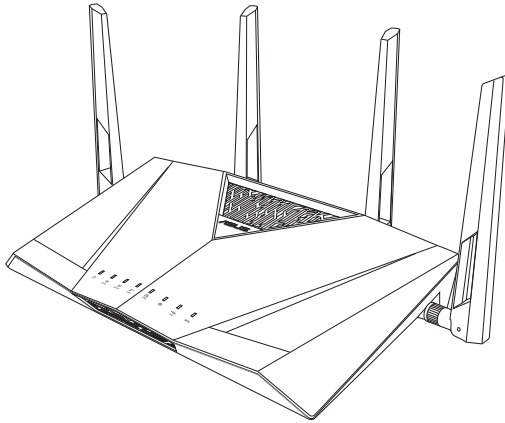


คู่มือผู้ใช้

RT-AX88U PRO

เราเตอร์สองแถบความถี่ AX6000 แบบไร้สาย



ASUS
IN SEARCH OF INCREDIBLE

TH22793

การแก้ไขครั้งที่ 1

เดือนพฤศจิกายน 2023

ลิขสิทธิ์ © 2023 ASUSTeK COMPUTER INC. ลิขสิทธิ์ถูกต้อง

ห้ามทำซ้ำ ส่งต่อ คัดลอก เก็บในระบบที่สามารถเรียกกลับมาได้ หรือแปลส่วนหนึ่งส่วนใดของคู่มือฉบับนี้เป็นภาษาอื่น ซึ่งรวมถึงผลิตภัณฑ์และซอฟต์แวร์ที่บรรจุอยู่ใน ยกเว้นเอกสารที่ผู้ซื้อเป็นผู้เก็บไว้เพื่อจุดประสงค์ในการสำรองเท่านั้น โดยไม่ได้รับความยินยอมเป็นลายลักษณ์อักษรอย่างชัดเจนจาก ASUSTeK COMPUTER INC. ("ASUS")

การรับประกันผลิตภัณฑ์หรือบริการ จะไม่ขยายออกไปถ้า: (1) ผลิตภัณฑ์ได้รับการซ่อมแซม, ดัดแปลง หรือเปลี่ยนแปลง ถ้าการซ่อมแซม, การดัดแปลง หรือการเปลี่ยนแปลงนั้นไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจาก ASUS; หรือ (2) หมายเลขผลิตภัณฑ์ของผลิตภัณฑ์ถูกขีดฆ่า หรือหายไป

ASUS ให้คู่มือฉบับนี้ "ในลักษณะที่เป็น" โดยไม่มีการรับประกันใดๆ ไม่ว่าจะมีขีดจำกัดหรือเป็นหนี้ ซึ่งรวมถึงแต่ไม่จำกัดอยู่เพียงการรับประกัน หรือเงื่อนไขของความสามารถเชิงพาณิชย์ หรือความเข้ากันได้สำหรับวัตถุประสงค์เฉพาะ ไม่ว่าจะในกรณีใดๆ ก็ตาม ASUS กรรมการ เจ้าหน้าที่ พนักงาน หรือตัวแทนของบริษัทไม่ยอมรับผิดชอบต่อความเสียหายที่เกิดขึ้นโดยอ้อม โดยกรณีพิเศษ โดยไม่ได้ตั้งใจ หรือโดยเป็นผลกระทบตามมา (รวมถึงความเสียหายจากการสูญเสียกำไร การขาดทุนของธุรกิจ การสูญเสียการใช้งานหรือข้อมูล การหยุดชะงักของธุรกิจ และอื่นๆ ในลักษณะเดียวกันนี้) แม้ว่า ASUS จะได้รับทราบถึงความเสียหายไปของความเสียหายดังกล่าว อันเกิดจากข้อบกพร่องหรือข้อผิดพลาดในคู่มือหรือผลิตภัณฑ์นี้

ข้อกำหนดและข้อมูลต่างๆ ที่ระบุในคู่มือฉบับนี้ เป็นเพียงข้อมูลเพื่อการใช้งานเท่านั้น และอาจเปลี่ยนแปลงได้ตามเวลาที่ผ่านไปโดยไม่ต้องแจ้งให้ทราบ จึงไม่ควรถือเป็นภาระผูกพันของ ASUS ASUS ไม่ขอรับผิดชอบหรือรับผิดชอบข้อผิดพลาด หรือความไม่ถูกต้องใดๆ ที่อาจเกิดขึ้นในคู่มือฉบับนี้ รวมทั้งผลิตภัณฑ์และซอฟต์แวร์ที่ระบุในคู่มือด้วย

ผลิตภัณฑ์และชื่อบริษัทที่ปรากฏในคู่มือนี้อาจเป็น หรือไม่เป็นเครื่องหมายการค้าจดทะเบียน หรือลิขสิทธิ์ของบริษัทที่เป็นเจ้าของ และมีการใช้เฉพาะสำหรับการอ้างอิง หรืออธิบายเพื่อประโยชน์ของเจ้าของเท่านั้น โดยไม่มีการละเมิดในทางละเมิดใดๆ

สารบัญ

1	ทำความรู้จัก"ไวร์เลสเราเตอร์ของคุณ	
1.1	ยินดีต้อนรับ!.....	6
1.2	สิ่งต่างๆ ในกล่องบรรจุ.....	6
1.3	"ไวร์เลสเราเตอร์ของคุณ.....	7
1.4	การวางตำแหน่ง"ไวร์เลส เราเตอร์ของคุณ	9
1.5	ความต้องการในการติดตั้ง.....	10
2	เริ่มต้นการใช้งาน	
2.1	การตั้งค่าเราเตอร์.....	11
	A. การเชื่อมต่อแบบมีสาย	12
	B. การเชื่อมต่อไร้สาย	12
2.2	การตั้งค่าอินเทอร์เน็ตคว้าน (QIS) ด้วยการตรวจพบ อัตโนมัติ	14
2.3	กำลังเชื่อมต่อไปยังเครือข่ายไร้สาย ของคุณ.....	17
3	การกำหนดค่าการตั้งค่าทั่วไป สำหรับ ROG Gaming Center	
3.1	การเข้าระบบไปยังเว็บ GUI	18
	3.1.1 การตั้งค่าระบบความปลอดภัยไร้สาย	20
	3.1.2 การจัดการเน็ตเวิร์ก"โคลเอ็นต์ของคุณ	21
	3.1.3 การตรวจสอบแลอูปกรณ USB ของคุณ.....	22
3.2	Adaptive QoS (อะแดปทีฟ QoS)	25
	3.2.1 การจัดการ QoS (คุณภาพของบริการ) แบนด์วิดธ.....	25
3.3	การดูแลระบบ	28
	3.3.1 โหมดการทำงาน.....	28
	3.3.2 ระบบ	29
	3.3.3 การอัปเดตเฟิร์มแวร์.....	30
	3.3.4 การกู้คืน/การจัดเก็บ/การอัปโหลดการตั้งค่า	30
3.4	AiCloud 2.0	31
	3.4.1 คลาวด์ดีส์ก์	32

สารบัญ

3.4.2	เข้าถึงแบบส്മาร์ต.....	33
3.4.3	AiCloudซิงค์.....	34
3.5	AiProtection	35
3.5.1	การป้องกันเครือข่าย.....	35
3.5.2	การตั้งค่าการควบคุมโดยผู้ปกครอง.....	39
3.6	ไฟร์วอลล์	42
3.6.1	ทั่วไป.....	42
3.6.2	ตัวกรอง URL.....	43
3.6.3	ตัวกรองคำสำคัญ.....	44
3.6.4	ตัวกรองบริการเครือข่าย.....	45
3.7	เกม	47
3.7.1	Gear Accelerator.....	47
3.7.2	โหมดเกมมือถือ.....	48
3.7.3	โหมด NAT.....	49
3.8	เครือข่ายแยก	50
3.9	IPv6	52
3.10	LAN	53
3.10.1	LAN IP.....	53
3.10.2	DHCP เซิร์ฟเวอร์.....	54
3.10.3	เส้นทาง.....	56
3.10.4	IPTV.....	57
3.11	บันทึกระบบ	58
3.12	ตัววิเคราะห์การรับส่งข้อมูล	59
3.13	การใช้งานผ่าน USB	60
3.13.1	การใช้ AiDisk.....	61
3.13.2	การใช้เซิร์ฟเวอร์เซินเตอร์.....	63
3.13.3	3G/4G.....	68
3.14	WAN	70
3.14.1	การเชื่อมต่ออินเทอร์เน็ต.....	70

สารบัญ

3.14.2	คู่มือ WAN.....	73
3.14.3	พอร์ตทริกเกอร์.....	74
3.14.4	เวอร์ชวลเซิร์ฟเวอร์/พอร์ตฟอร์เวิร์ดดิ้ง	76
3.14.5	DMZ.....	79
3.14.6	DDNS.....	80
3.14.7	NAT ผ่านตลอด	81
3.15	ไร้สาย.....	82
3.15.1	ทั่วไป	82
3.15.2	WPS.....	85
3.15.3	บริดจ์	87
3.15.4	ตัวกรอง MAC ไร้สาย.....	89
3.15.5	การตั้งค่า RADIUS.....	90
3.15.6	Professional (มืออาชีพ).....	91
4	ยูทิลิตี้	
4.1	การค้นหาลูปกรณ.....	94
4.2	การกู้คืนเฟิร์มแวร์.....	95
4.3	การตั้งค่าพรินเตอร์เซิร์ฟเวอร์ของคุณ.....	97
4.3.1	การแชร์เครื่องพิมพ์ ASUS EZ.....	97
4.3.2	การใช้ LPR เพื่อแชร์เครื่องพิมพ์.....	101
4.4	ดาวน์โหลดมาสเตอร์.....	106
4.4.1	การกำหนดค่าการตั้งค่าการดาวน์โหลดบิต ทอเรนต	107
4.4.2	การตั้งค่า NZB	108
5	การแก้ไขปัญหา	
5.1	การแก้ไขปัญหาพื้นฐาน	109
5.2	คำถามที่มีการถามบ่อยๆ (FAQs).....	112
	ภาคผนวก	
	ประกาศความปลอดภัย	130
	บริการและการสนับสนุน.....	132

1 ทำความรู้จักเราเตอร์ของคุณ

1.1 ยินดีต้อนรับ!

ขอบคุณที่ซื้อ ASUS RT-AX88U PRO เราเตอร์เราเตอร์!

หัวเครื่องสีดำที่ออกแบบมาอย่างโดดเด่น พร้อมด้วยสีแดงที่ได้รับแรงบันดาลใจจากเกมมิ่ง RT-AX88U PRO ทำงานด้วยแถบความถี่คู่ 2.4GHz และ 5GHz สำหรับการสตรีม HD แบบไร้สาย; SMB เซิร์ฟเวอร์, UPnP AV เซิร์ฟเวอร์, และ FTP เซิร์ฟเวอร์ สำหรับการแชร์ไฟล์ตลอด 24/7; ความสามารถในการจัดการเซสชันได้ถึง 300,000 รายการ และเทคโนโลยี ASUS กรีนเน็ตเวิร์ก ซึ่งเป็นโซลูชันที่ประหยัดพลังงานมากถึง 70% ซึ่งไม่มีใครเทียบได้ในขณะนี้

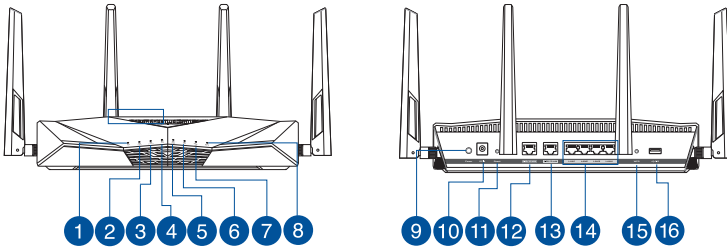
1.2 สิ่งต่างๆ ในกล่องบรรจุ

- RT-AX88U PRO เราเตอร์
- สายเคเบิลเครือข่าย(RJ-45)
- อะแดปเตอร์เสาอากาศ
- คู่มือเริ่มต้นอย่างรวดเร็ว
- ใบรับประกัน

หมายเหตุ:

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

1.3 ไวร์เลสเราเตอร์ของคุณ



-
- 1 LED เพาเวอร์**
ดับ: ไม่มีพลังงานเข้า
ติด: อุปกรณ์พร้อม
กะพริบช้า: โหมดช่วยเหลือน
-
- 2 LED 5GHz**
ดับ: ไม่มีสัญญาณ 5GHz
ติด: ระบบไร้สายพร้อม
กะพริบ: กำลังส่งหรือรับข้อมูลผ่านการเชื่อมต่อไร้สาย
-
- 3 LED 2.4GHz**
ดับ: ไม่มีสัญญาณ 2.4GHz
ติด: ระบบไร้สายพร้อม
กะพริบ: กำลังส่งหรือรับข้อมูลผ่านการเชื่อมต่อไร้สาย
-
- 4 LED WAN (อินเทอร์เน็ต) 2.5G/1G**
สีแดง: ไม่มีการเชื่อมต่อ WAN 2.5G/1G
ติด: มีการเชื่อมต่อทางกายภาพกับพอร์ต WAN 2.5G/1G
-
- 5 LAN LED 2.5G/1G**
ดับ: ไม่มีพลังงานเข้า หรือไม่มีการเชื่อมต่อทางกายภาพ
ติด: มีการเชื่อมต่อทางกายภาพไปยังเครือข่ายแลน (LAN)
-
- 6 LAN LED**
ดับ: ไม่มีพลังงานเข้า หรือไม่มีการเชื่อมต่อทางกายภาพ
ติด: มีการเชื่อมต่อทางกายภาพไปยังเครือข่ายแลน (LAN)
-
- 7 USB 3.2 Gen 1 LED**
ดับ: ไม่มีพลังงานเข้า หรือไม่มีการเชื่อมต่อทางกายภาพ
ติด: มีการเชื่อมต่อทางกายภาพกับอุปกรณ์ USB 3.2 Gen 1
-
- 8 WPS LED**
ดับ: WPS ไม่ได้กำลังประมวลผล
กะพริบเร็ว: WPS กำลังประมวลผล
-

