

ขั้นตอนการติดตั้งและการให้บริการเซิร์ฟเวอร์
หน่วยงานมหาวิทยาลัยเกษตรศาสตร์เพื่อให้
สอดคล้องกับ พรบ.คอมพิวเตอร์ 2550
ศูนย์ปฏิบัติการเครือข่าย
ฝ่ายระบบคอมพิวเตอร์และเครือข่าย
สำนักบริการคอมพิวเตอร์

หัวข้อ

- ส่วนประกอบของระบบ

- ระบบทะเบียนเครื่อง

- ระบบยืนยันตัวตนบุคคล

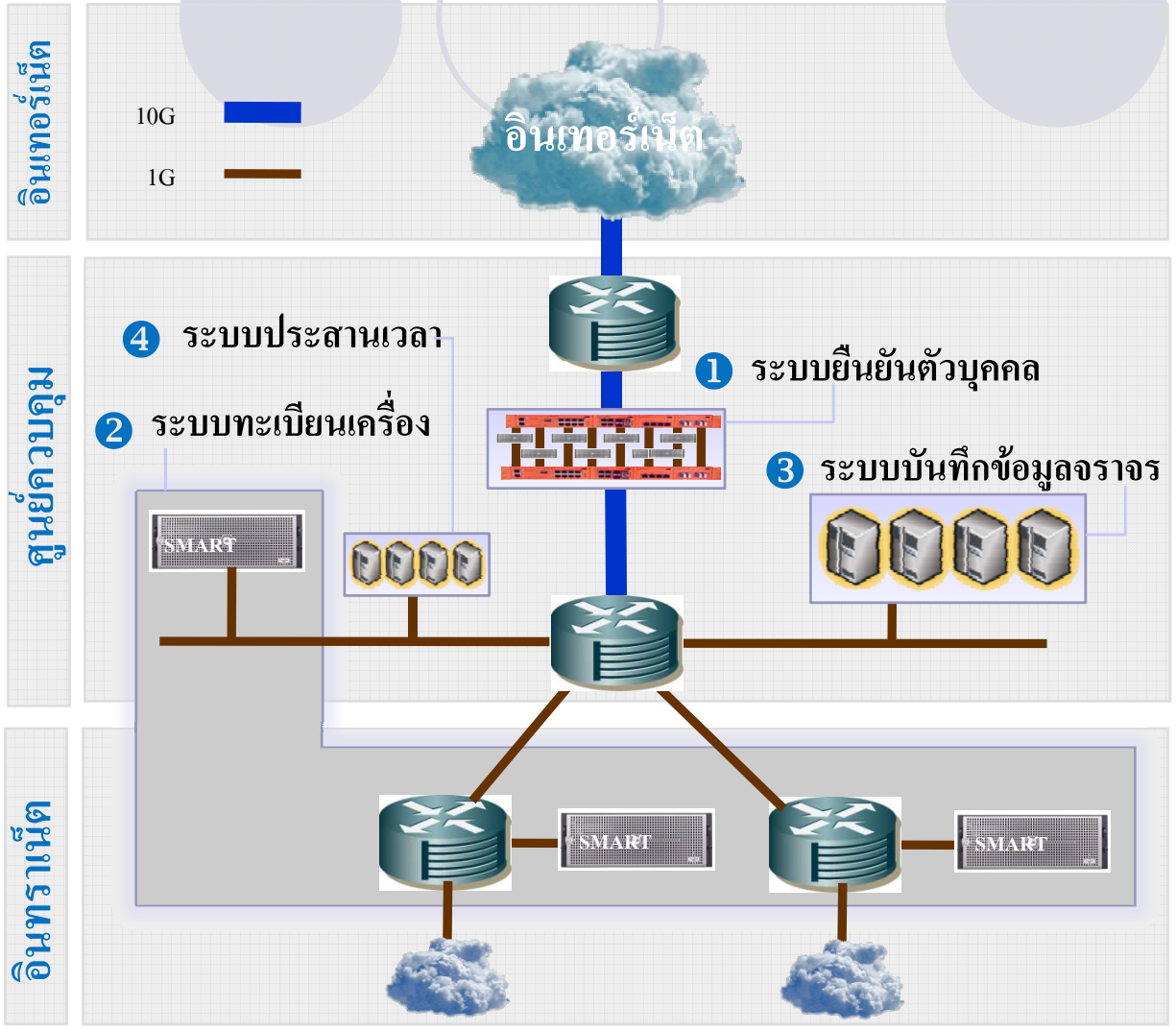
- ระบบบันทึกข้อมูลจราจร

- ระบบประสานเวลา

