยบริการและเทคโนโลยีสารสนเทศ มีสำนักงานชั่วคราว ตั้งอยู่ที่อาคาร 1 ชั้น 4 มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร เทเวศร์ ต่อมาเมื่อวันที่ 14 พฤศจิกายน พ.ศ. 2549 ได้มีกฎกระทรวงจัดตั้งส่วนราชการในมหาวิทยาลัยเทคโนโลยีราชมงคลให้เป็นสำนักวิทยบริการและเทคโนโลยีสารสนเทศ เป็นหน่วยงานหลักในการจัดหา พัฒนา ดูแล รวมถึงการประยุกต์ใช้เทคโนโลยีสารสนเทศให้กับหน่วยงานต่างๆ ในสังกัดของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร มีศูนย์วิทยบริการและเทคโนโลยีสารสนเทศ 4 แห่ง ได้แก่ ศูนย์โชติเวช ศูนย์พณิชยการพระนคร ศูนย์เทเวศร์ และศูนย์พระนครเหนือ การดำเนินงานของสำนักวิทยบริการและเทคโนโลยีสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร มีภารกิจดังนี้

ยุทธศาสตร์ที่ 1: (e-Learning) การสร้างโอกาส เพิ่มขีดความสามารถและยกระดับมาตรฐานการเรียนรู้ด้วยสื่ออิเล็กทรอนิกส์

ยุทธศาสตร์ที่ 2: (e-Management) การเป็นผู้นำในการใช้ ICT เพิ่มประสิทธิภาพการบริหารจัดการและการให้บริการทางการศึกษา

ยุทธศาสตร์ที่ 3: (e-Manpower) การผลิตและพัฒนาคุณภาพผู้จบการศึกษาให้มีสมรรถนะทาง ICT เพื่อพัฒนาประเทศ

การดำเนินงานในอดีต

การใช้งานทรัพยากรระบบเครือข่ายบางอย่างที่ผู้ใช้งานจะต้องอยู่ภายในมหาวิทยาลัยเท่านั้นถึงจะมีสิทธิเข้าใช้งานได้ หากอยู่นอกสถานที่จะต้องใช้เทคโนลียีที่เรียกว่า sslvpn เพื่อร้องขอหมายเลขไอพีแอดเดรสของมหาวิทยาลัยก่อนถึงจะสามารถเข้าใช้งานได้ ซึ่งในบางครั้งอาจมีผู้ใช้งานที่ไม่มีความรู้ทางด้านระบบคอมพิวเตอร์รวมอยู่ด้วยทำให้ไม่สามารถใช้งาน sslvpn ได้ตามความคาดหมาย ดังนั้นเพื่อเป็นการลดปัญาหาที่เกิดขึ้นทางสำนักวิทยบริการและเทคโนโลยีสารสนเทศจึงได้นำเทคนิคที่เรียกว่าการทำ remote ap มาช่วยเพิ่มความสะดวกในการเข้าใช้งานได้มากขึ้น

แนวทางการดำเนินงานตามหลัก (PDCA)

การดำเนินกิจกรรมดังกล่าวสามารถแยกออกเป็นขั้นตอนตามหลัก PDCA ได้ดังนี้

ระยะที่ 1 การวางแผน (Plan)

1. สำรวจความต้องการและปัญหาการใช้งานระบบเครือข่าย

   จากการสอบถามความคิดเห็นของบุคลากรและนักศึกษามหาวิทยาลัยพบว่า ในบางครั้งเกิดความไม่สะดวกในการเข้าถึงทรัพยากรระบบสารสนเทศบางอย่างที่จำเป็นที่จะต้องอยู่ในมหาวิทยาลัยเท่านั้นถึงจะใช้งานได้ ตัวอย่างเช่น การอบรม สัมนานอกสถานที่ที่จะต้องค้นหาข้อมูล เปิดเอกสาร หรือใช้งานคอมพิวเตอร์ของตนเองจากภายนอกได้
2. สืบค้นข้อมูลอุปกรณ์เครือข่ายที่รองรับการทำงาน Remote access point

