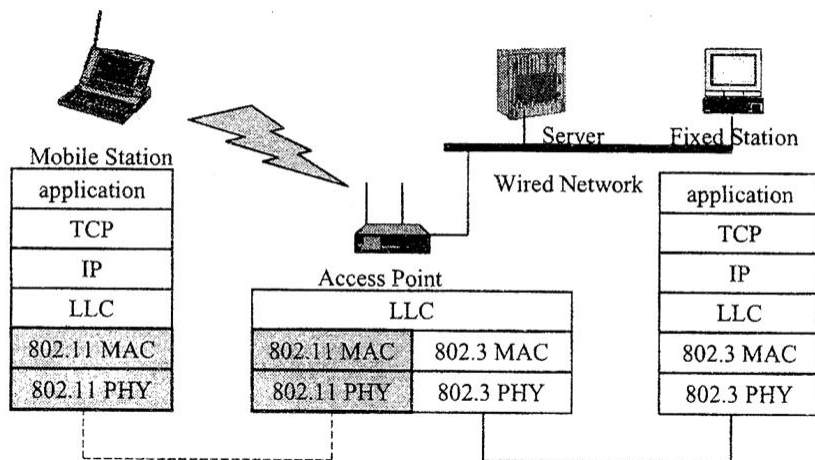


Wireless LAN Security

ดร. ธัญชัย ตรีกาภ

1

Wireless LAN model



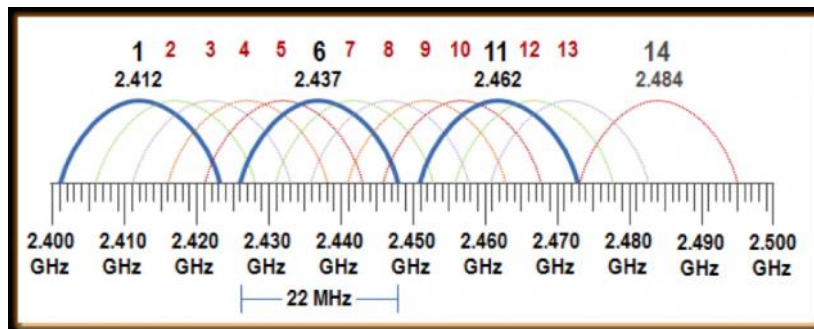
2

IEEE 802.11?

	802.11	802.11b	802.11a	802.11g	??
Year	1997	1999	2001	2002	??
Speed	1-2Mbps	5/11 Mbps	<54 Mbps	??	??
Freq.	2.4 GHz	2.4 GHz	??	2.4 GHz	??
Chan.	FHSS-75 DSSS-14	??	12 (3 n-over)	3 n-over	??
Range	-	100 m	30 m	100 m	??

