การจัดการอุปกรณ์เครือข่ายไร้สาย
ระดับหน่วยงานให้มีประสิทธิภาพ

โดย

นายนคร บริพนธ์มงคล

ฝ่ายระบบคอมพิวเตอร์และเครือข่าย
สำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ

SWU IT Best practice

หัวข้อนำเสนอ

- เครือข่ายไวเลสแลน
- เครือข่ายไวเลสแลนในมหาวิทยาลัย
- แนวทางกำหนดค่าอุปกรณ์ไวเลสแลน
- การติดตามและจัดเก็บสถิติ
- ประโยชน์สูงสุด
- แนวปฏิบัติเพื่อความมั่นคงปลอดภัย

SWU IT Best practice

เครือข่ายไวเลสแลน

- **เครือข่ายไวเลสแลน**

เครือข่ายคอมพิวเตอร์ไร้สาย หรือ ไวเลสแลน (Wireless LAN) เทคโนโลยีการสื่อสารข้อมูลระหว่างอุปกรณ์ไอซีที โดยผ่านคลื่นความถี่วิทยุแทนการใช้งานสัญญาณ

1

2

3

6

5

4

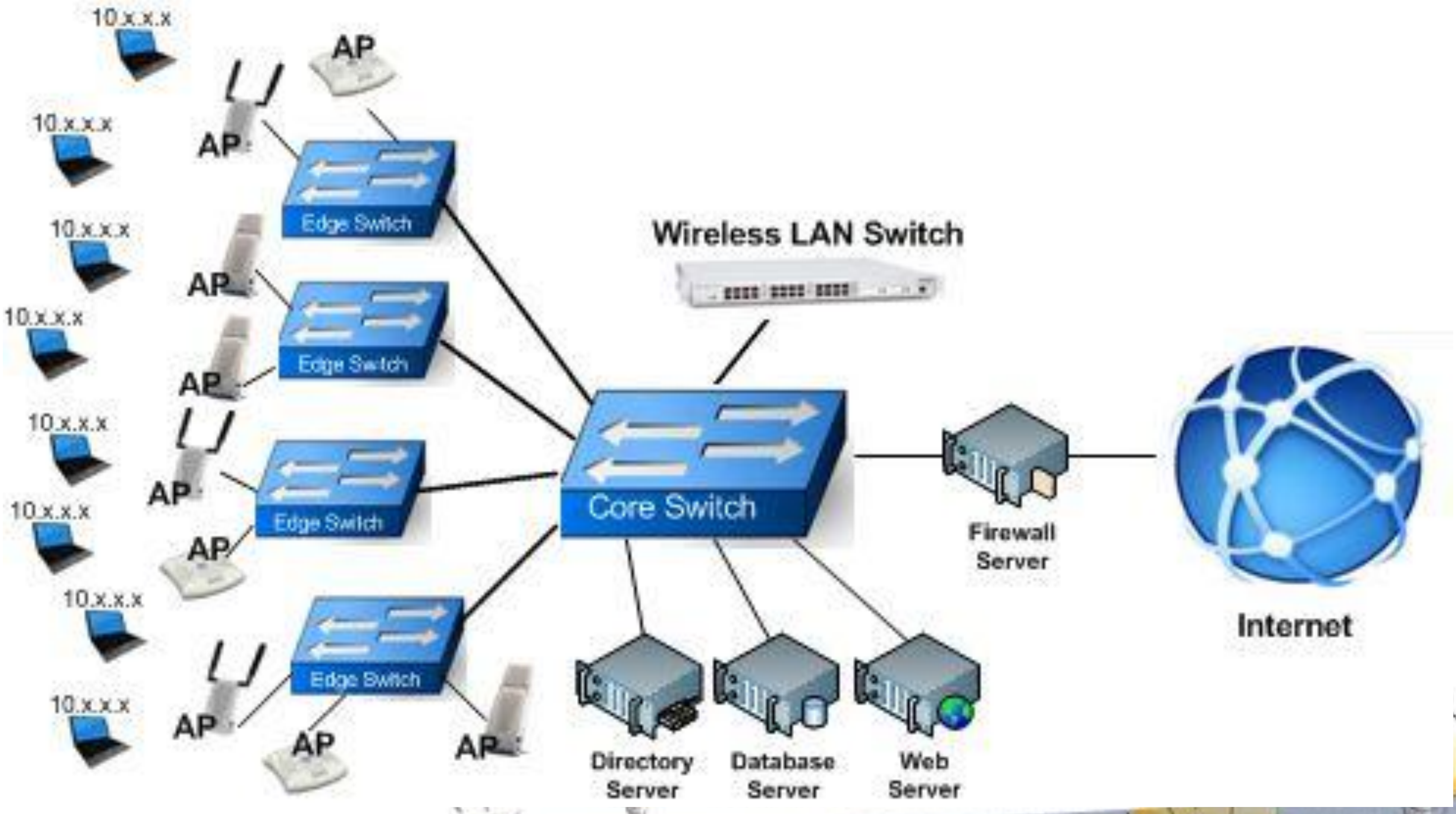
SWU IT Best practice

เครือข่ายไวเลสแลนในมหาวิทยาลัย

- **เครือข่ายไร้สาย WiSE (Wireless Service for Education)**
  - เพื่อเพิ่มช่องทางการเข้าถึงข้อมูลสารสนเทศ
  - เพื่ออำนวยความสะดวกให้นักศึกษา นิสิต คณาจารย์และบุคลากร สืบค้นข้อมูลสารสนเทศ
  - เพื่อสร้างสังคมแห่งการเรียนรู้นอกห้องเรียน
  - เพื่อลดพื้นที่และทรัพยากรคอมพิวเตอร์
- **นโยบายเครือข่ายไร้สาย**
  - บริการครอบคลุมพื้นที่ใต้อาคาร ห้องประชุมมหาวิทยาลัย และพื้นที่ส่วนกลาง
  - ผู้ใช้ต้องมี Buasri ID เพื่อพิสูจน์ตัวตนก่อนเข้าใช้บริการ
  - ดำเนินงานตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

