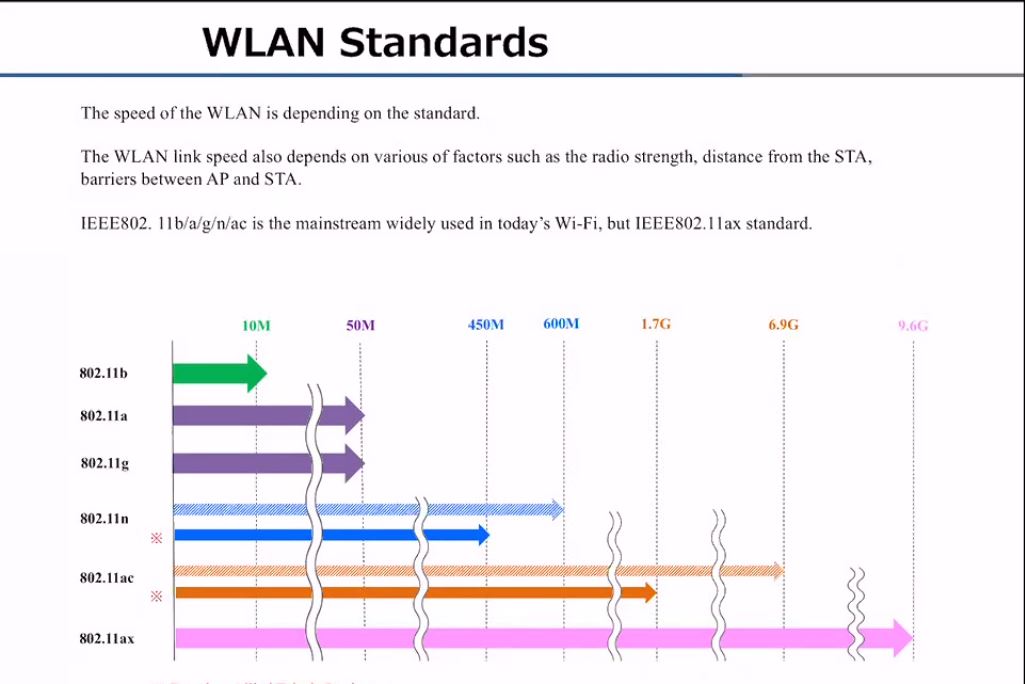
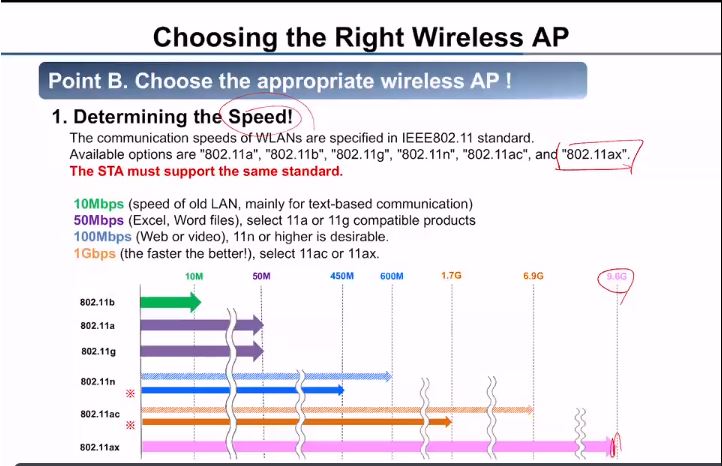
[**Wireless LAN communication method**](https://www.google.com/search?rlz=1C1CHBD_enTH859TH859&sxsrf=ALeKk006v5NhI4tfrHK_yV5hqm63TkpDFg:1598366473261&q=Wireless+LAN+communication+method&spell=1&sa=X&ved=2ahUKEwjw8e-Oy7brAhXEwTgGHVBnAPsQkeECKAB6BAgPECs)

เครือข่ายไร้สายเป็นวิธีการที่บ้าน[เครือข่ายโทรคมนาคม](https://translate.googleusercontent.com/translate_c?depth=1&hl=th&prev=search&pto=aue&rurl=translate.google.com&sl=en&sp=nmt4&u=https://en.m.wikipedia.org/wiki/Telecommunications_network&usg=ALkJrhiMlibEciI7h80cIxATCK9wh8hzvQ)และสถานที่ติดตั้งทางธุรกิจหลีกเลี่ยงกระบวนการที่มีค่าใช้จ่ายสูงในการนำสายเคเบิลเข้ามาในอาคารหรือเป็นการเชื่อมต่อระหว่างตำแหน่งอุปกรณ์ต่างๆ เครือข่ายผู้ดูแลระบบสื่อสารโทรคมนาคมจะดำเนินการโดยทั่วไปและบริหารงานโดยใช้วิทยุสื่อสารการใช้งานนี้เกิดขึ้นที่ระดับกายภาพ (เลเยอร์) ของโครงสร้างเครือข่าย[แบบจำลอง OSI](https://translate.googleusercontent.com/translate_c?depth=1&hl=th&prev=search&pto=aue&rurl=translate.google.com&sl=en&sp=nmt4&u=https://en.m.wikipedia.org/wiki/OSI_model&usg=ALkJrhhzeN-aEiD8dKZtCpuJvHGC7_VF5g" \o "แบบจำลอง OSI)

