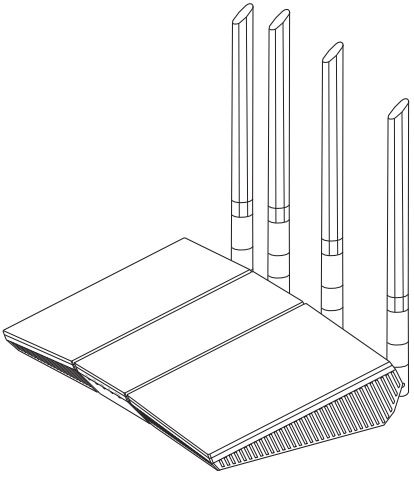
คู่มือผู้ใช้

RT-AX55

เราเตอร์ Wi-Fi แถบความถี่คู่



IN SEARCH OF INCREDIBLE

TH21014
ฉบับปรับปรุงรุ่นที่ 2
เดือนตุลาคม 2022

สารบัญ

สารบัญ

สารบัญ

1 ทำความรู้จักไวร์เลสเราเตอร์ของคุณ

1.1 ยินดีต้อนรับ!

ขอบคุณที่ซื้อ ASUS RT-AX55 ไวร์เลสเราเตอร์!

RT-AX55 ที่บางพิเศษและมีไสตล์นี้ ทำงานด้วยแถบความถี่คู่ 2.4GHz และ 5GHz สำหรับการสตรีม HD แบบไร้สาย และเทคโนโลยี ASUS กรีนเน็ตเวิร์ก ซึ่งเป็น โซลูชั่นที่ประหยัดพลังงานมากถึง 70% ซึ่งไม่มีใครเทียบได้ในขณะนี้

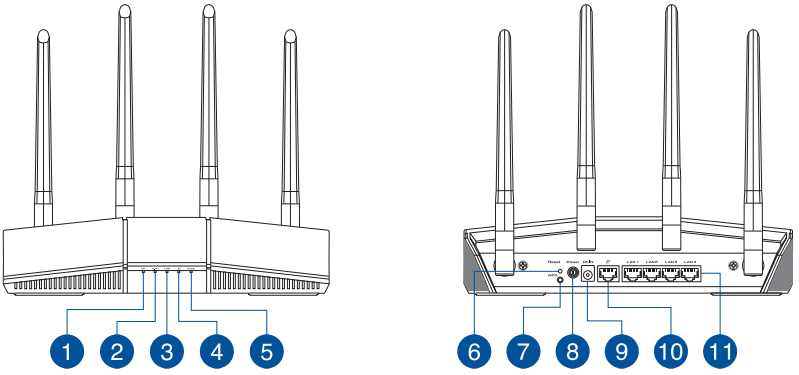
1.2 สิ่งต่างๆ ในกล่องบรรจุ

☑ RT-AX55 ไวร์เลส เราเตอร์
☑ สายเคเบิลเครือข่าย (RJ-45)
☑ อะแดปเตอร์เพาเวอร์
☑ คู่มือเริ่มต้นอย่างเร็ว

หมายเหตุ:

- ถ้ามีรายการใดๆ เสียหายหรือหายไป ให้ติดต่อ ASUS เพื่อสอบถามและรับการสนับสนุนทางเทคนิค โปรดดูรายการสายด่วนสนับสนุนของ ASUS ได้ที่ด้านหลังของคู่มือผู้ใช้ฉบับนี้
- เก็บวัสดุบรรจุหีบห่อดั้งเดิมไว้ ในกรณีที่คุณจำเป็นต้องรับบริการภายใต้การรับประกันในอนาคต เช่นการนำมาซ่อมหรือเปลี่ยนเครื่อง

1.3 ไวร์เลสเราเตอร์ของคุณ



1	**LED 5GHz** **ดับ**: ไม่มีสัญญาณ 5GHz **ติด**: ระบบไร้สายพร้อม **กะพริบ**: กำลังส่งหรือรับข้อมูลผ่านการเชื่อมต่อไร้สาย
2	**LED 2.4GHz** **ดับ**: ไม่มีสัญญาณ 2.4GHz **ติด**: ระบบไร้สายพร้อม **กะพริบ**: กำลังส่งหรือรับข้อมูลผ่านการเชื่อมต่อไร้สาย
3	**LED LAN** **ดับ**: ไม่มีพลังงานเข้า หรือไม่มีการเชื่อมต่อทางกายภาพ **ติด**: มีการเชื่อมต่อทางกายภาพไปยังเครือข่ายแลน (LAN)
4	**LED WAN (อินเทอร์เน็ต)** **สีแดง:** ไม่มี IP หรือไม่มีการเชื่อมต่อทางกายภาพ **ติด**: มีการเชื่อมต่อทางกายภาพไปยังเครือข่ายแวน (WAN)
5	**LED เพาเวอร์** **ดับ:** ไม่มีพลังงานเข้า **ติด**: อุปกรณ์พร้อม **กะพริบช้า**: โหมดช่วยเหลือ
6	**ปุ่มรีเซ็ต** ปุ่มนี้จะรีเซ็ต หรือกู้คืนระบบกลับเป็นการตั้งค่าเริ่มต้นจากโรงงาน
7	**ปุ่ม WPS** ปุ่มนี้ใช้เพื่อเปิดตัวช่วยสร้าง WPS
8	**ปุ่มพาวเวอร์** กดปุ่มนี้ เพื่อเปิดหรือปิดระบบ

9	**พอร์ตเพาเวอร์ (DCเข้า)** เสียบอะแดปเตอร์ AC ที่ให้มาเข้ากับพอร์ตนี้ และเชื่อมต่อเราเตอร์ของคุณเข้ากับแหล่งพลังงาน
10	**พอร์ต WAN (อินเทอร์เน็ต)** เชื่อมต่อสายเคเบิลเครือข่ายเข้ากับพอร์ตนี้ เพื่อสร้างการเชื่อมต่อ WAN
11	**พอร์ต LAN 1~4** เชื่อมต่อสายเคเบิลเครือข่ายเข้ากับพอร์ตเหล่านี้ เพื่อสร้างการเชื่อมต่อ LAN

หมายเหตุ:

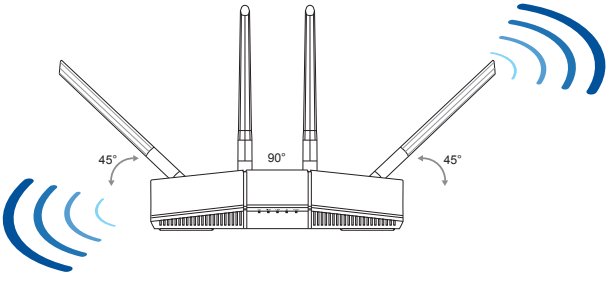
- ใช้เฉพาะอะแดปเตอร์ที่มาพร้อมกับแพคเกจของคุณเท่านั้น การใช้อะแดปเตอร์อื่นอาจทำให้อุปกรณ์เสียหาย
- **ข้อมูลจำเพาะ:**

อะแดปเตอร์เพาเวอร์ DC	เอาต์พุต DC: +12V โดยมีกระแสสูงสุด 1A/1.5A		
อุณหภูมิขณะทำงาน	0~40°C	ขณะเก็บรักษา	0~70°C
ความชื้นขณะทำงาน	50~90%	ขณะเก็บรักษา	20~90%

1.4 การวางตำแหน่งเราเตอร์

เพื่อให้การรับส่งสัญญาณไร้สายระหว่างไวร์เลสเราเตอร์ และอุปกรณ์เครือข่ายที่เชื่อมต่ออยู่มีคุณภาพดีที่สุด ให้แน่ใจว่าคุณ:

- วางไวร์เลสเราเตอร์ในบริเวณศูนย์กลาง เพื่อให้ครอบคลุมพื้นที่ไร้สายมากที่สุดสำหรับอุปกรณ์เครือข่าย
- วางอุปกรณ์ให้ห่างจากวัตถุขวางกั้นที่เป็นโลหะ และไม่ให้ถูกแสงแดดโดยตรง
- วางอุปกรณ์ให้ห่างจากอุปกรณ์ Wi-Fi 802.11g หรือ 20MHz, อุปกรณ์ต่อพ่วงคอมพิวเตอร์ 2.4GHz, อุปกรณ์บลูทูธ, โทรศัพท์ไร้สาย, หม้อแปลง, มอเตอร์พลังงานสูง, แสงฟลูออเรสเซนต์, เตาไมโครเวฟ, ตู้เย็น และอุปกรณ์อุตสาหกรรมอื่นๆ เพื่อป้องกันสัญญาณรบกวน หรือสัญญาณสูญหาย
- อัพเดตไปเป็นเฟิร์มแวร์ล่าสุดเสมอ เยี่ยมชมเว็บไซต์ ASUS ที่ **http://www.asus.com** เพื่อรับอัพเดตเฟิร์มแวร์ล่าสุด



1.5 ความต้องการในการติดตั้ง

ในการตั้งค่าเครือข่ายของคุณ คุณจำเป็นต้องมีคอมพิวเตอร์หนึ่งหรือสองเครื่อง ซึ่งมีคุณสมบัติระบบดังต่อไปนี้:

- พอร์ตอีเธอร์เน็ต RJ-45 (LAN) (10Base-T/100Base-TX/1000Base-TX)
- ความสามารถไร้สาย IEEE 802.11 a/b/g/n/ac/ax
- บริการ TCP/IP ที่ติดตั้งไว้แล้ว
- เว็บเบราเซอร์ เช่น Internet Explorer, Firefox, Safari หรือ Google Chrome

---

หมายเหตุ:

- ถ้าคอมพิวเตอร์ของคุณไม่มีความสามารถไร้สายในตัว คุณอาจติดตั้งอะแดปเตอร์ WLAN IEEE 802.11 a/b/g/n/ac/ax เข้ากับคอมพิวเตอร์ของคุณ เพื่อเชื่อมต่อไปยังเครือข่าย
- ด้วยเทคโนโลยีดูอัลแบนด์ของไวร์เรสเราเตอร์ของคุณ เครื่องจะสนับสนุนสัญญาณไร้สายความถี่ 2.4GHz และ 5GHz พร้อมกัน คุณสมบัตินี้ช่วยให้คุณทำกิจกรรมที่เกี่ยวข้องกับอินเทอร์เน็ตต่างๆ เช่น การท่องอินเทอร์เน็ต หรือการอ่าน/เขียนข้อความอีเมลโดยใช้แถบความถี่ 2.4GHz ในขณะเดียวกับที่กำลังสตรีมไฟล์เสียง/วิดีโอระดับไฮเดฟฟินิชั่น เช่น ภาพยนตร์ หรือเพลงโดยใช้แถบความถี่ 5GHz ไปพร้อมๆ กัน
- อุปกรณ์ IEEE 802.11n บางอย่างที่คุณต้องการเชื่อมต่อไปยังเครือข่ายของคุณ อาจสนับสนุนหรือไม่สนับสนุนแถบความถี่ 5GHz สำหรับข้อมูลจำเพาะ ให้ดูคู่มือผู้ใช้ของอุปกรณ์
- สายเคเบิลอีเธอร์เน็ต RJ-45 ซึ่งจะนำไปใช้เพื่อเชื่อมต่ออุปกรณ์เครือข่าย ไม่ควรมีความยาวเกิน 100 เมตร

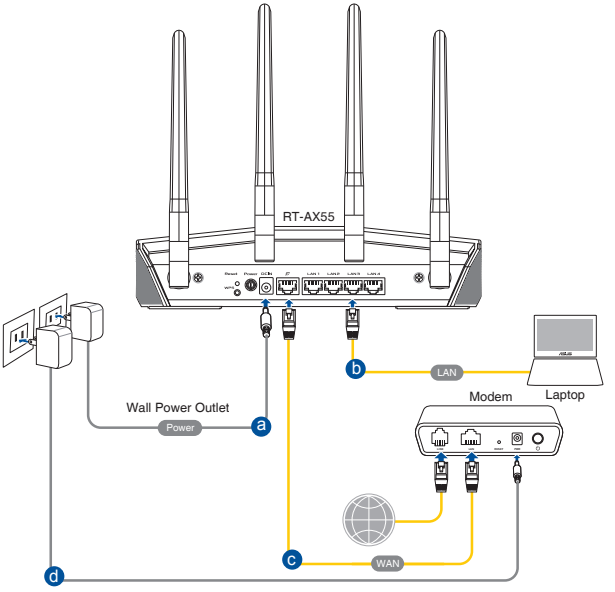
1.6 การตั้งค่าเราเตอร์

สำคัญ!

- ใช้การเชื่อมต่อแบบมีสาย ในการตั้งค่าไวร์เลสเราเตอร์ของคุณ เพื่อหลีกเลี่ยงปัญหาในการตั้งค่าที่อาจเกิดขึ้นได้ เนื่องจากความไม่แน่นอนของระบบไร้สาย
- ก่อนที่จะตั้งค่า ASUS ไวร์เลสเราเตอร์ ให้ทำสิ่งต่อไปนี้:
  - ถ้าคุณกำลังแทนที่เราเตอร์ที่มีอยู่ ให้ตัดการเชื่อมต่ออุปกรณ์เก่าจากเครือข่ายของคุณ
  - ถอดสายเคเบิล/สายไฟจากชุดโมเด็มที่มีอยู่ของคุณ ถ้าโมเด็มของคุณมีแบตเตอรี่สำรอง ให้ถอดออกด้วย
  - บูตคอมพิวเตอร์ใหม่ (แนะนำ)

1.6.1 การเชื่อมต่อแบบมีสาย

หมายเหตุ: ไวร์เลสเราเตอร์ของคุณสนับสนุนทั้งสายเคเบิลแบบต่อตรงหรือแบบไขว้ เมื่อตั้งค่าการเชื่อมต่อแบบมีสาย



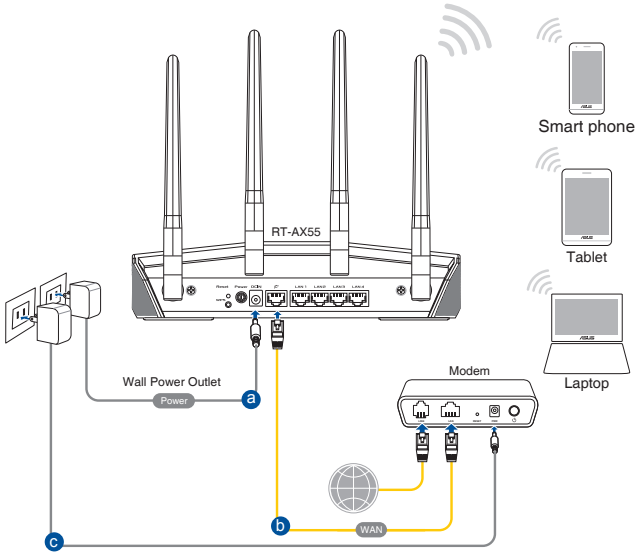
ในการตั้งค่าเครือข่ายโดยใช้การเชื่อมต่อแบบมีสาย:

1. เสียบอะแดปเตอร์ AC ของไวร์เลสเราเตอร์ของคุณเข้ากับพอร์ต DC-เข้า และเสียบเข้ากับเต้าเสียบไฟฟ้า
2. ใช้สายเคเบิลเครือข่ายที่ให้มา เชื่อมต่อโมเด็มของคุณเข้ากับพอร์ต LAN ของไวร์เลสเราเตอร์ของคุณ

สำคัญ! ตรวจดูให้แน่ใจว่า LED LAN กะพริบอยู่

3. ใช้สายเคเบิลเครือข่ายอีกเส้นหนึ่ง เชื่อมต่อโมเด็มของคุณเข้ากับพอร์ต WAN ของไวร์เลสเราเตอร์ของคุณ
4. เสียบอะแดปเตอร์ AC ของโมเด็มของคุณเข้ากับพอร์ต DC-เข้า และเสียบเข้ากับเต้าเสียบไฟฟ้า

1.6.2 การเชื่อมต่อไร้สาย



ในการตั้งค่าเครือข่ายไร้สายของคุณ:

1. เสียบอะแดปเตอร์ AC ของไวร์เลสเราเตอร์ของคุณเข้ากับพอร์ต DC-เข้า และเสียบเข้ากับเต้าเสียบไฟฟ้า
2. ใช้สายเคเบิลเครือข่ายที่ให้มา เชื่อมต่อโมเด็มของคุณเข้ากับพอร์ต WAN ของไวร์เลสเราเตอร์ของคุณ
3. เสียบอะแดปเตอร์ AC ของโมเด็มของคุณเข้ากับพอร์ต DC-เข้า และเสียบเข้ากับเต้าเสียบไฟฟ้า
4. ติดตั้งอะแดปเตอร์ WLAN IEEE 802.11 a/b/g/n/ac/ax บนคอมพิวเตอร์ ของคุณ

หมายเหตุ:

- สำหรับรายละเอียดในการเชื่อมต่อเข้ากับเครือข่ายไร้สาย ให้ดูคู่มือผู้ใช้ของอะแดปเตอร์ WLAN
- ในการตั้งค่าระบบความปลอดภัยสำหรับเครือข่ายของคุณ ให้ดูส่วน **การตั้งค่าระบบความปลอดภัยไร้สาย**

---

2 เริ่มต้นการใช้งาน

2.1 การเข้าระบบไปยังเว็บ GUI

ASUS ไวร์เลสเราเตอร์ของคุณใช้อินเตอร์เฟซผู้ใช้บนเว็บ ซึ่งอนุญาตให้คุณกำหนดค่าเราเตอร์โดยใช้เว็บเบราเซอร์ใดๆ เช่น Internet Explorer, Mozilla Firefox, Apple Safari หรือ Google Chrome

หมายเหตุ: คุณสมบัติอาจแตกต่างกันไปในเวอร์ชั่นเฟิร์มแวร์ต่างๆ

ในการเข้าระบบไปยังเว็บ GUI:

1. บนเว็บเบราเซอร์ของคุณ ป้อน IP แอดเดรสของไวร์เลสเราเตอร์: http://www.asusrouter.com
2. บนหน้าเข้าระบบ ให้ป้อนชื่อผู้ใช้เริ่มต้น **(admin)** และรหัสผ่าน **(admin)** เข้าไป
3. ขณะนี้คุณสามารถใช้เว็บ GUI เพื่อกำหนดค่าการตั้งค่าต่างๆ ของ ASUS ไวร์เลสเราเตอร์ของคุณได

หมายเหตุ: ถ้าคุณเข้ามายังระบบเว็บ GUI เป็นครั้งแรก คุณจะถูกนำไปยังหน้า การตั้งค่าอินเทอร์เน็ตด่วน (QIS) โดยอัตโนมัติ

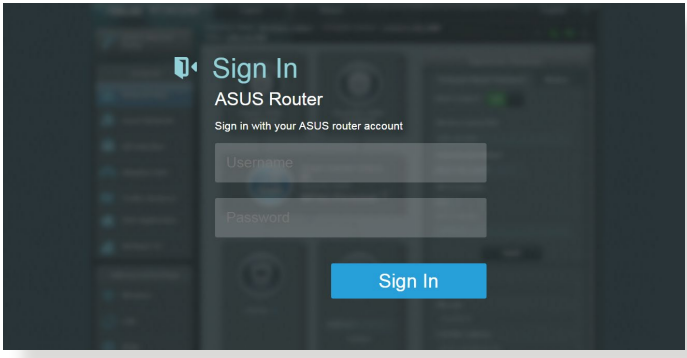
2.2 การตั้งค่าอินเทอร์เน็ตด่วน (QIS) ด้วยการตรวจพบอัตโนมัติ

ฟังก์ชั่น การตั้งค่าอินเทอร์เน็ตด่วน (QIS) จะแนะนำวิธีการในการตั้งค่าการเชื่อมต่ออินเทอร์เน็ตของคุณอย่างรวดเร็ว

หมายเหตุ: ในขณะที่ตั้งค่าการเชื่อมต่ออินเทอร์เน็ตเป็นครั้งแรก กดปุ่ม รีเซ็ต บนไวร์เลสเราเตอร์ของคุณ เพื่อรีเซ็ตเครื่องกลับเป็นการตั้งค่าเริ่มต้นจากโรงงาน

ในการใช้ QIS ด้วยการตรวจพบอัตโนมัติ:

1. เข้าระบบไปยังเว็บ GUI หน้า QIS จะเปิดโดยอัตโนมัติ



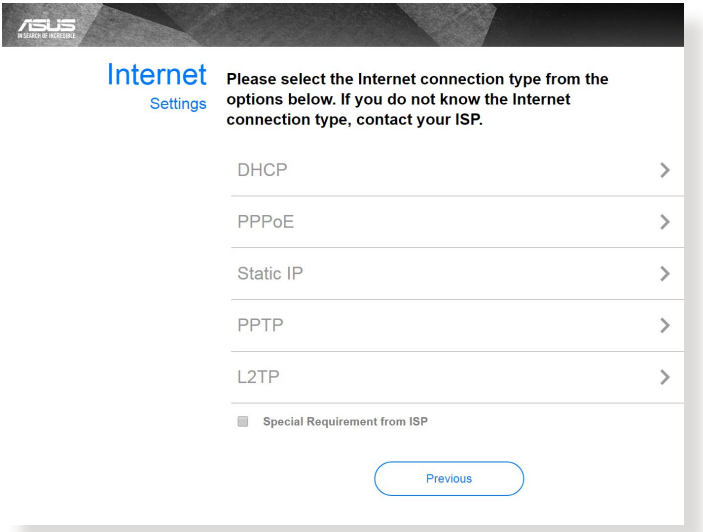
หมายเหตุ:

- ตามค่าเริ่มต้น ชื่อผู้ใช้และรหัสผ่านสำหรับเว็บ GUI ของไวร์เลสเราเตอร์ของคุณคือ **admin** สำหรับรายละเอียดในการเปลี่ยนแปลงชื่อผู้ใช้และรหัสผ่านในการล็อกอินของไวร์เลสเราเตอร์ของคุณ ให้ดูส่วน **4.6.2 ระบบ**
- ชื่อผู้ใช้และรหัสผ่านในการล็อกอินของไวร์เลสเราเตอร์นั้นแตกต่างจากชื่อเครือข่าย 2.4GHz/5GHz (SSID) และคีย์การป้องกัน ชื่อผู้ใช้และรหัสผ่านในการล็อกอินของไวร์เลสเราเตอร์ ใช้สำหรับการล็อกอินเข้าไปยังเว็บ GUI ของไวร์เลสเราเตอร์ของคุณ เพื่อกำหนดค่าการตั้งค่าต่างๆ ของไวร์เลสเราเตอร์ของคุณ ชื่อเครือข่าย 2.4GHz/5GHz (SSID) และคีย์การป้องกัน อนุญาตให้อุปกรณ์ Wi-Fi ล็อกอิน และเชื่อมต่อไปยังเครือข่าย 2.4GHz/5GHz ของคุณ

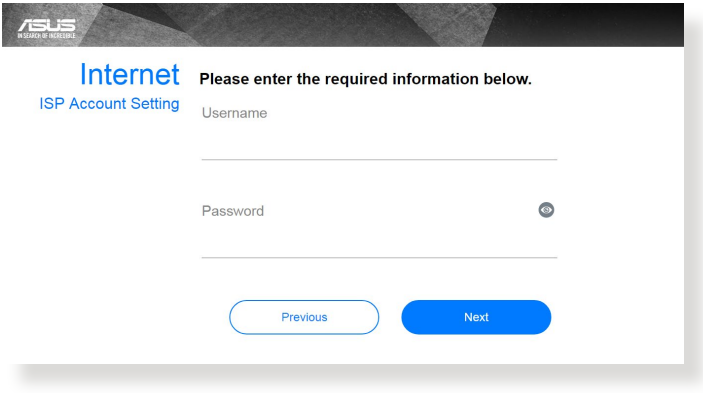
2. ไวร์เลสเราเตอร์จะตรวจพบโดยอัตโนมัติว่าชนิดการเชื่อมต่อ ISP ของคุณเป็น **ไดนามิก IP**, **PPPoE**, **PPTP**, **L2TP** และ **สแตติก IP** พิมพ์ข้อมูลที่จำเป็นสำหรับชนิดการเชื่อมตอ ISP ของคุณเขาไป