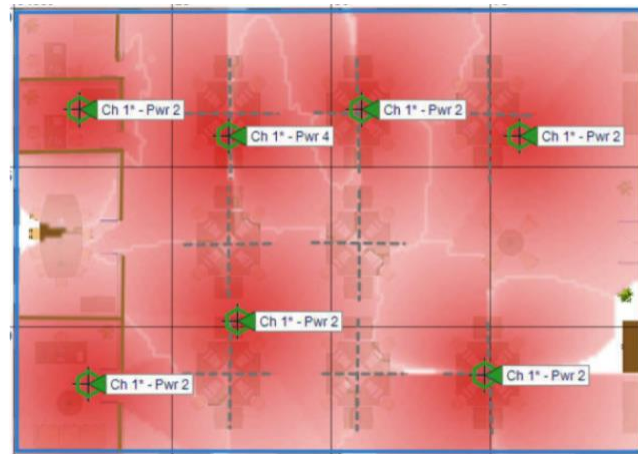
3

Channel



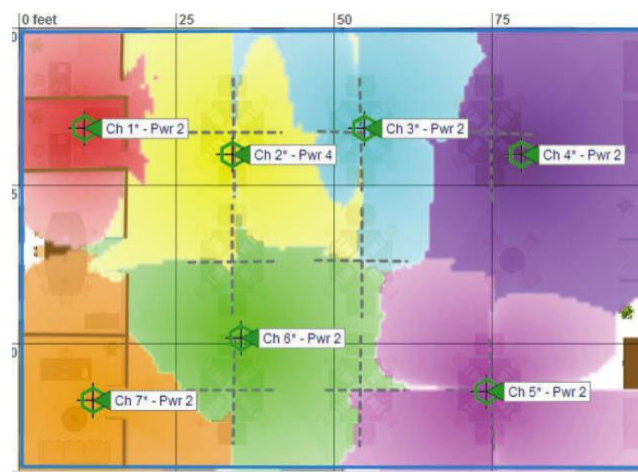
4

Channel



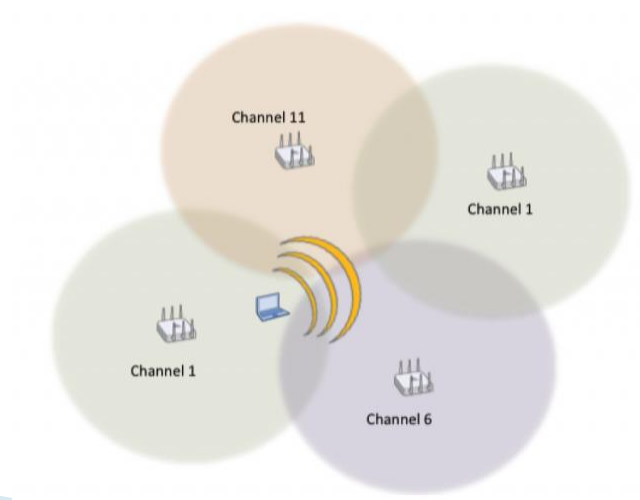
5

Channel



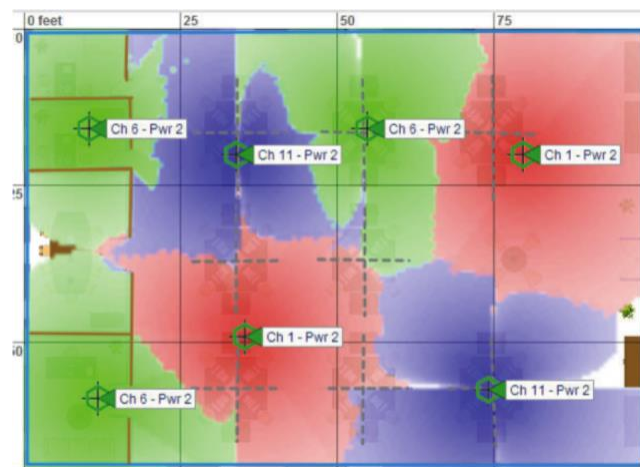
6

Channel

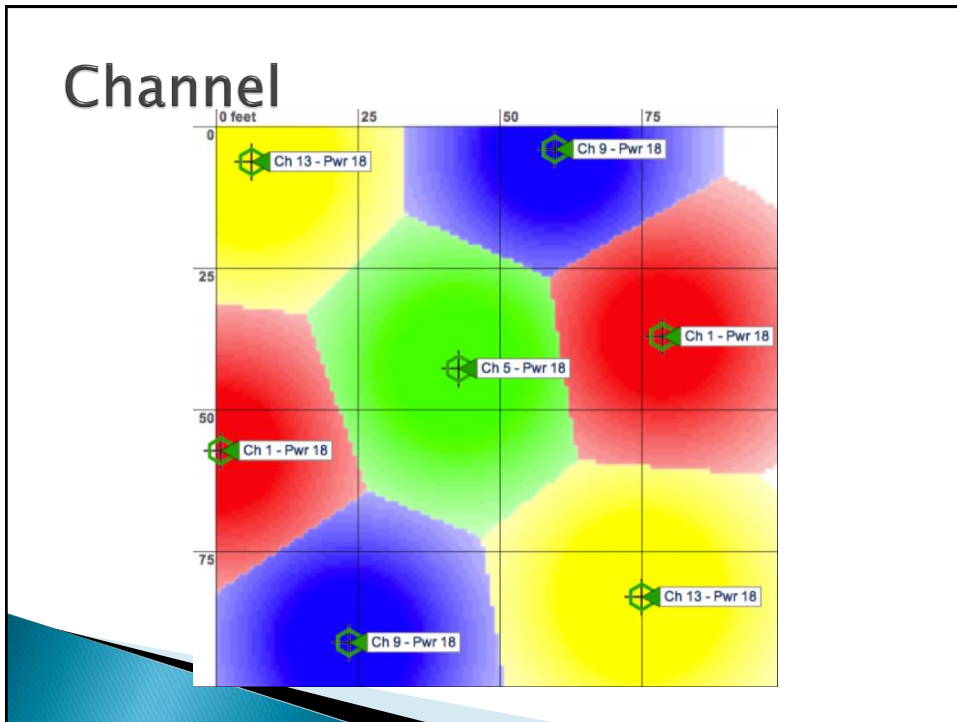


7

Channel





8



9

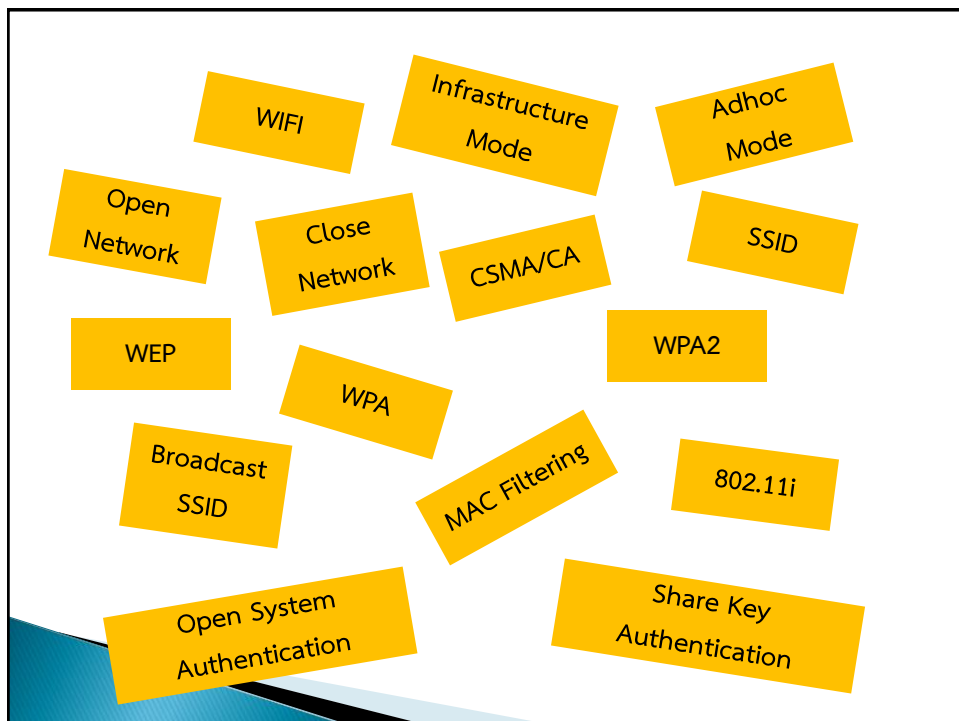
tools

- ▶ Wifi Analyzer 
- ▶ Vistumbler 

10



11



12

Security พื้นฐานของ 802.11 มีอะไรบ้าง