9	ปุ่มพาวเวอร์ กดปุ่มนี้ เพื่อเปิดหรือปิดระบบ
10	พอร์ตพาวเวอร์ (DCเข้า) เสียบอะแดปเตอร์ AC ที่ให้มาเข้ากับพอร์ตนี้ และเชื่อมต่อเราเตอร์ของคุณเข้ากับแหล่งพลังงาน
11	ปุ่มรีเซ็ต ปุ่มนี้จะรีเซ็ต หรือกู้คืนระบบกลับเป็นการตั้งค่าเริ่มต้นจากโรงงาน
12	พอร์ต WAN (อินเทอร์เน็ต) 2.5G/1G เชื่อมต่อสายเคเบิลเครือข่ายเข้ากับพอร์ตนี้ เพื่อสร้างการเชื่อมต่อ WAN 2.5G/1G
13	พอร์ต LAN 2.5G/1G เชื่อมต่อสายเคเบิลเครือข่ายเข้ากับพอร์ตเหล่านี้ เพื่อสร้างการเชื่อมต่อ LAN 2.5G/1G
14	พอร์ต LAN 1~4 เชื่อมต่อสายเคเบิลเครือข่ายเข้ากับพอร์ตเหล่านี้ เพื่อสร้างการเชื่อมต่อ LAN
15	ปุ่ม WPS ปุ่มนี้ใช้เพื่อเปิดตัวช่วยสร้าง WPS
16	พอร์ต USB 3.2 Gen 1 เสียบอุปกรณ์ USB 3.2 Gen 1 เช่น ฮาร์ดดิสก์ USB หรือ USB แฟลชไดรฟ์ลงในพอร์ตเหล่านี้ เสียบสายเคเบิล USB ของ iPad ลงในพอร์ตเพื่อชาร์จ iPad ของคุณ

หมายเหตุ:

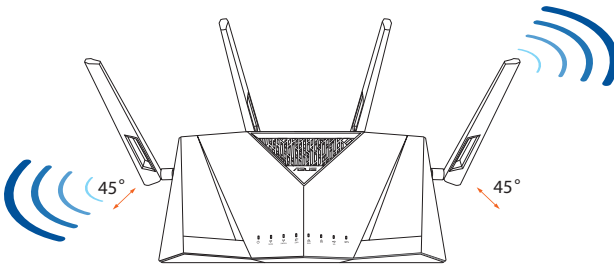
- ใช้เฉพาะอะแดปเตอร์ที่มาพร้อมกับแพ็คเกจของคุณเท่านั้น การใช้อะแดปเตอร์อื่นอาจทำให้อุปกรณ์เสียหาย
- ข้อมูลจำเพาะ:

อะแดปเตอร์พาวเวอร์ DC	เอาต์พุต DC: +19V ภัยมีกระแสสูงสุด 2.37A +19.5V ภัยมีกระแสสูงสุด 2.31A		
อุณหภูมิขณะทำงาน	0~40°C	ขณะเก็บรักษา	0~70°C
ความชื้นขณะทำงาน	50~90%	ขณะเก็บรักษา	20~90%

1.4 การวางตำแหน่งไวร์เลสเราเตอร์ของคุณ

เพื่อให้การรับส่งสัญญาณไร้สายระหว่างไวร์เลสเราเตอร์ และอุปกรณ์เครือข่ายที่เชื่อมต่ออยู่มีคุณภาพดีที่สุด ให้แน่ใจว่าคุณ:

- วางไวร์เลสเราเตอร์ในบริเวณศูนย์กลาง เพื่อให้ครอบคลุมพื้นที่รับสายมากที่สุดสำหรับอุปกรณ์เครือข่าย
- วางอุปกรณ์ให้ห่างจากวัตถุวางกันที่เป็นโลหะ และไม่ให้อุปกรณ์แสงแดดโดยตรง
- วางอุปกรณ์ให้ห่างจากอุปกรณ์ Wi-Fi 802.11g หรือ 20MHz, อุปกรณ์ต่อพ่วงคอมพิวเตอร์ 2.4GHz, อุปกรณ์บลูทูธ, วิทยุโทรศัพท์ไร้สาย, หม้อแปลง, มอเตอร์พลังงานสูง, แสงฟลูออเรสเซนต์, เตาไมโครเวฟ, ตู้เย็น และอุปกรณ์อุตสาหกรรมอื่นๆ เพื่อป้องกันสัญญาณรบกวน หรือสัญญาณสูญหาย
- อัปเดตไปเป็นเฟิร์มแวร์ล่าสุดเสมอ เยี่ยมชมเว็บไซต์ ASUS ที่ <http://www.asus.com> เพื่อรับอัปเดตเฟิร์มแวร์ล่าสุด
- ให้ปรับทิศทางเสาอากาศที่สามารถ อัน ในลักษณะที่แสดงในภาพด้านล่าง



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
- เว็บเบราว์เซอร์ เช่น Internet Explorer, Firefox, Safari หรือ Google Chrome

หมายเหตุ:

- ถ้าคอมพิวเตอร์ของคุณไม่มีความสามารถไร้สายในตัว คุณอาจติดตั้งอะแดปเตอร์ WLAN IEEE 802.11 a/b/g/n/ac/ax เข้ากับคอมพิวเตอร์ของคุณ เพื่อเชื่อมต่อไปยังเครือข่าย
- ด้วยเทคโนโลยีสองแบนด์ของไวร์เลสเราเตอร์ อุปกรณ์สนับสนุนสัญญาณไร้สายความถี่ 2.4GHz และ 5GHz พร้อมกันสนับสนุนให้คุณทำกิจกรรมที่เกี่ยวข้องกับอินเทอร์เน็ตต่างๆ เช่น การท่องอินเทอร์เน็ต หรือการอ่าน/เขียนข้อความอีเมลโดยใช้แถบความถี่ 2.4GHz ในขณะที่เดียวกับที่กำลังสตรีมไฟล์เสียง/วิดีโอระดับไฮเดฟฟินิชัน เช่น ภาพยนตร์ หรือเพลงโดยใช้แถบความถี่ 5GHz ไปพร้อมๆ กัน
- อุปกรณ์ IEEE 802.11n บางอย่างที่คุณต้องการเชื่อมต่อไปยังเครือข่ายของคุณ อาจสนับสนุนหรือไม่สนับสนุนแถบความถี่ 5GHz สำหรับข้อมูลจำเพาะ ให้ดูคู่มือผู้ใช้ของอุปกรณ์
- สายเคเบิลอีเธอร์เน็ต RJ-45 ซึ่งจะนำไปใช้เพื่อเชื่อมต่ออุปกรณ์เครือข่าย ไม่ควรมีความยาวเกิน 100 เมตร

สำคัญ!

- อะแดปเตอร์ไร้สายบางตัวอาจมีปัญหาการเชื่อมต่อกับ 802.11ax WiFi APs
- หากคุณกำลังประสบกับปัญหานี้ ให้แน่ใจว่าคุณได้อัปเดตไดรเวอร์เป็นเวอร์ชันล่าสุดแล้ว ตรวจสอบเว็บไซต์สนับสนุนอย่างเป็นทางการของบริษัทผู้ผลิตเพื่อขอรับไดรเวอร์ซอฟต์แวร์ การอัปเดต และข้อมูลที่เกี่ยวข้องอื่น ๆ
 - Realtek: <https://www.realtek.com/en/downloads>
 - Mediatek: <https://www.mediatek.com/products/connectivity-and-networking/broadband-wifi>
 - Intel: <https://downloadcenter.intel.com/>

2 เริ่มต้นการใช้งาน

2.1 การตั้งค่าเราเตอร์

สำคัญ:

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

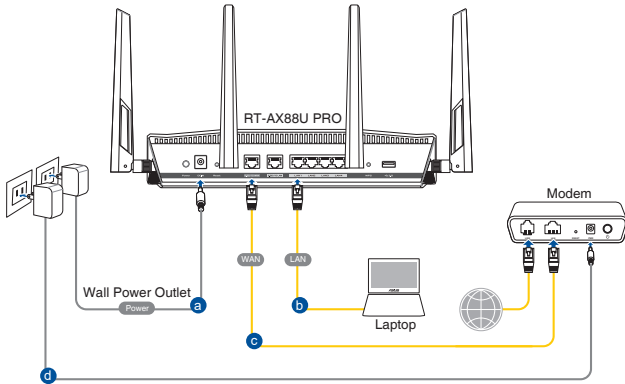


คำเตือน!

- ต้องเสียบสายไฟเข้ากับเต้ารับที่มีสายดินที่เหมาะสม เชื่อมต่ออุปกรณ์เข้ากับเต้ารับที่ใกล้เคียงที่เขาถึงได้ง่ายเท่านั้น
 - หากอะแดปเตอร์เสียหาย อย่าพยายามซ่อมด้วยตัวเอง ติดต่อช่างเทคนิคซ่อมแซมที่มีคุณสมบัติ หรือร้านค้าของคุณ
 - อย่าใช้สายไฟ อุปกรณ์เสริม หรืออุปกรณ์ต่อพ่วงที่ชำรุดเสียหาย
 - อย่าติดตั้งอุปกรณ์นี้สูงเกิน 2 เมตร
 - ใช้ผลิตภัณฑ์นี้ในสภาพแวดล้อมที่มีอุณหภูมิสิ่งแวดล้อมระหว่าง 0 °C (32 °F) ถึง 40 °C (104 °F)
-

A. การเชื่อมต่อแบบมีสาย

หมายเหตุ: ทีวีเสิร์สเราเตอร์ซึ่งออกแบบสำหรับเสียบสายเคเบิลแบบต่อตรง หรือแบบไขว้ เมื่อต้องการเชื่อมต่อแบบมีสาย



ในการตั้งค่าเครือข่ายโดยใช้การเชื่อมต่อแบบมีสาย:

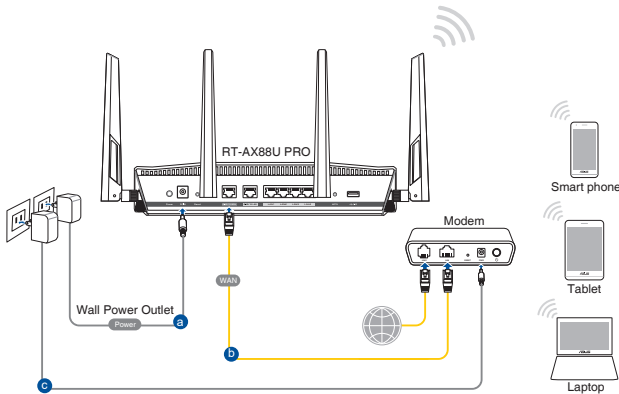
1. เสียบเราเตอร์เข้ากับเต้าเสียบและ เปิดเครื่อง เชื่อมต่อสายเคเบิลเครือข่ายจากคอมพิวเตอร์ไปยัง พอร์ต LAN บนเราเตอร์ของคุณ
2. เว็บ GUI จะเปิดใช้งานโดยอัตโนมัติเมื่อคุณเปิดเว็บเบราว์เซอร์ หากไม่เปิดใช้งานโดยอัตโนมัติ เข้าไปที่ <http://www.asusrouter.com>
3. ตั้งค่ารหัสผ่านสำหรับเราเตอร์ของคุณเพื่อความปลอดภัยจากการเข้าถึงที่ไม่ได้รับอนุญาต



B. การเชื่อมต่อไร้สาย

ในการตั้งค่าเครือข่ายโดยใช้การเชื่อมต่อแบบมีสาย:

1. เสียบเราเตอร์เข้ากับเต้าเสียบและ เปิดเครื่อง



2. เชื่อมต่อกับชื่อเครือข่าย (SSID) ที่แสดงบนฉลากผลิตภัณฑ์ที่ด้านหลังของเราเตอร์ เพื่อการรักษาความปลอดภัยของเครือข่ายที่ดีกว่า เปลี่ยนเป็น SSID ที่มีลักษณะเฉพาะและกำหนดรหัสผ่าน

ชื่อ Wi-Fi (SSID): ASUS_XX

- * XX หมายถึงตัวเลขสองหลักสุดท้ายของ MAC แอดเดรส 2.4GHz คุณสามารถค้นหาได้บนฉลากด้านหลังของ RT-AX88U PRO
3. เมื่อเชื่อมต่อแล้ว เว็บ GUI จะเปิดใช้งานโดยอัตโนมัติเมื่อคุณเปิดเว็บเบราว์เซอร์ หากไม่เปิดใช้งานโดยอัตโนมัติ เข้าไปที่ <http://www.asusrouter.com>
 4. ตั้งค่ารหัสผ่านสำหรับเราเตอร์ของคุณเพื่อความปลอดภัยจากการเข้าถึงที่ไม่ได้รับอนุญาต

หมายเหตุ:

- สำหรับรายละเอียดในการเชื่อมต่อเข้ากับเครือข่ายไร้สาย ให้ดูคู่มือผู้ใช้ของอะแดปเตอร์ WLAN
- ในการตั้งค่าระบบความปลอดภัยสำหรับเครือข่ายของคุณ ให้ดูส่วน 3.1.1 การตั้งค่าระบบความปลอดภัยไร้สาย

Login Information Setup

Change the router password to prevent unauthorized access to your ASUS wireless router.