สำคัญ! ขอรับข้อมูลที่จำเป็นจาก ISP ของคุณเกี่ยวกับชนิดการเชื่อมต่ออินเทอร์เน็ต

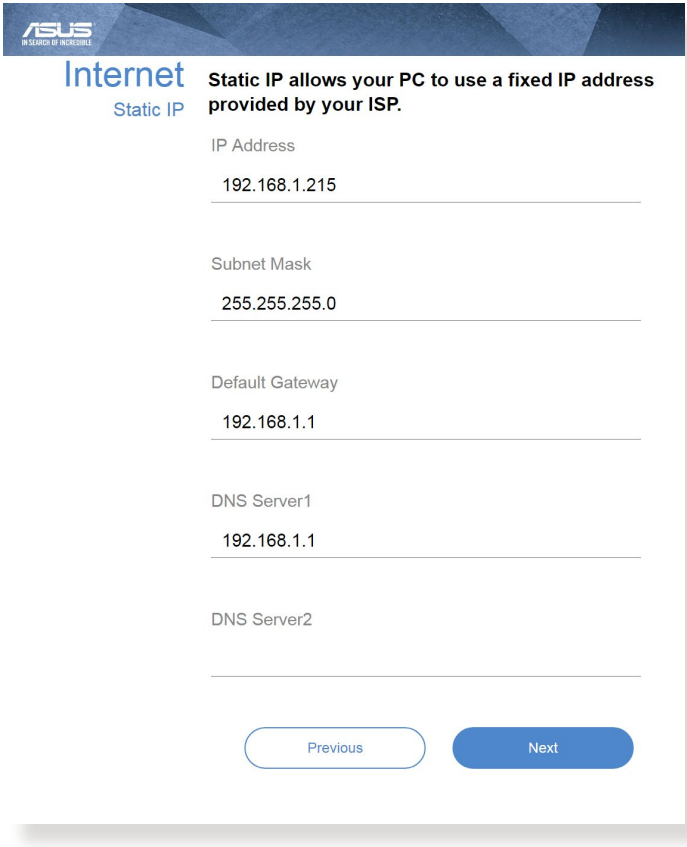
สำหรับ IP อัตโนมัติ (DHCP)



สำหรับ PPPoE, PPTP และ L2TP



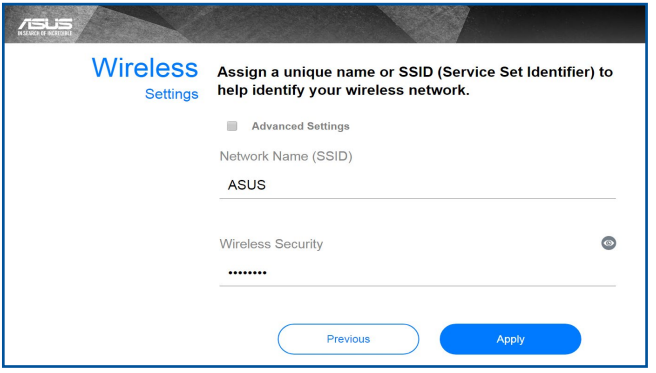
สำหรับสแตติก IP



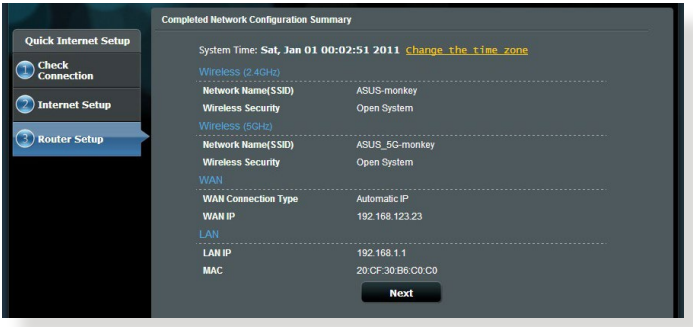
หมายเหตุ:

- การตรวจจับชนิดการเชื่อมต่อ ISP ของคุณโดยอัตโนมัติจะเกิดขึ้นเมื่อคุณกำหนดค่าไวร์เลสเราเตอร์เป็นครั้งแรก หรือเมื่อไวร์เลสเราเตอร์ของคุณถูกรีเซ็ตกลับเป็นการตั้งค่าเริ่มต้น
- ถ้า QIS ตรวจไม่พบชนิดการเชื่อมต่ออินเทอร์เน็ตของคุณ, คลิก **Skip to manual setting (ข้ามไปยังการตั้งค่าแบบแมนนวล)** และกำหนดค่าการตั้งค่าการเชื่อมต่อของคุณแบบแมนนวล

3. กำหนดชื่อเครือข่ายไร้สาย (SSID) และคีย์การป้องกันสำหรับการเชื่อมต่อไร้สาย 2.4GHz และ 5GHz ของคุณ คลิก **Apply (นำไปใช้)** เมื่อเสร็จ



4. การตั้งค่าอินเทอร์เน็ตและการตั้งค่าไร้สายของคุณจะแสดงขึ้น คลิก **Next (ถัดไป)** เพื่อทำต่อ



5. อ่านข้อมูลการสอนเกี่ยวกับการเชื่อมต่อเครือข่ายไร้สาย เมื่อทำเสร็จ, คลิก **Finish (เสร็จ)**

2.3 กำลังเชื่อมต่อไปยังเครือข่ายไร้สายของคุณ

หลังจากการตั้งค่าไวร์เลสเราเตอร์ของคุณด้วย QIS แล้ว คุณสามารถเชื่อมต่อคอมพิวเตอร์หรืออุปกรณ์สมาร์ตอื่นๆ ของคุณเข้ากับเครือข่ายไร้สายของคุณได้

ในการเชื่อมต่อไปยังเครือข่ายของคุณ:

1. บนคอมพิวเตอร์ของคุณ คลิกไอคอนเครือข่าย  ในบริเวณการแจ้งเตือน เพื่อแสดงเครือข่ายไร้สายที่ใช้ได้
2. เลือกเครือข่ายไร้สายที่คุณต้องการเชื่อมต่อไปยัง, จากนั้นคลิก **Connect (เชื่อมต่อ)**
3. คุณอาจจำเป็นต้องป้อนคีย์การป้องกันเครือข่าย สำหรับเครือข่ายไร้สายที่มีระบบป้องกัน, จากนั้นคลิก **OK (ตกลง)**
4. รอในขณะที่คอมพิวเตอร์ของคุณสร้างการเชื่อมต่อไปยังเครือข่ายไร้สายสำเร็จ สถานะการเชื่อมต่อถูกแสดง และไอคอนเครือข่ายแสดงสถานะที่เชื่อมต่อ 

หมายเหตุ:

- ดูบทถัดไป สำหรับรายละเอียดเพิ่มเติมในการกำหนดค่าการตั้งค่าเครือข่ายไร้สายของคุณ
- ดูคู่มือผู้ใช้อุปกรณ์ของคุณ สำหรับรายละเอียดเพิ่มเติมในการเชื่อมต่ออุปกรณ์เข้ากับเครือข่ายไร้สายของคุณ

---

3 การกำหนดค่าการตั้งค่าทั่วไป

3.1 การใช้แผนที่เครือข่าย

แผนที่เครือข่าย อนุญาตให้คุณกำหนดค่าการตั้งค่าระบบป้องกันของเครือข่ายของคุณ, จัดการเน็ตเวิร์กไคลเอ็นต์ของคุณ

3.1.1 การตั้งค่าระบบความปลอดภัยไร้สาย

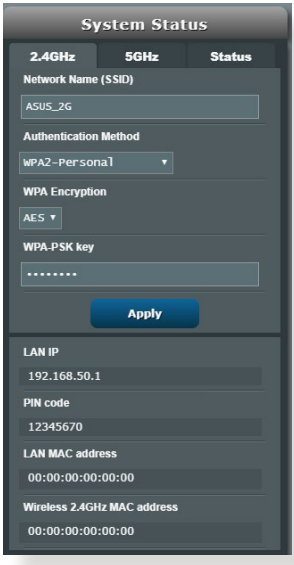
เพื่อป้องกันเครือข่ายของคุณจากการเข้าถึงโดยไม่ได้รับอนุญาต คุณจำเป็นต้องกำหนดค่าของการตั้งค่าระบบความปลอดภัยของเครือข่าย

ในการตั้งค่าระบบความปลอดภัยไร้สาย:

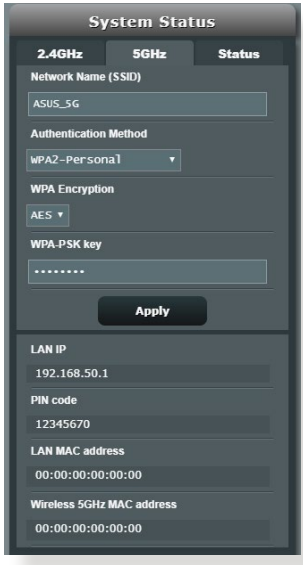
1. จากหน้าต่างระบบเมนู ไปยัง **General (ทั่วไป)** > **Network Map (แผนที่เครือข่าย)**
2. บนหน้าจอ Network Map (แผนที่เครือข่าย) และภายใต้ **System status (สถานะระบบ)**, คุณสามารถกำหนดค่าต่างๆ ของระบบความปลอดภัยไร้สาย เช่น SSID, ระดับความปลอดภัย และการตั้งค่าการเข้ารหัส

หมายเหตุ: คุณสามารถตั้งค่าระบบความปลอดภัยไร้สายที่แตกต่างกันสำหรับแถบความถี่ 2.4GHz และ 5GHz ได

การตั้งค่าระบบความปลอดภัย 2.4GHz



การตั้งค่าระบบความปลอดภัย 5GHz



3. บนฟิลด์ **Wireless name (SSID) (ชื่อไร้สาย (SSID))**, ป้อนชื่อที่เป็นเอกลักษณ์สำหรับเครือข่ายไร้สายของคุณ

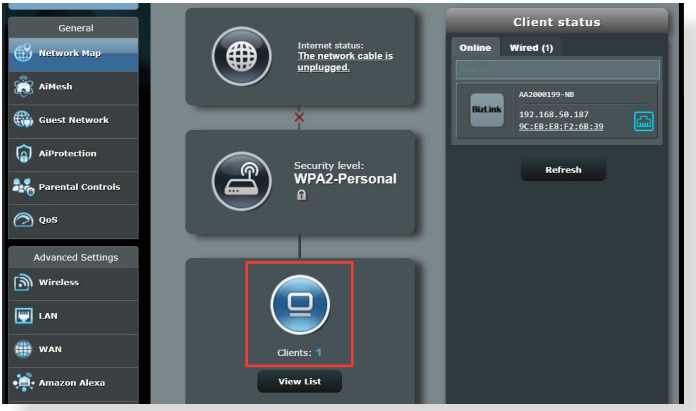
4. จากรายการแบบดึงลง **WEP Encryption (การเข้ารหัส WEP)** เลือกวิธีการเข้ารหัสสำหรับเครือข่ายไร้สายของคุณ

สำคัญ! มาตรฐาน IEEE 802.11n/ac/ax ห้ามการใช้ไฮทรูพุตกับ WEP หรือ WPA-TKIP เป็นยูนิแคสต์ไซเฟอร์ ถ้าคุณใช้วิธีการเข้ารหัสเหล่านี้ อัตราการรับส่งข้อมูลของคุณจะตกลงเป็นการเชื่อมต่อ IEEE 802.11g 54Mbps

---

5. ป้อนรหัสผ่านระบบความปลอดภัยของคุณ
6. คลิก **Apply (นำไปใช้)** เมื่อเสร็จ

3.1.2 การจัดการเน็ตเวิร์กไคลเอ็นต์ของคุณ



ในการจัดการเน็ตเวิร์กไคลเอ็นต์ของคุณ:

1. จากหน้าต่างระบบเมนู ไปยัง **General (ทั่วไป)** > แท็บ **Network Map (แผนที่เครือข่าย)**
2. บนหน้าจอ Network Map (แผนที่เครือข่าย), เลือกไอคอน **Client Status (สถานะไคลเอ็นต์)** เพื่อแสดงข้อมูลเกี่ยวกับเน็ตเวิร์กไคลเอ็นต์ของคุณ
3. เพื่อบล็อกการเข้าถึงของไคลเอ็นต์ไปยังเครือข่ายของคุณ, ให้เลือกไคลเอ็นต์ และคลิก **block (บล็อก)**

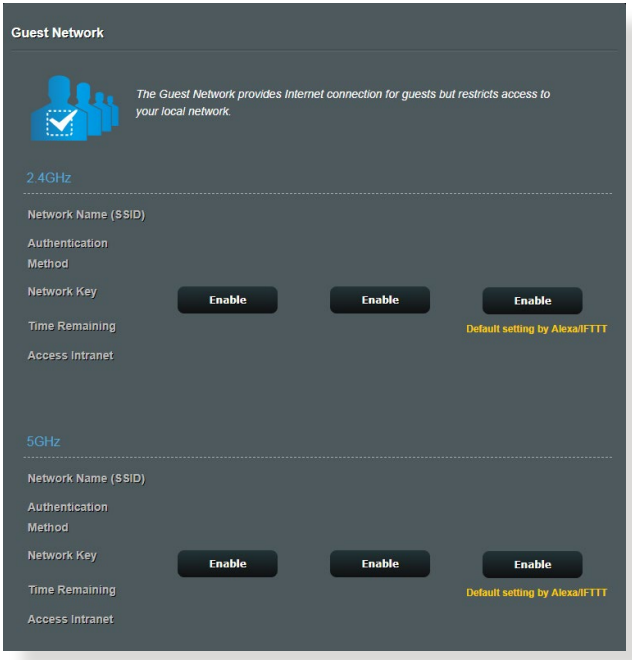
3.2 การสร้างเครือข่ายแขกของคุณ

เครือข่ายแขก ให้การเชื่อมต่ออินเทอร์เน็ตชั่วคราวแก่ผู้มาเยี่ยมผ่านการเข้าถึง SSID หรือเครือข่ายที่แยกกัน โดยไม่ต้องให้การเข้าถึงไปยังเครือข่ายส่วนตัวของคุณ

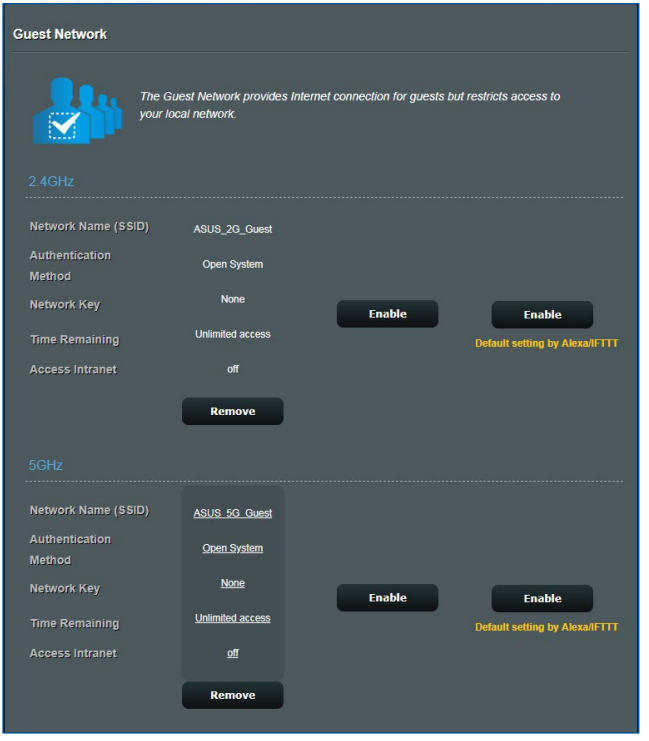
หมายเหตุ: RT-AX55 สนับสนุน SSID มาถึง 6 ตัว (SSID 2.4GHz 3 ตัว และ 5GHz 3 ตัว)

ในการสร้างเครือข่ายแขกของคุณ:

1. จากหน้าต่างระบบเมนู ไปยัง **General (ทั่วไป)** > **Guest Network (เครือขายแขก)**
2. บนหน้าจอ Guest Network (เครือข่ายแขก), เลือกแถบความถี่ 2.4Ghz หรือ 5Ghz สำหรับเครือขายแขกที่คุณตองการสราง
3. คลิก **Enable (เปิดทำงาน)**



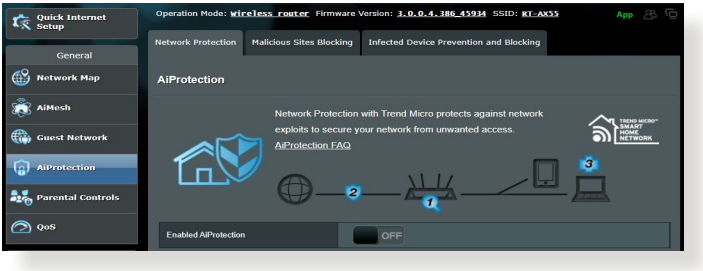
4. ในการกำหนดค่าตัวเลือกเพิ่มเติม, คลิก **Modify (แก้ไข)**



5. คลิก **Yes (ใช่)** บนหน้าจอ **Enable Guest Network (เปิดท่างานเครือขายแขก)**
6. กำหนดชื่อเครือข่ายไร้สายสำหรับเครือข่ายชั่วคราวของคุณบนฟิลด์ **Network name (ชื่อเครือขาย) (SSID)**
7. เลือก **Authentication Method (วิธีการยืนยันตัวบุคคล)**
8. เลือกวิธี **Encryption (การเข้ารหัส)**
9. ระบุ **Access time (เวลาการเข้าถึง)** หรือคลิก **Limitless (ไม่จำกัด)**
10. เลือก **Disable (ปิดท่างาน)** หรือ **Enable (เปิดท่างาน)** บนรายการ **Access Intranet (เขาถึงอินทราเน็ต)**
11. เมื่อทำเสร็จ, คลิก **Apply (น่าไปใช้)**

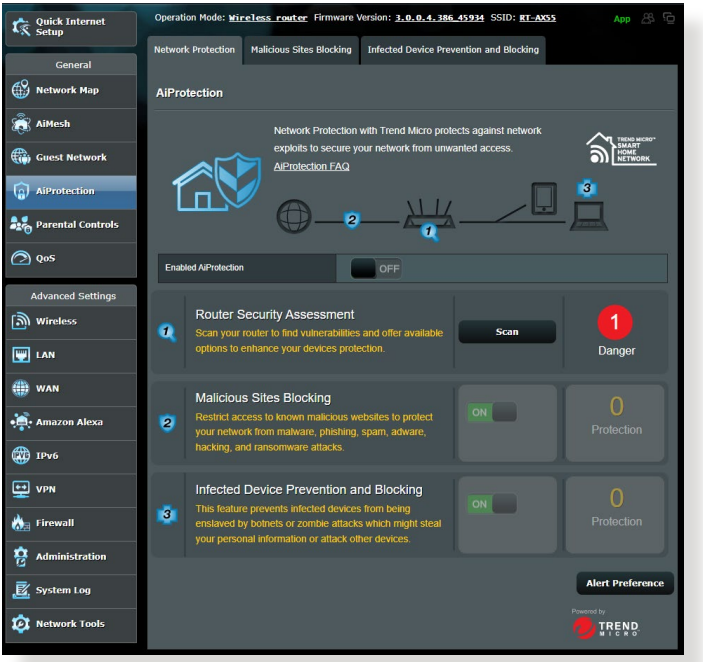
3.3 AiProtection

AiProtection ให้การตรวจดูแลแบบเรียลไทม์ที่ตรวจจับมัลแวร์ สปาย แวร์ และการเข้าถึงที่ไม่ต้องการ นอกจากนี้ยังอนุญาตให้คุณกำหนดตารางเวลาที่อุปกรณ์ที่เชื่อมต่อสามารถเข้าถึงอินเทอร์เน็ตได้



3.3.1 การป้องกันเครือข่าย

การป้องกันเครือข่าย ป้องกันการใช้ประโยชน์จากเครือข่าย และป้องกันเครือข่ายของคุณจากการเข้าถึงที่ไม่พึงประสงค์ข่ายของคุณจากการเข้าถึงที่ไม่พึงประสงค์

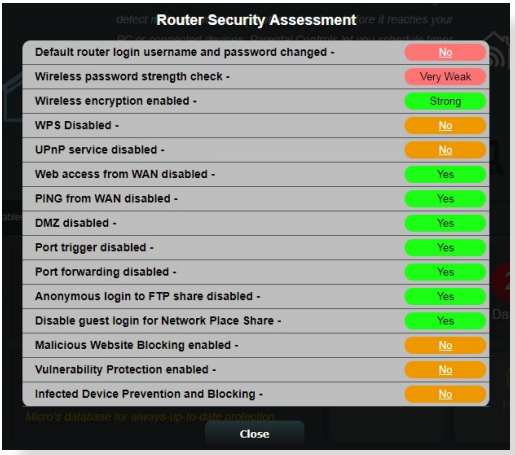


การกำหนดค่าการป้องกันเครือข่าย

ในการกำหนดค่าการป้องกันเครือข่าย:

1. จากแผงระบบนำทาง ไปที่ **General (ทั่วไป)** > **AiProtection**
2. จากหน้าหลักของ **AiProtection** คลิกที่ **Network Protection (การป้องกันเครือข่าย)**
3. จากแท็บ **Network Protection (การป้องกันเครือข่าย)** คลิก **Scan (สแกน)**

   เมื่อทำการสแกนเสร็จ ยูทิลิตี้จะแสดงผลลัพธ์บนหน้า **Router Security Assessment (การประเมินความปลอดภัยของเราเตอร์)**



สำคัญ! รายการที่ทำเครื่องหมายด้วย **Yes (ใช่)** บนหน้า **Router Security Assessment (การประเมินความปลอดภัยของเราเตอร์)** จะถูกการพิจารณาว่ามีสถานะ **ปลอดภัย** รายการที่ทำเครื่องมายด้วย **No (ไม่)**, **Weak (อ่อน)** หรือ **Very Weak (อ่อนมาก)** แนะนำให้ทำการกำหนดค่าอย่างเหมาะสม

---

4. (ทางเลือก) จากหน้า **Router Security Assessment (การประเมินความปลอดภัยของเราเตอร์)** ให้กำหนดค่ารายการที่ทำเครื่องหมายด้วย **No (ไม่)**, **Weak (อ่อน)** หรือ **Very Weak (อ่อนมาก)** ในการดำเนินการ:

   a. คลิกรายการ

หมายเหตุ: เมื่อคุณคลิกที่รายการ ยูทิลิตี้จะส่งคุณไปยังหน้าการตั้งค่าของรายการ

---

   b. จากหน้าการตั้งค่าด้านความปลอดภัยของรายการ ให้กำหนดค่า และทำการเปลี่ยนแปลงที่จำเป็น และคลิก **Apply (นำไปใช้)** เมื่อทำเสร็จ

   c. ไปที่หน้า **Router Security Assessment (การประเมินความปลอดภัยของเราเตอร์)** และคลิก **Close (ปิด)** เพื่อออก จากหน้า

5. ในการกำหนดค่าของการตั้งค่าด้านความปลอดภัยโดยอัตโนมัติ คลิก **Secure Your Router (ทำให้เราเตอร์ปลอดภัย)**
6. เมื่อข้อความปรากฏขึ้น คลิก **OK (ตกลง)**

การบล็อกไซต์ที่ประสงค์ร้าย

คุณสมบัตินี้จำกัดการเข้าถึงยังเว็บไซต์ที่ประสงค์ร้ายที่รู้จักในฐานข้อมูลบนคลาวด์ เพื่อการป้องกันที่ทันสมัยอยู่เสมอ

หมายเหตุ: ฟังก์ชั่นนี้จะเปิดทำงานโดยอัตโนมัติถ้าคุณรัน **Router Weakness Scan (สแกนความอ่อนแอของเราเตอร์)**

ในการเปิดท่างานการบล็อกไซต์ที่ประสงค์ร้าย:

1. จากแผงระบบนำทาง ไปที่ **General (ทั่วไป)** > **AiProtection**
2. จากหน้าหลักของ **AiProtection** คลิกที่ **Network Protection (การป้องกันเครือข่าย)**
3. จากแผง **Malicious Sites Blocking (การบล็อกไซต์ที่ประสงค์ร้าย)** คลิก **ON (เปิด)**

การป้องกันและการบล็อกอุปกรณ์ที่ติดเชื้อ

คุณสมบัตินี้ป้องกันอุปกรณ์ที่ติดเชื้อไม่ให้ส่งข้อมูลส่วนตัว หรือสถานะที่ติดเชื้อไปยังบุคคลภายนอก

หมายเหตุ: ฟังก์ชั่นนี้จะเปิดทำงานโดยอัตโนมัติถ้าคุณรัน **Router Weakness Scan (สแกนความอ่อนแอของเราเตอร์)**

ในการเปิดท่างานการป้องกันช่องโหว่:

1. จากแผงระบบนำทาง ไปที่ **General (ทั่วไป)** > **AiProtection**
2. จากหน้าหลักของ **AiProtection** คลิกที่ **Network Protection (การป้องกันเครือข่าย)**
3. จากแผง **Infected Device Prevention and Blocking (การป้องกันและการบล็อกอุปกรณ์ที่ติดเชื้อ)** คลิก **ON (เปิด)**

ในการกำหนดค่าการกำหนดลักษณะการแจ้ง:

1. จากแผง **Infected Device Prevention and Blocking (การป้องกันและการบล็อกอุปกรณ์ที่ติดเชื้อ)** คลิก **Alert Preference (การกำหนดลักษณะการแจ้ง)**
2. เลือกหรือพิมพ์ผู้ให้บริการอีเมล บัญชีอีเมล และรหัสผ่านเข้าไป จากนั้นคลิก **Apply (นำไปใช้)**

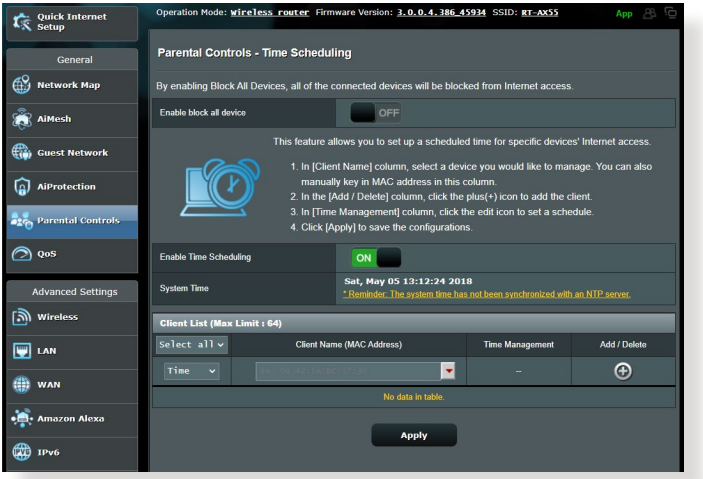
3.3.2 การตั้งค่าการควบคุมโดยผู้ปกครอง

การควบคุมโดยผู้ปกครอง อนุญาตให้คุณควบคุมเวลาใช้อินเทอร์เน็ต หรือตั้งค่าขีดจำกัดเวลาสำหรับการใช้เครือข่ายของไคลเอ็นต์ได้

การกำหนดตารางเวลา

การกำหนดตารางเวลา อนุญาตให้คุณตั้งค่าขีดจำกัดเวลาสำหรับการใช้เครือข่ายของไคลเอ็นต์

หมายเหตุ: ให้แน่ใจว่าเวลาระบบของคุณซิงโครไนซ์กับ NTP เซิร์ฟเวอร์



ในการกำหนดค่าตารางเวลา:

1. จากแผงระบบนำทาง ไปยัง **General (ทั่วไป)** > **AiProtection** > **Parental Controls (การควบคุมโดยผู้ปกครอง)** > **Time Scheduling (การกำหนดตารางเวลา)**
2. จากแผง **Enable Time Scheduling (เปิดทำงานการกำหนดตารางเวลา)** คลิก **ON (เปิด)**
3. จากคอลัมน์ **Clients Name (ชื่อไคลเอ็นต์)** เลือกหรือพิมพ์ชื่อไคลเอ็นต์จากรายการแบบดึงลงเข้าไป

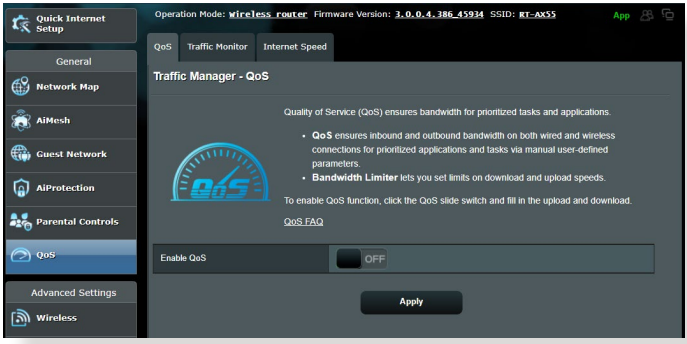
หมายเหตุ: นอกจากนี้ คุณยังอาจป้อน MAC แอดเดรสของไคลเอ็นต์ในคอลัมน์ **Client MAC Address (MAC แอดเดรสของไคลเอ็นต์)** ก็ได้ ตรวจดูให้แน่ใจว่าชื่อไคลเอ็นต์ไม่ได้บรรจุตัวอักษรพิเศษ หรือช่องว่าง เนื่องจากอาจทำให้เราเตอร์ทำงานผิดปกติ

4. คลิก ⊕ เพื่อเพิ่มโปรไฟล์ของไคลเอ็นต์
5. คลิก **Apply (นำไปใช้)** เพื่อจัดเก็บการตั้งค่า

3.4 การใช้ตัวจัดการจราจร

3.4.1 การจัดการ QoS (คุณภาพของบริการ) แบนด์วิดธ

คุณภาพของบริการ (QoS) อนุญาตให้คุณตั้งค่าลำดับความสำคัญของแบนด์วิดธ์ และจัดการจราจรเครือข่าย



ในการตั้งค่าลำดับความสำคัญแบนด์วิดธ์:

1. จากหน้าต่างระบบเมนู ไปยัง **General (ทั่วไป)** > **Traffic Manager (ตัวจัดการการจราจร)** > แท็บ **QoS (QoS)**
2. คลิก **ON (เปิด)** เพื่อเปิดทำงาน QoS กรอกข้อมูลในฟิลด์แบนด์วิดธ์สำหรับอัพโหลดและดาวน์โหลด

หมายเหตุ: ข้อมูลแบนด์วิดธ์ของคุณจาก ISP จะใช้ได้

3. คลิก **Save (บันทึก)**

หมายเหตุ: รายการกฎที่กำหนดโดยผู้ใช้ ใช้สำหรับการตั้งค่าขั้นสูง ถ้าคุณต้องการตั้งลำดับความสำคัญให้แอพพลิเคชั่นเครือข่ายและบริการเครือข่ายที่เจาะจง, เลือก **User-defined QoS rules (กฎ QoS ที่กำหนดโดยผู้ใช้)** หรือ **User-defined Priority (ลำดับความสำคัญที่กำหนดโดยผู้ใช้)** จากรายการแบบดึงลงที่มุมขวาบน

4. บนหน้า **user-defined QoS rules (กฎ QoS ที่กำหนดโดยผู้ใช้)**, มีชนิดบริการออนไลนเริ่มต้น 4 แบบ - เซิร์ฟเว็บ, HTTPS และการถ่ายโอนไฟล์ เลือกบริการที่คุณต้องการ, กรอก **Source IP or MAC (IP หรือ MAC ต้นทาง)**, **Destination Port (พอร์ตปลายทาง)**, **Protocol (โปรโตคอล)**, **Transferred (การถ่ายโอน)** และ **Priority (ลำดับความสำคัญ)**, จากนั้นคลิก **Apply (นำไปใช้)** ข้อมูลจะถูกกำหนดค่าในหน้าจอ QoS rules (กฎ QoS)

หมายเหตุ:

- ในการกรอก IP หรือ MAC ต้นทาง, คุณสามารถ:
  a) ป้อน IP แอดเดรสเฉพาะ เช่น "192.168.122.1"
  b) ป้อน IP แอดเดรสภายในซับเน็ต หรือภายใน IP พูลเดียวกัน เช่น “192.168.123.*” หรือ “192.168.*.*”
  c) ป้อน IP ทั้งหมดในรูปแบบ “*.*.*.*” หรือปล่อยฟิลด์ให้ว่าง
  d) รูปแบบสำหรับ MAC แอดเดรส เป็นเลขฐานสิบหก 2 ตัวจำนวน 6 กลุ่ม ซึ่งแยกกันด้วยเครื่องหมายโคลอน (:) ในลำดับการส่ง (เช่น 12:34:56:aa:bc:ef)
- สำหรับช่วงพอร์ตต้นทางหรือปลายทาง คุณสามารถ :
  a) ป้อนพอร์ตที่เจาะจงเข้าไป เช่น “95”
  b) ป้อนพอร์ตภายในช่วง เช่น “103:315”, “>100” หรือ “<65535”
- คอลัมน์ **Transferred (ถ่ายโอน)** ประกอบด้วยข้อมูลเกี่ยวกับการจราจรอัพสตรีมและดาวน์สตรีม (การจราจรเครือข่ายขาออกและขาเข้า) สำหรับเซสชั่นหนึ่ง ในคอลัมน์นี้, คุณสามารถตั้งค่าขีดจำกัดการจราจรเครือข่าย (ในหน่วย KB) สำหรับบริการที่เจาะจง เพื่อสร้างความสำคัญเฉพาะสำหรับบริการที่กำหนดไปยังพอร์ตที่เจาะจง ตัวอย่างเช่น ถ้าเน็ตเวิร์กไคลเอ็นต์ 2 ตัว คือ PC 1 และ PC 2 กำลังเข้าถึงอินเทอร์เน็ตทั้งคู่ (ตั้งค่าที่พอร์ต 80) แต่ PC 1 ใช้ปริมาณข้อมูลเกินขีดจำกัดการจราจรเครือข่ายเนื่องจากมีงานดาวน์โหลดบางอย่าง, PC 1 จะมีความสำคัญที่ต่ำกว่า ถ้าคุณไม่ต้องการตั้งค่าขีดจำกัดการจราจร ให้ปล่อยคอลัมน์นี้ว่างไว้

---

5. บนหน้า **User-defined Priority (ลำดับความสำคัญที่กำหนดโดยผู้ใช้)**, คุณสามารถตั้งลำดับความสำคัญของแอพพลิเคชั่นเครือข่ายหรืออุปกรณ์ต่างๆ เป็น 5 ระดับ จากรายการแบบดึงลง **user-defined QoS rules (กฎ QoS ที่กำหนดโดยผู้ใช้)**' คุณสามารถใช้วิธีการต่อไปนี้ในการส่งแพคเก็ตข้อมูล ตามระดับความสำคัญ:
   - เปลี่ยนลำดับของแพ็คเก็ตเครือข่ายอัพสตรีมซึ่งถูกส่งไปยังอินเทอร์เน็ต
   - ภายใต้ตาราง **Upload Bandwidth (แบนด์วิดธ์อัพโหลด)**, ตั้งค่า **Minimum Reserved Bandwidth (แบนด์วิดธ์ที่สงวนที่ต่ำที่สุด)** และ **Maximum Bandwidth Limit (ขีดจำกัดแบนด์วิดธ์มากที่สุด)** สำหรับแอพพลิเคชั่นเครือข่ายหลายรายการ ที่มีระดับความสำคัญแตกต่างกัน เปอร์เซ็นต์ระบุถึงอัตราแบนด์วิดธ์อัพโหลดที่ใช้ได้สำหรับแอพพลิเคชั่นเครือข่ายที่ระบุ

หมายเหตุ:

- แพคเก็ตที่มีความสำคัญต่ำจะไม่ได้รับความสนใจ เพื่อให้มั่นใจถึงการส่งข้อมูลของแพคเก็ตที่มีความสำคัญสูง
- ภายใต้ตาราง **Download Bandwidth (แบนด์วิดธ์ดาวน์โหลด)**, ตั้งค่า **Maximum Bandwidth Limit (ขีดจำกัดแบนด์วิดธ์มากที่สุด)** สำหรับแอพพลิเคชั่นเครือข่ายหลายรายการตามลำดับแพคเก็ตอัพสตรีมที่มีความสำคัญสูงกว่า จะทำให้เกิดแพคเก็ตดาวน์สตรีมที่มีความสำคัญสูงกว่า
- ถ้าไม่มีแพคเก็ตกำลังถูกส่งจากแอพพลิเคชั่นที่มีความสำคัญสูง อัตราการรับส่ง ของการเชื่อมต่ออินเทอร์เน็ตจะใช้สำหรับแพคเก็ตที่มีความสำคัญต่ำอย่างเต็มที่

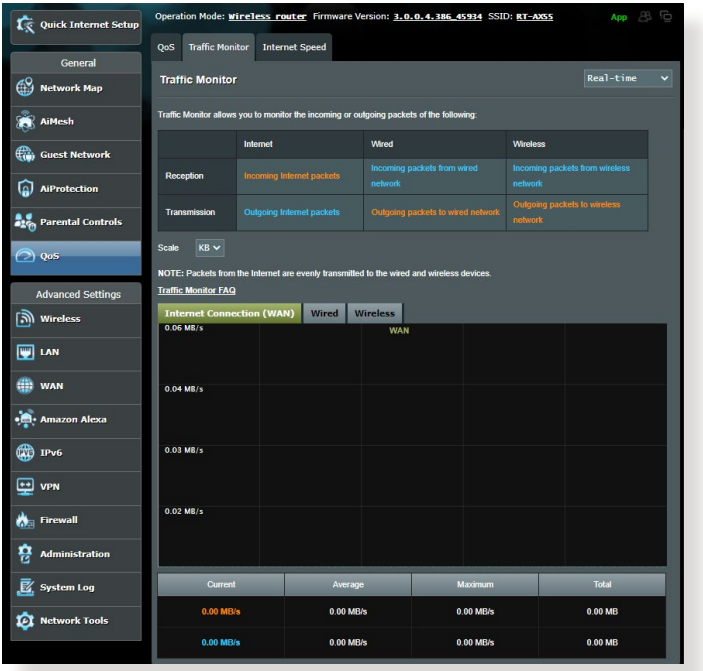
---

6. ตั้งค่าแพคเก็ตที่มีลำดับความสำคัญสูงที่สุด เพื่อให้มั่นใจถึงประสบการณ์การเล่นเกมออนไลน์ที่ราบรื่น คุณสามารถตั้งค่า ACK, SYN และ ICMP เป็นแพคเก็ตที่มีลำดับความสำคัญสูงที่สุดได

หมายเหตุ: ตรวจดูให้แน่ใจว่าเปิดทำงาน QoS ก่อน และตั้งค่าขีดจำกัดอัตราการอัพโหลดและดาวน์โหลด

3.5 ตัววิเคราะห์การรับส่งข้อมูล

ฟังก์ชั่นการตรวจดูแลปริมาณข้อมูลอนุญาตให้คุณเข้าถึงการใช้งานแบนด์วิดธ์และความเร็วของอินเทอร์เน็ตของทั้งเครือข่ายแบบมีสายและไร้สายของคุณ โดยฟังก์ชั่นนี้อนุญาตให้คุณตรวจดูแลการจราจรของเครือข่ายแบบเรียลไทม์



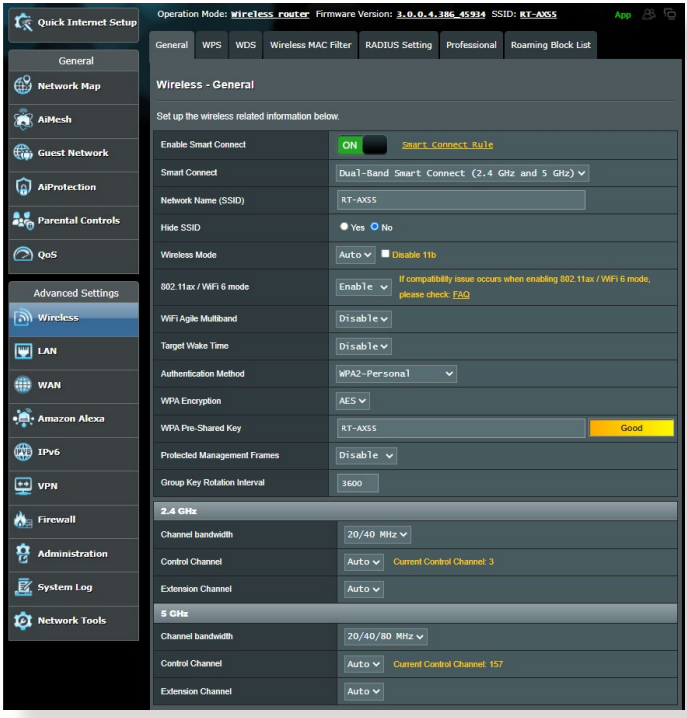
หมายเหตุ: แพคเก็ตจากอินเทอร์เน็ตถูกส่งไปยังอุปกรณ์มีสายและไร้สายเท่ากัน

4 การกำหนดค่าการตั้งค่าขั้นสูง

4.1 ไร้สาย

4.1.1 ทั่วไป

แท็บ General (ทั่วไป) อนุญาตให้คุณกำหนดค่าการตั้งค่าไร้สายพื้นฐาน



ในการกำหนดค่าการตั้งค่าไร้สายพื้นฐาน:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง)** > **Wireless (ไรสาย)** > แท็บ **General (ทั่วไป)**
2. เลือก 2.4GHz หรือ 5GHz เป็นแถบความถี่สำหรับเครือข่ายไร้สายของคุณ
3. กำหนดชื่อที่ไม่ซ้ำที่ประกอบด้วยตัวอักษรได้มากถึง 32 ตัว สำหรับ SSID (ตัวระบุชุดบริการ) หรือชื่อเครือข่ายของคุณ เพื่อระบุเครือข่ายไรสายของคุณ อุปกรณ์ Wi-Fi สามารถหาและเชื่อมต่อไปยังเครือข่ายไรสายผาน SSID ที่คุณกำหนดไว้ SSID บนแบนเนอร์ข้อมูลจะถูกอัพเดตทันทีที่ SSID ใหม่ถูกบันทึกไปยังการตั้งค่า

หมายเหตุ: คุณสามารถกำหนด SSID ที่ไม่ซ้ำสำหรับแถบความถี่ 2.4GHz และ 5GHz

---

4. ในฟิลด์ **Hide SSID (ซ่อน SSID)**, เลือก **Yes (ใช่)** เพื่อป้องกันอุปกรณ์ไรสายไม่ให้ตรวจพบ SSID ของคุณ เมื่อฟังก์ชั่นนี้เปิดทำงาน คุณจำเป็นต้องป้อน SSID ด้วยตัวเองบนอุปกรณ์ไรสายเพื่อเข้าถึงเครือข่ายไรสาย
5. เลือกตัวเลือกโหมดไร้สายเหล่านี้ เพื่อหาชนิดของอุปกรณ์ไร้สายที่สามารถเชื่อมต่อไปยังไวรเลสเราเตอร์ของคุณ:
   - **อัตโนมัติ**: เลือก **Auto (อัตโนมัติ)** เพื่ออนุญาตให้อุปกรณ์ 802.11AX, 802.11AC, 802.11n, 802.11g และ 802.11b เชื่อมต่อไปยัง ไวรเลสเราเตอร์
   - **ดั้งเดิม**: เลือก **Legacy (ดั้งเดิม)** เพื่ออนุญาตให้อุปกรณ์ 802.11b/g/n เชื่อมต่อไปยังไวรเลสเราเตอร์ อย่างไรก็ตาม ฮาร์ดแวร์ที่สนับสนุน 802.11n จะรันที่ความเร็วสูงสุด 54Mbps เท่านั้น
   - **เฉพาะ N**: เลือก **N only (เฉพาะ N)** เพื่อเพิ่มสมรรถนะไวรเลส N ให้สูงที่สุด การตั้งค่านี้ป้องกันไม่ให้อุปกรณ์ 802.11g และ 802.11b เชื่อมต่อไปยังไวรเลสเราเตอร์

6. เลือกแบนด์วิดธ์ช่องเหล่านี้เพื่อให้ได้ความเร็วการรับส่งข้อมูลสูงขึ้น:

   40MHz: เลือกแบนด์วิดธ์นี้เพื่อเพิ่มผลลัพธ์การส่งผ่านข้อมูลไร้สายให้สูงที่สุด

   20MHz (ค่าเริ่มต้น): เลือกแบนด์วิดธ์นี้ ถ้าคุณพบปัญหาบางอย่างกับการเชื่อมต่อไร้สายของคุณเลือกช่องการทำงาน

7. สำหรับไวร์เลสเราเตอร์ของคุณ เลือก **Auto (อัตโนมัติ)** เพื่ออนุญาตให้ไวร์เลสเราเตอร์เลือกช่องที่มีปริมาณการรบกวนน้อยที่สุดโดยอัตโนมัติ
8. เลือกวิธีการยืนยันตัวบุคคลเหล่านี้:
   - **ระบบเปิด**: ตัวเลือกนี้ไม่มีระบบรักษาความปลอดภัยใดๆ
   - **WPA/WPA2/WPA3 ส่วนตัว/WPA อัตโนมัติ-ส่วนตัว**: ตัวเลือกนี้ให้ระบบรักษาความปลอดภัยที่แข็งแกร่ง คุณสามารถใช้ WPA (กับ TKIP) WPA2 (กับ AES) หรือ WPA3 ได้ ถ้าคุณเลือกตัวเลือกนี้ คุณต้องใช้การเข้ารหัส TKIP + AES และป้อนวลีผ่าน WPA (เน็ตเวิร์กคีย์)
   - **WPA/WPA2/WPA3 เอ็นเตอร์ไพรส์/WPA อัตโนมัติ-เอ็นเตอร์ไพรส์**: ตัวเลือกนี้ให้ระบบรักษาความปลอดภัยที่แข็งแกร่งมาก โดยมาพร้อมกับ EAP เซิร์ฟเวอร์ในตัว หรือ RADIUS เซิร์ฟเวอร์ยืนยันตัวบุคคลแบ็ค-เอ็นด์ภายนอก

หมายเหตุ: ไวร์เลสเราเตอร์ของคุณสนับสนุนอัตราการรับส่งข้อมูลสูงที่สุด 54Mbps เมื่อ **Wireless Mode (โหมดไร้สาย)** ถูกตั้งค่าเป็น **Auto (อัตโนมัติ)** และ **encryption method (วิธีการเข้ารหัส)** เป็น **WEP** หรือ **TKIP**

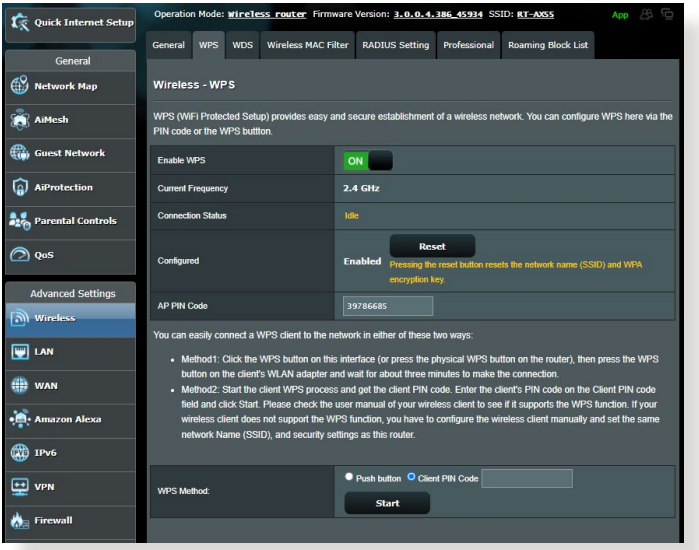
---

9. เลือกตัวเลือกการเข้ารหัส WEP (Wired Equivalent Privacy) เหล่านี้ สำหรับการรับส่งข้อมูลบนเครือข่ายไร้สายของคุณ:
   - **ปิด**: ปิดทำงานการเข้ารหัส WEP
   - **64 บิต**: เปิดทำงานการเข้ารหัส WEP ที่อ่อน
   - **128 บิต**: เปิดทำงานการเข้ารหัส WEP ที่ดีขึ้น
10. เมื่อทำเสร็จ, คลิก **Apply (นำไปใช้)**

4.1.2 WPS

WPS (การตั้งค่า Wi-Fi ที่มีการป้องกัน) เป็นมาตรฐานด้านความปลอดภัยไร้สาย ที่อนุญาตให้คุณเชื่อมต่ออุปกรณ์ต่างๆ ไปยังเครือข่ายไร้สายอย่างง่ายดาย คุณสามารถกำหนดค่าฟังก์ชั่น WPS ด้วยรหัส PIN หรือปุ่ม WPS

หมายเหตุ: ตรวจดูให้แน่ใจว่าอุปกรณ์สนับสนุน WPS



ในการเปิดท่างาน WPS บนเครือข่ายไร้สายของคุณ:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง)** > **Wireless (ไรสาย)** > แท็บ **WPS (WPS)**
2. ในฟิลด์ **Enable WPS (เปิดท่างาน WPS)**, เลื่อนตัวเลื่อนไปยัง **ON (เปิด)**
3. ตามค่าเริ่มต้น WPS ใช้ความถี่ 2.4GHz ถ้าคุณต้องการเปลี่ยนความถี่เป็น 5GHz, **ปิด** ฟังก์ชั่น WPS, คลิก **Switch Frequency (สลับความถี่)** ในฟิลด์ **Current Frequency (ความถี่ปัจจุบัน)**, จากนั้น **เปิด** WPS อีกครั้ง

หมายเหตุ: WPS สนับสนุนการยืนยันตัวบุคคลของระบบเปิด, WPA-ส่วนตัว, WPA2-ส่วนตัว และ WPA3-ส่วนตัว WPS ไม่สนับสนุนเครือข่ายไร้สายที่ใช้วิธีการเข้ารหัส แชร์คีย์, WPA-เอ็นเตอร์ไพรส์, WPA2-เอ็นเตอร์ไพรส์, WPA3-เอ็นเตอร์ไพรส และ RADIUS