- ข้อปฏิบัติสำหรับเครื่อง Server ที่ต้องการเปิดให้บริการ

- แนวทางการดำเนินการหากไม่ปฏิบัติตาม

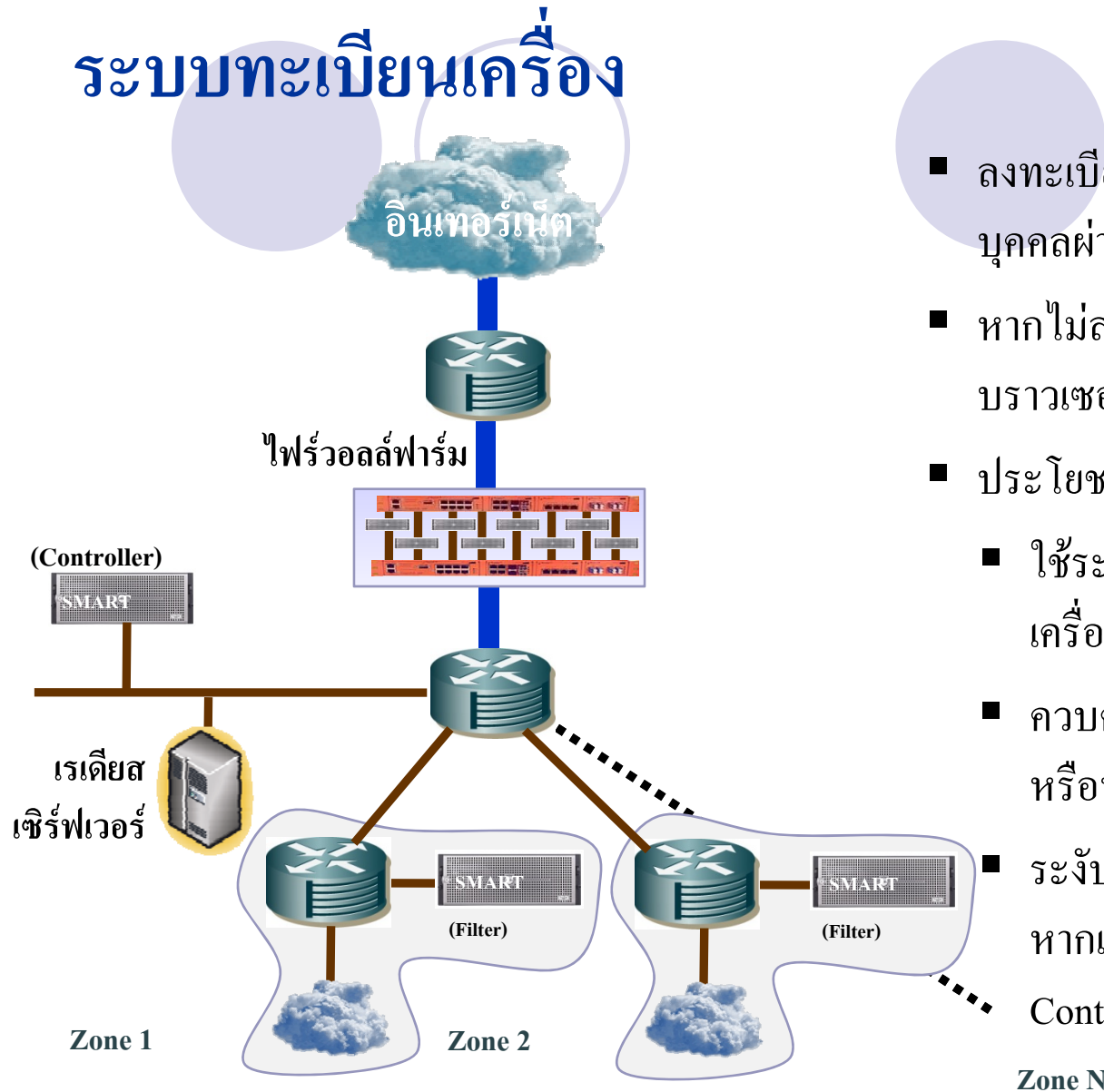
ส่วนประกอบของระบบ



- 1 ระบบยืนยันตัวตนบุคคลผ่านไฟร์วอลล์ ใช้ระบุตัวบุคคลเพื่อขอสิทธิ์เข้าใช้เครือข่าย
- 2 ระบบทะเบียนเครื่อง ใช้ระบุ MAC Address และบุคคลผู้ดูแลเครื่อง
- 3 ระบบบันทึกข้อมูลจราจรคอมพิวเตอร์
- 4 ระบบประสานเวลาผ่าน NTP