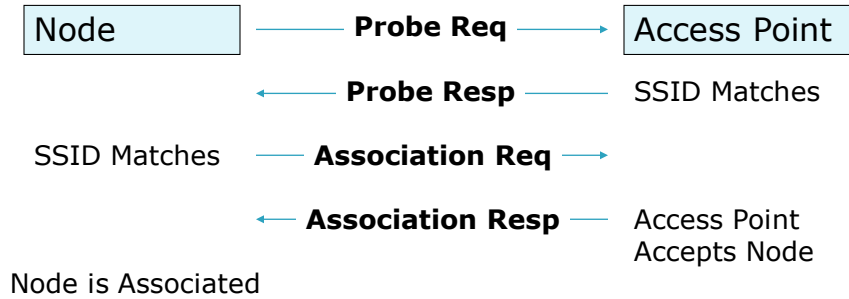
13

Discovery - Open Network



14

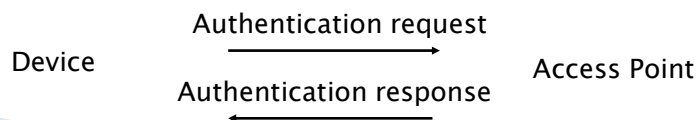
Discovery - Closed Network



15

User authentication

- ▶ ตามมาตรฐาน 802.11 กำหนดรูปแบบของการ Authentication ไว้ 2 รูปแบบคือ Open System Authentication และ Share-Key Authentication:
- ▶ Open System authentication
 - ทำการ Authentication ให้กับทุกคนที่ Request
 - ไม่มีการกำหนดรหัสผ่าน