   2.1 Wireless Controller : เป็นอุปกรณ์แม่ข่ายที่ต่อพ่วงมาจากอุปกรณ์เน็ตเวิร์คอีกทีนึงซึ่ง AP เพียงอย่างเดียวไม่สามารถควบคุมและแทรกซึมเข้าไปกรอง การใช้งานของผู้ใช้งานแต่ละคนได้อย่างละเอียด จึงมีการใช้ wireless controller เพื่อควบคุมและเป็นตัวกรองในการเชื่อมตัวสัญญาณ เพื่อเชื่อมต่ออินเตอร์เน็ตในองค์กรณ์ หรือ สถานที่ๆหนึ่งแบบมีตัวตน อีกทั้งการใช้งาน wireless controller นั้นจะช่วยคัดกรองและเป็นกุญแจสำคัญในการใช้งานที่ราบรื่นบนระบบสัญญาณอินเตอร์เน็ต อีกทั้ง wireless controller ยังช่วยในการจดจำค่าอุปกรณ์ที่เชื่อมจากการล็อกอินในแต่ละครั้งเพื่อยืนยันตัวตนในการเข้าใช้งานสำหรับการเชื่อมต่อ Access Point หรือ AP หลายๆตัวเข้าด้วยกันนั้นจำเป็นอย่างยิ่งที่จะต้องมี wireless controller เป็นอุปกรณ์ช่วยอีกอุปกรณ์หนึ่งอีกทั้ง wireless controller ยังเชื่อมต่อและพกพาได้ง่ายอีกด้วยทุกๆการทำงานจะราบรื่นและรวดเร็ว สำหรับ wireless controller ที่ทางมหาวิทยาลัยใช้จะเป็นของ Alcatel-Lucent OAW-4550

2.2 Access Point : อุปกรณ์กระจายสัญญาณ WiFi สำหรับ Access Point ที่ทางมหาวิทยาลัยใช้จะเป็น Alcatel-Lucent OmniAccess AP92 , AP104 ,AP105 ,AP204 ,AP205 ซึ่งจะรองรับการใช้งาน Remote access point ได้

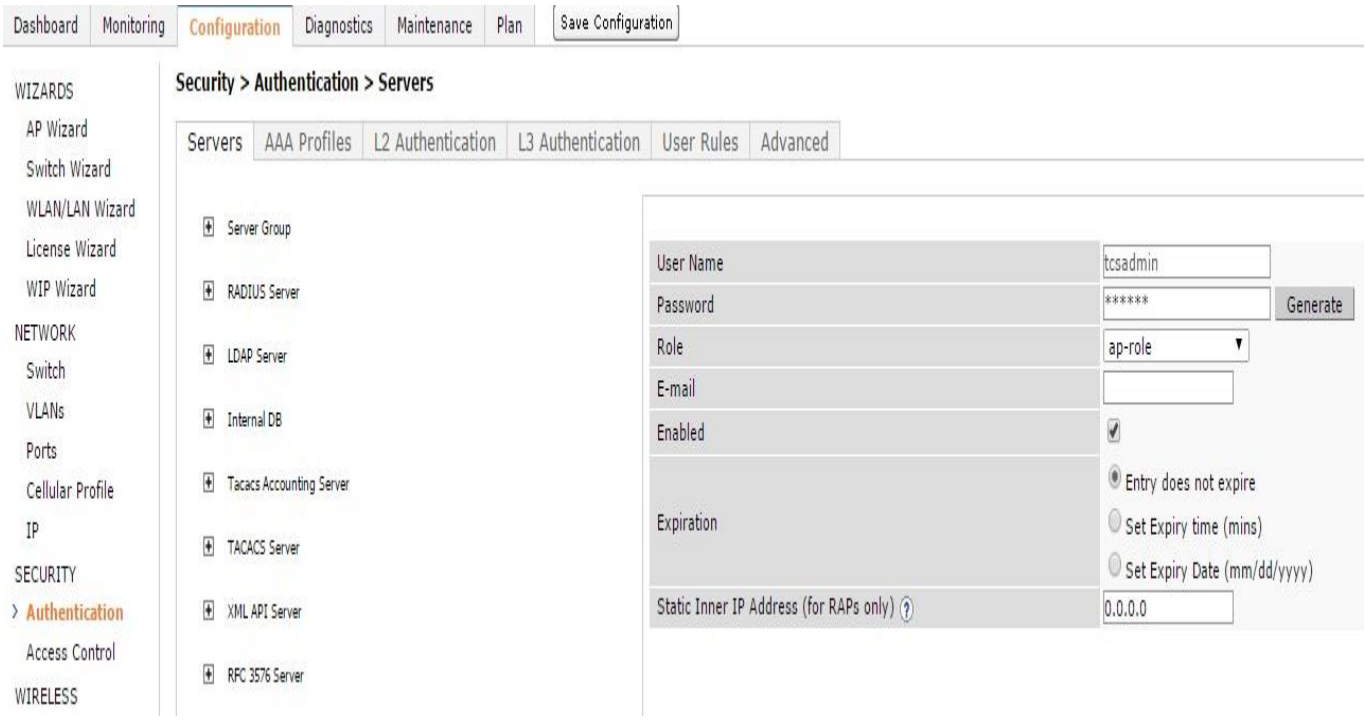
ระยะที่ 2 การลงมือปฏิบัติ (Do)