**WLAN Standards**

****



**High speed technology**

บรอดแบนด์ หมายถึงลักษณะสมบัติแบนด์วิดท์ที่กว้างของความถี่แม่เหล็กไฟฟ้าบนสื่อกลางการส่งและความสามารถในการขนส่งหลายสัญญาณและหลายประเภทของการจราจรได้พร้อมๆกัน สื่อกลางอาจเป็น สายเคเบิลแกนร่วม (coax), [ใยแก้วนำแสง](https://th.wikipedia.org/wiki/%E0%B9%83%E0%B8%A2%E0%B9%81%E0%B8%81%E0%B9%89%E0%B8%A7%E0%B8%99%E0%B8%B3%E0%B9%81%E0%B8%AA%E0%B8%87), สายเคเบิลตีเกรียว (twisted pair) หรือไร้สาย ตรงกันข้ามกับ baseband ที่เป็นระบบการสื่อสารที่ข้อมูลถูกส่งผ่านไปในความถี่เดียว.

ก่อนที่จะมีการประดิษฐ์ของบรอดแบนด์ที่บ้าน, การเข้าถึงอินเทอร์เน็ตทำได้เพียงวิธีการเดียวด้วยการใช้โทรศัพท์เรียกเข้าไป (dial-up) ซึ่งจะใช้เวลาราว 10-30 นาทีในการดาวน์โหลด เพลงหนึ่ง (3.5 MB) และกว่า 28 ชั่วโมงเพื่อดาวน์โหลดภาพยนตร์ (700 MB) อินเทอร์เน็ตแบบ Dial-Up ก็ถือว่าสะดวกมากที่สุดเท่าที่จะทำได้โดยหมดสิทธิ์การใช้สายโทรศัพท์บ้านและผู้ใช้จะต้องพิจารณาว่าจำเป็นหรือไม่ที่จะต้องมีสายโทรศัพท์สายที่สองและหากจำเป็นต้องมีก็ต้องพิจารณาว่าคุ้มค่าใช้จ่ายหรือไม่

ในปี 1997, เคเบิลโมเด็มเริ่มเปิดให้บริการ ถึงแม้ว่าการใช้งานทั่วไปของบรอดแบนด์ยังไม่เริ่มขึ้นจนกว่า 2001. การเชื่อมต่อบรอดแบนด์ทำให้การดาวน์โหลดทำได้เร็วกว่า dial-up อย่างมีนัยสำคัญ เช่นเดียวกับเทคโนโลยีใหม่ ๆ ที่ผู้บริโภคส่วนใหญ่ไม่สามารถที่จะจ่ายค่าใช้บริการอินเทอร์เน็ตที่เร็วกว่าได้ อย่างไรก็ตาม ค่าใช้จ่ายที่สูงไม่ได้เป็นปัจจัยอีกต่อไปในปี 2004 ครัวเรือนอเมริกันโดยเฉลี่ยถือว่าค่าบริการบรอดแบนด์พอจะจ่ายได้ นับตั้งแต่ก่อตั้งขึ้นบรอดแบนด์มีความเข้มแข็งมากขึ้นและความเร็วการเชื่อมต่อยังคงเพิ่มขึ้นอย่างต่อเนื่อง

เกณฑ์ที่แตกต่างกันสำหรับ "ความกว้าง" ได้ถูกนำมาใช้ในบริบทที่แตกต่างกันและเวลาที่ต่างกัน ต้นกำเนิดของมันคือในวิชาฟิสิกส์, วิศวกรรมระบบอะคูสติกและวิทยุ ที่มันได้ถูกนำมาใช้มีความหมายคล้ายกับ wideband. อย่างไรก็ตาม คำๆนี้กลายเป็นที่นิยมตลอดช่วงปี 1990 ว่าเป็นคำการตลาดที่คลุมเครือสำหรับการเข้าถึงอินเทอร์เน็ต