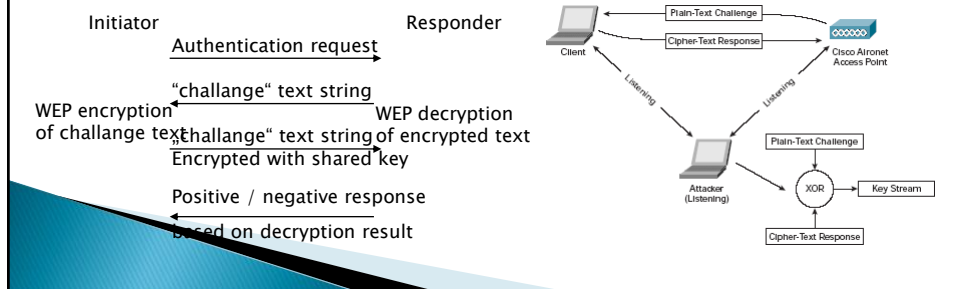


16

User authentication

▶ Shared-Key authentication

- มี Key ในการ Authentication เพื่อเข้าใช้งานระบบ
- ข้อเสียคือสามารถดักจับข้อมูลดังกล่าว และมีกระบวนการเพื่อหาคีย์ได้



17

Wire Equivalent Privacy (WEP) ใน 802.11b

▶ Confidentiality

- ใช้คีย์ขนาด 40-bit ในการเข้ารหัส (เพิ่มเป็น 104-bit ใน WEP2)
- ใช้ RC4 algorithm

▶ Access Control

- ใช้ Shared key authentication + Encryption

▶ Data Integrity

- มีการสร้าง checksum ในทุกๆ messages

18

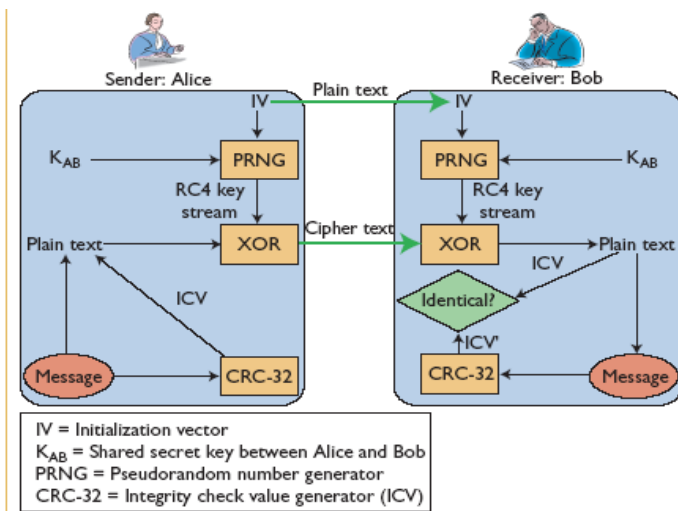
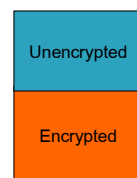
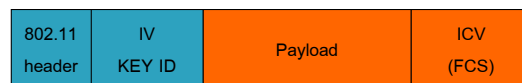


Figure 1. Security services in wired equivalent privacy protocol (WEP).

19

802.11 WEP Frame



ICV is a CRC-32 checksum over the Payload (802 Header and the Data)

20

ช่องโหว่ของ WEP คืออะไร .. มีวิธีการโจมตีอย่างไร .. จะแก้ไขอย่างไร ??



21

วิวัฒนาการด้าน Security ที่สำคัญของ 802.11 เป็นอย่างไร



22

พัฒนาการของ 802.11

- ▶ ปี 2003 : Wi-Fi ประกาศใช้ Wi-Fi Protected Access (WPA).
 - เพื่อแก้ไขปัญหabe้าต้นของ WEP
 - เป็นส่วนหนึ่งของมาตรฐาน IEEE 802.11i ที่มีการพัฒนาในขณะนั้น
- ▶ ปี 2004 : ประกาศใช้ WPA2
 - การทำงานตรงตามมาตรฐาน IEEE 802.11i

23

Wi-Fi Protected Access (WPA)