เครือข่ายไวเลสแลนในมหาวิทยาลัย

- Enterprise Wireless LAN
  - การบริหารจัดการทำจากศูนย์กลาง



เครือข่ายไวเลสแลนในมหาวิทยาลัย

- Enterprise Wireless LAN
  - รองรับผู้ใช้จำนวนมากอย่างมีประสิทธิภาพ

บริหารจากส่วนกลาง

อัตโนมัติคลื่นความถี่
และช่วงสัญญาณ

ตรวจสอบสิทธิ์

รักษาความปลอดภัย

ตรวจสอบผู้บุกรุก
ข้อมูลสถิติ

ตรวจสอบข้อมูลและไวรัส

ลงทะเบียนอุปกรณ์

รับ-ส่งข้อมูล

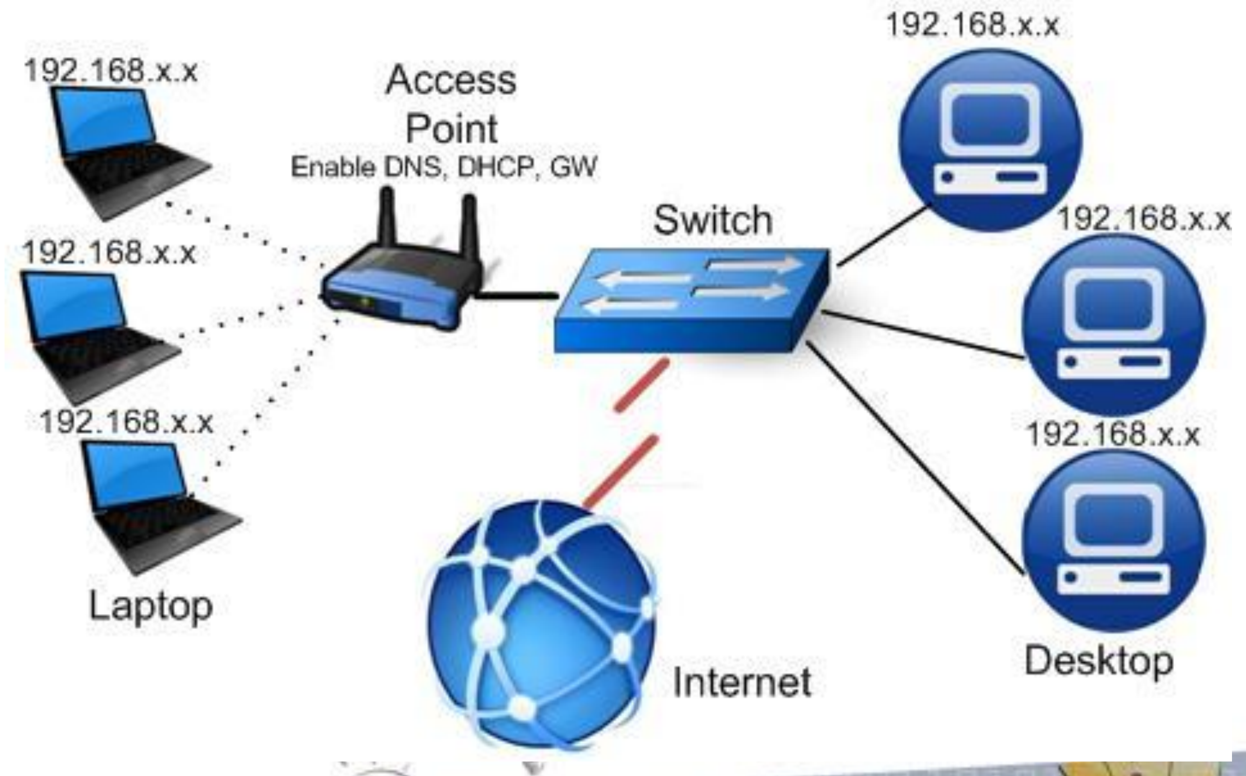
ทำงานตามนโยบาย

ไฟแสดงสถานะ

SWU IT Best practice

แนวทางกำหนดค่าอุปกรณ์ไวเลสแลน

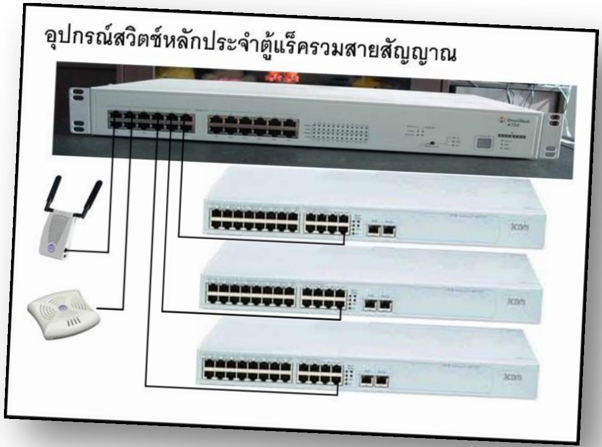
- SOHO Wireless LAN
  - จำกัดจำนวนผู้ใช้, ขาดการจัดการจากศูนย์กลาง
  - อุปกรณ์ทำงานหนักขึ้นเมื่อมีผู้ใช้งานมากขึ้น



แนวทางกำหนดค่าอุปกรณ์ไวเลสแลน

- SOHO Wireless LAN

กรณีหน่วยงานจัดซื้ออุปกรณ์เอง

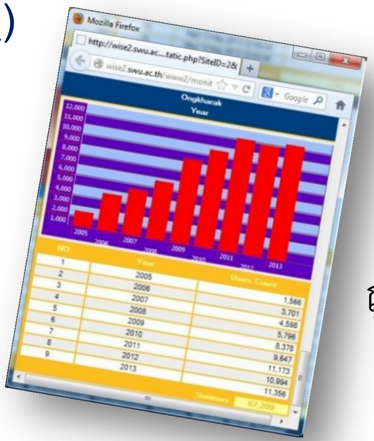