Router Login Name	<input type="text" value="admin"/>	
New Password	<input type="password"/>	
Retype Password	<input type="password"/>	<input type="checkbox"/> Show password

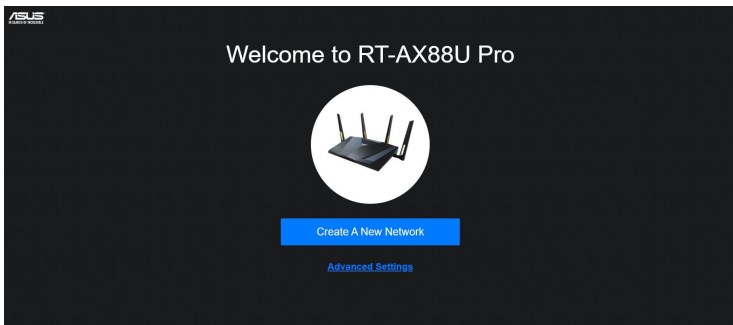
2.2 การตั้งค่าอินเทอร์เน็ตด้วย (QIS) ด้วยการตรวจพบอัตโนมัติ

ฟังก์ชัน การตั้งค่าอินเทอร์เน็ตด้วย (QIS) จะแนะนำวิธีการในการตั้งค่าการเชื่อมต่ออินเทอร์เน็ตของคุณอย่างรวดเร็ว

หมายเหตุ: ในขณะที่ตั้งค่าการเชื่อมต่ออินเทอร์เน็ตเป็นครั้งแรก กดปุ่มรีเซ็ต บนไวร์เลสเราเตอร์ของคุณ เพื่อรีเซ็ตเครื่องกลับเป็นการตั้งค่าเริ่มต้นจากโรงงาน

ในการใช้ QIS ด้วยการตรวจพบอัตโนมัติ:

1. เปิดเว็บเบราว์เซอร์ คุณจะถูกนำทางไปยัง ASUS Setup Wizard (การตั้งค่าอินเทอร์เน็ตด้วย) ถ้าไม่มี ให้ป้อนข้อมูล <http://www.asusrouter.com> ด้วยตนเอง

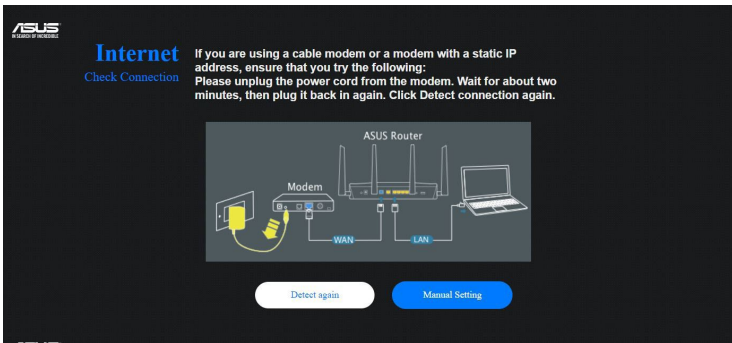


2. ไวร์เลสเราเตอร์จะตรวจพบโดยอัตโนมัติว่าชนิดการเชื่อมต่อ ISP ของคุณเป็น **ไดนามิก IP, PPPoE, PPTP, และ L2TP** พิมพ์ข้อมูลที่จำเป็นสำหรับชนิดการเชื่อมต่อ ISP ของคุณเข้าไป

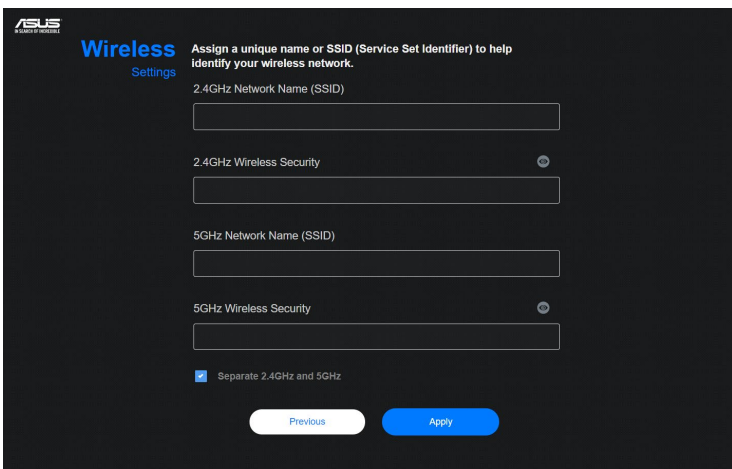
สำคัญ! ขอรับข้อมูลที่จำเป็นจาก ISP ของคุณเกี่ยวกับชนิดการเชื่อมต่ออินเทอร์เน็ต

หมายเหตุ:

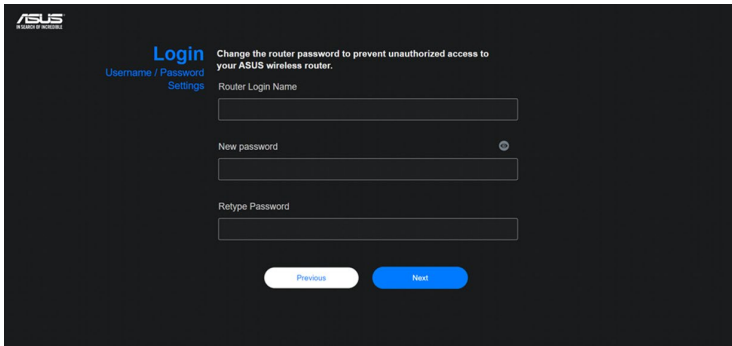
- การตรวจจับสนิทการเชื่อมต่อ ISP ของคุณโดยอัตโนมัติ จะเกิดขึ้นเมื่อคุณกำหนดค่าไวร์เลสเราเตอร์เป็นครั้งแรก หรือเมื่อไวร์เลสเราเตอร์ของคุณถูกรีเซ็ตกลับเป็นการตั้งค่าเริ่มต้น
- ถ้า QIS ตรวจไม่พบสนิทการเชื่อมต่ออินเทอร์เน็ตของคุณ, คลิก **Manual setting (ตั้งค่า แบบแมนนวล)** และกำหนดค่าการตั้งค่าการเชื่อมต่อของคุณแบบแมนนวล



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



4. บนหน้า **Login Information Setup** (การตั้งค่าข้อมูลล็อกอิน) ให้เปลี่ยนรหัสผ่านสำหรับการล็อกอินเราเตอร์เพื่อป้องกันการเข้าถึงเราเตอร์ไร้สายของคุณโดยไม่ได้รับอนุญาต





หมายเหตุ: ชื่อผู้ใช้และรหัสผ่านในการล็อกอินของไวร์เลสเราเตอร์นั้นแตกต่าง จากชื่อเครือข่าย 2.4GHz/5GHz (SSID) และคีย์การป้องกัน ชื่อผู้ใช้ และรหัสผ่านในการล็อกอินของไวร์เลสเราเตอร์ ใช้สำหรับการล็อกอิน เข้าไปยังเว็บ GUI ของไวร์เลสเราเตอร์ของคุณ เพื่อกำหนดค่าการตั้ง ค่าต่างๆ ของไวร์เลสเราเตอร์ของคุณ ชื่อเครือข่าย 2.4GHz/5GHz (SSID) และคีย์การป้องกัน อนุญาตให้อุปกรณ์ Wi-Fi ล็อกอิน และเชื่อมต่อไป ยังเครือข่าย 2.4GHz/5GHz ของคุณ

2.3 กำลังเชื่อมต่อไปยังเครือข่ายไร้สายของคุณ

หลังจากการตั้งค่าไวร์เลสเราเตอร์ของคุณด้วย QIS แล้ว คุณสามารถเชื่อมต่อคอมพิวเตอร์หรืออุปกรณ์เสริมอื่นๆ 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 สำหรับ ROG Gaming Center

3.1 การเข้าระบบไปยังเว็บ GUI

ASUS ไร้เลสเราเตอร์ของคุณมาพร้อมกับระบบติดต่อผู้ใช้แบบกราฟฟิกบนเว็บ (GUI) ที่คุณสามารถเรียนรู้การใช้งานได้เอง ซึ่งอนุญาตให้คุณทำการกำหนดค่าคุณสมบัติต่างๆ อย่างง่ายดายผ่านเว็บเบราว์เซอร์ เช่น Internet Explorer, Firefox, Safari หรือ Google Chrome

หมายเหตุ: คุณสมบัตินี้จะแตกต่างกันไปในเวอร์ชันเฟิร์มแวร์ต่างๆ

ในการเข้าระบบไปยังเว็บ GUI:

1. บนเว็บเบราว์เซอร์ของคุณ ป้อน IP แอดเดรสของไร้เลสเราเตอร์: <http://www.asusrouter.com>
2. บนหน้าเข้าสู่ระบบ ป้อนข้อมูลชื่อผู้ใช้ค่าเริ่มต้น (**admin**) และรหัสผ่านที่คุณได้ตั้งค่าไว้ใน **2.2 Quick Internet Setup (QIS) with Auto-detection (2.2 การตั้งค่าอินเทอร์เน็ตด่วน (QIS) พร้อมด้วยการตรวจอัตโนมัติ)**



3. ขณะนี้คุณสามารถใช้เว็บ GUI เพื่อกำหนดค่าการตั้งค่าต่างๆ ของ ASUS ไร้เลสเราเตอร์ของคุณได้

ปุ่มคำสั่งบนสุด



* รูปภาพนี้ใช้เพื่อการอ้างอิงเท่านั้น

หมายเหตุ: ถ้าคุณเข้ามายังระบบเว็บ GUI เป็นครั้งแรก
คุณจะถูกนำไปยังหน้า การตั้งค่าอินเทอร์เน็ตด่วน (QIS) โดยอัตโนมัติ

3.1.1 การตั้งค่าระบบความปลอดภัยไร้สาย

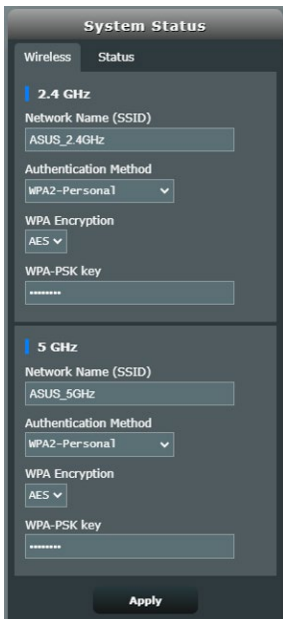
เพื่อป้องกันเครือข่ายของคุณจากการเข้าถึงโดยไม่ได้รับอนุญาต คุณจำเป็นต้องกำหนดค่าของการตั้งค่าระบบความปลอดภัยของเครือข่าย

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 ได้

การตั้งค่าระบบความปลอดภัย 2.4GHz / 5GHz



3. บนฟิลด์ **Network Name (SSID) (ชื่อเครือข่าย (SSID))**, ป้อนชื่อที่เป็นเอกลักษณ์สำหรับเครือข่ายไร้สายของคุณ

4. จากรายการแบบดิ่งลง **WEP Encryption (การเข้ารหัส WEP)**, เลือกวิธีการเข้ารหัสสำหรับเครือข่ายไร้สายของคุณ

สำคัญ! มาตรฐาน IEEE 802.11n/ac/ax ห้ามการใช้ไทรฟูตกับ WEP หรือ WPA-TKIP เป็นยูนิแควสต์ไซเฟอร์ หากคุณใช้วิธีการเข้ารหัสเหล่านี้ อัตราการรับส่งข้อมูลของคุณจะตกลงเป็นการเชื่อมต่อ IEEE 802.11g 54Mbps

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

3.1.2 การจัดการเน็ตเวิร์กไคลเอนต์ของคุณ



ในการจัดการเน็ตเวิร์กไคลเอนต์ของคุณ:

1. จากหน้าต่างระบบเมนู ไปยัง **General (ทั่วไป) > Network Map (แผนที่เครือข่าย)**
2. บนหน้าจอ Network Map (แผนที่เครือข่าย), เลือกไอคอน **Client status (สถานะไคลเอนต์)** เพื่อแสดงข้อมูลเกี่ยวกับเน็ตเวิร์กไคลเอนต์ของคุณ
3. เพื่อบล็อกการเข้าถึงของไคลเอนต์ไปยังเครือข่ายของคุณ, ให้เลือกไคลเอนต์ และคลิก **block (บล็อก)**