มหาวิทยาลัยเทคโนโลยีราชมงคลใช้อุปกรณ์แม่ข่ายสำหรับ Access Point เป็น Alcatel-Lucent OAW-4550

ขั้นตอนการทำ Remote Access Point (AP)

ตั้งค่าที่ Controller (Alcatel-Lucent(OAW-4550)

1. Create User
   - Security > Authentication > Servers เลือก **Internal DB**
   - ทำการ **Add User**
     User : **xxx**
     password : **xxx**
     Role : **ap-role**
     Static Inner IP Address : **0.0.0.0**



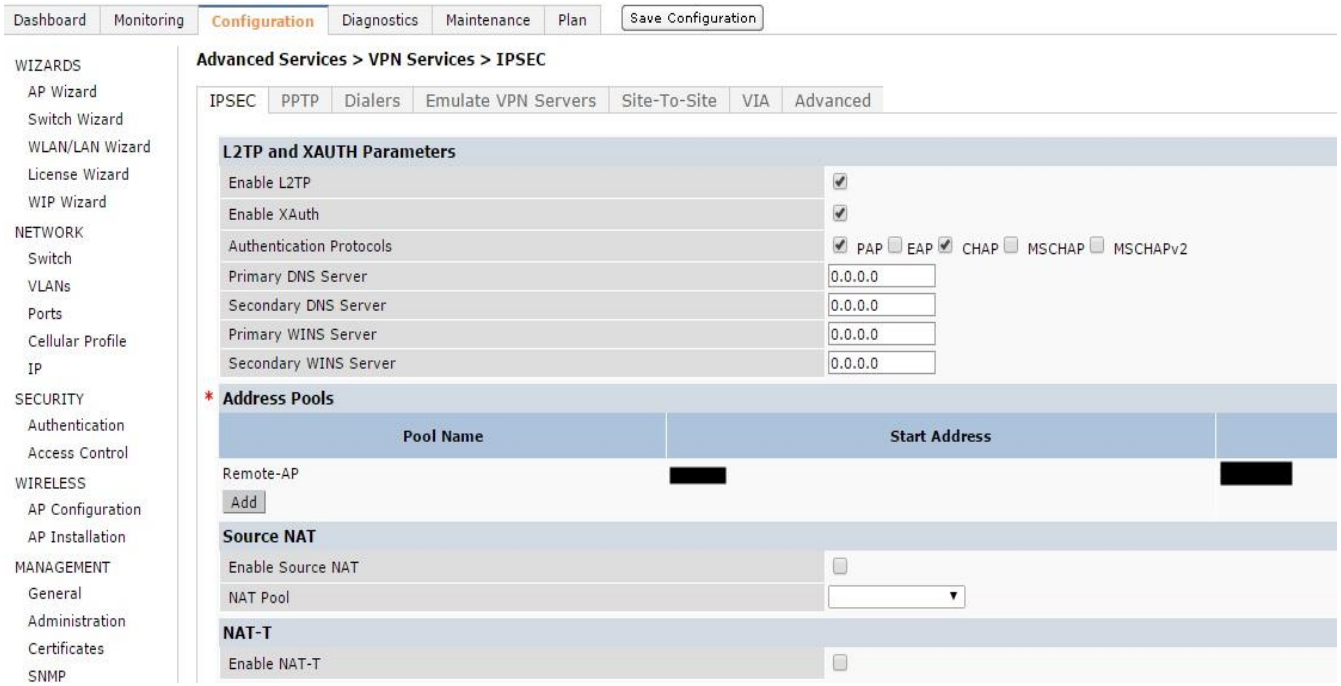
2. Create Address Pool

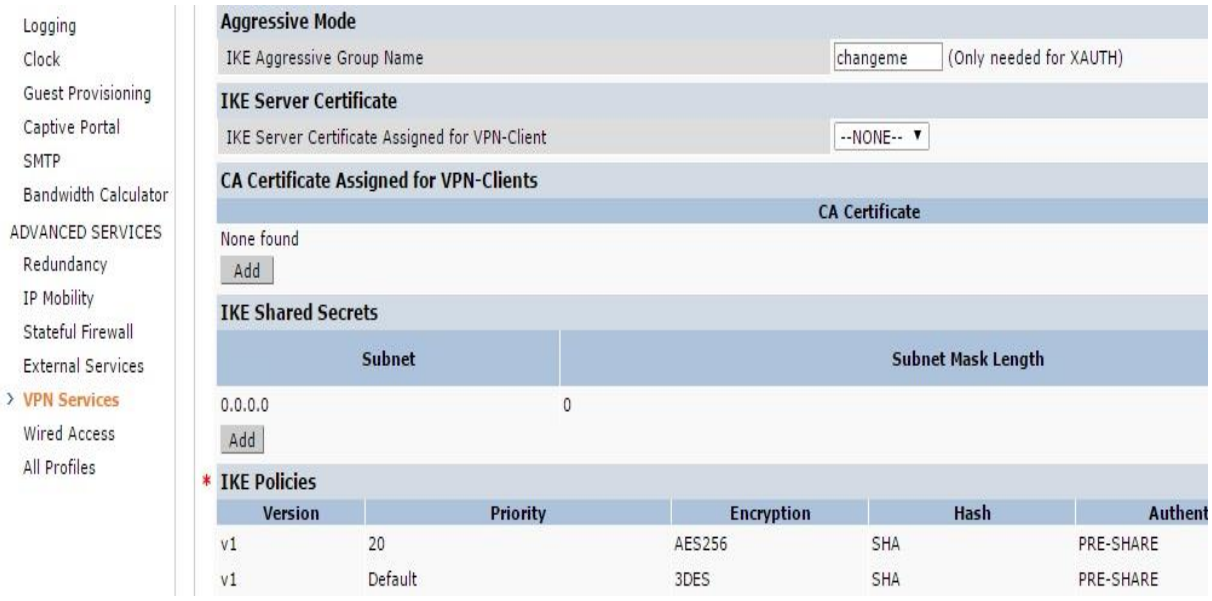
– Advanced Services> VPN Services > IPSEC

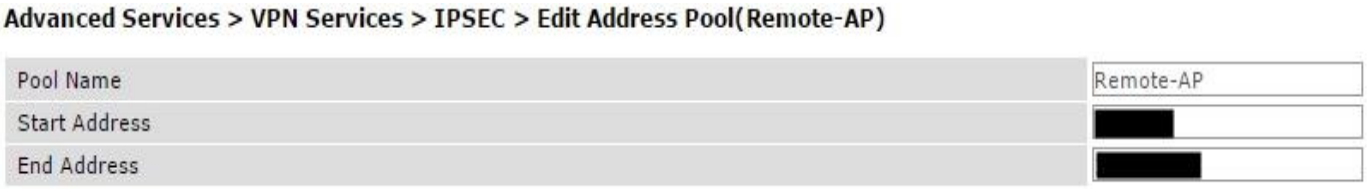
Pool Name : xxxx

Start Address : xxxx

End Address : xxxx







3. Create IKE Secret

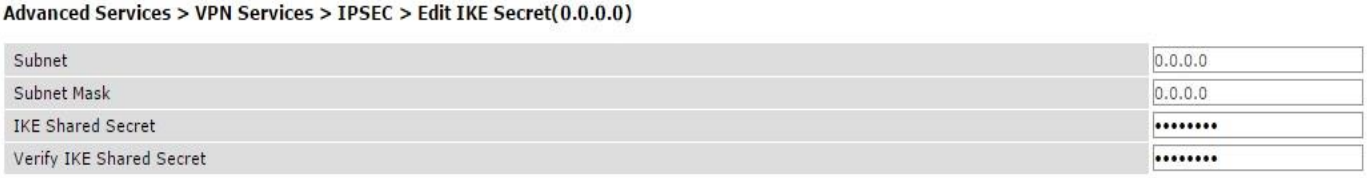
– Advanced Services > VPN Services > IPSEC > Edit IKE Secret