แหล่งที่มา: presentation ของ รศ. สุรศักดิ์ สงวนพงษ์ ในงาน WUNCA19

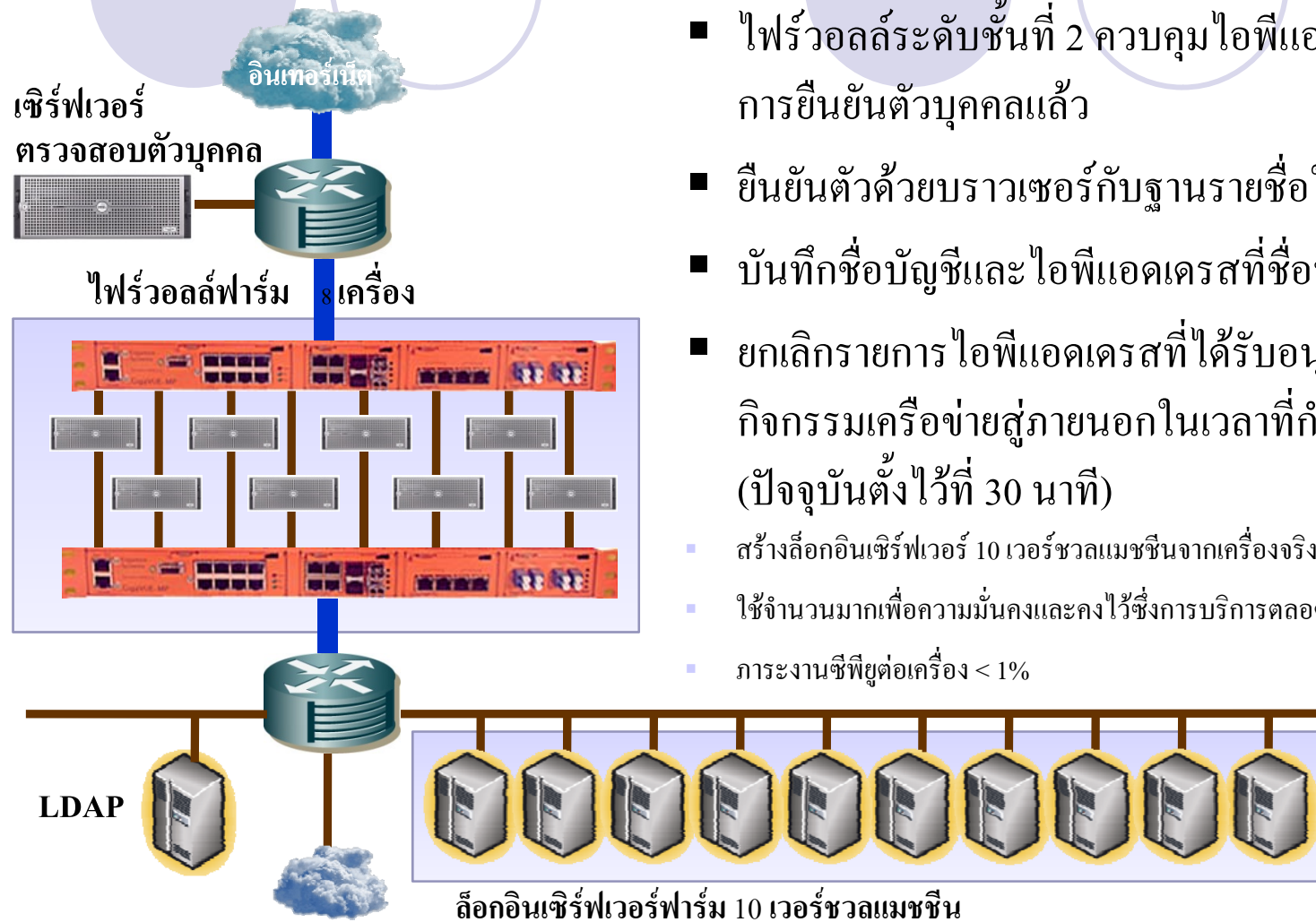
ระบบทะเบียนเครื่อง



- ลงทะเบียน MAC Address และข้อมูลส่วนบุคคลผ่านเว็บ ครั้งแรกเพียงครั้งเดียว
- หากไม่ลงทะเบียน จะถูกเปลี่ยนหน้าจอบราวเซอร์สู่จอลงทะเบียน เมื่อเข้าใช้เครือข่าย
- ประโยชน์
 - ใช้ระบุตัวบุคคลผู้เป็นเจ้าของหรือผู้ดูแลเครื่อง เพื่อติดตามปัญหา
 - ควบคุมการเข้าใช้เพื่อยืนยันเป็นบุคลากรหรือนิสิตที่มีบัญชีใน LDAP
 - ระบุหรือจำกัดขอบเขตการใช้เครือข่ายหากเครื่องสร้างปัญหาต่อระบบ (Zone Control)