3.1.3 การตรวจสอบอุปกรณ์ USB ของคุณ

ASUS ไร้สายเราเตอร์ ให้พอร์ต USB มาหนึ่งพอร์ต สำหรับเชื่อมต่ออุปกรณ์ USB หรือเครื่องพิมพ์ USB เพื่ออนุญาตให้ คุณแชร์ไฟล์และเครื่องพิมพ์กับโหนดอื่นต่างๆ ในเครือข่ายของคุณ



* รูปภาพนี้ใช้เพื่อการอ้างอิงเท่านั้น

หมายเหตุ: ในการใช้คุณสมบัตินี้ คุณจำเป็นต้องเสียบอุปกรณ์เก็บข้อมูล USB เช่น USB ฮาร์ดดิสก์ หรือ USB แฟลชไดรฟ์ เข้ากับพอร์ต USB 3.0 ที่แผงด้านหลังของไร้สายเราเตอร์ของคุณ ตรวจสอบให้แน่ใจว่า อุปกรณ์เก็บข้อมูล USB ได้รับการฟอร์แมตและแบ่งพาร์ติชันอย่างเหมาะสม ดูรายการสนับสนุนผลิตภัณฑ์แอ็นดแชร์ดิสก์ที่ <http://event.asus.com/networks/disksupport>

สำคัญ! แรกสุด คุณจำเป็นต้องสร้างบัญชีสำหรับแชร์ และกำหนดสิทธิ์การอนุญาต/การเข้าถึง เพื่ออนุญาตให้เน็ตเวิร์ก⁴คลเ็นต์อื่นๆ สามารถเข้าถึงอุปกรณ์ USB ของคุณผ่าน FTP ⁴เซต/ยูทิลิตี้ FTP ⁴คลเ็นต์ของบริษัทอื่น, เซิร์ฟเวอร์เซ็นเตอร์, แซมบ้า หรือ iCloud 2.0 สำหรับรายละเอียดเพิ่มเติม ให้อ่านส่วน **3.13 งานผ่าน USB** และ **3.4 iCloud 2.0** ในคู่มือผู้ใช้

ในการตรวจสอบอุปกรณ์ USB ของคุณ:

1. จากหน้าต่างระบบเมนู ⁴ไปยัง **General (ทั่วไป) > Network Map (แผนที่เครือข่าย)**
2. บนหน้าจอ Network Map (แผนที่เครือข่าย), เลือกไอคอน **USB Disk Status (สถานะ USB ดิสก์)** เพื่อแสดงข้อมูลของอุปกรณ์ USB ของคุณ
3. บนฟิลด์, AiDisk Wizard (ตัวช่วยสร้าง AiDisk), คลิก **GO (ไป)** เพื่อตั้งค่า FTP เซิร์ฟเวอร์สำหรับการแชร์⁴ไฟล์อินเทอร์เน็ต


หมายเหตุ:

- สำหรับรายละเอียดเพิ่มเติม ให้อ่านส่วน **3.13.2 ารใช้เซิร์ฟเวอร์เซ็นเตอร์** ในคู่มือผู้ใช้ฉบับนี้
 - ⁴ไวร์เลสเราเตอร์ทำงานกับ USB แฟลชดิสก์/HDD ขนาดใหญ่ (สูงสุด 2TB) และสนับสนุนการอ่าน-เขียนสำหรับระบบ FAT16, FAT32, EXT2, EXT3 และ NTFS
-

การถอด USB ดิสก์อย่างปลอดภัย

สำคัญ! การถอด USB ดิสก์อย่างไม่ถูกต้อง อาจทำให้ข้อมูลเสียหายได้

ในการถอด USB ดิสก์อย่างปลอดภัย:

1. จากหน้าต่างระบบเมนู ไปยัง **General (ทั่วไป) > Network Map (แผนที่เครือข่าย)**
2. ที่มุมขวาบน, คลิก  > **Eject USB disk (ถอด USB ออก)** เมื่อ USB ถูกถอดสำเร็จแล้ว, สถานะ USB จะแสดงคำว่า **Unmounted (เลิกเมตแล้ว)**

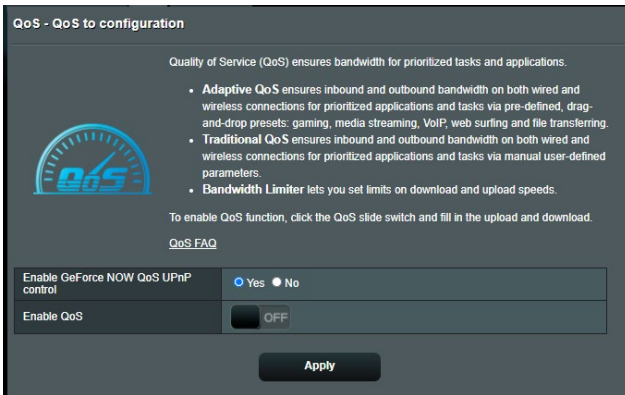


* รูปภาพนี้ใช้เพื่อการอ้างอิงเท่านั้น

3.2 Adaptive QoS (อะแดปทีฟ QoS)

3.2.1 การจัดการ QoS (คุณภาพของบริการ) แบนด์วิดธ์

คุณภาพของบริการ (QoS) อนุญาตให้คุณตั้งค่าลำดับความสำคัญของแบนด์วิดธ์ และจัดการจราจรเครือข่าย



ในการตั้งค่าลำดับความสำคัญแบนด์วิดธ์:

1. จากหน้าต่างระบบเมนู ไปยัง **General (ทั่วไป) > Adaptive QoS (อะแดปทีฟ QoS) > QoS (QoS)**
2. คลิก **ON (เปิด)** เพื่อเปิดทำงาน QoS กรอกข้อมูลในฟิลด์แบนด์วิดธ์สำหรับอัปโหลดและดาวน์โหลด

หมายเหตุ: ข้อมูลแบนด์วิดธ์ของคุณจาก ISP จะใช้ได้

3. คลิก **Apply (นำไปใช้)**

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

4. บนหน้า **user-defined QoS rules (กฎ QoS ที่กำหนดโดยผู้ใช้)**, มีชนิดบริการออนไลน์เริ่มต้น 4 แบบ - เซิร์ฟเวอร์, 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 "*.*.*.*" หรือปล่อยฟิลด์ไว้ว่าง
 - 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)** ประกอบด้วยข้อมูลเกี่ยวกับการจราจรที่สตรีมและดาวน์โหลด (การจราจรเครือข่ายขาออกและขาเข้า) สำหรับเซสชันหนึ่ง ในคอลัมน์นี้, คุณสามารถตั้งค่าขีดจำกัดการจราจรเครือข่าย (ในหน่วย KB) สำหรับบริการที่เจาะจง เพื่อสร้างความสำคัญเฉพาะสำหรับบริการที่กำหนดไปยังพอร์ตที่เจาะจง ตัวอย่างเช่น ถ้าเน็ตเวิร์ก 4 คู่เอ็นด์ 2 ตัว คือ PC 1 และ PC 2 กำลังเข้าถึงอินเทอร์เน็ตทั้งคู่ (ตั้งค่าที่พอร์ต 80) แต่ PC 1 ใช้ปริมาณข้อมูลเกินขีดจำกัดการจราจรเครือข่ายเนื่องจากมีงานดาวน์โหลดบางอย่าง, PC 1 จะมีความสำคัญที่ต่ำกว่า ถ้าคุณไม่ต้องการตั้งค่าขีดจำกัดการจราจรให้ปล่อยคอลัมน์นี้ว่างไว้

5. บนหน้า **User-defined Priority (ลำดับความสำคัญที่กำหนดโดยผู้ใช้)**, คุณสามารถตั้งลำดับความสำคัญของแอปพลิเคชันเครือข่ายหรืออุปกรณ์ต่างๆ เป็น 5 ระดับจากรายการแบบดิ่งลง **user-defined QoS rules (กฎ QoS ที่กำหนดโดยผู้ใช้)** คุณสามารถใช้วิธีการต่อไปนี้ในการส่งแพ็คเก็ตข้อมูล ตามระดับความสำคัญ:

- เปลี่ยนลำดับของแพ็คเก็ตเครือข่ายอัปสตรีมซึ่งถูกส่งไปยังอินเทอร์เน็ต
- ภายใต้อยู่ตาราง **Upload Bandwidth (แบนด์วิดธ์อัปโหลด)**, ตั้งค่า **Minimum Reserved Bandwidth (แบนด์วิดธ์สงวนที่ต่ำที่สุด)** และ **Maximum Bandwidth Limit (ขีดจำกัดแบนด์วิดธ์มากที่สุด)** สำหรับแอปพลิเคชันเครือข่ายหลายรายการ ที่มีระดับความสำคัญแตกต่างกัน เปอร์เซ็นต์ระบุถึงอัตราแบนด์วิดธ์อัปโหลดที่ใช้ได้สำหรับแอปพลิเคชันเครือข่ายที่ระบุ

หมายเหตุ:

- แพ็คเก็ตที่มีความสำคัญต่ำจะไม่ได้รับความสนใจ เพื่อให้มั่นใจถึงการส่งข้อมูลของแพ็คเก็ตที่มีความสำคัญสูง
- ภายใต้อยู่ตาราง **Download Bandwidth (แบนด์วิดธ์ดาวน์โหลด)**, ตั้งค่า **Maximum Bandwidth Limit (ขีดจำกัดแบนด์วิดธ์มากที่สุด)** สำหรับแอปพลิเคชันเครือข่ายหลายรายการตามลำดับ แพ็คเก็ตอัปสตรีมที่มีความสำคัญสูงกว่า จะทำให้เกิดแพ็คเก็ตดาวน์โหลดสตรีมที่มีความสำคัญสูงกว่า
- ถ้าไม่มีแพ็คเก็ตกำลังถูกส่งจากแอปพลิเคชันที่มีความสำคัญสูง อัตราการรับส่ง ของการเชื่อมต่ออินเทอร์เน็ตจะใช้สำหรับแพ็คเก็ตที่มีความสำคัญต่ำอย่างเต็มที่

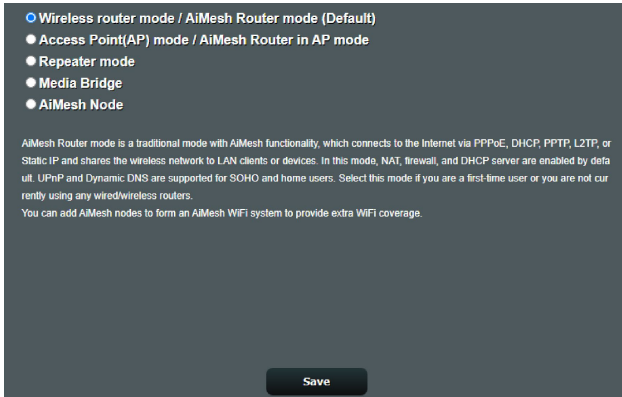
6. ตั้งค่าแพ็คเก็ตที่มีลำดับความสำคัญสูงที่สุด เพื่อให้มั่นใจถึงการประสานการเล่นเกมที่ออนไลน์ที่ราบรื่น คุณสามารถตั้งค่า ACK, SYN และ ICMP เป็นแพ็คเก็ตที่มีลำดับความสำคัญสูงที่สุดได้

หมายเหตุ: ตรวจสอบให้แน่ใจว่าเปิดทำงาน QoS ก่อน และตั้งค่าขีดจำกัดอัตราการอัปโหลดและดาวน์โหลด

3.3 การดูแลระบบ

3.3.1 โหมดการทำงาน

หน้า โหมดการทำงาน อนุญาตให้คุณเลือกโหมดที่เหมาะสมสำหรับเครือข่ายของคุณ



ในการตั้งค่าโหมดการทำงาน:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง) > Administration (การดูแลระบบ) > Operation Mode (โหมดการทำงาน)**
2. เลือกโหมดการทำงานเหล่านี้:
 - **โหมดไวร์เลสเราเตอร์(ค่าเริ่มต้น):** ในโหมดไวร์เลสเราเตอร์, ไวร์เลสเราเตอร์จะเชื่อมต่อไปยังอินเทอร์เน็ต และให้การเข้าถึง อินเทอร์เน็ตไปยังอุปกรณ์ที่ใช้ได้บนเครือข่ายแลนของตัวเอง
 - **โหมดแอดเซสพอยต์:** ในโหมดนี้ เราเตอร์จะสร้างเครือข่ายไร้สายบนเครือข่ายที่มีอยู่แล้ว
 - **โหมดรีพีตเตอร์:** โหมดนี้จะเปลี่ยนเราเตอร์เป็นรีพีตเตอร์ไร้สายเพื่อขยายช่วงสัญญาณของคุณ
 - **มีเดียบริดจ์:** โหมดมีเดียบริดจ์ ให้การเชื่อมต่อ Wi-Fi ที่เร็วที่สุด สำหรับใช้อุปกรณ์มีเดียหลายอย่างพร้อมกัน ในการตั้งค่าโหมดมีเดียบริดจ์ คุณจำเป็นต้องมี RT-AX88U PRO 2 ตัว: ตัวหนึ่งกำหนดค่าเป็นมีเดียสวิตช์ และอีกตัวเป็นเราเตอร์.
 - **โหมด AiMesh:** คุณสามารถตั้งค่า RT-AX88U PRO เป็นโหมด AiMesh เพื่อขยายพื้นที่ครอบคลุม WiFi ของเราเตอร์ AiMesh ที่มีอยู่ใด