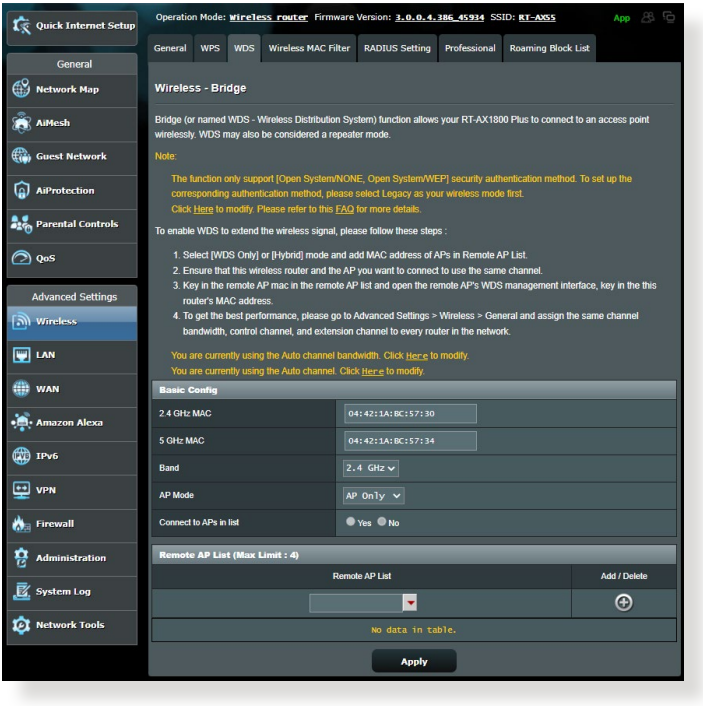
4. ในฟิลด์ WPS Method (วิธี WPS), เลือก **Push Button (ปุ่มกด)** หรือรหัส **Client PIN (ไคลเอ็นต PIN)** ถาคุณเลือก **Push Button (ปุมกด)**, ไปยังขั้นตอนที่ 5 ถาคุณเลือกรหัส **Client PIN (ไคลเอ็นต PIN)**, ไปยังขั้นตอนที่ 6
5. ในการตั้งค่า WPS โดยใช้ปุ่ม WPS ของเราเตอร์, ให้ปฏิบัติตามขั้นตอนเหลานี้:
   a. คลิก **Start (เริ่ม)** หรือกดปุ่ม WPS ที่พบที่ด้านหลังของไวร์เลสเราเตอร
   b. กดปุ่ม WPS บนอุปกรณ์ไร้สายของคุณ ซึ่งโดยปกติจะมีการระบุดวยโลโก WPS

หมายเหตุ: ตรวจสอบอุปกรณ์ไร้สายของคุณ หรือคู่มือผู้ใช้ของอุปกรณ์สำหรับตำแหนงของปุ่ม WPS

   c. ไวร์เลสเราเตอร์จะสแกนหาอุปกรณ์ WPS ที่ใช้ได้ ถ้าไวร์เลสเราเตอร์ไมพบอุปกรณ WPS ใดๆ, เครื่องจะสลับไปยังโหมดสแตนดบาย
6. ในการตั้งค่า WPS โดยใช้รหัส PIN ของไคลเอ็นต์, ให้ปฏิบัติตามขั้นตอนเหลานี้:
   a. ค้นหารหัส PIN WPS บนคู่มือผู้ใช้ของอุปกรณ์ไร้สายของคุณ หรือบนตัวอุปกรณ
   b. ป้อนรหัส PIN ของไคลเอ็นต์บนกล่องข้อความ
   c. คลิก **Start (เริ่ม)** เพื่อสั่งให้ไวร์เลสเราเตอร์ของคุณเข้าสูโหมดสำรวจ WPS ตัวแสดงสถานะ LED ของเราเตอรจะกะพริบ 3 ครั้งอยางรวดเร็ว จนกระทั่งตั้งคา WPS สมบูรณ์

4.1.3 บริดจ์

บริดจ์ หรือ WDS (ระบบการกระจายไร้สาย) อนุญาตให้ ASUS ไวร์เลสเราเตอร์ของคุณเชื่อมต่อไปยังไวร์เลสแอคเซสพอยต์อีกตัวหนึ่ง โดยป้องกันไม่ให้อุปกรณ์ไร้สายหรือสถานีอื่นๆ เข้าถึง ASUS ไวร์เลสเราเตอร์ของคุณ ระบบนี้อาจเรียกว่าเป็นไวร์เลสรีพีตเตอร์ก็ได้ ซึ่ง ASUS ไวร์เลสเราเตอร์ของคุณสื่อสารกับแอคเซสพอยต์อีกตัวหนึ่งและอุปกรณ์ไร้สายอื่นๆ



ในการตั้งค่าไวร์เลสบริดจ์:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง)** > **Wireless (ไร้สาย)** > แท็บ **WDS**
2. เลือกแถบความถี่สำหรับไวร์เลสบริดจ์
3. ในฟิลด์ **AP Mode (โหมด AP)**, เลือกระหว่างตัวเลือกต่อไปนี้:
   - **AP เท่านั้น**: ปิดทำงานฟังก์ชั่นไวร์เลสบริดจ์
   - **WDS เท่านั้น**: เปิดทำงานคุณสมบัติไวร์เลสบริดจ์ แต่ป้องกันไม่ให้อุปกรณ์ไร้สาย/สถานีอื่นเชื่อมต่อไปยังเราเตอร์
   - **ไฮบริด**: เปิดทำงานคุณสมบัติไวร์เลสบริดจ์ และอนุญาตให้อุปกรณ์ไรสาย/สถานีอื่นเชื่อมตอไปยังเราเตอร์ได

หมายเหตุ: ในโหมดไฮบริด, อุปกรณ์ไร้สายที่เชื่อมต่ออยู่กับ ASUS ไวร์เลสเราเตอร์ จะได้รับความเร็วการเชื่อมตอเพียงครึ่งหนึ่งของแอคเซสพอยต์เทานั้น

---

4. ในฟิลด์ **Connect to APs in list (เชื่อมต่อไปยัง AP ในรายการ)**, คลิก **Yes (ใช่)** ถาคุณตองการเชื่อมตอไปยังแอคเซสพอยต์ในรายการรีโมท AP
5. ในฟิลด์ **Control Channel (ช่องควบคม)**, เลือกช่องการทำงานสำหรับไวร์เลสบริดจ์ เลือก **Auto (อัตโนมัติ)** เพื่ออนุญาตใหเราเตอรเลือกช่องที่มีปริมาณการรบกวนนอยที่สุดโดยอัตโนมัติ

หมายเหตุ: ช่องที่ใช้ได้ แตกต่างกันไปตามประเทศหรือภูมิภาค

---

6. บนรายการ รีโมท AP, ป้อน MAC แอดเดรส และคลิกปุ่ม **Add (เพิ่ม)** เพื่อป้อน MAC แอดเดรสของแอคเซสพอยต์ที่ใช้ได้อื่นๆ

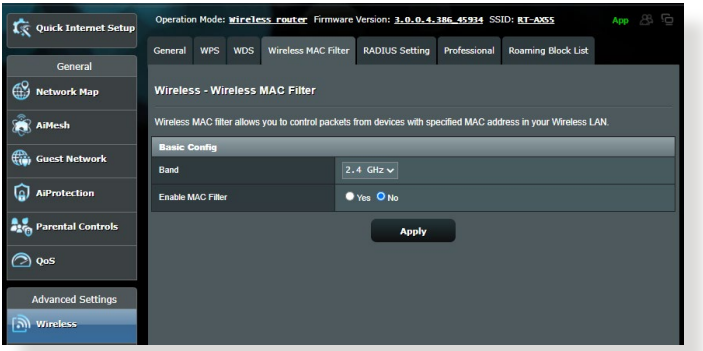
หมายเหตุ: แอคเซสพอยต์ใดๆ ที่เพิ่มไปยังรายการ ควรอยู่บนช่องควบคุมเดียวกันกับ ASUS ไวร์เลสเราเตอร์

---

7. คลิก **Apply (นำไปใช้)**

4.1.4 ตัวกรอง MAC ไร้สาย

ตัวกรอง MAC ไร้สาย ให้การควบคุมแพคเก็ตที่ส่งไปยัง MAC (การควบคุมการเข้าถึงสื่อ) แอดเดรสที่ระบุบนเครือข่ายไร้สายของคุณ

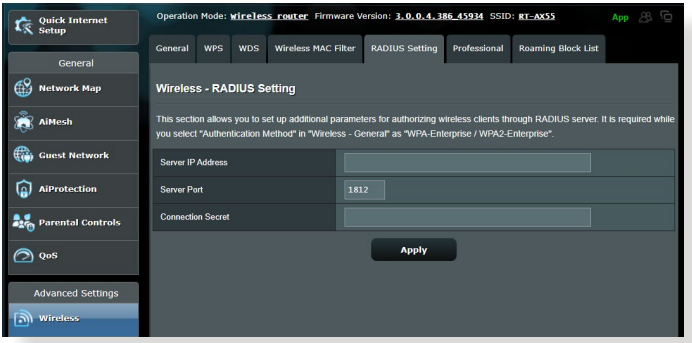


ในการตั้งค่าตัวกรอง MAC ไร้สาย:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง)** > **Wireless (ไร้สาย)** > แท็บ **Wireless MAC Filter (ตัวกรอง MAC ไร้สาย)**
2. ทำเครื่องหมายที่ **Yes (ใช่)** ในฟิลด์ **Enable Mac Filter (เปิดทำงานตัวกรอง Mac)**
3. ในรายการแบบดึงลง **MAC Filter Mode (โหมดตัวกรอง MAC)**, เลือกระหว่าง **Accept (ยอมรับ)** หรือ **Reject (ปฏิเสธ)**
   - เลือก **Accept (ยอมรับ)** เพื่ออนุญาตให้อุปกรณ์ต่างๆ ในรายการตัวกรอง MAC เข้าถึงยังเครือข่ายไร้สายได
   - เลือก **Reject (ปฏิเสธ)** เพื่อป้องกันไม่ให้อุปกรณ์ต่างๆ ในรายการตัวกรอง MAC เข้าถึงยังเครือข่ายไร้สาย
4. บนรายการตัวกรอง MAC, คลิกปุ่ม **Add (เพิ่ม)** และพิมพ์ MAC แอดเดรสของอุปกรณ์ไร้สายเข้าไป
5. คลิก **Apply (นำไปใช้)**

4.1.5 การตั้งค่า RADIUS

การตั้งค่า RADIUS (บริการผู้ใช้โทรเข้าเพื่อยืนยันตัวบุคคลระยะไกล) ให้ระบบป้องกันชั้นพิเศษเมื่อคุณเลือก WPA-เอ็นเตอร์ไพรส์, WPA2-เอ็นเตอร์ไพรส์,WPA3-เอ็นเตอร์ไพรส หรือ Radius กับ 802.1x เป็นโหมดการ ยืนยันตัวบุคคลของคุณ



ในการตั้งค่า RADIUS ไร้สาย:

1. ให้แน่ใจว่าโหมดการยืนยันตัวบุคคลของไวร์เลสเราเตอร์ถูกตั้งค่าเป็น WPA-เอ็นเตอร์ไพรส์, WPA2-เอ็นเตอร์ไพรส์ หรือ WPA3-เอ็นเตอร์ไพรส

หมายเหตุ: โปรดดูส่วน **4.1.1 ทั่วไป** สำหรับการกำหนดค่าโหมดการยืนยันตัวบุคคลของไวร์เลสเราเตอร์ของคุณ

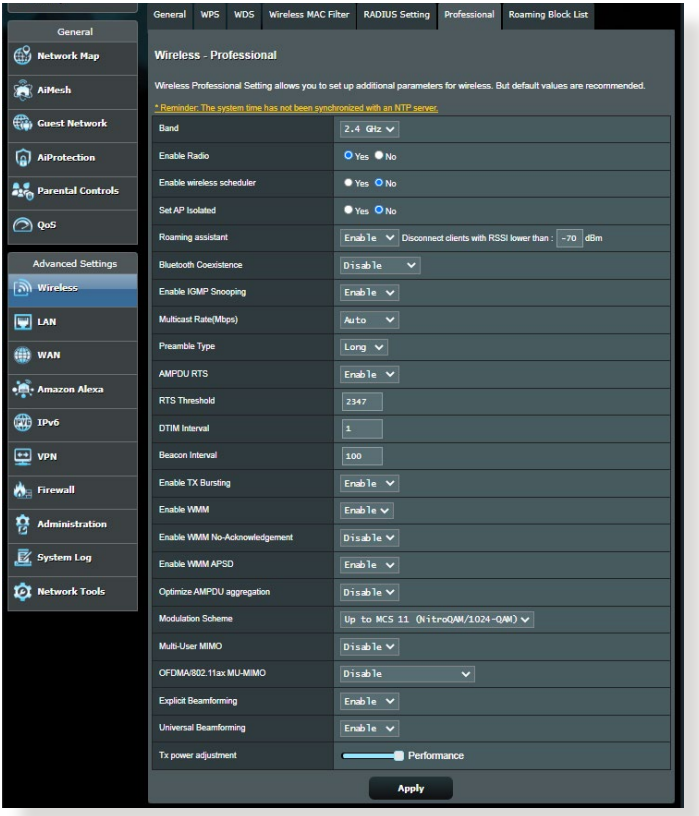
---

2. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง)** > **Wireless (ไรสาย)** > **RADIUS Setting (การตั้งค่า RADIUS)**
3. เลือกแถบความถี่
4. ในฟิลด์ **Server IP Address (เซิร์ฟเวอร์ IP แอดเดรส)**, ป้อน IP แอดเดรสของ RADIUS เซิร์ฟเวอร์ของคุณ
5. ในฟิลด์ **Connection Secret (ความลับการเชื่อมต่อ)**, กำหนดรหัสผ่านเพื่อเข้าถึง RADIUS เซิร์ฟเวอร์ของคุณ
6. คลิก **Apply (นำไปใช้)**

4.1.6 Professional (มืออาชีพ)

หน้าจอ Professional (มืออาชีพ) ให้ตัวเลือกการกำหนดค่าขั้นสูง

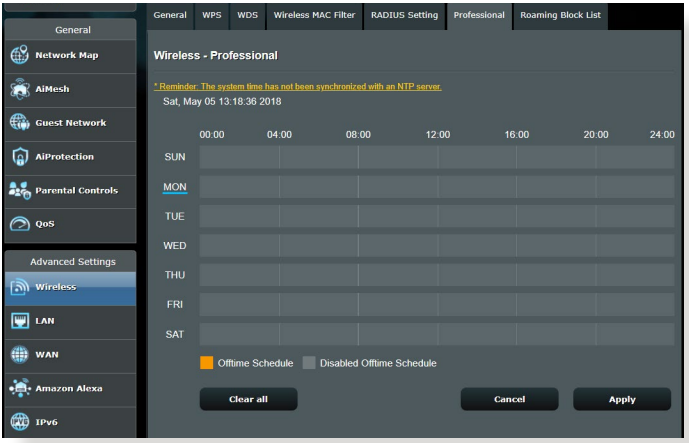
หมายเหตุ: เราแนะนำให้คุณใช้ค่าเริ่มต้นบนหน้านี้



ในหน้าจอ **Professional Settings (การตั้งค่าแบบมืออาชีพ)**, คุณสามารถกำหนดค่าต่อไปนี้:

- **แถบความถี่**: เลือกแถบความถี่ซึ่งการตั้งค่าแบบมืออาชีพจะถูกนำไปใช้ยัง
- **เปิดทำงานวิทยุ**: เลือก **Yes (ใช่)** เพื่อเปิดทำงานเครือข่ายไร้สาย เลือก **No (ไม่)** เพื่อปิดทำงานเครือข่ายไร้สาย
- **เปิดใช้ตัวกำหนดเวลาแบบไร้สาย:** คุณสามารถเลือกรูปแบบนาฬิกาเป็น 24 ชั่วโมงหรือ 12 ชั่วโมง สีในตารางระบุว่า

Allow (อนุญาต) หรือ Deny (ปฏิเสธ) คลิกที่แต่ละเฟรมเพื่อเปลี่ยนการตั้งค่าของช่วโมงในสัปดาหต่าง ๆ และคลิกที่ **OK (ตกลง)** เมื่อเสร็จสิ้น



- **ตั้งค่า AP ที่แยกกัน**: รายการ Set AP isolated (ตั้งค่า AP ที่แยกกัน) ป้องกันอุปกรณ์ไร้สายบนเครือข่ายของคุณไม่ให้สื่อสารซึ่งกันและกัน คุณสมบัตินี้มีประโยชน์ ถ้ามีแขกจำนวนมากเข้ามาใช้หรือออกจากเครือข่ายของคุณบ่อยๆ เลือก **Yes (ใช่)** เพื่อเปิดทำงานคุณสมบัตินี้ หรือเลือก **No (ไม่)** เพื่อปิดทำงาน
- **อัตรามัลติคาสต (Mbps)**: เลือกอัตราการส่งข้อมูลมัลติคาสต์ หรือคลิก **Disable (ปิดทำงาน)** เพื่อปิดการส่งข้อมูลเดี่ยวพร้อมกัน
- **ประเภทพรีแอมเบิล**:ประเภทพรีแอมเบิล กำหนดความยาวของเวลาที่เราเตอร์ใช้สำหรับ CRC (ตรวจสอบความซ้ำซ้อนแบบวงกลม) CRC เป็นวิธีในการตรวจจับข้อผิดพลาดระหว่างการส่งข้อมูล เลือก **Short (สั้น)** สำหรับเครือข่ายไร้สายที่ยุ่งที่มีการจราจรเครือข่ายสูง เลือก **Long (ยาว)** ถ้าเครือข่ายไร้สายของคุณประกอบด้วยอุปกรณ์ไร้สายรุ่นเก่า หรือแบบดั้งเดิม

- **ขีดจำกัด RTS**: เลือกค่าที่ต่ำกว่าสำหรับขีดจำกัด RTS (คำขอให้ส่ง) เพื่อปรับปรุงการสื่อสารไร้สายในเครือข่ายไร้สายที่ยุ่ง ที่มีการจราจรเครือข่ายสูง และอุปกรณ์ไร้สายจำนวนมาก
- **ช่วง DTIM**: ช่วง DTIM (ข้อความระบุการจราจรที่ส่ง) หรืออัตราการส่งข้อมูล คือช่วงเวลาก่อนที่สัญญาณจะถูกส่งไปยังอุปกรณ์ไร้สายในโหมดสลีป เพื่อเป็นการระบุว่ามีแพคเก็ตข้อมูลที่รอการส่ง ค่าเริ่มต้นคือ 3 มิลลิวินาที
- **ช่วงเวลาบีคอน**: ช่วงเวลาบีคอน คือเวลาระหว่าง DTIM หนึ่งกับตัวถัดไป ค่าเริ่มต้นคือ 100 มิลลิวินาที ลดค่าช่วงเวลาบีคอนลง สำหรับการเชื่อมต่อไร้สายที่ไม่มีเสถียรภาพ หรือสำหรับอุปกรณ์โรมมิ่ง
- **เปิดทำงาน TX เบิร์สติ้ง**: เปิดทำงาน TX เบิร์สติ้ง ช่วยปรับปรุงความเร็วการส่งข้อมูลระหว่างไวร์เลสเราเตอร์ และอุปกรณ์ 802.11g
- **เปิดทำงาน WMM APSD**: เปิดทำงาน WMM APSD (Wi-Fi มัลติมีเดีย การส่งการประหยัดพลังงานอัตโนมัติ) เพื่อปรับปรุงการจัดการพลังงานระหว่างอุปกรณ์ไร้สายต่างๆ เลือก **Disable (ปิดทำงาน)** เพื่อปิด WMM APSD

4.2 LAN

4.2.1 LAN IP

หน้าจอ LAN IP อนุญาตให้คุณแก้ไขการตั้งค่า LAN IP ของไวร์เลสเราเตอร์ของคุณ

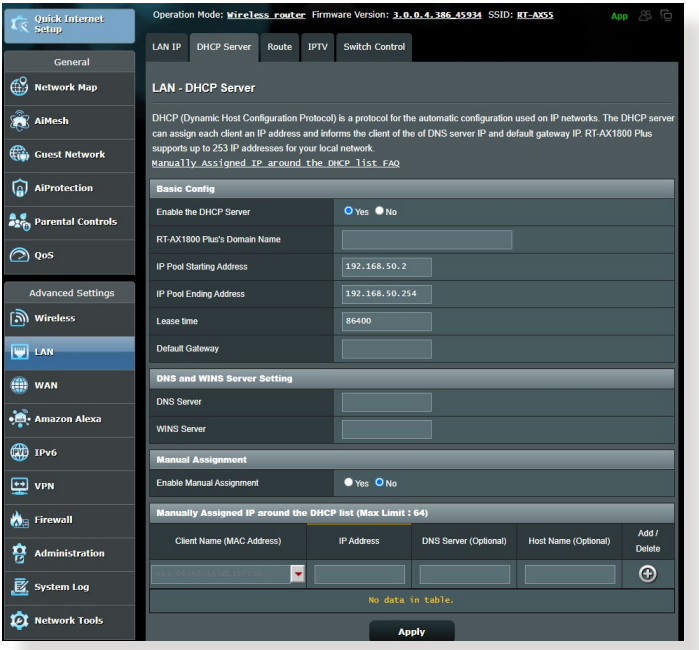
หมายเหตุ: การเปลี่ยนแปลงใดๆ ต่อ LAN IP แอดเดรสจะถูกสะท้อนบนการตั้งค่า DHCP

ในการปรับเปลี่ยนการตั้งค่า LAN IP:

1. จากหน้าต่างระบบเมนู ไปยังแท็บ **Advanced Settings (การตั้งค่าขั้นสูง)** > **LAN (แลน)** > **LAN IP (แลน IP)**
2. แก้ไข **IP** แอดเดรส และ **Subnet Mask (ซับเน็ต มาสก์)**
3. เมื่อทำเสร็จ, คลิก **Apply (นำไปใช้)**

4.2.2 DHCP เซิร์ฟเวอร์

ไวร์เลสเราเตอร์ของคุณใช้ DHCP เพื่อกำหนด IP แอดเดรสบนเครือข่ายของคุณโดยอัตโนมัติ คุณสามารถระบุช่วง IP แอดเดรสและลีสไทม์ สำหรับไคลเอ็นต์ต่างๆ บนเครือข่ายของคุณ



ในการกำหนดค่า DHCP เซิร์ฟเวอร์:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง)** > **LAN (แลน)** > แท็บ **DHCP Server (DHCP เซิร์ฟเวอร์)**
2. ในฟิลด์ **Enable the DHCP Server (เปิดทำงาน DHCP เซิร์ฟเวอร์หรือไม่)**, คลิก **Yes (ใช่)**
3. ในกล่องข้อความ **Domain Name (ชื่อโดเมน)**, ป้อนชื่อโดเมนสำหรับไวร์เลสเราเตอร์
4. ในฟิลด์ **IP Pool Starting Address (แอดเดรสเริ่มต้น IP พูล)**, ป้อน IP แอดเดรสเริ่มต้นเข้าไป

5. ในฟิลด์ **IP Pool Ending Address (แอดเดรสสิ้นสุด IP พูล)**, ป้อน IP แอดเดรสสิ้นสุดเข้าไป
6. ในฟิลด์ **Lease Time (เวลาลีส)**, ป้อนเวลาที่ IP แอดเดรสจะหมดอายุ และไวร์เลสเราเตอร์จะกำหนด IP แอดเดรสใหม่สำหรับเน็ตเวิร์กไคลเอ็นต์โดยอัตโนมัติ

หมายเหตุ:

- ASUS แนะนำให้คุณใช้รูปแบบ IP แอดเดรสเป็น 192.168.50.xxx (ซึ่ง xxx สามารถเป็นตัวเลขใดๆ ก็ได้ระหว่าง 2 ถึง 254) ในขณะที่ระบุช่วง IP แอดเดรส
- แอดเดรสเริ่มต้น IP พูล ไม่ควรมีค่ามากกว่าแอดเดรสสิ้นสุด IP พูล