แหล่งที่มา: presentation ของ รศ. สุรศักดิ์ สงวนพงษ์ ในงาน WUNCA19

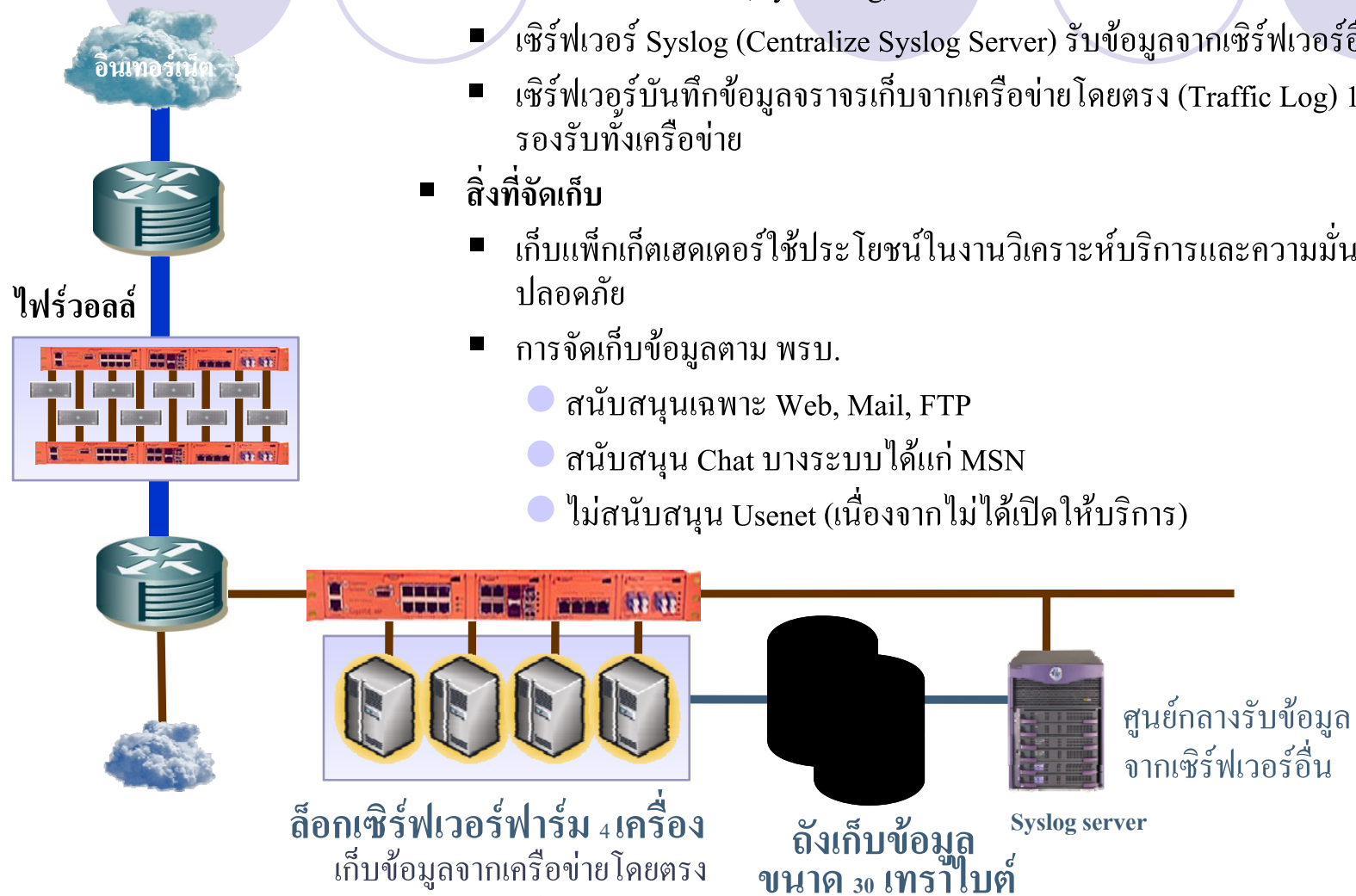
ระบบยืนยันตัวตนบุคคล



- ไฟร์วอลล์ระดับชั้นที่ 2 ควบคุมไอพีแอดเดรสที่ผ่านการยืนยันตัวตนแล้ว
- ยืนยันตัวด้วยบราวเซอร์กับฐานรายชื่อใน LDAP
- บันทึกชื่อบัญชีและไอพีแอดเดรสที่ชื่อบัญชื่อนั้นใช้งาน
- ยกเลิกรายการไอพีแอดเดรสที่ได้รับอนุญาต หากไม่มีกิจกรรมเครือข่ายสู่ภายนอกในเวลาที่กำหนด (ปัจจุบันตั้งไว้ที่ 30 นาที)
 - สร้างล็อกอินเซิร์ฟเวอร์ 10 เวอร์ชวลแมชชีนจากเครื่องจริง 2 เครื่อง
 - ใช้จำนวนมากเพื่อความมั่นคงและคงไว้ซึ่งการบริการตลอดเวลา
 - ภาระงานซีพียูต่อเครื่อง < 1%