3. คลิก **Save** (บันทึก)

หมายเหตุ: เราเตอร์จะบูตใหม่เมื่อคุณเปลี่ยนโหมด

3.3.2 ระบบ

หน้า **System (ระบบ)** อนุญาตให้คุณกำหนดค่าการตั้งค่าไวร์เลสเราเตอร์ของคุณ

ในการตั้งค่าระบบ:

1. จากหน้าต่างระบบเมนู "ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง) > Administration (การดูแลระบบ) > System (ระบบ)**
2. คุณสามารถกำหนดค่าการตั้งค่าต่อไปนี้:
 - **เปลี่ยนรหัสผ่านล็อกอินของเราเตอร์:** คุณสามารถเปลี่ยนรหัสผ่านและชื่อล็อกอินของไวร์เลสเราเตอร์ โดยการป้อนชื่อและรหัสผ่านใหม่
 - **พฤติกรรมปุ่ม WPS:** ปุ่ม WPS บนตัวเครื่องไวร์เลสเราเตอร์ สามารถถูกใช้เพื่อเปิดทำงาน WPS
 - **ระยะเวลา:** เลือกระยะเวลาสำหรับเครือข่ายของคุณ
 - **NTP เซิร์ฟเวอร์:** ไวร์เลสเราเตอร์สามารถเข้าถึง NTP (โปรโตคอลเวลาเครือข่าย) เซิร์ฟเวอร์เพื่อที่จะซิงโครไนซ์เวลาได้
 - **เปิดทำงาน Telnet:** คลิก **Yes (ใช่)** เพื่อเปิดทำงานบริการ Telnet บนเครือข่าย คลิก **No (ไม่)** เพื่อปิดทำงาน Telnet
 - **วิธีการยืนยันตัวตน:** 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

3. คลิก **Apply** (นำไปใช้)

3.3.3 การอัปเดตเฟิร์มแวร์

หมายเหตุ: ดาวน์โหลดเฟิร์มแวร์ล่าสุดจากเว็บไซต์ ASUS ที่ <http://www.asus.com>

ในการอัปเดตเฟิร์มแวร์:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง) > Administration (การดูแลระบบ) > Firmware Upgrade (เฟิร์มแวร์อัปเดต)**
2. ในฟิลด์ **Firmware Version (Laiteohjelmiston versio)**, คลิก **Check (ตรวจสอบ)** เพื่อค้นหาเฟิร์มแวร์ใหม่ในคอมพิวเตอร์ของคุณ
3. คลิก **Upload (อัปเดต)**

หมายเหตุ:

- เมื่อกระบวนการอัปเดตสมบูรณ์ ให้รอสักครู่เพื่อให้ระบบบูตใหม่
- ถ้ากระบวนการอัปเดตล้มเหลว ไวลเลสเราเตอร์จะเข้าสู่โหมดช่วยเหลือโดยอัตโนมัติ และไฟแสดงสถานะ LED เพาเวอร์ที่แผงด้านหน้าจะกะพริบซ้ำๆ ในการเรียกคืน หรือกู้คืนระบบ ให้ใช้ยูทิลิตี้ **4.2 Firmware Restoration (การกู้คืนเฟิร์มแวร์)**

3.3.4 การกู้คืน/การจัดเก็บ/การอัปเดตการตั้งค่า

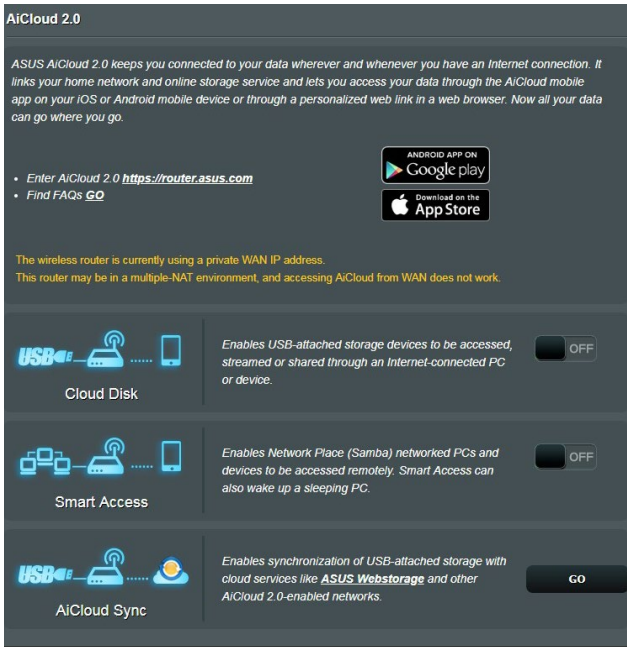
ในการกู้คืน/จัดเก็บ/อัปเดตการตั้งค่า:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง) > Administration (การดูแลระบบ) > Restore/Save/Upload Setting (กู้คืน/บันทึก/อัปเดตการตั้งค่า)**
2. เลือกงานที่คุณต้องการทำ:
 - ในการกู้คืนการตั้งค่ากลับเป็นค่าเริ่มต้นจากโรงงาน, คลิก **Restore (กู้คืน)**, และคลิก **OK (ตกลง)** ในข้อความการยืนยัน
 - ในการจัดเก็บการตั้งค่าระบบปัจจุบัน, คลิก **Save setting (บันทึกการตั้งค่า)**, และคลิก **Save (จัดเก็บ)** ในหน้าต่างดาวน์โหลดไฟล์ เพื่อจัดเก็บไฟล์ระบบลงในพาร์ตที่คุณต้องการ
 - ในการกู้คืนการตั้งค่าระบบก่อนหน้า, คลิก **Upload (อัปเดต)** เพื่อค้นหาไฟล์ระบบที่คุณต้องการกู้คืน, จากนั้นคลิก **Open (เปิด)**

สำคัญ! ถ้าเกิดปัญหาขึ้น ให้อัปเดตเฟิร์มแวร์เวอร์ชันล่าสุด และกำหนดค่าการตั้งค่าใหม่ อยากรู้คืนเราเตอร์กลับเป็นการตั้งค่าเริ่มต้น

3.4 AiCloud 2.0

AiCloud 2.0 เป็นแอปพลิเคชันบริการคลาวด์ที่อนุญาตให้คุณบันทึกซิงค์ แชร์ และเข้าถึงไฟล์ของคุณ



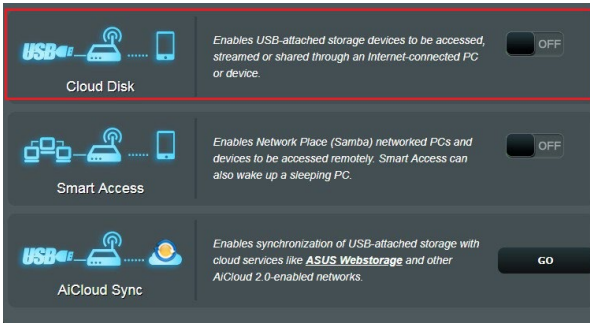
ในการใช้ AiCloud 2.0:

1. จาก Google เพลย์สโตร์ หรือ Apple สโตร์, ดาวน์โหลดและติดตั้งแอป ASUS AiCloud 2.0 ไปยังอุปกรณ์สมารถของคุณ
2. เชื่อมต่ออุปกรณ์สมารถของคุณเข้ากับเครือข่าย ปฏิบัติตามขั้นตอนเพื่อทำการบวกราคา AiCloud 2.0 ให้สมบูรณ์

3.4.1 คลาวด์ดิสก์

ในการสร้างคลาวด์ดิสก์:

1. เสียบอุปกรณ์เก็บข้อมูล USB เข้ากับไวร์เลสเราเตอร์
2. เปิด คลาวด์ดิสก์

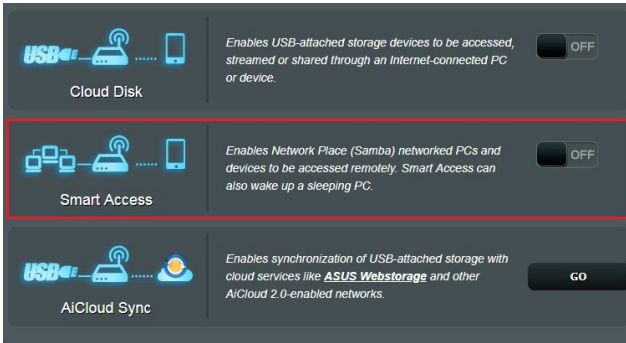


3. ไปที่ <http://www.asusrouter.com> และป้อนบัญชีล็อกอิน และรหัสผ่านของเราเตอร์ เพื่อให้ได้ประสบการณ์ผู้ใช้ที่ดีกว่า เราแนะนำให้คุณใช้ **Google Chrome** หรือ **Firefox**
4. ขณะนี้คุณสามารถเริ่มการใช้งานไฟล์บนคลาวด์ดิสก์กับอุปกรณ์ที่เชื่อมต่อกับเครือข่ายได้แล้ว

หมายเหตุ: ในขณะที่เข้าถึงอุปกรณ์ที่เชื่อมต่ออยู่กับเครือข่าย คุณจำเป็นต้องป้อนชื่อผู้ใช้และรหัสผ่านของอุปกรณ์ด้วยตัวเอง ซึ่งจะไม่ถูกบันทึกโดย AiCloud 2.0 เนื่องจากเหตุผลด้านความปลอดภัย

3.4.2 เข้าถึงแบบสมาร์ท

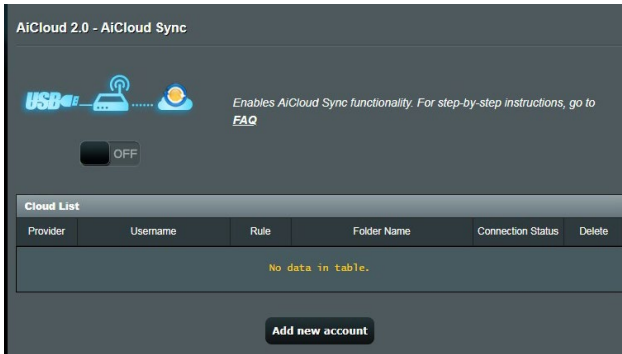
ฟังก์ชัน เข้าถึงแบบสมาร์ท อนุญาตให้คุณเข้าถึงเครือข่ายที่บ้านของคุณผ่านชื่อโดเมนของเราเตอร์ของคุณได้



หมายเหตุ:

- คุณสามารถสร้างชื่อโดเมนสำหรับเราเตอร์ของคุณด้วย ASUS DDNS สำหรับรายละเอียดเพิ่มเติม โปรดดูส่วน **3.14.6 DDNS**
- ตามค่าเริ่มต้น AiCloud 2.0 ให้การเชื่อมต่อ HTTPS ที่มีระบบรักษาความปลอดภัย ป้อน **[https://\[ชื่อ ASUSDDNS ของคุณ\].asuscomm.com](https://[ชื่อ ASUSDDNS ของคุณ].asuscomm.com)** สำหรับการใช้งานคลาวด์ดีเอสก์ และการเข้าถึงแบบสมาร์ทที่มีความปลอดภัยมาก

3.4.3 AiCloudซิงค์



ในการใช้ AiCloud 2.0 ซิงค์:

1. เปิด AiCloud 2.0, คลิก **AiCloud Sync (AiCloudซิงค์)**
2. เลือก **ON (เปิด)** เพื่อเปิดทำงาน AiCloudซิงค์
3. คลิก **Add new account (เพิ่มบัญชีใหม่)**
4. ป้อนรหัสผ่านบัญชี ASUS WebStorage ของคุณ และเลือกไดเรกทอรีที่คุณต้องการซิงค์กับ WebStorage
5. คลิก **Apply (นำไปใช้)**

3.5 AiProtection

AiProtection ให้การตรวจดูแลแบบเรียลไทม์ ที่ตรวจจับมัลแวร์ ส�파ย เวิร์ และการเข้าถึงที่ไม่ต้องการ นอกจากนี้ยังช่วยกรองเว็บไซต์และ แอปที่ไม่พึงประสงค์ออกไป และอนุญาตให้คุณกำหนดตารางเวลาที่ อุปกรณ์ที่เชื่อมต่อสามารถเข้าถึงอินเทอร์เน็ตได้

3.5.1 การป้องกันเครือข่าย

การป้องกันเครือข่าย ป้องกันการใช้ประโยชน์จากเครือข่าย และป้องกันเครือข่ายของคุณจากการเข้าถึงที่ไม่พึงประสงค์ของคุณจากการเข้าถึงที่ไม่พึงประสงค์