**Wi-Fi connection name**

SSID หรือ Service Set Identifier เป็นชื่อที่ใช้อ้างถึง Wireless Access Point สำหรับการเชื่อมต่อ โดยปกติแล้วผู้ที่จะเชื่อมต่อ Wireless Network ใดๆ จำเป็นต้องรู้ชื่อ SSID ของ Wireless Access Point นั้นๆเพื่อเชื่อมต่อสำหรับเข้าใช้งาน แต่ในบางกรณีผู้ดูแลระบบเครือข่ายจะทำการซ่อนชื่อ SSID เอาไว้ โดยมีจุดประสงค์เพื่อลดความเสี่ยงในการมองเห็นจากสาธารณะและจากการถูกโจมตี การตั้งชื่อ SSID สามารถตั้งโดยใช้ตัวเลขและตัวอักษรภาษาอังกฤษ (Alphanumeric) ไม่เกิน 32 ตัว

**Radio interference from wireless LAN**

กระบวนการส่งและรับสัญญาณวิทยุและเลเซอร์ผ่านอากาศทำให้ระบบไร้สายเสี่ยงต่อเสียงรบกวนในชั้นบรรยากาศและการส่งสัญญาณจากระบบอื่น นอกจากนี้เครือข่ายไร้สายสามารถรบกวนเครือข่ายไร้สายอื่น ๆ ที่อยู่ใกล้เคียงและอุปกรณ์คลื่นวิทยุ การรบกวนอาจมีทิศทางเข้าหรือออก

ตัวอย่างเช่น LAN แบบใช้คลื่นวิทยุสามารถพบสัญญาณรบกวนภายในทั้งจากฮาร์มอนิกของระบบส่งสัญญาณหรือจากผลิตภัณฑ์อื่น ๆ ที่ใช้ความถี่วิทยุที่คล้ายกันในพื้นที่ท้องถิ่น เตาอบไมโครเวฟทำงานในย่าน S (2.4GHz) ที่ LAN ไร้สายจำนวนมากใช้ในการส่งและรับ สัญญาณเหล่านี้ส่งผลให้ผู้ใช้เกิดความล่าช้าโดยการปิดกั้นการส่งสัญญาณจากสถานีบน LAN หรือทำให้เกิดข้อผิดพลาดเล็กน้อยในข้อมูลที่ส่ง การรบกวนประเภทนี้สามารถ จำกัด พื้นที่ที่คุณสามารถปรับใช้เครือข่ายไร้สายได้ ผลิตภัณฑ์รุ่นใหม่ที่ใช้เทคโนโลยีวิทยุบลูทู ธ ยังทำงานในย่านความถี่ 2.4GHz และอาจทำให้เกิดสัญญาณรบกวนกับ LAN ไร้สายโดยเฉพาะอย่างยิ่งในบริเวณขอบที่ไม่ครอบคลุมโดยจุดเชื่อมต่อ LAN ไร้สายโดยเฉพาะ

**Roaming**

การโรมมิ่งแบ่งออกเป็น "การโรมมิ่งโดยใช้ SIM" และ "การโรมมิ่งตามชื่อผู้ใช้ / รหัสผ่าน" โดยคำศัพท์ทางเทคนิค "โรมมิ่ง" ยังครอบคลุมการโรมมิ่งระหว่างเครือข่ายที่มีมาตรฐานเครือข่ายที่แตกต่างกันเช่น[WLAN (Wireless Local Area Network)](https://en.wikipedia.org/wiki/Wireless_LAN)หรือ[GSM (Global System](https://en.wikipedia.org/wiki/GSM)สำหรับการสื่อสารเคลื่อนที่) อุปกรณ์และฟังก์ชันการทำงานของอุปกรณ์เช่นความสามารถของ[ซิมการ์ด](https://en.wikipedia.org/wiki/Subscriber_identity_module)[เสาอากาศ](https://en.wikipedia.org/wiki/Radio_antenna)และ[อินเทอร์เฟซเครือข่าย](https://en.wikipedia.org/wiki/Computer_interface)และ[การจัดการพลังงานเป็น](https://en.wikipedia.org/wiki/Power_management)ตัวกำหนดความเป็นไปได้ในการเข้าถึง

โดยใช้ตัวอย่างของการโรมมิ่ง WLAN / GSM สถานการณ์ต่อไปนี้สามารถสร้างความแตกต่างได้ (อ้างอิงเอกสารอ้างอิงถาวรของสมาคม GSM AA.39):

- ใช้ SIM (โรมมิ่ง): ผู้สมัครใช้งาน GSM ข้ามไปยัง WLAN สาธารณะที่ดำเนินการโดย:

- ผู้ให้บริการระบบ GSM หรือ ผู้ให้บริการรายอื่นที่มีข้อตกลงโรมมิ่งกับผู้ให้บริการระบบ GSM

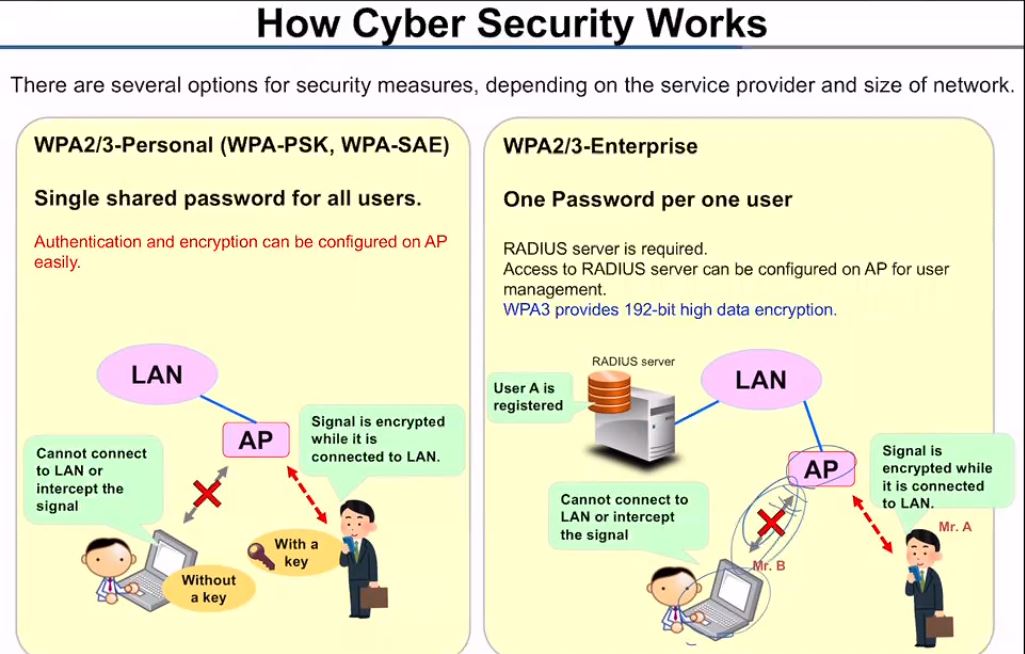
- การโรมมิ่งตามชื่อผู้ใช้ / รหัสผ่าน: ผู้สมัครสมาชิก GSM ข้ามไปยัง WLAN สาธารณะที่ดำเนินการโดย:

- ผู้ให้บริการระบบ GSM หรือ ผู้ให้บริการรายอื่นที่มีข้อตกลงโรมมิ่งกับผู้ให้บริการระบบ GSM

แม้ว่าสถานการณ์ของผู้ใช้ / เครือข่ายเหล่านี้จะมุ่งเน้นไปที่การโรมมิ่งจากเครือข่ายของผู้ให้บริการเครือข่าย GSM แต่การโรมมิ่งอาจเป็นแบบสองทิศทางได้อย่างชัดเจนเช่นจากผู้ให้บริการ WLAN สาธารณะไปยังเครือข่าย GSM การโรมมิ่งแบบดั้งเดิมในเครือข่ายที่มีมาตรฐานเดียวกันเช่นจาก WLAN ไปยัง WLAN หรือเครือข่าย GSM ไปยังเครือข่าย GSM ได้มีการอธิบายไว้แล้วข้างต้นและได้รับการกำหนดเช่นเดียวกันโดยความแปลกแยกของเครือข่ายตามประเภทของรายการสมาชิกในบ้าน สมัครสมาชิก

**Mutiple SSID**

ในโหมด Multi - SSIDจุดเชื่อมต่อจะสร้างเครือข่ายไร้สายหลายเครือข่ายเพื่อให้ความปลอดภัยและกลุ่ม VLAN ที่แตกต่างกัน โหมดนี้เหมาะเมื่อคุณต้องการให้อุปกรณ์ของคุณเชื่อมต่อกับเครือข่ายไร้สายที่แตกต่างกันและถูกแยกโดย VLAN 1



**Wirelrss AP-to-AP**

AP เชื่อมต่อโดยตรงกับเครือข่ายท้องถิ่นแบบใช้สายโดยทั่วไปคืออีเทอร์เน็ตจากนั้น AP จะให้การเชื่อมต่อไร้สายโดยใช้เทคโนโลยี LAN ไร้สายซึ่งโดยทั่วไปคือ Wi-Fi สำหรับอุปกรณ์อื่น ๆ เพื่อใช้การเชื่อมต่อแบบมีสายนั้น AP รองรับการเชื่อมต่ออุปกรณ์ไร้สายหลายเครื่องผ่านการเชื่อมต่อแบบมีสายเดียว