แหล่งที่มา: presentation ของ รศ. สุรศักดิ์ สงวนพงษ์ ในงาน WUNCA19

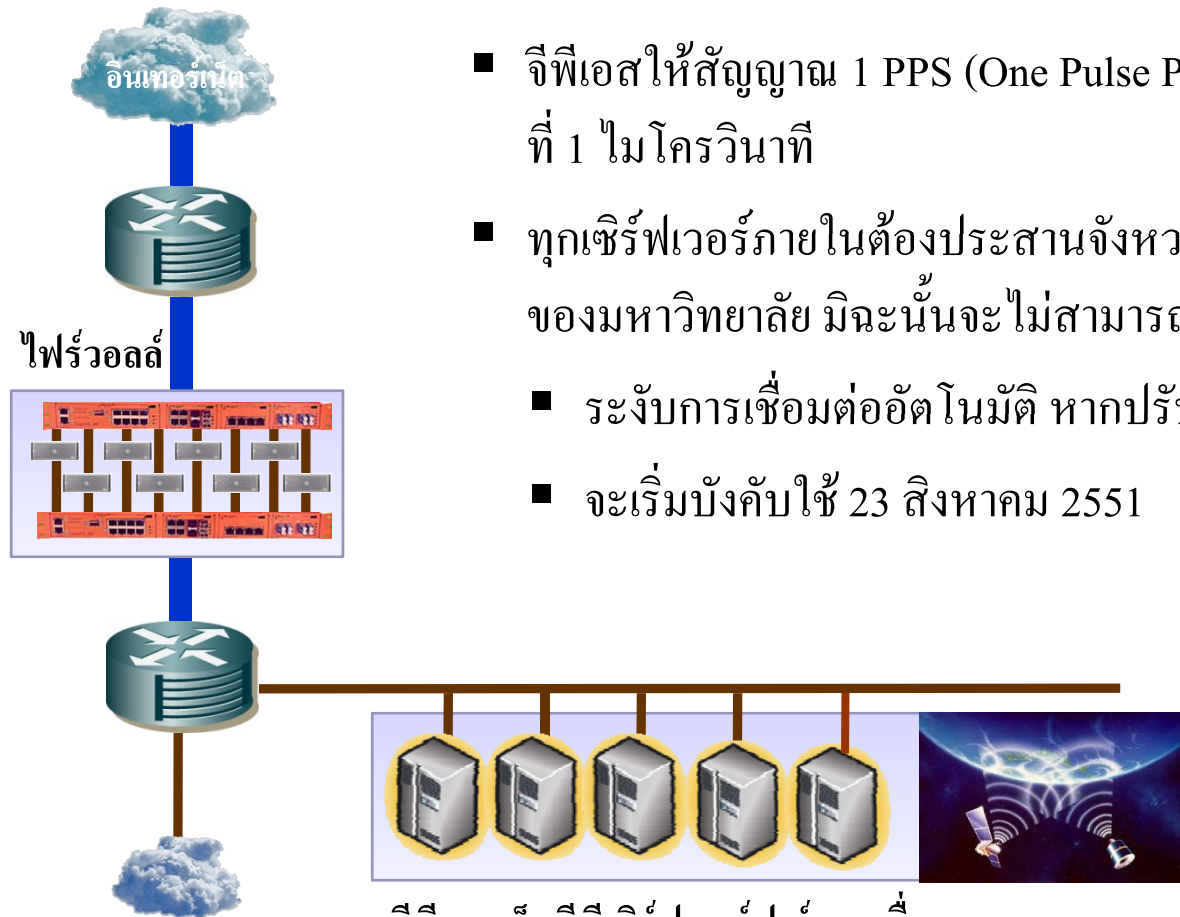
ระบบบันทึกข้อมูลจราจร



- ระบบบันทึกแบบผสม (Hybrid log)
 - เซิร์ฟเวอร์ Syslog (Centralize Syslog Server) รับข้อมูลจากเซิร์ฟเวอร์อื่น
 - เซิร์ฟเวอร์บันทึกข้อมูลจราจรเก็บจากเครือข่ายโดยตรง (Traffic Log) 1 ชุดรองรับทั้งเครือข่าย
- สิ่งที่จัดเก็บ
 - เก็บแพ็กเก็ตแฮดเดอร์ใช้ประโยชน์ในงานวิเคราะห์บริการและความมั่นคงปลอดภัย