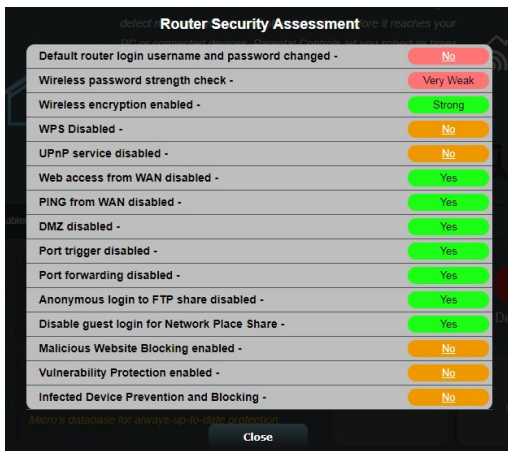


การกำหนดค่าการป้องกันเครือข่าย

ในการกำหนดค่าการป้องกันเครือข่าย:

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

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



สำคัญ! รายการที่ทำเครื่องหมายด้วย **Yes (ใช่)** บนหน้า **Router Security Assessment (การประเมินความปลอดภัยของเราเตอร์)** จะถูกพิจารณาว่ามีสถานะ **ปลอดภัย** รายการที่ทำเครื่องหมายด้วย **No (ไม่)**, **Weak (อ่อน)** หรือ **Very Weak (อ่อนมาก)** แนะนำให้ทำการ กำหนดค่าอย่างเหมาะสม

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

การบล็อกไซต์ที่ประสงค์ร้าย

คุณสมบัตินี้จำกัดการเข้าถึงยังเว็บไซต์ที่ประสงค์ร้ายที่รู้จักในฐานข้อมูลบนคลาวด์ เพื่อการป้องกันที่ทันสมัยอยู่เสมอ

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

ในการเปิดทำงานการบล็อกไซต์ที่ประสงค์ร้าย

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

IPS แบบสองทาง

IPS แบบสองทาง (ระบบป้องกันการบุกรุก) ช่วยปกป้องเราเตอร์ของคุณจากการโจมตีทางเครือข่ายโดยการ บล็อกทั้งแพ็คเก็ตขาเข้าที่เป็นอันตราย และตรวจจับแพ็คเก็ตขาออกที่น่าสงสัย

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

ในการเปิดทำงานการป้องกันช่องโหว่:

1. จากแผงระบบหน้าทาง ไปที่ **General (ทั่วไป) > AiProtection**
2. จากหน้าหลักของ **AiProtection** คลิกที่ **Network Protection (การป้องกันเครือข่าย)**
3. จากแผง **IPS แบบสองทาง** คลิก **ON (เปิด)**

การป้องกันและการบล็อกอุปกรณ์ที่ติดเชื้อ

คุณสมบัตินี้ป้องกันอุปกรณ์ที่ติดเชื้อไม่ให้ส่งข้อมูลส่วนตัว หรือสถานะ ที่ติดเชื้อไปยังบุคคลภายนอก

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

ในการเปิดทำงานการป้องกันช่องโหว่:

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

ในการกำหนดค่าการกำหนดลักษณะการแจ้ง:

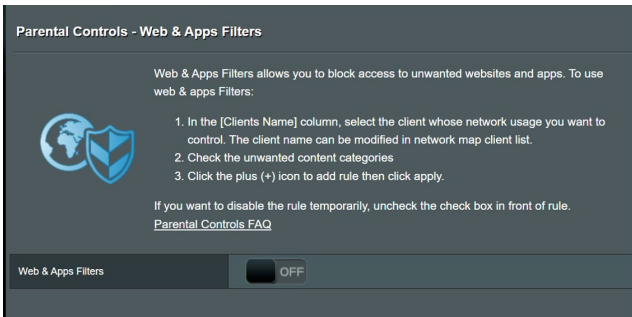
1. จากแผง **Infected Device Prevention and Blocking (การป้องกันและการบล็อกอุปกรณ์ที่ติดเชื้อ)** คลิก **Alert Preference (การกำหนดลักษณะการแจ้ง)**
2. เลือกหรือพิมพ์ผู้ให้บริการอีเมล บัญชีอีเมล และรหัสผ่านเข้าไปจากนั้นคลิก **Apply (นำไปใช้)**

3.5.2 การตั้งค่าการควบคุมโดยผู้ปกครอง

การควบคุมโดยผู้ปกครอง อนุญาตให้คุณควบคุมเวลาใช้อินเทอร์เน็ต หรือตั้งค่าขีดจำกัดเวลาสำหรับการใช้เครือข่ายของไคลเอ็นต์ได้

ในการเข้าไปยังหน้าหลักของ การควบคุมโดยผู้ปกครอง:

จากแผงระบบนำทาง ไปที่ **General (ทั่วไป) > Parental Controls (การควบคุมโดยผู้ปกครอง)**




ตัวกรองเว็บ & แอป

ตัวกรองเว็บ & แอป เป็นคุณสมบัติหนึ่งของ การควบคุมโดยผู้ปกครอง ที่อนุญาตให้คุณบล็อกการเข้าถึงไปยังเว็บไซต์หรือแอปพลิเคชันที่ไม่ต้องการ

ในการกำหนดค่าตัวกรองเว็บ & แอป:

1. จากแผงระบบนำทาง ไปที่ **General (ทั่วไป) > Parental Controls (การควบคุมโดยผู้ปกครอง)**
2. จากแผง **Web & Apps Filters (นตัวกรองเว็บ & แอป)** คลิก **ON (เปิด)**
3. เมื่อข้อความ ข้อตกลงในการอนุญาตให้ใช้งานของผู้ใช้ (EULA) ปรากฏขึ้น คลิก **I agree (ยอมรับ)** เพื่อทำต่อ
4. จากคอลัมน์ **Client List (รายการไคลเอ็นต์)** เลือกหรือพิมพ์ชื่อไคลเอ็นต์จากรายการแบบดิ่งลงเข้าไป

5. จากคอลัมน์ **Content Category (ประเภทเนื้อหา)** เลือกตัวกรองจากประเภทหลัก 4 ประเภท: **Adult (ผู้ใหญ่)**, **Instant Message and Communication (ข้อความทันทีและการสื่อสาร)**, **P2P and File Transfer (P2P และการถ่ายโอนไฟล์)** และ **Streaming and Entertainment (การสตรีมและความบันเทิง)**
6. คลิก  เพื่อเพิ่มโปรไฟล์ของไอคลเอ็นด์
7. คลิก **Apply (นำไปใช้)** เพื่อจัดเก็บการตั้งค่า

Parental Controls - Web & Apps Filters


Web & Apps Filters allows you to block access to unwanted websites and apps. To use web & apps Filters:

1. In the [Clients Name] column, select the client whose network usage you want to control. The client name can be modified in network map client list.
2. Check the unwanted content categories
3. Click the plus (+) icon to add rule then click apply.

If you want to disable the rule temporarily, uncheck the check box in front of rule.
[Parental Controls FAQ](#)

Web & Apps Filters ON

Client List (Max Limit : 64)

<input type="checkbox"/>	Client Name (MAC Address)	Content Category	Add / Delete
<input checked="" type="checkbox"/>	192.168.1.100	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Adult Block adult/mature content to prevent children from visiting sites that contain material of a sexual, violent, and illegal nature. <input checked="" type="checkbox"/> Instant Message and Communication Block instant communication software and messaging apps to prevent children from becoming addicted to social networking sites. <input checked="" type="checkbox"/> P2P and File Transfer By blocking P2P and File Transferring you can make sure your network has a better quality of data transmission. <input checked="" type="checkbox"/> Streaming and Entertainment By blocking streaming and entertainment services you can limit the time your children spend online. 	

No data in table.

Apply

การกำหนดตารางเวลา

การกำหนดตารางเวลา อนุญาตให้คุณตั้งค่าขีดจำกัดเวลาสำหรับการใช้เครือข่ายของไคลเอนต์

หมายเหตุ: ให้แน่ใจว่าเวลาระบบของคุณซิงโครไนซ์กับ NTP เซิร์ฟเวอร์

Parental Controls - Time Scheduling

By enabling Block All Devices, all of the connected devices will be blocked from Internet access.

Enable block all devices OFF

This feature allows you to set up a scheduled time for specific devices' Internet access.

1. In [Client Name] column, select a device you would like to manage. You can also manually key in MAC address in this column.
2. In the [Add / Delete] column, click the plus(+) icon to add the client.
3. In [Time Management] column, click the edit icon to set a schedule.
4. Click [Apply] to save the configurations.

Enable Time Scheduling ON

System Time Thu, Sep 21 12:34:41 2023

Client List (Max Limit : 64)

Select	Client Name (MAC Address)	Time Management	Add / Delete
Time		-	+

No data in table.

Apply

ในการกำหนดค่าตารางเวลา:

1. จากแผงระบบหน้าทาง ไปยัง **General (ทั่วไป) > Parental Controls (การควบคุมโดยผู้ปกครอง) > Time Scheduling (การกำหนดตารางเวลา)**
2. จากแผง **Enable Time Scheduling (เปิดทำงานการกำหนดตารางเวลา)** คลิก ON (เปิด)
3. จากคอลัมน์ **Clients Name (ชื่อไคลเอนต์)** เลือกหรือพิมพ์ชื่อไคลเอนต์จากรายการแบบดิ่งลงเข้าไป

หมายเหตุ: นอกจากนี้ คุณยังอาจป้อน MAC แอดเดรสของไคลเอนต์ในคอลัมน์ **Client MAC Address (MAC แอดเดรสของไคลเอนต์)** ก็ได้ ตรวจสอบให้แน่ใจว่าชื่อไคลเอนต์ไม่ได้บรรจุตัวอักษรพิเศษ หรือช่องว่าง เนื่องจากอาจทำให้เราเตอร์ทำงานผิดพลาด

4. คลิก **+** เพื่อเพิ่มโปรไฟล์ของไคลเอนต์
5. คลิก **Apply (นำไปใช้)** เพื่อจัดเก็บการตั้งค่า

3.6 ไฟร์วอลล์

ไวร์เลสเราเตอร์สามารถทำหน้าที่เป็นฮาร์ดแวร์ไฟร์วอลล์สำหรับเครือข่ายของคุณได้

หมายเหตุ: ตามค่าเริ่มต้น คุณสมบัติไฟร์วอลล์จะเปิดทำงาน

3.6.1 ทั่วไป

Firewall

General

Enable the firewall to protect your local area network against attacks from hackers. The firewall filters the incoming and outgoing packets based on the filter rules.
[DoS Protection FAQ](#)

Enable Firewall Yes No

Enable DoS protection Yes No

Logged packets type

Respond ICMP Echo (ping) Request from WAN Yes No

Basic Config

Enable IPv4 inbound firewall rules Yes No

Inbound Firewall Rules (Max Limit : 128)

Source IP	Port Range	Protocol	Add / Delete
<input type="text"/>	<input type="text"/>	TCP	<input type="button" value="⊕"/>
No data in table.			

IPv6 Firewall

All outbound traffic coming from IPv6 hosts on your LAN is allowed, as well as related inbound traffic. Any other inbound traffic must be specifically allowed here.

You can leave the remote IP blank to allow traffic from any remote host. A subnet can also be specified. (2001::1111:2222:3333/64 for example)

Basic Config

Enable IPv6 Firewall Yes No

Famous Server List

Inbound Firewall Rules (Max Limit : 128)

Service Name	Remote IP/CIDR	Local IP	Port Range	Protocol	Add / Delete
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	TCP	<input type="button" value="⊕"/>
No data in table.					

ในการตั้งค่าไฟร์วอลล์พื้นฐาน:

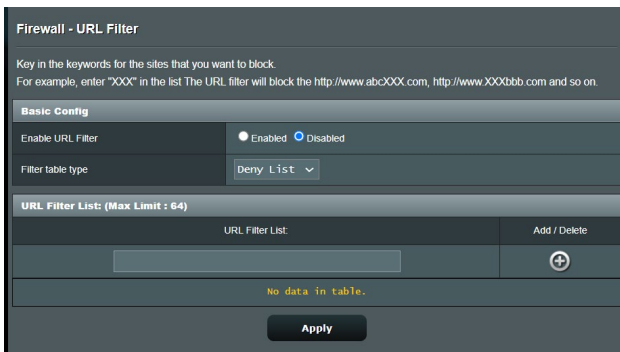
1. จากหน้าดั่งระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง) > Firewall (ไฟร์วอลล์) > General (ทั่วไป)**
2. บนฟิลต์ **Enable Firewall (เปิดทำงานไฟร์วอลล์)**, เลือก **Yes (ใช่)**

3. บนการป้องกัน **Enable DoS (เปิดทำงาน DoS)**, เลือก **Yes (ใช่)** เพื่อป้องกันเครือข่ายของคุณจากการโจมตี DoS (การปฏิเสธบริการ) แมวว่าคุณสมบัตินี้อาจส่งผลกระทบต่อสมรรถนะของเราเตอร์ก็ตาม
4. คุณยังสามารถตรวจสอบแลการแลกเปลี่ยนแพคเกจระหว่างการเชื่อมต่อ LAN และ WAN ได้ด้วย บนชนิดแพคเกจที่บันทึก, เลือก **Dropped (หลุด)**, **Accepted (ยอมรับ)** หรือ **Both (ทั้งคู่)**
5. คลิก **Apply (นำไปใช้)**