- ห้ามเชื่อมต่อสายแลนกับอุปกรณ์ไวเลสแลนตัวใหม่
- ติดต่อเจ้าหน้าที่สำนักคอมพิวเตอร์ (ก่อนซื้อ/หลังซื้อ)
- ปิดการแจกหมายเลขไอพีแอดเดรส (IP Address)
- ปิดระบบรักษาความปลอดภัย (Firewall)
- ปิดการตรวจสอบสิทธิ์ และให้ระบบ IPass ดำเนินการ
- ตำแหน่ง/ช่อง การเชื่อมต่อสายแลนกับอุปกรณ์ไวเลสแลน
- ***(ควรจัดซื้ออุปกรณ์ไวเลสแลนตามมาตรฐานที่สำนักคอมพิวเตอร์กำหนด)***

SWU IT Best practice

การติดตามและจัดเก็บสถิติ

- เว็บไซต์ WiSE (http://wise.swu.ac.th)
  - ตำแหน่งติดตั้งอุปกรณ์ไวเลสแลน
  - สถานะอุปกรณ์, จำนวนผู้ใช้งาน, ข้อมูลข่าวสาร, สถิติการใช้งาน
  - ตรวจสอบสถานะอุปกรณ์เคลื่อนที่ถูกตัดการเชื่อมต่อ



- แฟนเพจ สนค. (http://www.facebook.com/SWUComputerCenter
  - บริการประชาสัมพันธ์ข้อมูลข่าวสาร
  - บริการตอบปัญหาผู้ใช้
  - สร้างกลุ่มความร่วมมือผู้ใช้บริการกับสำนักคอมพิวเตอร์