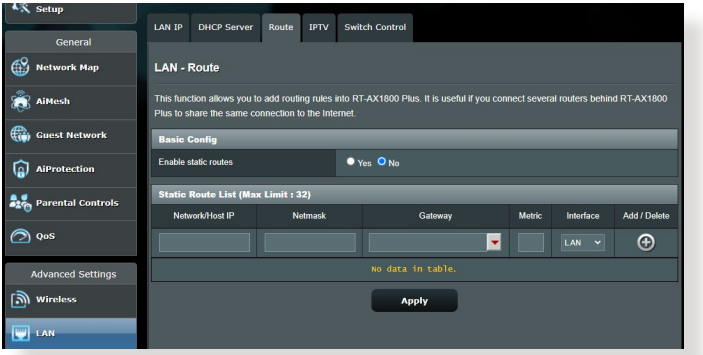
---

7. ในส่วน **DNS and Server Settings (การตั้งค่า DNS และเซิร์ฟเวอร์)**, ป้อน DNS เซิร์ฟเวอร์และ WINS เซิร์ฟเวอร์ IP แอดเดรส ถ้าจำเป็น
8. ไวร์เลสเราเตอร์ของคุณยังสามารถกำหนด IP แอดเดรสด้วยตัวเอง ไปยังอุปกรณ์ต่างๆ บนเครือข่ายได้ด้วย บนฟิลด์ **Enable Manual Assignment (เปิดทำงานการกำหนดด้วยตัวเอง)**, เลือก **Yes (ใช่)** เพื่อกำหนด IP แอดเดรสให้กับ MAC แอดเดรสเฉพาะบนเครือข่าย คุณสามารถเพิ่ม MAC แอดเดรส ได้ถึง 32 รายการไปยังรายการ DHCP สำหรับการกำหนดด้วย ตัวเอง

4.2.3 เส้นทาง

ถ้าเครือข่ายของคุณใช้ไวร์เลสเราเตอร์มากกว่าหนึ่งตัว คุณสามารถกำหนดค่าตารางเส้นทาง เพื่อแชร์บริการอินเทอร์เน็ตเดียวกันได้

หมายเหตุ: เราแนะนำให้คุณอย่าเปลี่ยนการตั้งค่าเส้นทางเริ่มต้น ถ้าคุณไม่มีความรู้ขั้นสูงเกี่ยวกับตารางเส้นทาง

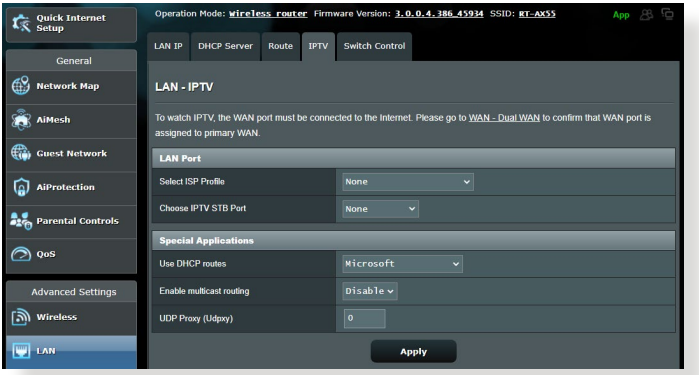


ในการกำหนดค่าตารางเส้นทาง LAN:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง)** > **LAN (แลน)** > แท็บ **Route (เส้นทาง)**
2. ในฟิลด์ **Enable static routes (เปิดทำงานเส้นทางสแตติก)**, เลือก **Yes (ใช่)**
3. บน **Static Route List (รายการเส้นทางสแตติก)**, ป้อนข้อมูลเครือข่ายของแอคเซสพอยต์หรือโหนดอื่นๆ เข้าไป คลิกปุ่ม **Add (เพิ่ม)** หรือ **Delete (ลบ)** เพื่อเพิ่มหรือลบอุปกรณ์บนรายการ
4. คลิก **Apply (นำไปใช้)**

4.2.4 IPTV

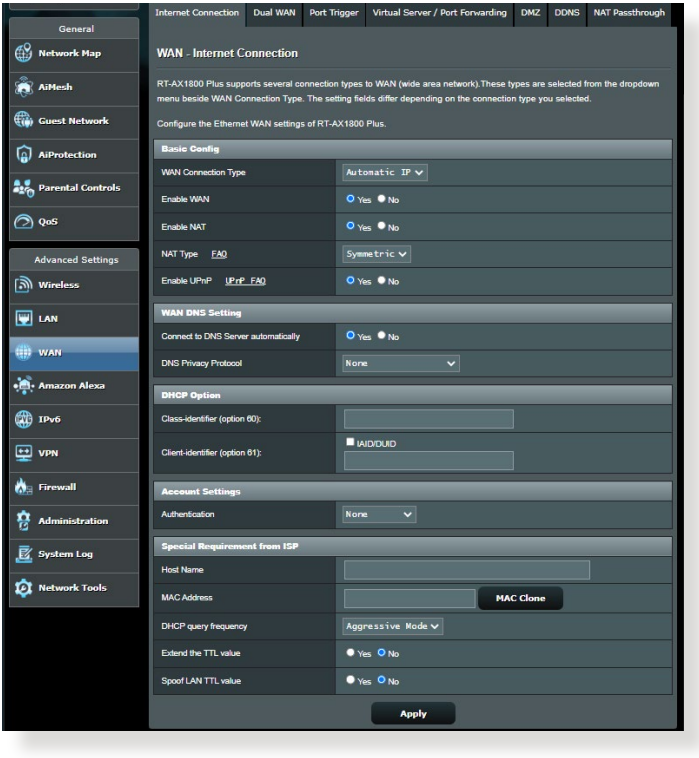
ไวร์เลสเราเตอร์สนับสนุนการเชื่อมต่อไปยังบริการ IPTV ผ่าน ISP หรือ LAN แท็บ IPTV ให้การตั้งค่าการกำหนดค่าต่างๆ ที่จำเป็นในการตั้งค่า IPTV, VoIP, มัลติคาสติ้ง และ UDP สำหรับบริการของคุณ ติดต่อ ISP ของคุณ สำหรับข้อมูลเฉพาะที่เกี่ยวกับบริการของคุณ



4.3 WAN

4.3.1 การเชื่อมต่ออินเทอร์เน็ต

หน้าจอ Internet Connection (การเชื่อมต่ออินเทอร์เน็ต) อนุญาตให้คุณกำหนดค่าการตั้งค่าต่างๆ ของชนิดการเชื่อมต่อ WAN ที่หลากหลาย



ในการกำหนดค่าการตั้งค่าการเชื่อมต่อ WAN:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง)** > **WAN (WAN)** > แท็บ **Internet Connection (การเชื่อมต่ออินเทอร์เน็ต)**
2. กำหนดค่าการตั้งค่าต่อไปนี้ดังแสดงด้านล่าง: เมื่อทำเสร็จ, คลิก **Apply (นำไปใช้)**
   - **ชนิดการเชื่อมต่อ WAN**: เลือกชนิดผู้ให้บริการอินเทอร์เน็ตของ คุณ ทางเลือกต่างๆ คือ **Automatic IP (IP อัตโนมัติ)**,

PPPoE (PPPoE), **PPTP (PPTP)**, **L2TP (L2TP)** หรือ **fixed IP (IP คงที่)** ปรึกษา ISP ของคุณถ้าเราเตอร์ไม่สามารถรับ IP แอดเดรสที่ถูกต้อง หรือถ้าคุณไม่แน่ใจถึงชนิดการเชื่อมต่อ WAN

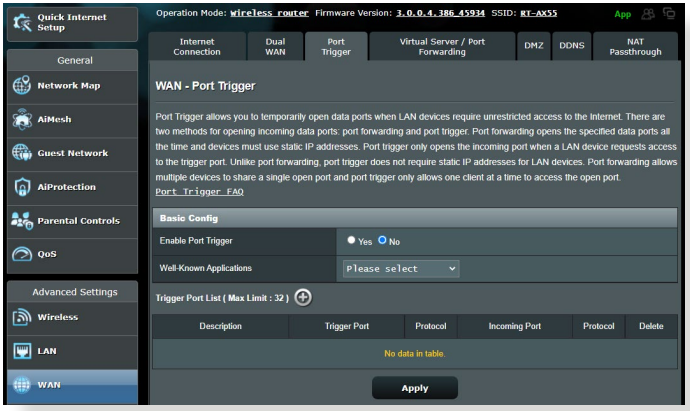
- **เปิดท่างาน WAN**: เลือก **Yes (ใช่)** เพื่ออนุญาตให้เราเตอร์เข้าถึงอินเทอร์เน็ต เลือก **No (ไม่)** เพื่อปิดท่างานการเข้าถึงอินเทอร์เน็ต
- **เปิดท่างาน NAT**: NAT (การแปลเน็ตเวิร์กแอดเดรส) เป็นระบบซึ่ง IP สาธารณะ (WAN IP) หนึ่งตัวถูกใช้ เพื่อให้การเข้าถึงอินเทอร์เน็ตแก่เน็ตเวิร์กไคลเอ็นต์ที่มี IP แอดเดรสส่วนตัวใน LAN IP แอดเดรสส่วนตัวของเน็ตเวิร์กไคลเอ็นต์แต่ละตัวถูกบันทึกในตาราง NAT และถูกใช้เพื่อเปลี่ยนเส้นทางแพคเก็ตขอมูลขาเข้า
- **เปิดท่างาน UPnP**: UPnP (พลักแอนด์เพลย์สากล) อนุญาตให้คุณควบคุมอุปกรณ์หลายชนิด (เช่น เราเตอร์, โทรทัศน์, ระบบสเตอริโอ, เกมคอนโซล, โทรศัพท์เซลลูลาร์) ผ่านเครือข่ายที่ใช้ IP โดยมีหรือไม่มีการควบคุมจากศูนย์กลางผ่านเกตเวย์ก็ได้ UPnP เชื่อมต่อ PC ทุกรูปแบบ โดยให้เครือข่ายที่ไร้รอยต่อสำหรับการกำหนดค่าจากระยะไกล และการถ่ายโอนข้อมูล เมื่อใช้ UPnP, อุปกรณ์เครือข่ายใหม่จะถูกค้นพบโดยอัตโนมัติ หลังจากที่เชื่อมต่อไปยังเครือข่ายแล้ว, อุปกรณ์สามารถถูกกำหนดค่าจากระยะไกลเพื่อสนับสนุนแอพพลิเคชั่น P2P, เกมอินเตอร์แอกทีฟ, การประชุมผ่านวิดีโอ และเว็บหรือพร็อกซี่เฟิร์เวอร์ได้ ไม่เหมือนกับพอร์ตฟอร์เวิร์ดดิ้ง ซึ่งเกี่ยวข้องกับการกำหนดค่าการตั้งค่าพอร์ตด้วยตัวเอง, UPnP จะกำหนดค่าเราเตอร์โดยอัตโนมัติ เพื่อให้เราเตอร์ยอมรับการเชื่อมต่อขาเข้าและส่งคำขอไปยัง PC ที่เจาะจงบนเครือข่ายแลนโดยตรง
- **เชื่อมต่อไปยัง DNS เซิร์ฟเวอร์**: อนุญาตให้เราเตอร์นี้รับ DNS IP แอดเดรสจาก ISP โดยอัตโนมัติ DNS เป็นโฮสต์บนอินเทอร์เน็ต ซึ่งแปลชื่ออินเทอร์เน็ตไปยัง IP แอดเดรสที่เป็นตัวเลข
- **การยืนยันตัวบุคคล**: รายการนี้อาจถูกกำหนดโดย ISP บางแห่ง ตรวจสอบกับ ISP ของคุณ และกรอกข้อมูลลงไป ถ้าจำเป็น

- **ชื่อโฮสต์**: ฟิลด์นี้อนุญาตให้คุณใส่ชื่อโฮสต์สำหรับเราเตอร์ของคุณ โดยปกติเป็นความต้องการพิเศษจาก ISP ของคุณ ถ้า ISP ของคุณกำหนดชื่อโฮสต์ให้กับคอมพิวเตอร์ของคุณ ให้ป้อนชื่อโฮสต์ที่นี่
- **MAC แอดเดรส**: MAC (การควบคุมการเข้าถึงมีเดีย) แอดเดรส เป็นหมายเลขระบุที่ไม่ซ้ำกัน สำหรับอุปกรณ์เครือข่ายของคุณ ISP บางแห่งตรวจดูแล MAC แอดเดรสของอุปกรณ์เครือข่าย ซึ่งเชื่อมต่อไปยังบริการของบริษัท และปฏิเสธอุปกรณ์ที่ไม่รู้จักที่พยายามเชื่อมต่อเข้ามา เพื่อหลีกเลี่ยงปัญหาในการเชื่อมต่อเนื่องจาก MAC แอดเดรสที่ไม่ได้ลงทะเบียน คุณสามารถ:
  - ติดต่อ ISP ของคุณและอัพเดต MAC แอดเดรสที่เชื่อมโยงกับบริการของ ISP ของคุณ
  - โคลน หรือเปลี่ยนแปลง MAC แอดเดรสของ ASUS ไวร์เลสเราเตอร์ เพื่อให้ตรงกับ MAC แอดเดรสของอุปกรณ์เครือข่ายก่อนหน้าที่ ISP รู้จัก

4.3.2 พอร์ตทริกเกอร์

ช่วงพอร์ตทริกเกอร์ริ่ง จะเปิดพอร์ตขาเข้าที่ไม่ได้กำหนดเป็นช่วงเวลาที่จำกัด เมื่อใดก็ตามที่ไคลเอ็นต์บนเครือข่ายแลนทำการเชื่อมต่อขาออกไปยังพอร์ตที่ระบุ พอร์ตทริกเกอร์ริ่งถูกใช้ในสถานการณ์ต่อไปนี้:

- มีไคลเอ็นต์ท้องถิ่นมากกว่าหนึ่งเครื่องจำเป็นต้องส่งต่อพอร์ตสำหรับการใช้งานเดียวกันในเวลาที่แตกต่างกัน
- การใช้งานต้องการให้มีพอร์ตขาเข้าเฉพาะที่แตกต่างจากพอร์ตขาออก



ในการตั้งค่าพอร์ตทริกเกอร์:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง)** > **WAN** > แท็บ **Port Trigger (พอร์ตทริกเกอร์)**
2. กำหนดค่าการตั้งค่าต่อไปนี้ดังแสดงด้านล่าง เมื่อทำเสร็จ, คลิก **Apply (นำไปใช้)**
   - **เปิดทำงานพอร์ตทริกเกอร์**: เลือก **Yes (ใช่)** เพื่อเปิดทำงานพอร์ตทริกเกอร์
   - **แอพพลิเคชั่นที่เป็นที่รู้จักกันดี**: เลือกเกมและบริการเว็บที่เป็นที่นิยม เพื่อเพิ่มไปยังรายการพอร์ตทริกเกอร์

- **คำอธิบาย**: ป้อนชื่อหรือคำอธิบายสั้นๆ สำหรับบริการ
- **ทริกเกอร์พอร์ต**: ระบุทริกเกอร์พอร์ตเพื่อเปิดพอร์ตขาเข้า
- **โปรโตคอล**: เลือกโปรโตคอล, TCP หรือ UDP
- **พอร์ตขาเข้า**: ระบุพอร์ตขาเข้าเพื่อรับข้อมูลขาเข้าจากอินเทอร์เน็ต

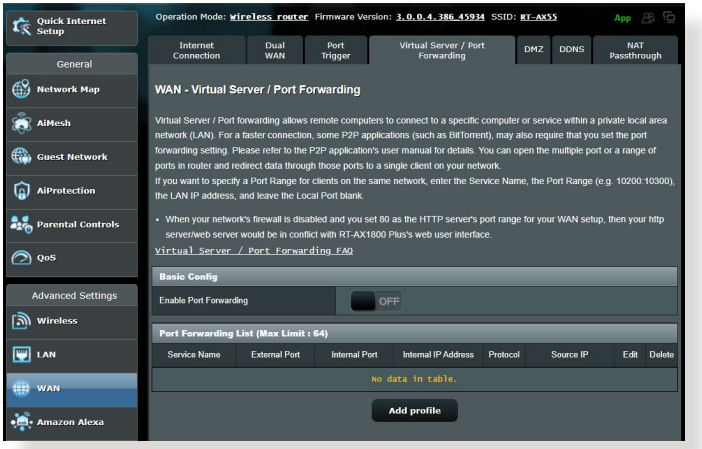
หมายเหตุ:

- ในขณะที่เชื่อมต่อไปยัง IRC เซิร์ฟเวอร์, ไคลเอ็นต์ PC ทำการเชื่อมต่อขาออกโดยใช้ช่วงพอร์ตทริกเกอร์ 66660-7000 IRC เซิร์ฟเวอร์ตอบสนองโดยการตรวจสอบชื่อผู้ใช้ และสร้างการเชื่อมต่อใหม่ไปยังไคลเอ็นต์ PC โดยใช้พอร์ตขาเข้า
- ถ้า พอร์ตทริกเกอร์ ถูกปิดทำงาน, เราเตอร์จะตัดการเชื่อมต่อ เนื่องจากไม่สามารถหาว่า PC เครื่องใดที่กำลังขอการเข้าถึง IRC อยู่ เมื่อพอร์ตทริกเกอร์ เปิดทำงาน, เราเตอร์จะกำหนดพอร์ตขาเข้า เพื่อรับข้อมูลขาเข้า พอร์ตขาเข้านี้จะปิดหลังจากถึงช่วงเวลาที่กำหนด เนื่องจากเราเตอร์ไม่แน่ใจว่าเมื่อใดที่แอพพลิเคชั่นสิ้นสุดการทำงาน
- พอร์ตทริกเกอร์ริ่ง อนุญาตไคลเอ็นต์เพียงหนึ่งเครื่องในเครือข่ายให้ใช้บริการที่เจาะจง และพอร์ตขาเข้าที่เจาะจงในเวลาเดียวกัน
- คุณไม่สามารถใช้แอพพลิเคชั่นเดียวกันเพื่อทริกเกอร์พอร์ตใน PC มากกว่าหนึ่งเครื่องในเวลาเดียวกันได้ เราเตอร์จะส่งพอร์ตกลับไปยังคอมพิวเตอร์เครื่องล่าสุดที่ส่งค่าขอ/ทริกเกอร์ไปให้เราเตอร์เท่านั้น

4.3.3 เวอร์ชวลเซิร์ฟเวอร์/พอร์ตฟอร์เวิร์ดดิ้ง

พอร์ตฟอร์เวิร์ดดิ้ง เป็นวิธีการเพื่อเปลี่ยนเส้นทางการจราจรเครือข่ายจากอินเทอร์เน็ตไปยังพอร์ตที่เจาะจง หรือช่วงพอร์ตที่เจาะจงไปยังอุปกรณ์บนเครือข่ายแลนของคุณ การตั้งค่าพอร์ตฟอร์เวิร์ดดิ้งบนเราเตอร์ของคุณ อนุญาตให้ PC ที่อยู่นอกเครือข่ายเข้าถึงบริการที่เจาะจงที่มีให้โดย PC ในเครือข่ายของคุณได้

หมายเหตุ: เมื่อพอร์ตฟอร์เวิร์ดดิ้งเปิดทำงาน, ASUS เราเตอร์จะบล็อกการจราจรขาเข้าที่ไม่พึงประสงค์จากอินเทอร์เน็ต และอนุญาตเฉพาะการตอบกลับจากคำขอขาออกจาก LAN เท่านั้น เน็ตเวิร์กไคลเอ็นต์ไม่สามารถเข้าถึงอินเทอร์เน็ตได้โดยตรง รวมทั้งในทางกลับกันด้วย



ในการตั้งค่าการส่งต่อพอร์ต:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง)** > **WAN** > แท็บ **Virtual Server / Port Forwarding (เวอร์ชวลเซิร์ฟเวอร์ / พอร์ตฟอร์เวิร์ดดิ้ง)**

2. กำหนดค่าการตั้งค่าต่อไปนี้ดังแสดงด้านล่าง: เมื่อทำเสร็จ, คลิก **Apply (นำไปใช้)**

- **เปิดทำงานพอร์ตฟอร์เวิร์ดดิ้ง**: เลือก **Yes (ใช่)** เพื่อเปิดทำงานพอร์ตฟอร์เวิร์ดดิ้ง
- **รายการเซิร์ฟเวอร์ที่มีชื่อเสียง**: หาชนิดของบริการที่คุณต้องการเข้าถึง
- **รายการเกมที่มีชื่อเสียง**: รายการนี้แสดงพอร์ตที่ต้องการสำหรับเกมออนไลน์ที่เป็นที่นิยมเพื่อให้ทำงานอย่างถูกต้อง
- **FTP เซิร์ฟเวอร์พอร์ต**: หลีกเลี่ยงการกำหนดช่วงพอร์ต 20:21 สำหรับ FTP เซิร์ฟเวอร์ของคุณ เนื่องจากการทำเช่นนี้จะทำให้เกิดข้อขัดแย้งกับการกำหนดเนทีฟ FTP เซิร์ฟเวอร์ของเราเตอร์
- **ชื่อบริการ**: ป้อนชื่อบริการ
- **ช่วงพอร์ต**: ถ้าคุณต้องการระบุช่วงพอร์ตสำหรับไคลเอ็นต์บนเครือข่ายเดียวกัน, ป้อน Service Name (ชื่อบริการ), Port Range (ช่วงพอร์ต) (เช่น 10200:10300), LAN IP address (LAN IP แอดเดรส), และปล่อยให้ Local Port (พอร์ตในเครื่อง) ว่าง ช่วงพอร์ตยอมรับรูปแบบต่างๆ เช่น ช่วงพอร์ต (300:350), พอร์ตส่วนตัว (566,789) หรือผสม (1015:1024,3021)

หมายเหตุ:

- เมื่อไฟร์วอลล์ของเครือข่ายของคุณถูกปิดทำงาน และคุณตั้งค่า 80 เป็นช่วงพอร์ตของ HTTP เซิร์ฟเวอร์สำหรับการตั้งค่า WAN ของคุณ, ในกรณีนี้ http เซิร์ฟเวอร์/เว็บเซิร์ฟเวอร์อาจเกิดข้อขัดแย้งกับระบบติดต่อผู้ใช้แบบเว็บของเราเตอร์
- เครือข่ายใช้พอร์ตต่างๆ เพื่อแลกเปลี่ยนข้อมูล ซึ่งแต่ละพอร์ตถูกกำหนดหมายเลขพอร์ต และงานที่เจาะจงไว้ ตัวอย่างเช่น พอร์ต 80 ใช้สำหรับ HTTP พอร์ตที่เจาะจงสามารถถูกใช้โดยแอพพลิเคชั่นหรือบริการเดียวได้ในแต่ละขณะเวลา ดังนั้น การที่ PC สองตัวพยายามเข้าถึงข้อมูลผ่านพอร์ตเดียวกันในเวลาเดียวกัน ก็อาจทำให้การทำงานล้มเหลว ตัวอย่างเช่น คุณไม่สามารถตั้งค่าพอร์ตฟอร์เวิร์ดดิ้ง สำหรับพอร์ต 100 สำหรับ PC สองเครื่องในเวลาเดียวกันได

- **โลคัล IP**: ป้อน LAN IP แอดเดรสของไคลเอ็นต์

หมายเหตุ: ใช้สแตติก IP แอดเดรสสำหรับไคลเอ็นต์ท้องถิ่น เพื่อทำให้พอร์ตฟอร์เวิร์ดดิ้งทำงานอย่างเหมาะสม สำหรับข้อมูล ให้ดูส่วน **4.2 LAN**

- **โลคัลพอร์ต**: ป้อนพอร์ตที่เจาะจง เพื่อรับแพคเก็ตที่ส่งต่อมา ปล่อยฟิลด์นี้ให้ว่างไว้ ถ้าคุณต้องการแพคเก็ตขาเข้าให้ถูกเปลี่ยนเส้นทางไปยังช่วงพอร์ตที่ระบุ
- **โปรโตคอล**: เลือกโปรโตคอล ถ้าคุณไม่แน่ใจ เลือก **BOTH (ทั้งคู่)**

ในการตรวจสอบว่าพอร์ตฟอร์เวิร์ดดิ้งถูกกำหนดค่าสำเร็จหรือไม่:

- ให้แน่ใจว่าเซิร์ฟเวอร์หรือแอพพลิเคชั่นของคุณถูกตั้งค่าแล้วและกำลังรันอยู่
- คุณจำเป็นต้องให้ไคลเอ็นต์อยู่นอก LAN ของคุณแต่มีการเข้าถึงอินเทอร์เน็ต (เรียกว่า “อินเทอร์เน็ตไคลเอ็นต์”) ไคลเอ็นต์นี้ไม่ควรเชื่อมต่ออยู่กับ ASUS เราเตอร์
- บนอินเทอร์เน็ตไคลเอ็นต์, ใช้ WAN IP ของเราเตอร์เพื่อเข้าถึงเซิร์ฟเวอร์ ถ้าพอร์ตฟอร์เวิร์ดดิ้งถูกตั้งค่าสำเร็จ, คุณควรสามารถเข้าถึงไฟล์หรือแอพพลิเคชั่นได้

ความแตกต่างระหว่างพอร์ตทริกเกอร์ และพอร์ตฟอร์เวิร์ดดิ้ง:

- พอร์ตทริกเกอร์จะทำงานแม้ว่าไม่มีการตั้งค่า LAN IP แอดเดรสที่เฉพาะเจาะจง ไม่เหมือนกับพอร์ตฟอร์เวิร์ดดิ้ง ซึ่งจำเป็นต้องมีสแตติก LAN IP แอดเดรส, พอร์ตทริกเกอร์ยืดหยุ่นอนุญาตให้ส่งต่อพอร์ตแบบไดนามิกโดยใช้เราเตอร์ได้ ช่วงพอร์ตที่กำหนดไว้ล่วงหน้า ถูกกำหนดค่าเพื่อให้ยอมรับการเชื่อมต่อขาเข้าภายในช่วงระยะเวลาที่จำกัด พอร์ตทริกเกอร์ยืดหยุ่นอนุญาตให้คอมพิวเตอร์หลายเครื่องรันแอพพลิเคชั่นที่โดยปกติอาจต้องการให้ส่งต่อพอร์ตเดียวกันไปยัง PC แต่ละเครื่องบนเครือข่ายด้วยตัวเอง
- พอร์ตทริกเกอร์ยืดหยุ่นมีความปลอดภัยมากกว่าพอร์ตฟอร์เวิร์ดดิ้ง เนื่องจากพอร์ตขาเข้าไม่ได้เปิดตลอดเวลา พอร์ตเหล่านั้นเปิดเฉพาะเมื่อแอพพลิเคชั่นทำการเชื่อมต่อขาออกผ่านทริกเกอร์พอร์ตเท่านั้น

4.3.4 DMZ

เวอร์ชวล DMZ เปิดเผยไคลเอ็นต์หนึ่งเครื่องไปยังอินเทอร์เน็ต ทำให้ไคลเอ็นต์นี้รับแพคเก็ตขาเข้าทั้งหมดโดยตรงไปยังเครือข่ายแลนของคุณ

โดยปกติ การจราจรขาเข้าจากอินเทอร์เน็ตถูกทิ้งและเปลี่ยนเส้นทางไปยังไคลเอ็นต์ที่เจาะจงเฉพาะเมื่อพอร์ตฟอร์เวิร์ดดิ้ง หรือพอร์ตทริกเกอร์ถูกกำหนดค่าไว้บนเครือข่าย ในการกำหนดค่า DMZ, เน็ตเวิร์กไคลเอ็นหนึ่งเครื่องจะรับแพคเก็ตขาเข้าทั้งหมด

การตั้งค่า DMZ บนเครือข่ายมีประโยชน์เมื่อคุณต้องการให้พอร์ตขาเข้าเปิด หรือเมื่อคุณต้องการโฮสต์โดเมน เว็บ หรืออีเม เซิร์ฟเวอร์

ข้อควรระวัง: การเปิดพอร์ตทั้งหมดบนไคลเอ็นต์ไปยังอินเทอร์เน็ต ทำให้เครือข่ายออนแอต่อการโจมตีภายนอก โปรดระมัดระวังความเสี่ยงด้านความปลอดภัยที่เกี่ยวข้องกับการใช้ DMZ

ในการตั้งค่า DMZ:

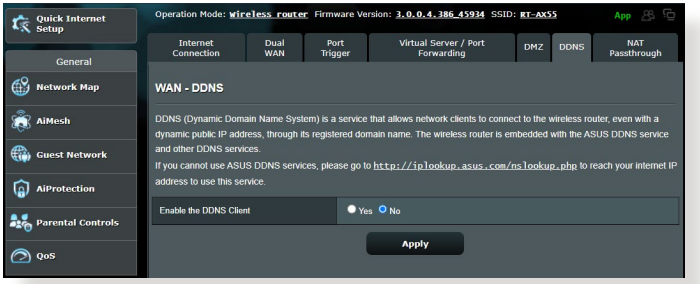
1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง)** > **WAN** > แท็บ **DMZ (DMZ)**
2. กำหนดค่าการตั้งค่าด้านล่าง: เมื่อทำเสร็จ, คลิก **Apply (นำไปใช้)**
   - **IP แอดเดรสของสถานีที่เปิดออก:** ป้อน LAN IP แอดเดรสของไคลเอ็นต์ที่จะให้บริการ DMZ และถูกเปิดออกบนอินเทอร์เน็ต ตรวจดูให้แน่ใจว่าเซิร์ฟเวอร์ไคลเอ็นต์มีสแตติก IP แอดเดรส

ในการลบ DMZ:

1. ลบ LAN IP แอดเดรสของไคลเอ็นต์จากกล่องข้อความ **IP Address of Exposed Station (IP แอดเดรสของสถานีที่เปิดออก)**
2. เมื่อทำเสร็จ, คลิก **Apply (นำไปใช้)**

4.3.5 DDNS

การตั้งค่า DDNS (ไดนามิก DNS) อนุญาตให้คุณเข้าถึงเราเตอร์จากภายนอกเครือข่ายของคุณผ่านบริการ ASUS DDNS ที่ให้มา หรือบริการ DDNS อื่น



ในการตั้งค่า DDNS:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง)** > **WAN** > แท็บ**DDNS (DDNS)**
2. กำหนดค่าการตั้งค่าต่อไปนี้ดังแสดงด้านล่าง: เมื่อทำเสร็จ, คลิก **Apply (นำไปใช)**
   - **เปิดทำงาน DDNS ไคลเอ็นต์**: เปิดทำงาน DDNS เพื่อเข้าถึง ASUS เราเตอร์ผ่านชื่อ DNS แทนที่จะเป็น WAN IP แอดเดรส
   - **ชื่อเซิร์ฟเวอร์และโฮสต์**: เลือก ASUS DDNS หรือ DDNS อื่น ถ้าคุณต้องการใช้ ASUS DDNS, ให้กรอกชื่อโฮสต์ในรูปแบบ xxx.asuscomm.com (xxx คือชื่อโฮสต์ของคุณ)
   - ถ้าคุณต้องการใช้บริการ DDNS อื่น, คลิก **FREE TRIAL (ทดลองใช้ฟรี)** และลงทะเบียนออนไลน์ก่อน กรอกฟิลด์ชื่อผู้ใช้ หรืออีเมลแอดเดรส และรหัสผ่าน หรือ DDNS คีย์
   - **เปิดทำงานอักขระตัวแทน**: เปิดทำงานอักขระตัวแทนถ้าบริการ DDNS จำเป็นต้องใช้

หมายเหตุ:

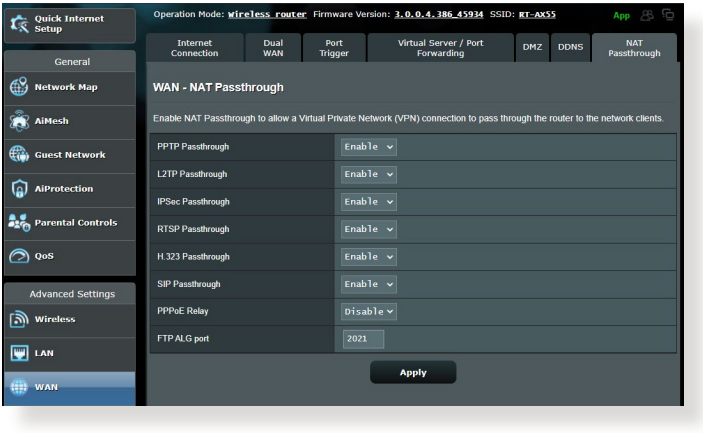
บริการ DDNS จะไม่ทำงานภายใต้เงื่อนไขเหล่านี้:

- เมื่อไวร์เลสเราเตอร์กำลังใช้ WAN IP แอดเดรสส่วนตัว (192.168.x.x, 10.x.x.x หรือ 172.16.x.x) ตามที่ระบุด้วยข้อความสีเหลือง
- เราเตอร์อาจอยู่บนเครือข่ายที่ใช้ตาราง NAT หลายตาราง

4.3.6 NAT ผ่านตลอด

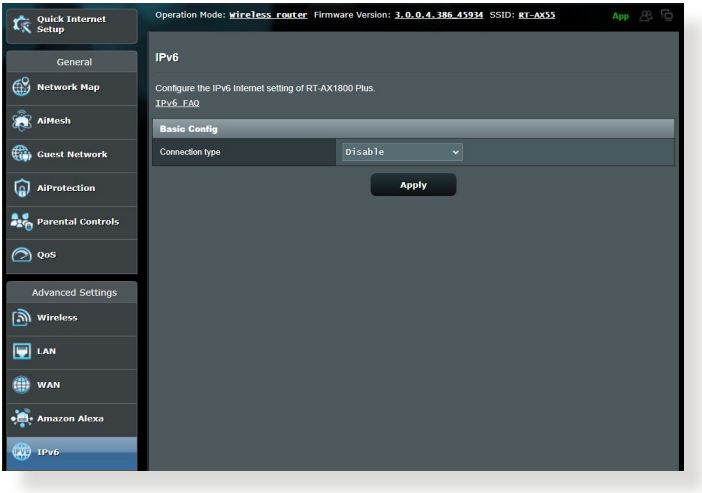
NAT ผ่านตลอด อนุญาตการเชื่อมต่อเครือข่ายส่วนตัวเสมือน (VPN) ให้ผ่านเราเตอร์ไปยังเน็ตเวิร์กไคลเอ็นต์ ตามค่าเริ่มต้น PPTP Passthrough (PPTP ผ่านตลอด), L2TP Passthrough (L2TP ผ่านตลอด), IPsec Passthrough (IPsec ผ่านตลอด) และ RTSP Passthrough (RTSP ผ่านตลอด) ถูกเปิดทำงาน

ในการเปิดทำงาน / ปิดทำงานการตั้งค่า NAT ผ่านตลอด ไปที่ **Advanced Settings (การตั้งค่าขั้นสูง)** > **WAN** > แท็บ **NAT Passthrough (NAT ผ่านตลอด)** เมื่อทำเสร็จ, คลิก **Apply (นำไปใช้)**



4.4 IPv6

ไวร์เลสเราเตอร์นี้สนับสนุน IPv6 แอดเดรสซึ่ง ซึ่งเป็นระบบที่สนับสนุน IP แอดเดรสมากกว่า มาตรฐานนี้ยังไม่มีใช้กันอย่างกว้างขวาง ติดต่อ ISP ของคุณถ้าบริการอินเทอร์เน็ตของคุณสนับสนุน IPv6



ในการตั้งค่า IPv6:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง)** > **IPv6 (IPv6)**
2. เลือก **Connection Type (ชนิดการเชื่อมต่อ)** ของคุณ ตัวเลือกการกำหนดค่าจะแตกต่างกันไป ขึ้นอยู่กับชนิดการเชื่อมต่อที่คุณเลือก
3. ป้อนการตั้งค่า IPv6 LAN และ DNS ของคุณ
4. คลิก **Apply (นำไปใช้)**

หมายเหตุ: โปรดสอบถาม ISP ของคุณเกี่ยวกับข้อมูล IPv6 เฉพาะสำหรับบริการอินเทอร์เน็ตของคุณ

4.5 ไฟร์วอลล์

ไวร์เลสเราเตอร์สามารถทำหน้าที่เป็นฮาร์ดแวร์ไฟร์วอลล์สำหรับเครือข่ายของคุณได้

หมายเหตุ: ตามค่าเริ่มต้น คุณสมบัติไฟร์วอลล์จะเปิดทำงาน

4.5.1 ทั่วไป

ในการตั้งค่าไฟร์วอลล์พื้นฐาน:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง)** > **Firewall (ไฟร์วอลล์)** > แท็บ **General (ทั่วไป)**
2. บนฟิลด์ **Enable Firewall (เปิดทำงานไฟร์วอลล์)**, เลือก **Yes (ใช่)**
3. บนการป้องกัน **Enable DoS (เปิดทำงาน DoS)**, เลือก **Yes (ใช่)** เพื่อป้องกันเครือข่ายของคุณจากการโจมตี DoS (การปฏิเสธบริการ) แม้ว่าคุณสมบัตินี้อาจส่งผลกับสมรรถนะของเราเตอร์ก็ตาม
4. คุณยังสามารถตรวจดูแลการแลกเปลี่ยนแพคเก็ตระหว่างการเชื่อมต่อ LAN และ WAN ได้ด้วย บนชนิดแพคเก็ตที่บันทึก, เลือก **Dropped (หลุด)**, **Accepted (ยอมรับ)** หรือ **Both (ทั้งคู่)**
5. คลิก **Apply (นำไปใช้)**

4.5.2 ตัวกรอง URL

คุณสามารถระบุคำสำคัญหรือเว็บแอดเดรส เพื่อป้องกันการเข้าถึงยัง URL ที่เจาะจงได้

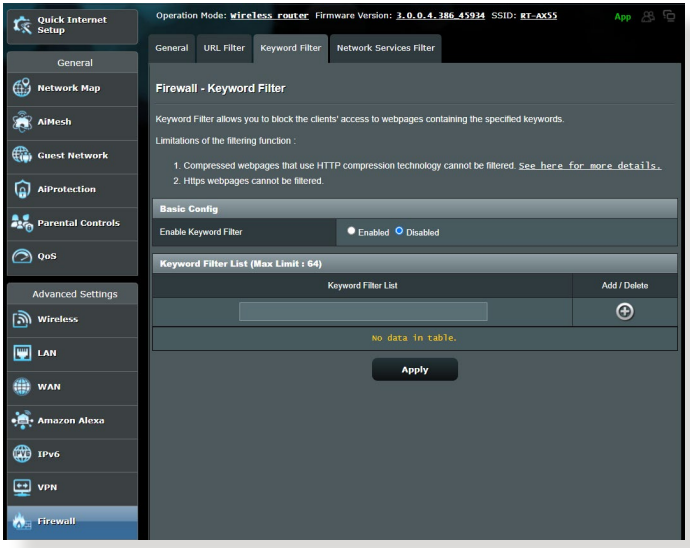
หมายเหตุ: ตัวกรอง URL เป็นไปตามการสอบถาม DNS ถ้าเน็ตเวิร์กไคลเอ็นต์เข้าถึงเว็บไซต์อยู่แล้ว เช่น http://www.abcxxx.com, เว็บไซต์จะไม่ถูกบล็อก (DNS แคชในระบบเก็บเว็บไซต์ที่เข้าชมก่อนหน้าไว้) ในการแก้ไขปัญหานี้ ให้ล้าง DNS แคชก่อนที่จะตั้งค่าตัวกรอง URL

ในการตั้งค่าตัวกรอง URL:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง)** > **Firewall (ไฟร์วอลล์)** > แท็บ **URL Filter (ตัวกรอง URL)**
2. บนฟิลด์ Enable URL Filter (เปิดทำงานตัวกรอง URL), เลือก **Enabled (เปิดทำงาน)**
3. ป้อน URL และคลิกปุ่ม 
4. คลิก **Apply (นำไปใช้)**

4.5.3 ตัวกรองคำสำคัญ

ตัวกรองคำสำคัญจะบล็อกการเข้าถึงไปยังเว็บเพจที่ประกอบด้วยคำสำคัญที่ระบุ



ในการตั้งค่าตัวกรองคำสำคัญ:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง)** > **Firewall (ไฟร์วอลล์)** > แท็บ **Keyword Filter (ตัวกรองคำสำคัญ)**
2. บนฟิลด์ Enable Keyword Filter (เปิดทำงานตัวกรองคำสำคัญ), เลือก **Enabled (เปิดทำงาน)**

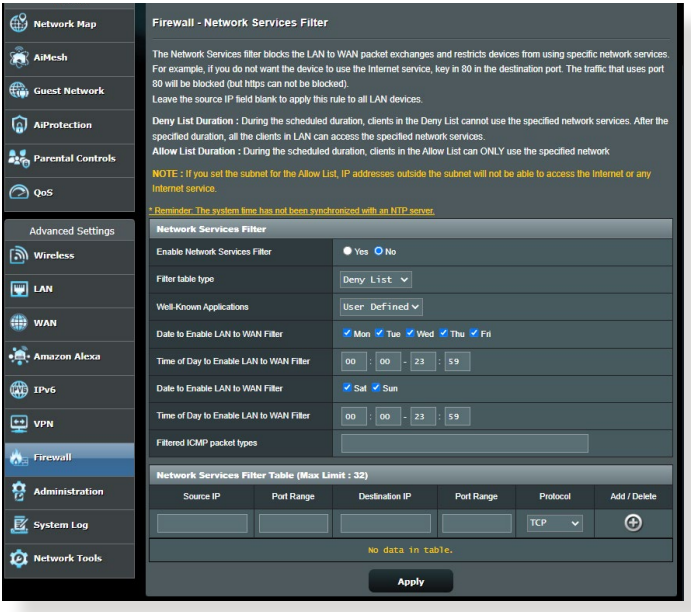
3. ป้อนคำหรือวลี และคลิกปุ่ม **Add (เพิ่ม)**
4. คลิก **Apply (นำไปใช้)**

หมายเหตุ:

- ตัวกรองคำสำคัญ เป็นไปตามการสอบถาม DNS ถ้าเน็ตเวิร์กไคลเอ็นต์เข้าถึงเว็บไซต์อยู่แล้ว เช่น http://www.abcxxx.com, เว็บไซต์จะไม่ถูกบล็อก (DNS แคชในระบบเก็บเว็บไซต์ที่เข้าชมก่อนหน้าไว้) ในการแก้ไขปัญหานี้ ให้ล้าง DNS แคชก่อนที่จะตั้งค่าตัวกรองคำสำคัญ
- เว็บเพจที่บีบขนาดโดยใช้การบีบขนาด HTTP ไม่สามารถถูกกรองได้ เพจ HTTPS ยังไม่สามารถถูกบล็อกโดยใช้ตัวกรองคำสำคัญได้เช่นกัน

4.5.4 ตัวกรองบริการเครือข่าย

ตัวกรองบริการเครือข่าย บล็อกการแลกเปลี่ยนแพคเก็ต LAN ไปยัง WAN และจำกัดเน็ตเวิร์กไคลเอ็นต์ไม่ให้เข้าถึงยังบริการเว็บไซต์ที่เจาะจง เช่น Telnet หรือ FTP



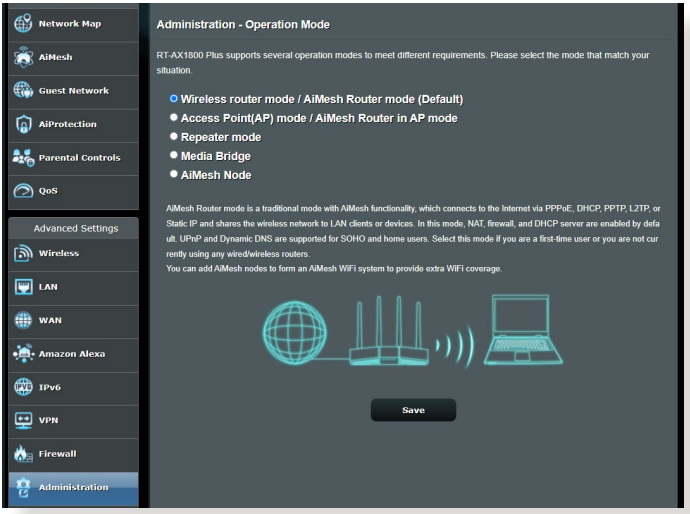
ในการตั้งค่าตัวกรองบริการเครือข่าย:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง)** > **Firewall (ไฟร์วอลล์)** > แท็บ **Network Service Filter (ตัวกรองบริการเครือขาย)**
2. บนฟิลด์ Enable Network Services Filter (เปิดทำงานตัวกรองบริการเครือขาย), เลือก **Yes (ใช่)**
3. เลือกชนิดตารางตัวกรอง **Black List (บัญชีดำ)** บล็อกบริการเครือขายที่ระบุ **White List (บัญชีขาว)** จำกัดการเขาถึงไปยังเฉพาะบริการเครือขายที่ระบุ
4. ระบุวันที่และเวลาที่ตัวกรองจะแอกทีฟ
5. ในการระบุบริการเครือข่ายไปยังตัวกรอง, ป้อน Source IP (IP ต้นทาง), Destination IP (IP ปลายทาง), Port Range (ช่วงพอร์ต) และ Protocol (โปรโตคอล) คลิกปุ่ม 
6. คลิก **Apply (นำไปใช้)**

4.6 การดูแลระบบ

4.6.1 โหมดการทำงาน

หน้า โหมดการทำงาน อนุญาตให้คุณเลือกโหมดที่เหมาะสมสำหรับเครือข่ายของคุณ



ในการตั้งค่าโหมดการทำงาน:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง)** > **Administration (การดูแลระบบ)** > แท็บ **Operation Mode (โหมดการทำงาน)**
2. เลือกโหมดการทำงานเหล่านี้:
   - **โหมดไวร์เลสเราเตอร์(ค่าเริ่มต้น)**: ในโหมดไวร์เลสเราเตอร์, ไวร์เลสเราเตอร์จะเชื่อมต่อไปยังอินเทอร์เน็ต และให้การเข้าถึง อินเทอร์เน็ตไปยังอุปกรณ์ที่ใช้ได้บนเครือข่ายแลนของตัวเอง
   - **โหมดรีพีตเตอร์**: โหมดนี้จะเปลี่ยนเราเตอร์เป็นรีพีตเตอร์ไร้สายเพื่อขยายช่วงสัญญาณของคุณ
   - **โหมดแอคเซสพอยต์**: ในโหมดนี้ เราเตอร์จะสร้างเครือข่ายไร้สายบนเครือข่ายที่มีอยู่แล้ว
3. คลิก **Save (บันทึก)**

หมายเหตุ: เราเตอร์จะบูตใหม่เมื่อคุณเปลี่ยนโหมด

4.6.2 ระบบ

หน้า **System (ระบบ)** อนุญาตให้คุณกำหนดค่าการตั้งค่าไวร์เลสเราเตอร์ของคุณ

ในการตั้งค่าระบบ:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง)** > **Administration (การดูแลระบบ)** > แท็บ **System (ระบบ)**
2. คุณสามารถกำหนดค่าการตั้งค่าต่อไปนี้:
   - **เปลี่ยนรหัสผ่านล็อกอินของเราเตอร์**: คุณสามารถเปลี่ยนรหัสผ่านและชื่อล็อกอินของไวร์เลสเราเตอร์ โดยการป้อนชื่อและรหัสผ่านใหม่
   - **พฤติกรรมปุ่ม WPS**: ปุ่ม WPS บนตัวเครื่องไวร์เลสเราเตอร์สามารถถูกใช้เพื่อเปิดทำงาน WPS
   - **โซนเวลา**: เลือกโซนเวลาสำหรับเครือข่ายของคุณ
   - **NTP เซิร์ฟเวอร์**: ไวร์เลสเราเตอร์สามารถเข้าถึง NTP (โปรโตคอลเวลาเครือข่าย) เซิร์ฟเวอร์เพื่อที่จะซิงโครไนซ์เวลาได้
   - **เปิดทำงาน Telnet**: คลิก **Yes (ใช่)** เพื่อเปิดทำงานบริการ Telnet บนเครือข่าย คลิก **No (ไม่)** เพื่อปิดทำงาน Telnet
   - **วิธีการยืนยันตัวบุคคล**: คุณสามารถเลือกโปรโตคอล HTTP, HTTPS หรือทั้งสองอย่าง เพื่อรักษาความปลอดภัยในการเข้าถึงเราเตอร์ได้
   - **เปิดทำงานการเข้าถึงเว็บจาก WAN**: เลือก **Yes (ใช่)** เพื่ออนุญาตให้คุณอุปกรณ์ด้านนอกเครือข่ายสามารถเข้าถึงการตั้งค่า GUI ของไวร์เลสเราเตอร์ได้ เลือก **No (ไม่)** เพื่อป้องกันการเข้าถึง
   - **อนุญาตเฉพาะ IP ที่เจาะจง**:คลิก **Yes (ใช่)** ถ้าคุณต้องการระบุ IP แอดเดรสของอุปกรณ์ที่ได้รับอนุญาตให้เข้าถึงยังการตั้งค่า GUI ของไวร์เลสเราเตอร์จาก WAN
   - **รายการไคลเอ็นต์**: ป้อน WAN IP แอดเดรสของอุปกรณ์เครือข่ายที่อนุญาตให้เข้าถึงยังการตั้งค่าของไวร์เลสเราเตอร์ รายการนี้จะถูกใช้ ถ้าคุณคลิก **Yes (ใช่)** ในรายการ **Only allow specific IP (อนุญาตเฉพาะ IP ที่เจาะจง)**
3. คลิก **Apply (นำไปใช้)**

4.6.3 การอัปเกรดเฟิร์มแวร์

หมายเหต: ดาวน์โหลดเฟิร์มแวร์ล่าสุดจากเว็บไซต์ ASUS ที่ **http://www.asus.com**

ในการอัปเกรดเฟิร์มแวร์:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง)** > **Administration (การดูแลระบบ)** > แท็บ **Firmware Upgrade (เฟิร์มแวรอัพเกรด)**
2. ในฟิลด์ **New Firmware File (ไฟล์เฟิร์มแวร์ใหม่)**, คลิก **Browse (เรียกดู)** เพื่อค้นหาเฟิร์มแวร์ใหม่ในคอมพิวเตอร์ของคุณ
3. คลิก **Upload (อัปโหลด)**