Subnet : 0.0.0.0

Subnet Mask : 0.0.0.0

IKE Shared Secret : xxxx

Verify IKE Shared Secret : xxxx



การตั้งค่า Access Point หรือการ Provision AP

1. ทำการ Reset factory AP

2. Provision AP

– Wireless > AP Installation > Provisioning

AP Group : ชื่อ pool address ที่สร้าง

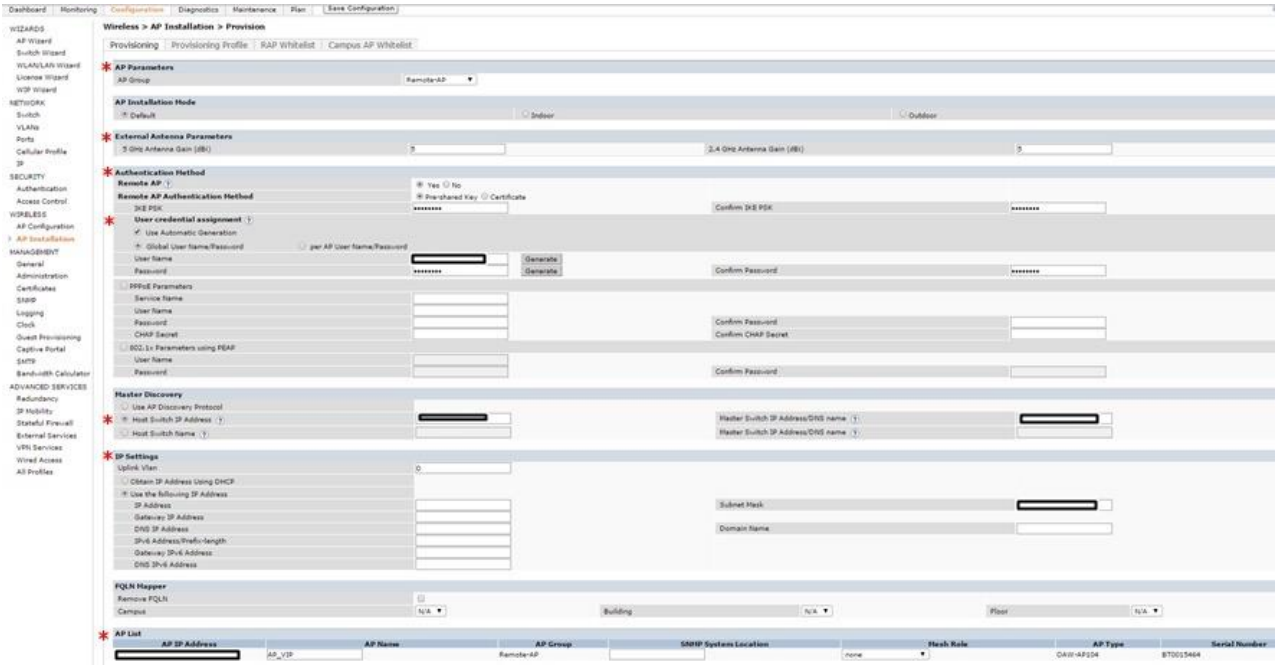
Authentication Method : Remote AP เลือก **Yes**

เลือก **Preshared Key :** ใส่รหัส IKE ที่สร้างไว้

ใส่ **User** และ **Password** ที่สร้าง

Host Switch IP Address : ใส่ IP Controller

IP Settings : เลือก DHCP หรือ กำหนดเอง



ระยะที่ 3 ตรวจสอบ (Check)

ตรวจสอบสถานะของ Access point

หลังจากได้ทำการตั้งค่าที่ Wireless controller และ Access point แล้วให้นำ Access point ไปติดตั้งเข้ากับระบบเครือข่ายอื่นที่ไม่ใช่ระบบเครือข่ายภายในมหาวิทยาลัย เช่น ต่อเข้ากับอินเตอร์เน็ตที่บ้าน ที่มหาวิทยาหรือสำนักงานอื่นๆ จะพบว่า Access point กระจายสัญญาณที่มี SSID เดียวกับในมหาวิทยาลัย ซึ่งสามารถตรวจสอบจาก wireless controller ได้