ประโยชน์สูงสุง

- ตั้งเป้าหมายร่วมกัน...
  - แนวทางการใช้นวัตกรรมด้านไอซีที่เป็นไปในทิศทางเดียวกัน
  - มีมาตรฐานเดียวกัน, เกิดคุณภาพการบริการ และเกิดประโยชน์สูงสุดกับผู้ใช้และองค์กร

แนวปฏิบัติเพื่อความมั่นคงปลอดภัย

- แนวปฏิบัติการจัดการเครือข่ายไร้สาย (Wireless Management)

วัตถุประสงค์

– เพื่อเป็นแนวปฏิบัติสำหรับการบริหารจัดการระบบเครือข่ายไร้สาย WiSE (Wireless Service for Education) ของมหาวิทยาลัย ให้มีความเหมาะสมและสอดคล้องกับนโยบายด้านความมั่นคงปลอดภัยของสารสนเทศ มหาวิทยาลัยศรีนครินทรวิโรฒ

ผู้ปฏิบัติ

– ผู้ดูแลระบบ และผู้ใช้งาน

แนวปฏิบัติ

– ผู้ดูแลระบบต้องควบคุมสัญญาณอุปกรณ์กระจายสัญญาณไวเลสแลน (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

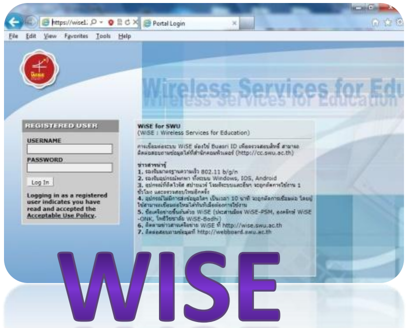
– ผู้ดูแลระบบควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าเริ่มต้นไว้ (Default setting) โดยเจ้าของผลิตภัณฑ์ เมื่อนำอุปกรณ์กระจายสัญญาณไวเลสแลนมาใช้งาน

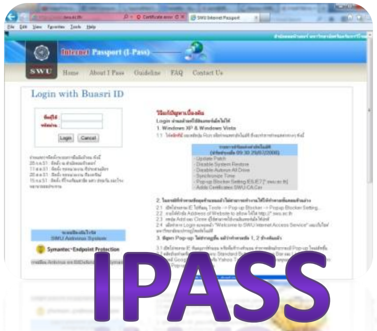
แนวปฏิบัติเพื่อความมั่นคงปลอดภัย

- แนวปฏิบัติการจัดการเครือข่ายไร้สาย (Wireless Management)

แนวปฏิบัติ (ต่อ)

- อุปกรณ์กระจายสัญญาณไวเลสแลนที่มีคุณสมบัติตามข้อกำหนดมาตรฐานของมหาวิทยาลัย ต้องถูกกำหนดการยืนยันพิสูจน์ตัวตนการเข้าใช้งานเครือข่ายบัวศรีของมหาวิทยาลัย
- กรณีอุปกรณ์กระจายสัญญาณไวเลสแลนที่จัดหาไม่สามารถติดตั้งระบบการยืนยันพิสูจน์ตัวตนการเข้าใช้งานเครือข่ายบัวศรีตามข้อ 3 ได้นั้น ผู้ดูแลระบบต้องกำหนดค่าเป็นแบบบริดจ์ (Bridge) เท่านั้น เพื่อให้ผู้ใช้งานยืนยันตัวตนผ่านระบบของมหาวิทยาลัย





SWU IT Best practice

แนวปฏิบัติเพื่อความมั่นคงปลอดภัย

- **แนวปฏิบัติการจัดการเครือข่ายไร้สาย (Wireless Management)**

  แนวปฏิบัติ (ต่อ)

  – ผู้ดูแลระบบควรมีการติดตั้งไฟร์วอลล์ (Firewall) ป้องกันระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

  – ผู้ดูแลระบบควรมีซอฟต์แวร์ หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย เพื่อติดตามและบันทึกเหตุการณ์น่าสงสัยในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก 3 เดือน และในกรณีที่ตรวจพบความผิดปกติในการใช้งาน ผู้ดูแลระบบต้องรายงานต่อผู้บริหารของหน่วยงานให้ทราบทันที

  – ผู้ดูแลระบบต้องควบคุมมิให้บุคคล หรือหน่วยงานภายนอกที่มิได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายของมหาวิทยาลัย เพื่อป้องกันการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในของมหาวิทยาลัย

การจัดการอุปกรณ์เครือข่ายไร้สาย

ระดับหน่วยงานให้มีประสิทธิภาพ

SWU IT Best practice