 - การจัดเก็บข้อมูลตาม พรบ.
 - สนับสนุนเฉพาะ Web, Mail, FTP
 - สนับสนุน Chat บางระบบได้แก่ MSN
 - ไม่สนับสนุน Usenet (เนื่องจากไม่ได้เปิดให้บริการ)

แหล่งที่มา: presentation ของ รศ. สุรศักดิ์ สงวนพงษ์ ในงาน WUNCA19
Office of Computer Services

ระบบประสานเวลา

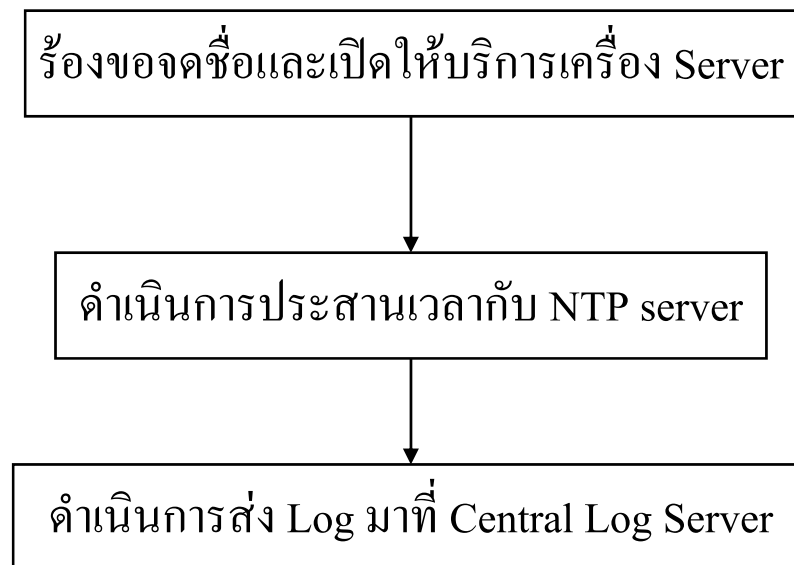


จีพีเอส เอ็นทีพีเซิร์ฟเวอร์ฟาร์ม 5 เครื่อง
แหล่งที่มา: presentation ของ รศ. สุรศักดิ์ สงวนพงษ์ ในงาน WUNCA19