**Image of wireless security**

การรักษาความปลอดภัยแบบไร้สายคือการป้องกันการเข้าถึงไม่ได้รับอนุญาตหรือความเสียหายให้กับเครื่องคอมพิวเตอร์หรือข้อมูลโดยใช้[แบบไร้สาย](https://en.wikipedia.org/wiki/Wireless)เครือข่ายซึ่งรวมถึงเครือข่าย[Wi-Fi](https://en.wikipedia.org/wiki/Wi-Fi_network)ประเภทที่พบบ่อยที่สุดคือการรักษาความปลอดภัย Wi-Fiซึ่งรวมถึง[ความเป็นส่วนตัวแบบ](https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy)มี[สายเทียบเท่า](https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy) (WEP) และ[Wi-Fi Protected Access](https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access) (WPA) WEP เป็นมาตรฐานการรักษาความปลอดภัยที่อ่อนแออย่างฉาวโฉ่[ [จำเป็นต้องอ้างอิง](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed) ] : รหัสผ่านที่ใช้มักจะถูกถอดรหัสภายในไม่กี่นาทีด้วยคอมพิวเตอร์แล็ปท็อปพื้นฐานและเครื่องมือซอฟต์แวร์ที่มีอยู่ทั่วไป WEP เป็นมาตรฐาน IEEE 802.11 เก่าจากปี 1997 ซึ่งถูกแทนที่ในปี 2546 โดย WPA หรือ Wi-Fi Protected Access WPA เป็นทางเลือกที่รวดเร็วในการปรับปรุงความปลอดภัยผ่าน WEP มาตรฐานปัจจุบันคือ WPA2; ฮาร์ดแวร์บางตัวไม่รองรับ WPA2 หากไม่มีการอัพเกรดหรือเปลี่ยนเฟิร์มแวร์ WPA2 ใช้อุปกรณ์เข้ารหัสที่เข้ารหัสเครือข่ายด้วยคีย์ 256 บิต ความยาวของคีย์ที่ยาวขึ้นจะช่วยเพิ่มความปลอดภัยผ่าน WEP องค์กรต่างๆมักบังคับใช้การรักษาความปลอดภัยโดยใช้ระบบที่ใช้[ใบรับรอง](https://en.wikipedia.org/wiki/Public_key_certificate)เพื่อตรวจสอบอุปกรณ์เชื่อมต่อตามมาตรฐาน 802.1X

คอมพิวเตอร์แล็ปท็อปจำนวนมากติดตั้ง[การ์ดไร้สาย](https://en.wikipedia.org/wiki/Wireless_card)ไว้แล้ว ความสามารถในการเข้าสู่เครือข่ายในขณะที่มือถือมีประโยชน์มากมาย อย่างไรก็ตามระบบเครือข่ายไร้สายมีปัญหาด้านความปลอดภัยบางอย่าง [แฮกเกอร์](https://en.wikipedia.org/wiki/White_hat_(computer_security))พบว่าเครือข่ายไร้สายนั้นค่อนข้างง่ายที่จะเจาะเข้าไปและยังใช้เทคโนโลยีไร้สายเพื่อเจาะเข้าสู่เครือข่ายแบบมีสาย ด้วยเหตุนี้จึงเป็นเรื่องสำคัญมากที่องค์กรต่างๆจะต้องกำหนดนโยบายความปลอดภัยแบบไร้สายที่มีประสิทธิภาพเพื่อป้องกันการเข้าถึงทรัพยากรที่สำคัญโดยไม่ได้รับอนุญาต [ระบบป้องกันการบุกรุกแบบไร้สาย](https://en.wikipedia.org/wiki/Wireless_Intrusion_Prevention_System) (WIPS) หรือ[ระบบตรวจจับการบุกรุกแบบไร้สาย](https://en.wikipedia.org/wiki/Wireless_Intrusion_Detection_System) (WIDS) มักใช้เพื่อบังคับใช้นโยบายความปลอดภัยแบบไร้สาย

**Control Communications**

Control Communications เป็นกระบวนการตรวจสอบและควบคุมการสื่อสารตลอดวงจรชีวิตของโครงการทั้งหมดเพื่อให้แน่ใจว่ามีการตอบสนองความต้องการข้อมูลของผู้มีส่วนได้ส่วนเสียในโครงการ