3.6.2 ตัวกรอง URL

คุณสามารถระบุคำสำคัญหรือเว็บแอดเดรส เพื่อป้องกันการเข้าถึงยัง URL ที่เจาะจงได้

หมายเหตุ: ตัวกรอง URL เป็นไปตามการสอบถาม DNS ถ้าเน็ตเวิร์กใดเ็นตเข้าถึงเว็บไซต์โดยแล้ว เช่น <http://www.abcxxx.com>, เว็บไซต์จะไม่ถูกบล็อก (DNS แคชในระบบเก็บเว็บไซต์ที่เข้าชมก่อนหน้านี้) ในการแก้ไขปัญหานี้ ใหลาง DNS แคชก่อนที่จะตั้งค่าตัวกรอง URL

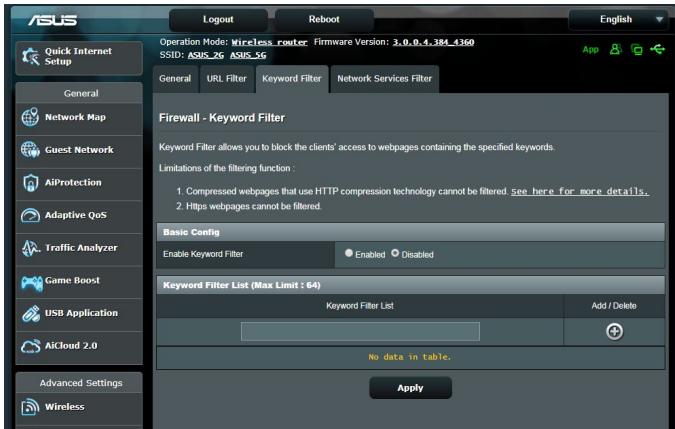


ในการตั้งค่าตัวกรอง URL:

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

3.6.3 ตัวกรองคำสำคัญ

ตัวกรองคำสำคัญจะบล็อกการเข้าถึงไปยังเว็บเพจที่ประกอบด้วยคำสำคัญที่ระบุ



ในการตั้งค่าตัวกรองคำสำคัญ:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง) > Firewall (ไฟร์วอลล์) > 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 ถ้าเน็ตเวิร์กใดคลเ็นต์เข้าถึงเว็บไซต์อยู่แล้ว เช่น <http://www.abcxxx.com>, เว็บไซต์จะไม่ถูกบล็อก (DNS แคชในระบบเก็บเว็บไซต์ที่เขาชมก่อนหน้านี้) ในการแก้ไขปัญหานี้ ให้ล้าง DNS แคชก่อนที่จะตั้งค่าตัวกรองคำสำคัญ
- เว็บเพจที่มีขนาดคิโดยใช้การบีบขนาด HTTP ไม่สามารถถูกกรองได้ เพจ HTTPS ยังไม่สามารถถูกบล็อกโดยใช้ตัวกรองคำสำคัญใดเช่นกัน

3.6.4 ตัวกรองบริการเครือข่าย

ตัวกรองบริการเครือข่าย บล็อกการแลกเปลี่ยนแพคเกจ LAN ไปยัง WAN และจำกัดเน็ตเวิร์กโพลีโคลเอนต์ไม่ให้เข้าถึงยังบริการเว็บไซด์ที่เจาะจง เช่น Telnet หรือ FTP

Firewall - Network Services Filter

The Network Services filter blocks the LAN to WAN packet exchanges and restricts devices from using specific network services. For example, if you do not want the device to use the Internet service, key in 80 in the destination port. The traffic that uses port 80 will be blocked (but https can not be blocked).
Leave the source IP field blank to apply this rule to all LAN devices.

Deny List Duration : During the scheduled duration, clients in the Deny List cannot use the specified network services. After the specified duration, all the clients in LAN can access the specified network services.

Allow List Duration : During the scheduled duration, clients in the Allow List can ONLY use the specified network

NOTE : If you set the subnet for the Allow List, IP addresses outside the subnet will not be able to access the Internet or any Internet service.

Network Services Filter

Enable Network Services Filter Yes No

Filter table type: Deny List

Well-Known Applications: User Defined

Date to Enable LAN to WAN Filter: Mon Tue Wed Thu Fri

Time of Day to Enable LAN to WAN Filter: 00 : 00 - 23 : 59

Date to Enable LAN to WAN Filter: Sat Sun

Time of Day to Enable LAN to WAN Filter: 00 : 00 - 23 : 59

Filtered ICMP packet types: [Empty]


Network Services Filter Table (Max Limit : 32)

Source IP	Port Range	Destination IP	Port Range	Protocol	Add / Delete
				TCP	+

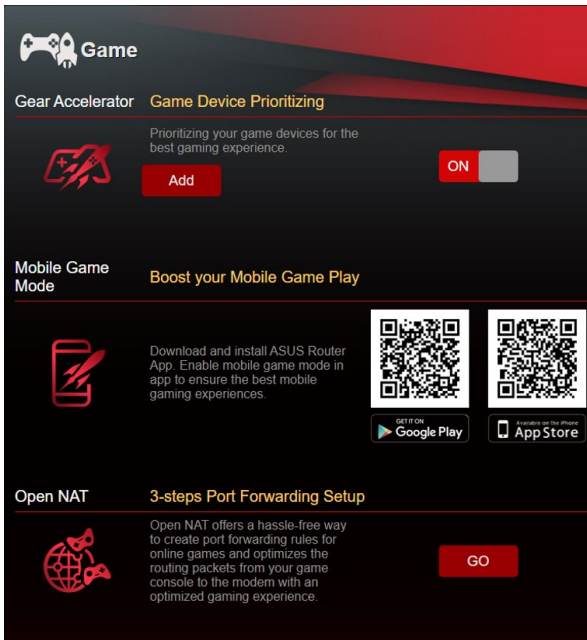
No data in table.

Apply

ในการตั้งค่าตัวกรองบริการเครือข่าย:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง) > Firewall (ไฟร์วอลล์) > Network Service Filter (ตัวกรองบริการเครือข่าย)**
2. บนฟิลด์ **Enable Network Services Filter (เปิดทำงานตัวกรองบริการเครือข่าย)**, เลือก **Yes (ใช่)**
3. เลือกชนิดตารางตัวกรอง **Deny (ปฏิเสธ)**
บล็อกบริการเครือข่ายที่ระบุ **Allow (อนุญาต)**
จำกัดการเข้าถึงไปยังเฉพาะบริการเครือข่ายที่ระบุ
4. ระบุวันที่และเวลาที่ตัวกรองจะแยกที่ฟ
5. ในกฎระบบบริการเครือข่ายไปยังตัวกรอง, ป้อน **Source IP (IP ต้นทาง)**, **Destination IP (IP ปลายทาง)**, **Port Range (ช่วงพอร์ต)** และ **Protocol (โพรโทคอล)** คลิกปุ่ม 
6. คลิก **Apply (นำไปใช้)**


3.7 เกม



3.7.1 Gear Accelerator

Gear Accelerator อนุญาตให้คุณจัดลำดับความสำคัญของอุปกรณ์เกมแบบไร้สาย ผ่านแผงควบคุมออนไลน์สำหรับประสบการณ์การเล่นเกมที่ดียิ่งที่สุด

ในการกำหนดค่า Gear Accelerator:


1. จากหน้าต่างระบบเมนู ไปที่ **General (ทั่วไป) > Game (เกม)**
2. จากแท็บ **Gear Accelerator (ตัวเร่งความเร็วอุปกรณ์)** คลิก **ON (เปิด)**
3. หลังจากที่ใช้การตั้งค่า คลิก **Add (เพิ่ม)** เพื่อเลือกชื่อไอคลเอ็นต์
4. คลิก  เพื่อเพิ่มโปรไฟล์ของไอคลเอ็นต์
5. คลิก **Apply (นำไปใช้)** เพื่อจัดเก็บการตั้งค่า

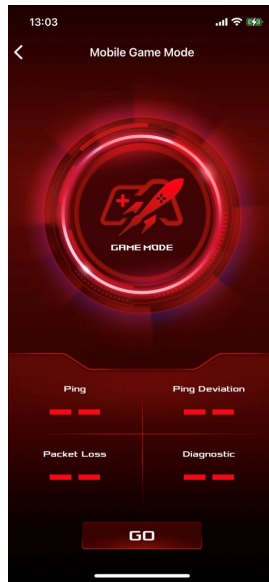
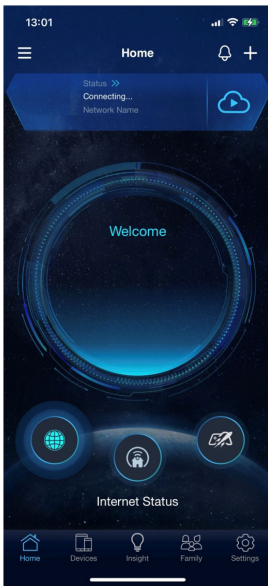
หมายเหตุ: ถ้าคุณต้องการลบโปรไฟล์ของไอคลเอ็นต์ คลิก 

3.7.2 โหมดเกมมือถือ

ดาวน์โหลดแอป ASUS เราเตอร์ บนโทรศัพท์มือถือของคุณ, เปิดใช้งานโหมดเกมมือถือด้วยการคลิกหนึ่งครั้ง เพื่อจัดลำดับความสำคัญของโทรศัพท์มือถือเพื่อให้ได้ประสบการณ์การเล่นเกมออนไลน์ที่ดีที่สุด

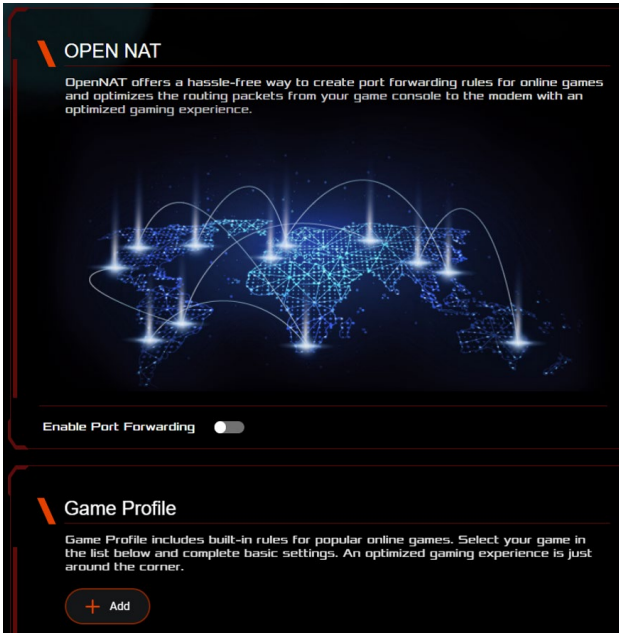
ในการกำหนดค่าโหมดเกมมือถือ

1. ดาวน์โหลดแอป ASUS เราเตอร์ ปฏิบัติตามขั้นตอนที่แนะนำ เพื่อทำการตั้งค่าเครือข่ายไร้สายให้สมบูรณ์
2. จากหน้าหลัก คลิก 
3. คลิก **GO (ไป)** เพื่อกำหนดค่าโหมดเกมมือถือบนโทรศัพท์มือถือของคุณ



3.7.3 ropicpen NAT

ropicpen NAT เป็นวิธีที่ง่ายในการสร้างกฎพอร์ตฟอร์เวิร์ด ดั้งสำหรับเกมออนไลน์ และเพิ่มประสิทธิภาพเราดิ่งแพ็กเก็ตจาก คอนโซลเกมของคุณไปยังโอมเต็ม ซึ่งให้ประสบการณ์การเล่นเกมที่ดีที่สุด



ในการกำหนดค่าropicpen NAT:

1. จากหน้าด่างระบบเมนู ไปที่ **General (ทั่วไป) > Game (เกม)**
2. จากแท็บ **Open NAT (ropicpen NAT)**, คลิก **GO (ไป)**
3. เปิดทำงานพอร์ตฟอร์เวิร์ดดิ่ง
4. จากฟิลต์ **Game Profile (โปรไฟล์เกม)**, คลิก **Add (เพิ่ม)**
5. เลือกเกมของคุณ และทำการดั่งค่าพื้นฐานให้สมบูรณ์
6. คลิก **OK (ตกลง)**

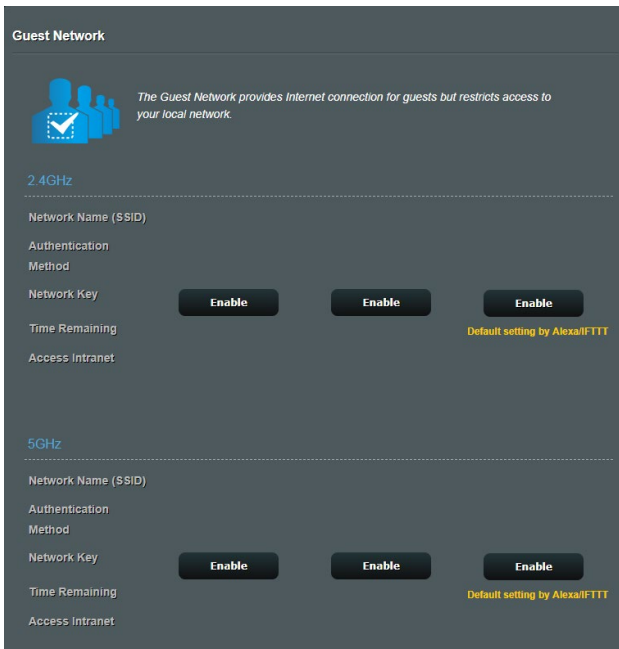
3.8 เครือข่ายแขก

เครือข่ายแขก ใ้ให้การเชื่อมต่ออินเทอร์เน็ตชั่วคราวแก่ผู้มาเยี่ยมชม ผ่านการเข้าถึง SSID หรือเครือข่ายที่แยกกัน โดยไม่ต้องให้การเข้าถึงไปยังเครือข่ายส่วนตัวของคุณ

หมายเหตุ: RT-AX88U PRO สนับสนุน SSID มากถึง 6 ตัว (SSID 2.4GHz 3 ตัว และ 5GHz 3 ตัว)

ในการสร้างเครือข่ายแขกของคุณ:

1. จากหน้าดั่งระบบเมนู ไปยัง **General (ทั่วไป) > Guest Network (เครือข่ายแขก)**
2. บนหน้าจอ Guest Network (เครือข่ายแขก), เลือกแถบความถี่ 2.4GHz หรือ 5GHz สำหรับเครือข่ายแขกที่คุณต้องการสร้าง
3. คลิก **Enable (เปิดทำงาน)**



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

The screenshot shows the 'Guest Network' configuration page. At the top, there is a blue icon of three people with a checkmark and a text box stating: 'The Guest Network provides Internet connection for guests but restricts access to your local network.' Below this, there are two sections for 2.4GHz and 5GHz. Each section has a table of settings and two 'Enable' buttons. The 2.4GHz section has a 'Remove' button below the table. The 5GHz section also has a 'Remove' button below its table. The 'Time Remaining' field in both sections is set to 'Unlimited access' and is noted as a 'Default setting by Alexa/FTT'. The 'Access Intranet' field is set to 'off'.