หมายเหตุ:

- เมื่อกระบวนการอัพเกรดสมบูรณ์ ให้รอสักครู่เพื่อให้ระบบบูตใหม่
- ถ้ากระบวนการอัปเกรดล้มเหลว ไวร์เลสเราเตอร์จะเข้าสู่โหมดช่วยเหลือโดยอัตโนมัติ และไฟแสดงสถานะ LED เพาเวอร์ที่แผงด้านหน้าจะกะพริบช้าๆ ในการเรียกคืน หรือกู้คืนระบบ ให้ใช้ยูทิลิตี้ **5.2 Firmware Restoration (การกู้คืนเฟิร์มแวร์)**

4.6.4 การกู้คืน/การจัดเก็บ/การอัปโหลดการตั้งค่า

ในการกู้คืน/จัดเก็บ/อัปโหลดการตั้งค่า:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง)** > **Administration (การดูแลระบบ)** > แท็บ **Restore/Save/Upload Setting (กู้คืน/บันทึก/อัพโหลดการตั้งค่า)**
2. เลือกงานที่คุณต้องการทำ:
   - ในการกู้คืนการตั้งค่ากลับเป็นค่าเริ่มต้นจากโรงงาน, คลิก **Restore (กู้คืน)**, และคลิก **OK (ตกลง)** ในข้อความการยืนยัน
   - ในการจัดเก็บการตั้งค่าระบบปัจจุบัน, คลิก **Save (จัดเก็บ)**, และคลิก **Save (จัดเก็บ)** ในหน้าต่างดาวน์โหลดไฟล์ เพื่อจัดเก็บไฟล์ระบบลงในพาธที่คุณต้องการ
   - ในการกู้คืนการตั้งค่าระบบก่อนหน้า, คลิก **Browse (เรียกดู)** เพื่อค้นหาไฟล์ระบบที่คุณต้องการกู้คืน, จากนั้นคลิก **Upload (อัปโหลด)**

สำคัญ! ถ้าเกิดปัญหาขึ้น ให้อัพโหลดเฟิร์มแวร์เวอร์ชั่นล่าสุด และกำหนดค่าการ ตั้งค่าใหม่ อย่ากู้คืนเราเตอร์กลับเป็นการตั้งค่าเริ่มต้น

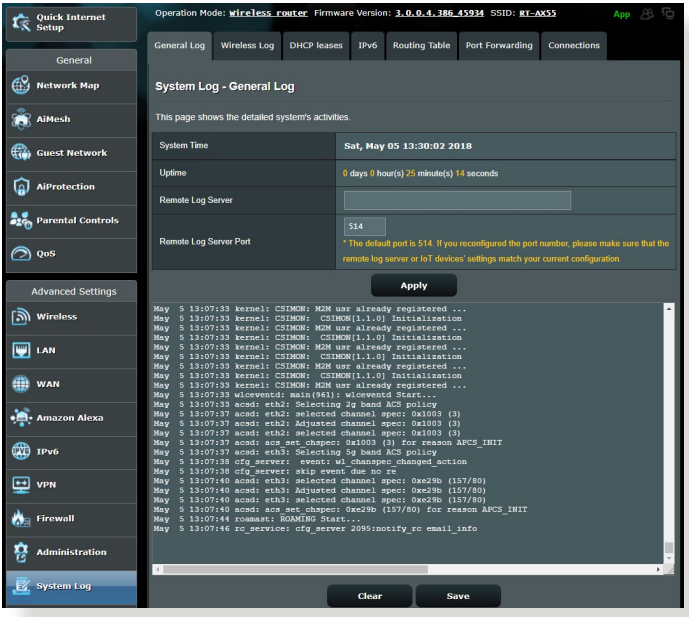
4.7 บันทึกระบบ

บันทึกระบบ ประกอบด้วยกิจกรรมต่างๆ ของเครือข่ายที่บันทึกไว้

หมายเหตุ: บันทึกระบบ รีเซ็ตเมื่อเราเตอร์ถูกบูตใหม่ หรือปิดเครื่อง

ในการดูบันทึกระบบของคุณ:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง) > System Log (บันทึกระบบ)**
2. คุณสามารถดูกิจกรรมเครือข่ายของคุณในแท็บเหล่านี้ได้:
   - บันทึกทั่วไป
   - DHCP ลีส
   - บันทึกไร้สาย
   - พอร์ตฟอร์เวิร์ดดิ้ง
   - ตารางเราติ้ง



5 ยูทิลิตี้

หมายเหตุ:

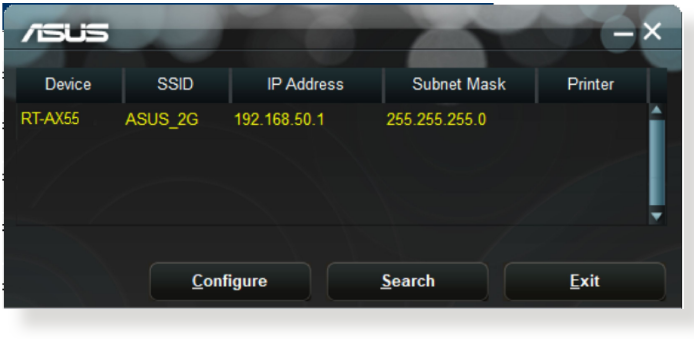
- ดาวน์โหลดและติดตั้งยูทิลิตี้ของไวร์เลสเราเตอร์จากเว็บไซต์ ASUS:
  - การสำรวจอุปกรณ์ v1.4.7.1 ท http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Discovery.zip
  - การกู้คืนเฟิร์มแวร์ v1.9.0.4 ที่ http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Rescue.zip
- ยูทิลิตี้เหล่านี้ไม่ได้รับการสนับสนุนบน MAC OS

5.1 การค้นหาอุปกรณ

Device Discovery (การค้นหาอุปกรณ์) เป็นยูทิลิตี้ ASUS WLAN ซึ่งทำหน้าที่ตรวจ หาอุปกรณ์ ASUS ไวร์เลส เราเตอร์ และอนุญาตให้คุณตั้งค่าคอนฟิกอุปกรณ์

ในการเปิดยูทิลิตี้ การค้นหาอุปกรณ์:

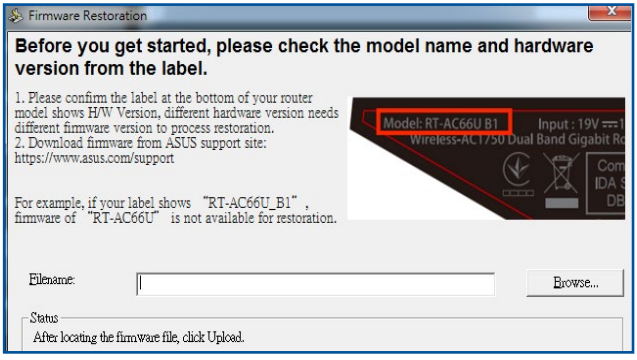
- จากเดสก์ทอปของคอมพิวเตอร์ของคุณ, คลิก **Start (เริ่ม) > All Programs (โปรแกรมทั้งหมด) > ASUS Utility (ยูทิลิตี้ ASUS) > Wireless Router (ไวร์เลส เราเตอร์) > Device Discovery (การค้นหา อุปกรณ์)**



หมายเหตุ: เมื่อคุณตั้งค่าเราเตอร์เป็นโหมดแอคเซสพอยต์, คุณจำเป็นต้องใช้ การสำรวจอุปกรณ์ เพื่อรับ IP แอดเดรสของเราเตอร์

5.2 การกู้คืนเฟิร์มแวร์

การกู้คืนเฟิร์มแวร์ ถูกใช้บน ASUS ไวร์เลส เราเตอร์ หลังจากที่ทำการอัปเกรดเฟิร์มแวร์ล้มเหลว ยูทิลิตี้นี้จะอัปโหลดไฟล์เฟิร์มแวร์ไปยังไวร์เลส เราเตอร์ กระบวนการจะใช้เวลาประมาณ 3 ถึง 4 นาที



สำคัญ! ปิดโหมดช่วยเหลือ ก่อนที่จะใช้ยูทิลิตี้ การกู้คืนเฟิร์มแวร์

หมายเหตุ: คุณสมบัตินี้ไม่ได้รับการสนับสนุนบน MAC OS

ในการเปิดโหมดช่วยเหลือ และใช้ยูทิลิตี้ การกู้คืนเฟิร์มแวร์:

1. ถอดปลั๊กไวร์เลสเราเตอร์จากแหล่งพลังงาน
2. กดปุ่มกู้คืน ที่แผงด้านหลังค้างไว้ ในขณะเดียวกันก็เสียบปลั๊กไวร์เลสเราเตอร์กลับเข้าไป ยังแหล่งพลังงาน ปล่อยปุ่มกู้คืน เมื่อ LED เพาเวอร์ที่แผงด้านหน้ากะพริบช้าๆ ซึ่งเป็นการ ระบุว่าไวร์เลส เราเตอร์อยู่ในโหมดช่วยเหลือ
3. ตั้งค่าสแตติก IP บนคอมพิวเตอร์ของคุณ และใช้สิ่งต่อไปนี้เพื่อตั้งค่าการตั้งค่า TCP/IP ของคุณ:

   IP แอดเดรส: 192.168.1.x

   ซับเน็ต มาสก: 255.255.255.0
4. จากเดสก์ท็อปของคอมพิวเตอร์ของคุณ, คลิก **Start (เริ่ม) > All Programs (โปรแกรมทั้งหมด) > ASUS Utility (ยูทิลิตี้ ASUS) > Wireless Router (ไวร์เลส เราเตอร์) > Firmware Restoration (การกู้คืนเฟิร์มแวร์)**
5. เลือกไฟล์เฟิร์มแวร์ จากนั้นคลิก **Upload (อัปโหลด)**

หมายเหตุ: นี่ไม่ใช่ยูทิลิตี้สำหรับอัพเกรดเฟิร์มแวร์ และไม่สามารถใช้กับ ASUS ไวร์เลสเราเตอร์ที่ทำงานได้ คุณต้องทำการอัพเกรดเฟิร์มแวร์ตามปกติผ่านอินเตอร์เฟซบนเว็บ ดู **บทที่ 4: การกำหนดค่าการตั้งค่าขั้นสูง** สำหรับรายละเอียดเพิ่มเติม

---

6 การแก้ไขปัญหา

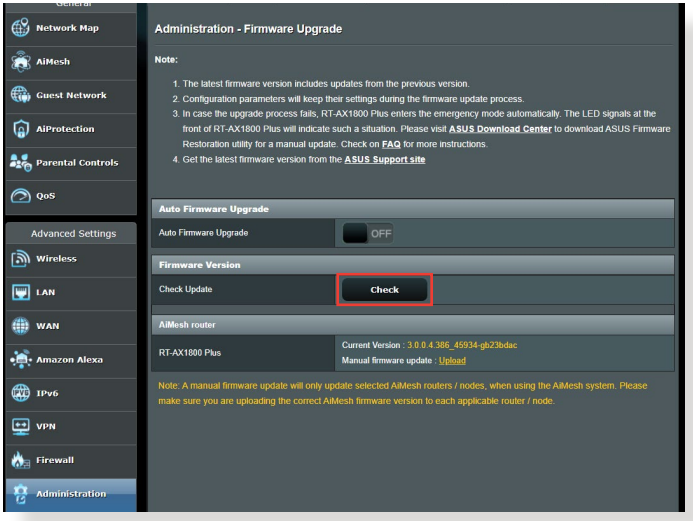
บทนี้ให้วิธีแก้ไขปัญหาที่คุณอาจพบกับเราเตอร์ของคุณ ถ้าคุณพบปัญหาที่ไม่ได้กล่าวถึงในบทนี้ ให้เยี่ยมชมเว็บไซต์สนับสนุนของ ASUS ที่: https://www.asus.com/support/ สำหรับข้อมูลผลิตภัณฑ์เพิ่มเติม และรายละเอียดการติดต่อฝ่ายสนับสนุนด้านเทคนิคของ ASUS

6.1 การแก้ไขปัญหาพื้นฐาน

ถ้าคุณมีปัญหากับเราเตอร์ของคุณ ให้ลองขั้นตอนพื้นฐานในส่วนนี้ก่อนที่จะมองหาวิธีการแก้ไขปัญหาเพิ่มเติม

อัพเกรดเฟิร์มแวร์ไปเป็นเวอร์ชั่นล่าสุด

1. เปิดเว็บ GUI ไปที่ **Advanced Settings (การตั้งค่าขั้นสูง)** > **Administration (การดูแลระบบ)** > แท็บ **Firmware Upgrade (เฟิร์มแวร์อัพเกรด)** คลิก **Check (ตรวจสอบ)** เพื่อตรวจสอบว่ามีเฟิร์มแวร์ล่าสุดหรือไม่



2. ถ้ามีเฟิร์มแวร์ล่าสุด ให้เยี่ยมชมเว็บไซต์ทั่วโลกของ ASUS ที่ https://www.asus.com/Networking/RT-AX55/HelpDesk/ เพื่อดาวน์โหลดเฟิร์มแวร์ล่าสุด

3. จากหน้า **Firmware Upgrade (เฟิร์มแวร์อัพเกรด)**, คลิก **Browse (เรียกดู)** เพื่อค้นหาไฟล์เฟิร์มแวร์
4. คลิก **Upload (อัพโหลด)** เพื่ออัพเกรดเฟิร์มแวร์

เริ่มเครือข่ายของคุณใหม่ในลำดับต่อไปนี้:

1. ปิดโมเด็ม
2. ถอดปลั๊กโมเด็ม
3. ปิดเราเตอร์และคอมพิวเตอร์
4. เสียบปลั๊กโมเด็ม
5. เปิดโมเด็ม จากนั้นรอเป็นเวลา 2 นาที
6. เปิดเราเตอร์ จากนั้นรอเป็นเวลา 2 นาที
7. เปิดคอมพิวเตอร์

ตรวจสอบว่าสายเคเบิลอีเธอร์เน็ตของคุณเสียบอยู่อย่างเหมาะสมหรือไม่

- เมื่อสายเคเบิลอีเธอร์เน็ตที่เชื่อมต่อเราเตอร์กับโมเด็มถูกเสียบอย่างเหมาะสม, LED WAN จะติด
- เมื่อสายเคเบิลอีเธอร์เน็ตที่เชื่อมต่อคอมพิวเตอร์ที่เปิดเครื่องอยู่กับเราเตอร์ถูกเสียบอย่างเหมาะสม, LED LAN ที่ตรงกับเครื่องจะติด

ตรวจสอบว่าการตั้งค่าไร้สายบนคอมพิวเตอร์ของคุณตรงกับค่าของคอมพิวเตอร์ของคุณ

- เมื่อคุณเชื่อมต่อคอมพิวเตอร์ของคุณไปยังเราเตอร์แบบไร้สาย, ให้แน่ใจว่า SSID (ชื่อเครือข่ายไร้สาย), วิธีการเข้ารหัส และรหัสผ่านนั้นถูกต้อง

ตรวจสอบว่าการตั้งค่าเครือข่ายของคุณถูกต้องหรือไม่

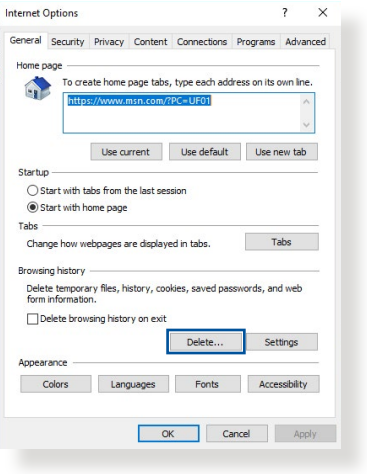
- ไคลเอ็นต์แต่ละตัวบนเครือข่ายควรมี IP แอดเดรสที่ถูกต้อง ASUS แนะนำให้คุณใช้ DHCP เซิร์ฟเวอร์ของไวร์เลสเราเตอร์เพื่อกำหนด IP แอดเดรสให้กับคอมพิวเตอร์ต่างๆ บนเครือข่ายของคุณ

- ผู้ให้บริการเคเบิลโมเด็มบางราย จำเป็นต้องให้คุณใช้ MAC แอดเดรสของคอมพิวเตอร์ที่ลงทะเบียนครั้งแรกในบัญชี คุณสามารถดู MAC แอดเดรสในเว็บ GUI, **Network Map (แผนที่เครือข่าย)** > หน้า **Clients (ไคลเอ็นต์)**, และวางตัวชี้เมาส์เหนืออุปกรณ์ของคุณใน **Client Status (สถานะไคลเอ็นต์)**

6.2 คำถามที่มีการถามบ่อยๆ (FAQ)

ฉันไม่สามารถเข้าถึง GUI ของเราเตอร์โดยใช้เว็บเบราเซอร์ได้

- ถ้าคอมพิวเตอร์ของคุณเป็นแบบมีสาย ให้ตรวจสอบการเชื่อมต่อสายเคเบิลอีเธอร์เน็ต และสถานะ LED ตามที่อธิบายในส่วนก่อนหน้า
- ตรวจดูให้แน่ใจว่าคุณใช้ข้อมูลการล็อกอินที่ถูกต้อง ชื่อล็อกอินและรหัสผ่านเริ่มต้นคือ "admin/admin" ตรวจดูให้แน่ใจว่าปุ่ม Caps Lock ถูกปิดการทำงานในขณะที่คุณป้อนข้อมูลการล็อกอิน
- ลบคุกกี้และไฟล์ในเว็บเบราเซอร์ของคุณ สำหรับ Internet Explorer ปฏิบัติตามขั้นตอนเหล่านี้:



    1. เปิดเว็บเบราเซอร์, จากนั้นคลิก **Tools (เครื่องมือ)** > **Internet Options (ตัวเลือกอินเตอร์เน็ต)**
    2. บนแท็บ **General (ทั่วไป)**, คลิก **Delete (ลบ)** ภายใต้ **Browsing history (ประวัติการเบราซ์)** เลือก **Temporary Internet files and website files (ไฟล์อินเทอร์เน็ตชั่วคราวและไฟล์เว็บไซต์)** รวมถึง **Cookies and website data (ข้อมูลคุกกี้และเว็บไซต์)** จากนั้นคลิกที่ **Delete (ลบ)**

หมายเหตุ:

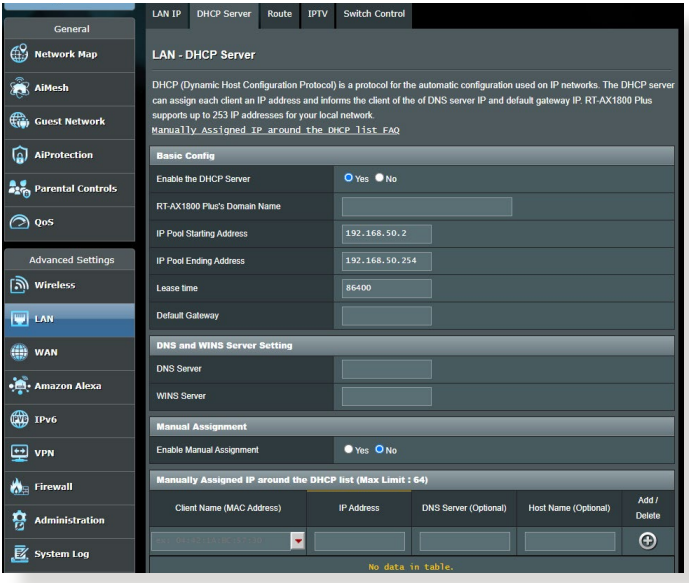
- คำสั่งสำหรับการลบคุกกี้และไฟล์นั้นแตกต่างกันในเว็บเบราเซอร์แต่ละตัว
- ปิดทำงานการตั้งค่าพร็อกซี่เซิร์ฟเวอร์, ยกเลิกการเชื่อมต่อแบบโทรเข้า และตั้งค่า TCP/IP ให้รับ IP แอดเดรสโดยอัตโนมัติ สำหรับรายละเอียดเพิ่มเติม ให้ดูบทที่ 1 ของคู่มือผู้ใช้ฉบับนี้
- ให้แน่ใจว่าคุณใช้สายเคเบิลอีเธอร์เน็ต CAT5e หรือ CAT6

ไคลเอ็นต์ไม่สามารถสร้าง การเชื่อมต่อไร้สายกับ เราเตอร์ได้

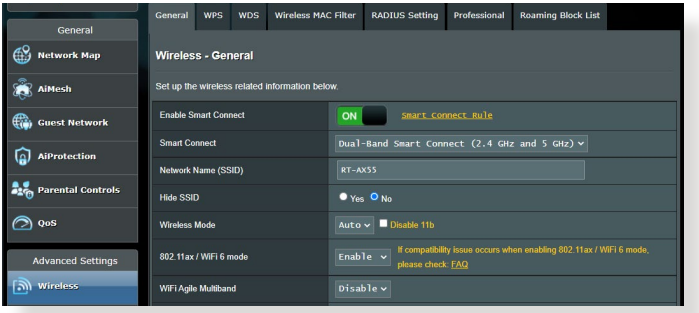
หมายเหตุ: ถ้าคุณกำลังมีปัญหาในการเชื่อมต่อไปยังเครือข่าย 5Ghz, ตรวจดูให้แน่ใจว่าอุปกรณ์ไร้สายของคุณสนับสนุนความถี่ 5Ghz หรือมีความสามารถแบบดูอัลแบนด์

- **อยู่นอกพื้นที่ทำงาน:**
  - ย้ายเราเตอร์ให้เข้าใกล้ไวร์เลส ไคลเอ็นต์ มากขึ้น
  - พยายามปรับเสาอากาศของเราเตอร์ไปยังทิศทางที่ดีที่สุดตามที่อธิบายไว้ในส่วน **1.4 การวางตำแหน่งเราเตอร์ของคุณ**

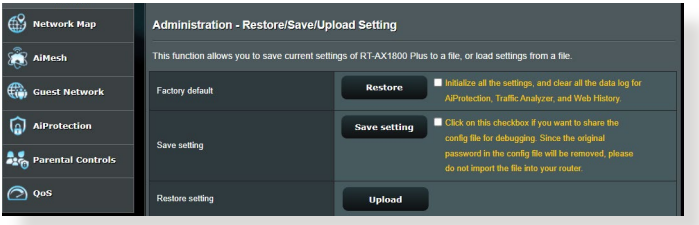
- **DHCP เซิร์ฟเวอร์ถูกปิดการทำงาน:**
  1. เปิดเว็บ GUI ไปที่ **General (ทั่วไป) > Network Map (แผนที่เครือข่าย) > Clients (ไคลเอ็นต์)** และค้นหาอุปกรณ์ที่คุณต้องการเชื่อมต่อไปยังเราเตอร์
  2. ถ้าคุณไม่สามารถพบอุปกรณ์ใน **Network Map (แผนที่เครือข่าย)**, ให้ไปที่ **Advanced Settings (การตั้งค่าขั้นสูง) > LAN > รายการ DHCP Server (DHCP เซิร์ฟเวอร์), Basic Config (การกำหนดค่าพื้นฐาน)**, เลือก **Yes (ใช่)** บน **Enable the DHCP Server (เปิดทำงาน DHCP เซิร์ฟเวอร์)**



- SSID ถูกซ่อน ถ้าอุปกรณ์ของคุณสามารถพบ SSID จากเราเตอร์อื่น แต่ไม่สามารถพบ SSID ของเราเตอร์ของคุณ, ให้ไปที่ **Advanced Settings (การตั้งค่าขั้นสูง)** > **Wireless (ไร้สาย)** > **General (ทั่วไป)**, เลือก **No (ไม่)** บน **Hide SSID (ซ่อน SSID)**, และเลือก **Auto (อัตโนมัติ)** บน **Control Channel (ช่องควบคุม)**



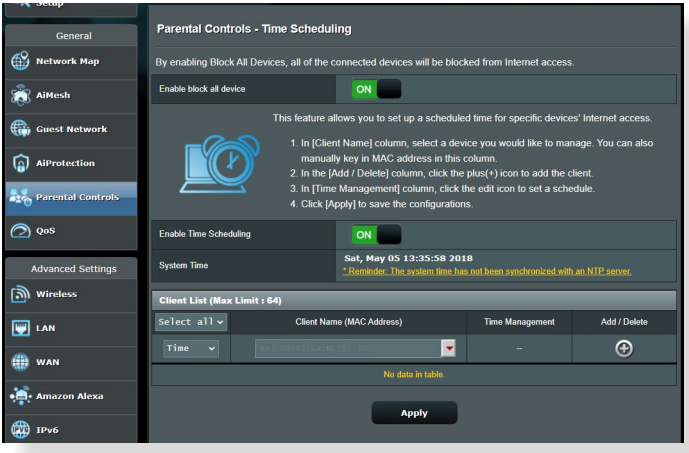
- ถ้าคุณกำลังใช้อะแดปเตอร์ LAN ไร้สาย, ตรวจสอบว่าช่องไร้สายที่ใช้ สอดคล้องกับช่องที่ใช้ได้ในประเทศ/พื้นที่ของคุณหรือไม่ ถ้าไม่ ให้ปรับช่อง, แบนด์วิดธ์ช่อง และโหมดไร้สาย
- ถ้าคุณยังคงไม่สามารถเชื่อมต่อไปยังเราเตอร์แบบไร้สายได้ คุณสามารถรีเซ็ตเราเตอร์ของคุณกลับเป็นการตั้งค่าเริ่มต้นจากโรงงาน ใน GUI ของเราเตอร์, คลิก **Administration (การดูแลระบบ)** > **Restore/Save/Upload Setting (การตั้งค่าการกู้คืน/บันทึก/อัพโหลด)** และคลิก **Restore (กู้คืน)**