- เซิร์ฟเวอร์ NTP Stratum 1 ผ่านจีพีเอส จำนวน 5 เครื่อง
- จีพีเอสให้สัญญาณ 1 PPS (One Pulse Per Second) ที่ความถูกต้องที่ 1 ไมโครวินาที
- ทุกเซิร์ฟเวอร์ภายในต้องประสานจังหวะนาฬิกาผ่าน NTP หลักของมหาวิทยาลัย มิฉะนั้นจะไม่สามารถให้บริการได้
 - ระวังการเชื่อมต่ออัตโนมัติ หากปรับตั้ง NTP
 - จะเริ่มบังคับใช้ 23 สิงหาคม 2551



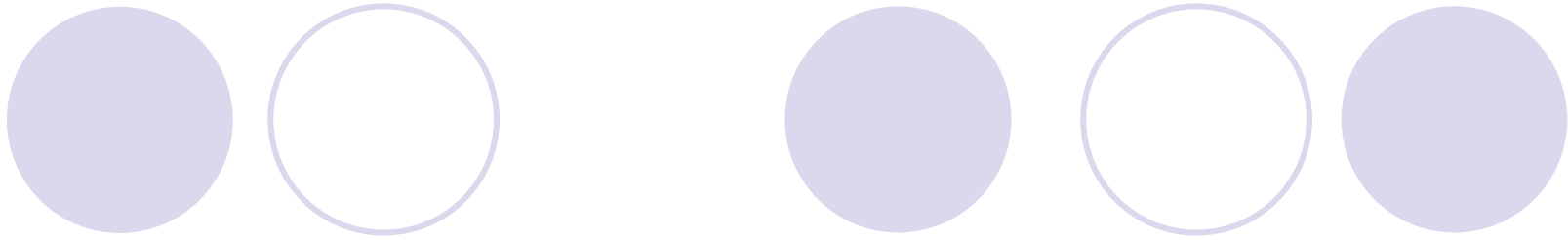
ข้อปฏิบัติสำหรับเครื่อง Server ที่ต้องการเปิดให้บริการ



- ผู้ให้บริการเครื่อง Server ต้องดำเนินการจัดซื้อเครื่อง และขออนุญาตเปิดให้บริการ โดยได้รับการรับรองจาก หัวหน้าหน่วยงานระดับคณะขึ้นไป
- ผู้ให้บริการเครื่อง Server ต้องประสานจังหวัดหระนาพิกา ผ่าน NTP หลักของมหาวิทยาลัย
- ผู้ให้บริการเครื่อง Server ต้องส่ง Log ของเครื่อง ที่ให้บริการมายัง Central Log Server ของ มหาวิทยาลัย

แนวทางการดำเนินการหากไม่ปฏิบัติตาม

- หากไม่ดำเนินการประสานแจ้งหวนาพิกากับ NTP ของทางมหาวิทยาลัย และไม่ส่ง Log มาให้เครื่อง Central Log Server ของมหาวิทยาลัย ทางสำนักบริการคอมพิวเตอร์จำเป็นต้อง “ระงับการให้บริการเครื่อง Server นั้น” โดยจะดำเนินการตรวจสอบในช่วงเวลา 1 วันและจะทำการตรวจสอบและดำเนินการทุกเที่ยงคืนของวัน



คำถามและคำตอบ

ข้อปฏิบัติสำหรับเครื่อง Server ที่ต้องการเปิดให้บริการ

- ผู้ให้บริการเครื่อง Server ต้องดำเนินการจดชื่อเครื่องและขออนุญาตเปิดให้บริการ
- ผู้ให้บริการเครื่อง Server ต้องประสานแจ้งหระนาพิก้าผ่าน NTP หลัคของมหาวิทยาลัย
- ผู้ให้บริการเครื่อง Server ต้องส่ง Log ของเครื่องที่ให้บริการมายัง Central Log Server ของมหาวิทยาลัย