- ▶ แก้ไขช่องโหว่ต่างๆ เบื้องต้นใน WEP
- ▶ ใช้งานกับอุปกรณ์ตามมาตรฐาน 802.11 เดิมได้ แต่ต้อง update firmware
- ▶ เป้าหมายคือการเพิ่มความสามารถในการเข้ารหัสข้อมูลและการทำ User Authentication
- ▶ มีการทำงาน 2 โหมด
 - WPA Enterprise : TKIP/MIC ; 802.1X/EAP
 - WPA Personal : TKIP/MIC ; PSK

24

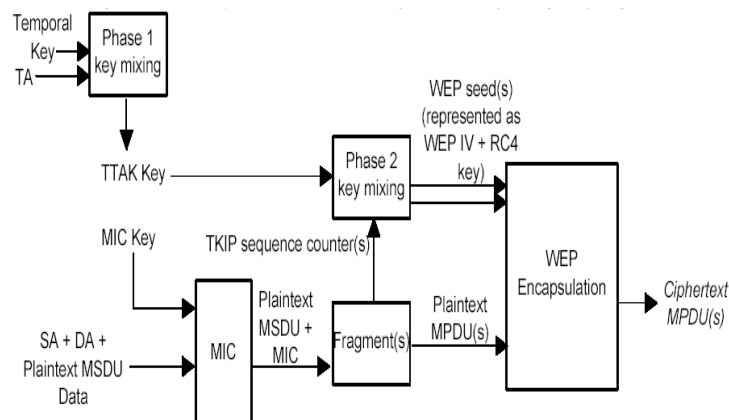
WPA : Enterprise Mode

- ▶ Authentication ใช้มาตรฐาน IEEE 802.1X/EAP
 - มีการบริหารจัดการ user credentials แบบรวมศูนย์
 - มีการใช้อุปกรณ์เพิ่มเติมคือ AAA Server
- ▶ ใช้ RADIUS protocols ในการทำ AAA และการแจกจ่ายคีย์
 - รองรับกระบวนการทำ Authentication ที่หลากหลาย
 - ส่วนใหญ่ใช้รหัสผ่านและ digital Certificates.
- ▶ ยกตัวอย่างเช่น
 - TLS, TTLS: Certificates based methods.
 - PEAP, LEAP: Password based methods.

25

Encryption: TKIP

- ▶ ออกแบบให้ครอบคลุมการทำงานของ WEP
- ▶ ใช้ RC4-Engine เหมือนใน WEP
- ▶ ป้องกันการ Spoof ข้อมูลได้



26

ประโยชน์ของ TKIP

- ▶ ใช้ Key ในการเข้ารหัสแต่ละ Packet แยกกัน
- ▶ Key มีความยาวมากขึ้น
- ▶ จำนวนคีย์ที่เป็นไปได้มากถึง 280 trillion
- ▶ IV ขนาด 48bit โดยขั้นตอนมีการลดการใช้งาน IV ซ้ำ
- ▶ ส่งข้อมูล IV แบบเข้ารหัส
- ▶ ใช้ MIC แทน CRC-Check ซึ่งปลอมแปลงได้ยากมากกว่า
- ▶ สามารถ upgrade ใน firmware ที่ใช้งาน WEP ได้

27

WPA2 / 802.11 Task Group i

- ▶ WPA2 = 802.11i
- ▶ 802.11i ใช้หลักการของ Robust Security Network (RSN)
- ▶ การปรับปรุงหลักจาก WPA คือการใช้ AES ในการเข้ารหัส มักใช้ Hardware ในการเข้ารหัส AES
- ▶ มีการทำงานเป็น 2 โหมดเหมือน WPA:
 - Enterprise Mode: authentication ใช้ 802.1X/EAP และ encryption ใช้ AES-CCMP
 - Personal Mode: authentication ใช้ PSK และ encryption ใช้ AES-CCMP