Network Summary

WLAN Network Status	Total Up	Total Down	IPSEC Up	IPSEC Down
WLAN Switches	1	0		
Access Points	148	0	1	0
Mesh Portals	0	0		
Mesh Points	0	0		
Air Monitors	0	0	0	0
Spectrum Monitors	0	0	0	0
Unprovisioned Access Points	0			
Duplicate AP Name	0			

จะสังเกตุเห็นได้ว่าเมื่อนำ Access point ไปติดตั้งยังนอกสถานที่ เมื่อดูสถานะของ wireless controller จะเห็น Access point ที่ขึ้นมาอยู่ในโหมด IPSEC UP อยู่หนึ่งตัว

Network > All IPSEC Access Points

Global APs

Name ▲	AP Group ▲	Status ▲	AP IP ▼	Outer AP IP	AP Type	Switch IP
remote-ap104	wifi-tw	up	1.1.1.170	203.158.176.118	OAW-AP104	10.1.255.2

Access point ที่นำไปติดตั้งยังนอกสถานที่ทางผู้ทดสอบได้ provision ไว้ชื่อ remote-ac104 จะสังเกตุเห็นได้ว่าหมายเลขไอพีแอดเดรสในช่อง Outer AP IP จะเป็นของเครือข่ายสถานที่นั้นๆที่นำไปติดตั้ง

ระยะที่ 4 การนำไปใช้ (Action)

1. นำไปใช้ในการพัฒนาระบบสารสนเทศของมหาวิทยาลัยให้มีประสิทธิภาพ รองรับความต้องการของนักศึกษาและมหาวิทยาลัย
2. ความสะดวกสบายในการใช้งานเครือข่ายไร้สายในมหาวิทยาลัยจากนอกสถานที่

ผลกระทบที่เป็นประโยชน์หรือการสร้างคุณค่า

1. ประโยชน์ที่บุคลากรในมหาวิทยาลัยได้รับ
   1.1 เจ้าหน้าที่ นักศึกษาสามารถเข้าใช้ทรัพยากรสารสนเทศได้สะดวกขึ้น
   1.2 ลดปัญหาที่อาจเกิดจากผู้ใช้ไม่มีความรู้ด้านระบบคอมพิวเตอร์
   1.3 สามารถเก็บข้อมูลการเข้าใช้งานของผู้ใช้ได้

2. ประโยชน์ที่มหาวิทยาลัยจะได้รับ
   2.1 มหาวิทยาลัยมีความก้าวทันทางเทคโนโลยี ส่งผลดีต่อชื่อเสียงของมหาวิทยาลัย
   2.2 เป็นต้นแบบแนวความคิดในการพัฒนาระบบเครือข่ายให้กับมหาลัยวิทยาลัยอื่นๆที่สนใจนำไปใช้

ปัจจัยแห่งความสำเร็จ

1. เครือข่ายภายนอกที่นำ Access Point ไปเชื่อมต่อจะต้องมีความเร็วของอินเตอร์เน็ตไม่ต่ำกว่า 10 เมกกะบิท
2. สามารถติดต่อกับผู้ดูแลระบบเครือข่ายปลายทางได้ในกรณีเกิดปัญหาในการนำอุปกรณ์ภายนอกไปเชื่อมต่อ
3. ความเร็วในการใช้งานอินเตอร์เน็ตจะขึ้นอยู่กับสถานที่นั้นๆที่นำไปติดตั้ง

1. ปัญหาและอุปสรรค

1.1 ระบบเครือข่ายภายนอกที่นำไปเชื่อต่อ อาจมีการทำระบบยืนยันตัวตน (authentication) ทำให้ ap ไม่สามารถวิ่งกลับไปหาอุปกรณ์แม่ข่าย (wireless controller) ได้ ดังนั้นจึงต้องผสานงานกับทางผู้ดูแลระบบให้บายพาส พาสเวิร์ดให้ชั่วคราว

1.2 ความเร็วและความเสถียรของระบบเครือข่ายที่นำไปติดตั้งไม่เพียงพอแต่การทำ remote ap อาจทำให้เมื่อผู้ใช้งานเชื่อมต่อเข้ามาแล้วไม่สามารถใช้งานได้อย่างมีประสิทธิภาพ

2. แนวทางแก้ไข

จะต้องมีการติดต่อผสานงานกับผู้ดูแลระบบเครือข่ายภายทางก่อนที่จะนำอุปกรณ์ไปติดตั้ง