ไม่สามารถเข้าถึงอินเตอร์เน็ตได้

- ตรวจสอบว่าเราเตอร์ของคุณสามารถเชื่อมต่อไปยัง WAN IP แอดเดรสของ ISP ได้หรือไม่ ในการดำเนินการ, เปิดเว็บ GUI และไปที่ **General (ทั่วไป)**> **Network Map (แผนที่เครือข่าย)**, และตรวจสอบ **Internet Status (สถานะอินเทอร์เน็ต)**
- ถ้าเราเตอร์ของคุณไม่สามารถเชื่อมต่อไปยัง WAN IP แอดเดรสของ ISP ได้, ให้ลองเริ่มเครือข่ายของคุณใหม่ ตามที่อธิบายในส่วน **เริ่มเครือข่ายของคุณใหม่ในลำดับต่อไปนี้** ภายใต้ **การแก้ไขปัญหาพื้นฐาน**

- อุปกรณ์ถูกบล็อกผ่านฟังก์ชั่น Parental Control (การควบคุมโดยผู้ปกครอง) ไปที่ **General (ทั่วไป)** > **AiProtection** > **Parental Control (การควบคุมโดยผู้ปกครอง)** และดูว่าอุปกรณ์อยู่ในรายการหรือไม่ ถ้าอุปกรณ์ถูกแสดงอยู่ภายใต้ **Client Name (ชื่อไคลเอ็นต์)**, ให้ลบอุปกรณ์ออก โดยใช้ปุ่ม **Delete (ลบ)** หรือปรับ การตั้งค่าการจัดการเวลา



- ถ้ายังคงเข้าถึงอินเทอร์เน็ตไม่ได้, ให้ลองบูตคอมพิวเตอร์ของคุณใหม่ และตรวจสอบ IP แอดเดรส และเกตเวย์แอดเดรสของเครือข่าย

- ตรวจสอบไฟแสดงสถานะบนโมเด็ม ADSL และไวร์เลส เราเตอร์ ถ้า LED WAN บนไวร์เลสเราเตอร์ไม่ติด, ให้ตรวจสอบว่าสายเคเบิลทั้งหมดเสียบอยู่อย่างเหมาะสมหรือไม่

คุณลืม SSID (ชื่อเครือข่าย) หรือรหัสผ่านเครือข่าย

- ตั้งค่า SSID และคีย์การเข้ารหัสใหม่ ผ่านการเชื่อมต่อแบบมีสาย (สายเคเบิลอีเธอร์เน็ต) เปิดเว็บ GUI, ไปที่ **Network Map (แผนที่เครือข่าย)**, คลิกไอคอนเราเตอร์, ป้อน SSID และคีย์การเข้ารหัสใหม่, จากนั้นคลิก **Apply (นำไปใช้)**
- รีเซ็ตเราเตอร์ของคุณกลับเป็นการตั้งค่าเริ่มต้น เปิดเว็บ GUI, ไปที่ **Administration (การดูแลระบบ)** > **Restore/Save/Upload Setting (การตั้งค่าการกู้คืน/บันทึก/อัพโหลด)**, และคลิก **Restore (กู้คืน)** บัญชีและรหัสผ่านการล็อกอินเริ่มต้นเป็น “admin” ทั้งสองอย่าง

วิธีการกู้คืนระบบกลับเป็นการ ตั้งค่าเริ่มต้น

- ไปที่ **Administration (การดูแลระบบ)** > **Restore/Save/Upload Setting (การตั้งค่าการกู้คืน/บันทึก/อัพโหลด)**, และคลิก **Restore (กู้คืน)**

  ค่าต่อไปนี้คือการตั้งค่าเริ่มต้นจากโรงงาน:

ชื่อผู้ใช้:	admin
รหัสผ่าน:	admin
เปิดทำงาน DHCP:	ใช่ (ถ้าเสียบสายเคเบิล WAN)
IP แอดเดรส:	192.168.50.1
ชื่อโดเมน:	(ว่าง)
ซับเน็ต มาสก์:	255.255.255.0
DNS เซิร์ฟเวอร์ 1:	router.asus.com
DNS เซิร์ฟเวอร์ 2:	(ว่าง)
SSID (2.4GHz):	ASUS
SSID (5GHz):	ASUS_5G

การอัพเกรดเฟิร์มแวร์ล้มเหลว

เปิดโหมดช่วยเหลือ และรันยูทิลิตี้ การกู้คืนเฟิร์มแวร์ ดูส่วน **5.2 การกู้คืนเฟิร์มแวร์** เกี่ยวกับการใช้ยูทิลิตี้ การกู้คืนเฟิร์มแวร์

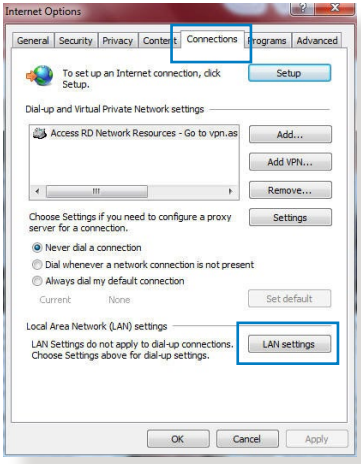
ไม่สามารถเข้าถึงเว็บ GUI

ก่อนที่จะกำหนดค่าไวร์เลสเราเตอร์ของคุณ ให้ทำขั้นตอนตามที่อธิบายในส่วนนี้ สำหรับโฮสต์คอมพิวเตอร์และเน็ตเวิร์กไคลเอ็นต์ของคุณ

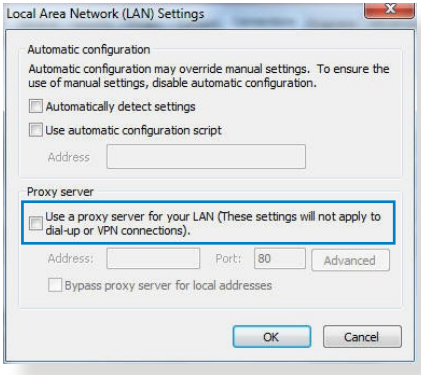
A. ปิดทำงานพร็อกซีเซิร์ฟเวอร์ ถ้าเปิดทำงานอยู่

Windows®

1. คลิก **Start (เริ่ม)** > **Internet Explorer (อินเทอร์เน็ตเอ็กซ์พลอเรอร์)** เพื่อเปิดเบราเซอร์
2. คลิก **Tools (เครื่องมือ)** > **Internet options (ตัวเลือกอินเทอร์เน็ต)** > แท็บ **Connections (การเชื่อมต่อ)** > **LAN settings (การตั้งค่า LAN)**

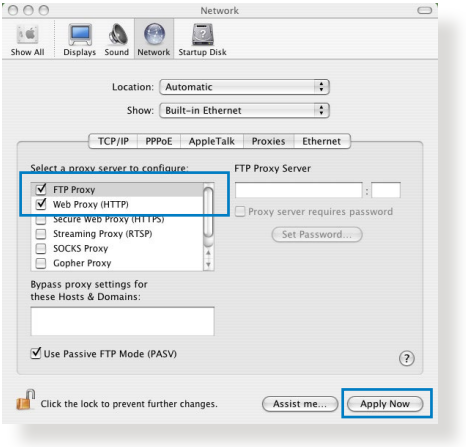


3. จากหน้าจอ Local Area Network (LAN) Settings (การตั้งค่าเครือข่ายท้องถิ่น (LAN)), ลบเครื่องหมายจาก **Use a proxy server for your LAN (ใช้พร็อกซีเซิร์ฟเวอร์สำหรับ LAN ของคุณ)**
4. คลิก **OK (ตกลง)** จากนั้น **Apply (ใช้)**



MAC OS

1. จากเบราเซอร์ Safari ของคุณ, คลิก **Safari (ซาฟารี) > Preferences (การกำหนดลักษณะ) > Advanced (ขั้นสูง) > Change Settings (เปลี่ยนแปลงการตั้งค่า) ...**
2. จากหน้าจอ Network (เครือข่าย), ยกเลิกการเลือก **FTP Proxy (FTP พร็อกซี่)** และ **Web Proxy (HTTP) (เว็บพร็อกซี่ (HTTP))**
3. คลิก **Apply Now (นำไปใช้เดี๋ยวนี้)** เมื่อเสร็จ

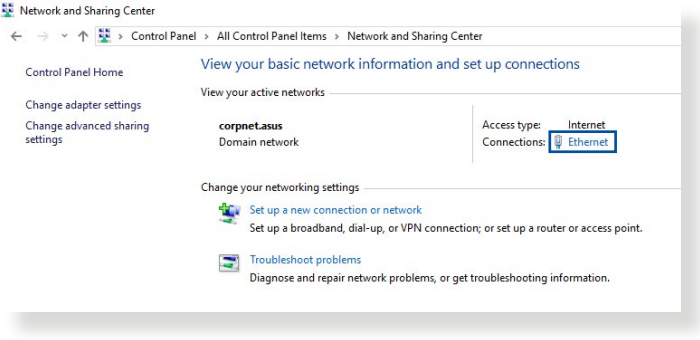


หมายเหตุ: ดูคุณสมบัติวิธีใช้ของเบราเซอร์ของคุณ สำหรับรายละเอียดเกี่ยวกับการปิดทำงานพร็อกซี่เซิร์ฟเวอร์

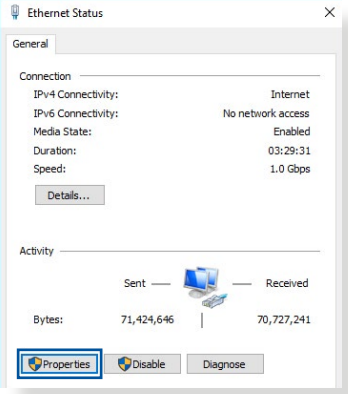
B. ตั้งค่าการตั้งค่า TCP/IP เป็น Automatically obtain an IP address (รับที่อยู่ IP โดยอัตโนมัติ)

Windows®

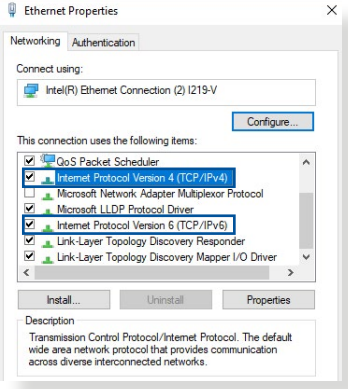
1. **คลิก Start (เริ่ม) > Control Panel (แผงควบคุม) > Network and Sharing Center (เครือข่ายและศูนย์การใช้ร่วมกัน)** จากนั้นคลิกที่การเชื่อมต่อเครือข่ายเพื่อแสดงหน้าต่างสถานะ



2. คลิกที่ **Properties (คุณสมบัติ)** เพื่อแสดงหน้าต่างคุณสมบัติอีเธอร์เน็ต



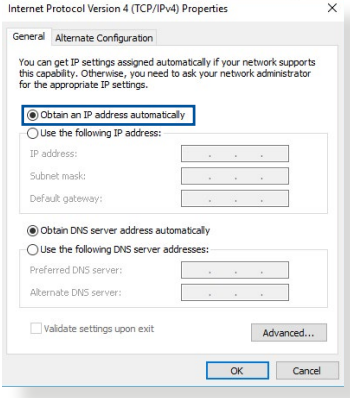
3. เลือก **Internet Protocol Version 4 (TCP/IPv4) (อินเตอร์เน็ตโปรโตคอลเวอร์ชัน4 (TCP/IPv4))** หรือ **Internet Protocol Version 6 (TCP/IPv6) (อินเตอร์เน็ตโปรโตคอลเวอร์ชัน6 (TCP/IPv6))**, จากนั้นคลิก **Properties (คุณสมบัติ)**



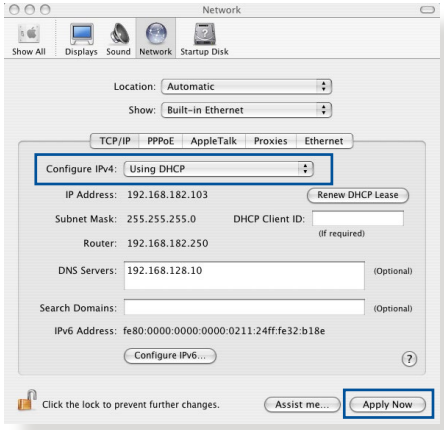
4. เพื่อรับการตั้งค่า IPv4 IP โดยอัตโนมัติ, ทำเครื่องหมายที่ **Obtain an IP address automatically (รับ IP แอดเดรสโดยอัตโนมัติ)**

   เพื่อรับการตั้งค่า IPv6 IP โดยอัตโนมัติ, ทำเครื่องหมายที่ **Obtain an IPv6 address automatically (รับ IPv6 แอดเดรสโดยอัตโนมัติ)**

5. คลิก **OK (ตกลง)** เมื่อทำเสร็จ



MAC OS

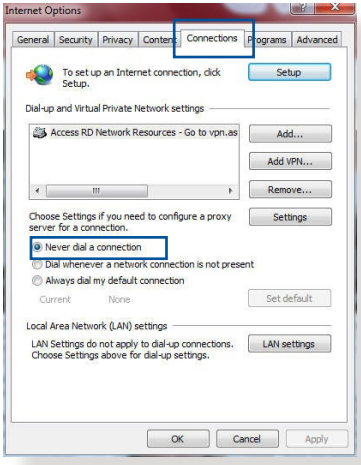


1. คลิกไอคอนแอปเปิ้ล ที่อยู่บริเวณมุมซ้ายบนของหน้าจอ
2. คลิก System **Preferences (การกำหนดลักษณะระบบ) > Network (เครือข่าย) > Configure (กำหนดค่า)...**
3. จากแท็บ **TCP/IP (TCP/IP)**, เลือก **Using DHCP (การใช้ DHCP)** ในรายการ **Configure IPv4 (กำหนดค่า IPv4)**
4. คลิก **Apply Now (นำไปใช้เดี๋ยวนี้)** เมื่อเสร็จ

หมายเหตุ: ดูวิธีใช้ของระบบปฏิบัติการของคุณ และคุณสมบัติที่สนับสนุนสำหรับรายละเอียดเกี่ยวกับการกำหนดค่า TCP/IP ของคอมพิวเตอร์ของคุณ

C. เปิดการทำงานเครือข่ายแบบโทรเข้า

Windows®



1. คลิก **Start (เริ่ม) > Internet Explorer (อินเทอร์เน็ตเอ็กซ์พลอเรอร์)** เพื่อเปิดเบราเซอร
2. คลิก **Tools (เครื่องมือ) > Internet options (ตัวเลือกอินเทอร์เน็ต) > แท็บ Connections (การเชื่อมต่อ)**
3. ทำเครื่องหมายที่ **Never dial a connection (ไม่โทรเพื่อเชื่อมต่อ)**
4. คลิก **OK (ตกลง)** เมื่อทำเสร็จ

หมายเหตุ: ดูคุณสมบัติวิธีใช้ของเบราเซอร์ของคุณ สำหรับรายละเอียดเกี่ยวกับการปิดทำงานการเชื่อมต่อแบบโทรเข้า

ภาคผนวก

การแจ้งเตือน

This device is an Energy Related Product (ErP) with High Network Availability (HiNA), the power consumption will be less than 12watts when the system is in network standby mode (idle mode).

ASUS Recycling/Takeback Services

ASUS recycling and takeback programs come from our commitment to the highest standards for protecting our environment. We believe in providing solutions for you to be able to responsibly recycle our products, batteries, other components, as well as the packaging materials. Please go to http://csr.asus.com/english/Takeback.htm for the detailed recycling information in different regions.

REACH

Complying with the REACH (Registration, Evaluation, Authorisation, and Restriction of Chemicals) regulatory framework, we published the chemical substances in our products at ASUS REACH website at

http://csr.asus.com/english/index.aspx

Federal Communications Commission Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC

Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

IMPORTANT! This device within the 5.15 ~ 5.25 GHz is restricted to indoor operations to reduce any potential for harmful interference to co-channel MSS operations.

CAUTION! Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Prohibition of Co-location

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with FCC multi-transmitter product procedures. For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels in not possible.

Safety Information

To maintain compliance with FCC's RF exposure guidelines, this equipment should be installed and operated with minimum distance 21cm between the radiator and your body. Use on the supplied antenna.

Declaration of Conformity for Ecodesign directive 2009/125/EC

Testing for eco-design requirements according to (EC) No 1275/2008 and (EU) No 801/2013 has been conducted. When the device is in Networked Standby Mode, its I/O and network interface are in sleep mode and may not work properly. To wake up the device, press the Wi-Fi on/off, LED on/off, reset, or WPS button.

Simplified EU Declaration of Conformity

ASUSTek Computer Inc. hereby declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU. Full text of EU declaration of conformity is available at https://www.asus.com/support/.

This equipment complies with EU radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 24 cm between the radiator & your body.

All operational modes:

2.4GHz: 802.11b, 802.11g, 802.11n (HT20), 802.11n (HT40), 802.11ac (VHT20), 802.11ac (VHT40), 802.11ax(HE20), 802.11ax(HE40)

5GHz: 802.11a, 802.11n (HT20), 802.11n (HT40), 802.11ac (VHT20), 802.11ac (VHT40), 802.11ac (VHT80), 802.11ax (HE20), 802.11ax (HE40), 802.11ax (HE80)

The frequency, mode and the maximum transmitted power in EU are listed below:

2412-2472MHz (802.11g 6Mbps): 19.96 dBm
5180-5240MHz (802.11ac VHT20 MCS0): 22.97 dBm
5260-5320MHz (802.11ac VHT40 MCS0): 22.97 dBm
5500-5700MHz (802.11ac VHT80 MCS0): 29.98 dBm

The device is restricted to indoor use only when operating in the 5150 to 5350 MHz frequency range.

	AT	BE	BG	CZ	DK	EE	FR
	DE	IS	IE	IT	EL	ES	CY
	LV	LI	LT	LU	HU	MT	NL
	NO	PL	PT	RO	SI	SK	TR
	FI	SE	CH	UK	HR	UA	

Canada, Industry Canada (IC) Notices

This device complies with Industry Canada's license-exempt RSSs. Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

The device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

Radio Frequency (RF) Exposure Information

The radiated output power of the ASUS Wireless Device is below the Industry Canada (IC) radio frequency exposure limits. The ASUS Wireless Device should be used in such a manner such that the potential for human contact during normal operation is minimized.

This equipment should be installed and operated with a minimum distance of 24 cm between the radiator and any part of your body.

This device has been certified for use in Canada. Status of the listing in the Industry Canada's REL (Radio Equipment List) can be found at the following web address:
http://www.ic.gc.ca/app/sitt/reltel/srch/nwRdSrch.do?lang=eng
Additional Canadian information on RF exposure also can be found at the following web:
http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf08792.html

Canada, avis d'Industry Canada (IC)

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence.

Son utilisation est sujette aux deux conditions suivantes : (1) cet appareil ne doit pas créer d'interférences et (2) cet appareil doit tolérer tout type d'interférences, y compris celles susceptibles de provoquer un fonctionnement non souhaité de l'appareil.

Les dispositifs fonctionnant dans la bande de 5 150 à 5 250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

Informations concernant l'exposition aux fréquences radio (RF)

La puissance de sortie émise par l'appareil de sans l ASUS est inférieure à la limite d'exposition aux fréquences radio d'Industry Canada (IC). Utilisez l'appareil de sans l ASUS de façon à minimiser les contacts humains lors du fonctionnement normal.

Cet équipement doit être installé et utilisé avec une distance minimale de 24 cm entre le radiateur et toute partie de votre corps.

Ce périphérique est homologué pour l'utilisation au Canada. Pour consulter l'entrée correspondant à l'appareil dans la liste d'équipement radio (REL - Radio Equipment List) d'Industry Canada rendez-vous sur:

http://www.ic.gc.ca/app/sitt/reltel/srch/nwRdSrch.do?lang=eng

Pour des informations supplémentaires concernant l'exposition aux RF au Canada rendezvous sur :
http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf08792.html

Precautions for the use of the device

- Do not use the ASUS product in this situation (Driving, in airports, hospitals, gas stations and professional garages).
- Medical device interference: Maintain a minimum distance of at least 15 cm (6 inches) between implanted medical devices and ASUS products in order to reduce the risk of interference, especially, during the phone call.
- Kindly use ASUS products in good reception conditions in order to minimize the radiation's level.
- Use the hand-free device, especially, during the communication situation, in order to keep the device away from pregnant women and the lower abdomen of the teenager (Especially, using cell phone).

NCC 警語

低功率射頻器材技術規範

「取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前述合法通信，指依電信管理法規定作業之無線電通信。低功率射頻器材須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。」

*應避免影響附近雷達系統之操作。

此設備的安裝與操作要離使用者之最小距離為 21 公分；電磁波曝露量MPE標準值 1 mWcm2，送測產品實測值為：0.621 mWcm2。

「產品之限用物質含有情況」之相關資訊 請參考下表：

單元	限用物質及其化學符號					
	鉛 (Pb)	汞 (Hg)	鎘 (Cd)	六價鉻 (Cr^{+6})	多溴聯苯 (PBB)	多溴二苯醚 (PBDE)
印刷電路板及電子組件	—	○	○	○	○	○
外殼	○	○	○	○	○	○
天線	—	○	○	○	○	○
其他及其配件	—	○	○	○	○	○

備考1. "○" 係指該項限用物質之百分比含量未超出百分比含量基準值。
備考2. "—" 係指該項限用物質為排除項目。

D33005
RoHS

电子电气产品有害物质限制使用标识：图中之数字为产品之环保使用期限。仅指电子电气产品中含有的有害物质不致发生外泄或突变，从而对环境造成污染或对人身、财产造成严重损害的期限。

部件名称	有害物质					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr(VI))	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
印刷电路板及其电子组件	×	○	○	○	○	○
外壳	○	○	○	○	○	○
电源适配器	×	○	○	○	○	○
外部信号连接头及线材	×	○	○	○	○	○
中央处理器与内容	×	○	○	○	○	○

GNU General Public License

Licensing information

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please see The GNU General Public License for the exact terms and conditions of this license. All future firmware updates will also be accompanied with their respective source code. Please visit our web site for updated information. Note that we do not offer direct support for the distribution.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or

can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

Terms & conditions for copying, distribution, & modification

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

   These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

   Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

   The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

   This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission.

    For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

ข้อมูลการติดต่อกับ ASUS

ASUSTeK COMPUTER INC. (เอเชีย แปซิฟิก)

ที่อยู่	1F., No. 15, Lide Rd., Beitou Dist., Taipei City 112
โทรศัพท์	+886-2-2894-3447
แฟกซ์	+886-2-2890-7798
เว็บไซต์	https://www.asus.com

ฝ่ายสนับสนุนด้านเทคนิค

โทรศัพท์	+86-21-38429911
การสนับสนุนออนไลน์	https://qr.asus.com/techserv

ASUS COMPUTER INTERNATIONAL (อเมริกา)

ที่อยู่	48720 Kato Rd., Fremont, CA 94538, USA
โทรศัพท์	+1-510-739-3777
แฟกซ์	+1-510-608-4555
เว็บไซต์	https://www.asus.com/us/

ฝ่ายสนับสนุนด้านเทคนิค

Support fax	+1-812-284-0883
โทรศัพท์	+1-812-282-2787
การสนับสนุนออนไลน์	https://qr.asus.com/techserv

ASUS COMPUTER GmbH (เยอรมันนีและออสเตรีย)

ที่อยู่	Harkortstrasse 21-23, 40880 Ratingen, Germany
เว็บไซต์	https://www.asus.com/de
การติดต่อออนไลน์	https://www.asus.com/support/Product/ContactUs/Services/questionform/?lang=de-de

ฝ่ายสนับสนุนด้านเทคนิค

โทรศัพท์ (DE)	+49-2102-5789557
โทรศัพท์ (AT)	+43-1360-2775461
การสนับสนุนออนไลน์	https://www.asus.com/de/support