28

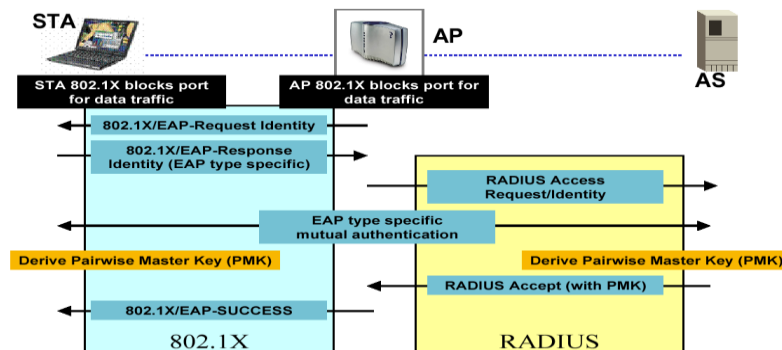
WPA2 / 802.11i AES-CCMP

- ▶ AES เป็นการเข้ารหัสแบบ symmetric key-cipher
- ▶ มี block-Size ขนาด 128bits และ key มีความยาว 128bits.
- ▶ การเข้ารหัสแต่ละรอบมีการทำงาน 4 ขั้นตอน จำนวนรอบจะเป็น 10,12 หรือ 14 รอบขึ้นอยู่กับจำนวนบิต ซึ่งใน WPA2 จะมีการทำเท่ากับ 10 รอบ
- ▶ AES ใช้โปรโตคอล Counter-Mode/CBC-Mac Protocol (CCMP)
- ▶ CCMP ถูกออกแบบมาเป็นพิเศษสำหรับ 802.11i

29

802.11i Authentication

Authentication Overview



Source: Cam-Winget, Moore, Stanley and Walker

30

Comparison of the standards

	WEP	WPA	WPA2
● Cipher	RC4	RC4	AES
● Key Size	40 or 104bits	104bits perPack	128bits encry.
● Key Life	24bit IV	48bit IV	48bit IV
● Packet Key	Concatenation	TwoPhaseMix	Not Needed
● Data Integrity	CRC32	Michael MIC	CCM
● Key Management	None	802.1X/EAP/PSK	802.1X/EAP/PSK

Security Level



31

พฤติกรรมการใช้เครือข่ายไร้สาย ที่ส่งผลกระทบต่อระบบ
สารสนเทศ มีอะไรบ้าง



32

วิวัฒนาการของ 802.11 เพียงพอในการรักษาความปลอดภัย
ระบบ IT หรือไม่



33

นักศึกษาคิดว่า.. เทคโนโลยีการรักษาความปลอดภัยของ
802.11 ในระดับสูงสุด .. จะไม่สามารถจัดการกับปัญหา
อะไรได้บ้าง



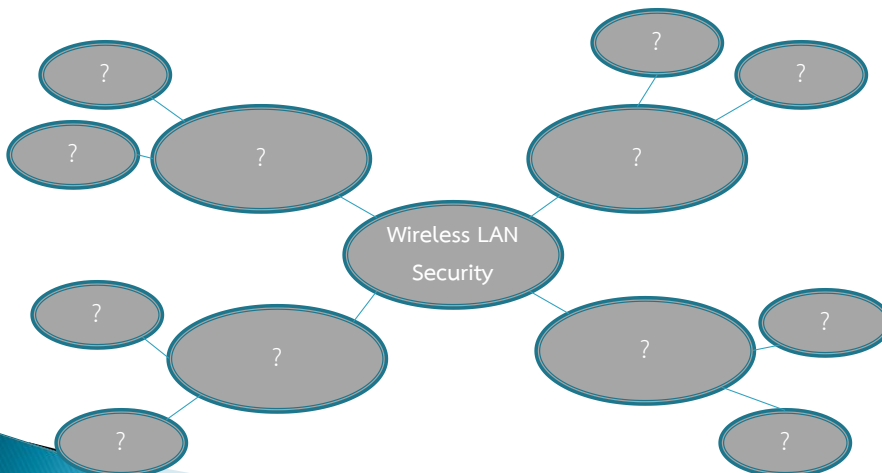
34

นอกจาก 802.11 Security ควรมีการรักษาความปลอดภัย
ระบบ IT อะไรเพิ่มเติมบ้าง



35

Mind Map : สรุปเกี่ยวกับ Wireless LAN Security



36

Q : สำหรับองค์กรที่มีจำนวนเครื่อง 1-10 เครื่องควรกำหนดการ
รักษาความปลอดภัยเครือข่ายไร้สายอย่างไร



37

Q : สำหรับองค์กรที่มีจำนวนเครื่อง 20-60 เครื่องควร
กำหนดการรักษาความปลอดภัยเครือข่ายไร้สายอย่างไร



38

Q : สำหรับองค์กรที่มีจำนวนเครื่อง 200+ เครื่องควร
กำหนดการรักษาความปลอดภัยเครือข่ายไร้สายอย่างไร



39

สรุป / บทเรียน

40