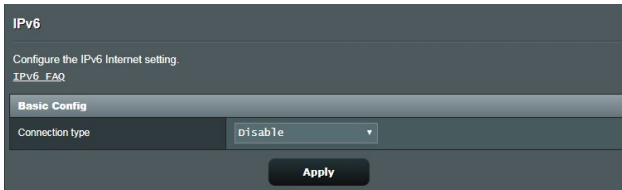
2.4GHz	
Network Name (SSID)	ASUS_2G_Guest
Authentication Method	Open System
Network Key	None
Time Remaining	Unlimited access
Access Intranet	off

5GHz	
Network Name (SSID)	ASUS_5G_Guest
Authentication Method	Open System
Network Key	None
Time Remaining	Unlimited access
Access Intranet	off

5. คลิก **Yes (ใช่)** บนหน้าจอ **Enable Guest Network (เปิดทำงานเครือข่ายแขก)**
6. กำหนดชื่อเครือข่ายไร้สายสำหรับเครือข่ายชั่วคราวของคุณบนฟิลด์ **ชื่อเครือข่าย (SSID)**
7. เลือก **วิธีการยืนยันตัวตน**
8. เลือกวิธี **Encryption (การเข้ารหัส)**
9. ระบุ **เวลาการเข้าถึง** หรือคลิก **Limitless (ไม่จำกัด)**
10. เลือก **Disable (ปิดทำงาน)** หรือ **Enable (เปิดทำงาน)** บนรายการ **Access Intranet (เข้าถึงอินทราเน็ต)**
11. เมื่อทำเสร็จ, คลิก **Apply (นำไปใช้)**

3.9 IPv6

ไวร์เลสเราเตอร์นี้สนับสนุน IPv6 แอดเดรสซิ่ง ซึ่งเป็นระบบที่สนับสนุน IP แอดเดรสมากกว่า มาตรฐานนี้ยังไม่ค่อยใช้กันอย่างกว้างขวาง ติดต่อ ISP ของคุณถ้าบริการอินเทอร์เน็ตของคุณสนับสนุน IPv6



ในการตั้งค่า IPv6:

1. จากหน้าจอรูขุมลับเมนู 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)**

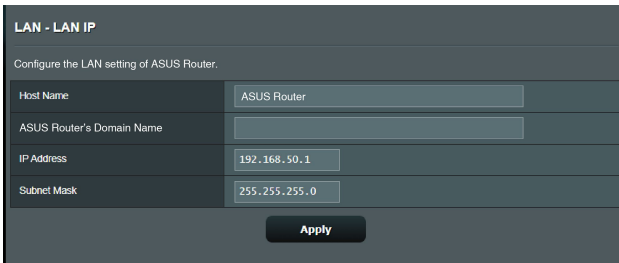
หมายเหตุ: โปรดสอบถาม ISP ของคุณเกี่ยวกับข้อมูล IPv6 เฉพาะสำหรับบริการอินเทอร์เน็ตของคุณ

3.10 LAN

3.10.1 LAN IP

หน้าจอ LAN IP อนุญาตให้คุณแก้ไขการตั้งค่า LAN IP ของไวร์เลสเราเตอร์ของคุณ

หมายเหตุ: การเปลี่ยนแปลงใดๆ ต่อ LAN IP แอดเดรสจะถูกสะท้อนบนการตั้งค่า DHCP



LAN - LAN IP	
Configure the LAN setting of ASUS Router.	
Host Name	ASUS Router
ASUS Router's Domain Name	
IP Address	192.168.50.1
Subnet Mask	255.255.255.0
Apply	

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)**

3.10.2 DHCP เซิร์ฟเวอร์

เราใช้เราเตอร์ของคุณใช้ DHCP เพื่อกำหนด IP แอดเดรสบนเครือข่ายของคุณโดยอัตโนมัติ คุณสามารถระบุช่วง IP แอดเดรสและลิสต์ใหม่ สำหรับไคลเอนต์ต่างๆ บนเครือข่ายของคุณ

LAN - DHCP Server

DHCP (Dynamic Host Configuration Protocol) is a protocol for the automatic configuration used on IP networks. The DHCP server can assign each client an IP address and informs the client of the DNS server IP and default gateway IP. RT-AX88U Pro supports up to 253 IP addresses for your local network.
[Manually Assigned IP around the DHCP list FAQ](#)

Basic Config

Enable the DHCP Server Yes No

RT-AX88U Pro's Domain Name

IP Pool Starting Address

IP Pool Ending Address

Lease time

Default Gateway

DNS and WINS Server Setting

DNS Server 1

DNS Server 2

Advertise router's IP in addition to user-specified DNS Yes No

WINS Server

Manual Assignment

Enable Manual Assignment Yes No

Manually Assigned IP around the DHCP list (Max Limit : 64)

Client Name (MAC Address)	IP Address	DNS Server (Optional)	Host Name (Optional)	Add / Delete
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="⊕"/>

No data in table.

ในการกำหนดค่า DHCP เซิร์ฟเวอร์:

1. จากหน้าตาของระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง) > LAN (แลน) > 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 แอดเดรสใหม่สำหรับเน็ตเวิร์กไคลเอนต์โดยอัตโนมัติ

หมายเหตุ:

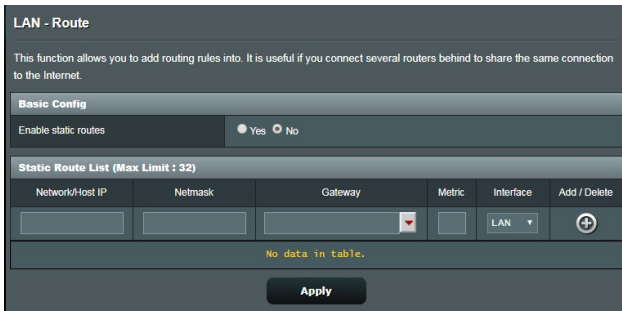
- ASUS แนะนำให้คุณใช้รูปแบบ IP แอดเดรสเป็น 192.168.50.xxx (ซึ่ง xxx สามารถเป็นตัวเลขใดๆ ก็ได้ระหว่าง 2 ถึง 254) ในขณะที่ระบุช่วง IP แอดเดรส
- แอดเดรสเริ่มต้น IP พูล ไม่ควรมีค่ามากกว่าแอดเดรสสิ้นสุด IP พูล

-
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 (เปิดทางการกำหนดด้วยตัวเอง)**, เลือก **Yes (ใช่)** เพื่อกำหนด IP แอดเดรสให้กับ MAC แอดเดรสเฉพาะบนเครือข่าย คุณสามารถเพิ่ม MAC แอดเดรสได้ถึง 32 รายการไปยังรายการ DHCP สำหรับการกำหนดด้วย ตัวเอง

3.10.3 เส้นทาง

ถ้าเครือข่ายของคุณใช้ไวร์เลสเราเตอร์มากกว่าหนึ่งตัว คุณสามารถกำหนดค่าตารางเส้นทาง เพื่อแชร์บริการอินเทอร์เน็ตเดียวกันได้

หมายเหตุ: เราแนะนำให้ท่านอย่าเปลี่ยนการตั้งค่าเส้นทางเริ่มต้น ถ้าคุณไม่มีความรู้ขั้นสูงเกี่ยวกับตารางเส้นทาง



ในการกำหนดค่าตารางเส้นทาง LAN:

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

3.10.4 IPTV

เราเตอร์ของเราสนับสนุนการเชื่อมต่อไปยังบริการ IPTV ผ่าน ISP หรือ LAN IPTV ให้การตั้งค่าที่กำหนดค่าต่างๆ ที่จำเป็นในการตั้งค่า IPTV, VoIP, มัลติคาสต์ และ UDP สำหรับบริการของคุณ ติดต่อ ISP ของคุณ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับบริการของคุณ

LAN - IPTV

To watch IPTV, the WAN port must be connected to the Internet. Please go to [WAN - Dual WAN](#) to confirm that WAN port is assigned to primary WAN.

LAN Port	
Select ISP Profile	None ▾
Choose IPTV STB Port	None ▾

Special Applications	
Use DHCP routes	Microsoft ▾
Enable multicast routing (IGMP Proxy)	Disable ▾
UDP Proxy (Udpxy)	0

Apply

3.11 บันทึกกระบบ

บันทึกกระบบ ประกอบด้วยกิจกรรมต่างๆ ของเครือข่ายที่บันทึกไว้

หมายเหตุ: บันทึกกระบบ รีเซ็ตเมื่อเราเตอร์ถูกบูตใหม่ หรือปิดเครื่อง

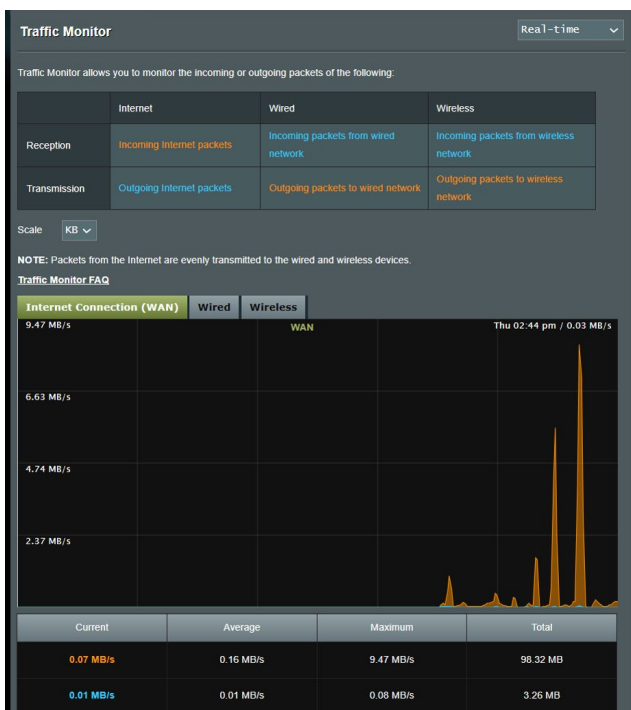
ในการดูบันทึกกระบบของคุณ:

1. จากหน้าตากระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง) > System Log (บันทึกกระบบ)**
2. คุณสามารถดูกิจกรรมเครือข่ายของคุณในแถบเหล่านี้ได้:
 - บันทึกทั่วไป
 - บันทึกไร้สาย
 - DHCP ลีส
 - IPv6
 - ตารางเราตัง
 - พอร์ตฟอว์เวิร์ดตัง
 - การเชื่อมต่อ

The screenshot displays the 'System Log - General Log' interface. At the top, it states 'This page shows the detailed system's activities.' Below this, the 'System Time' is 'Thu, Aug 23 07:15:34 2018' and the 'Uptime' is '0 days 1 hours 18 minute(s) 11 seconds'. There is a 'Remote Log Server' field with an 'Apply' button. The main area contains a list of system events with timestamps and descriptions, such as 'miniupnpd[7139]: version 1.9 started', 'HTTP listening on port 52102', and 'shutting down MiniUPnPd'. At the bottom, there are 'Clear' and 'Save' buttons.

3.12 ตั๋ววิเคราะห์การรับส่งข้อมูล

ฟังก์ชันการตรวจดูแลปริมาณข้อมูล อนุญาตให้คุณเข้าถึงการใช้งาน แบนด์วิดท์ และความเร็วของอินเทอร์เน็ตของทั้งเครือข่ายแบบมีสาย และไร้สายของคุณ โดยฟังก์ชันนี้อนุญาตให้คุณตรวจดูแลการจราจร ของเครือข่ายแบบเรียลไทม์ หรือแบบรายวัน นอกจากนี้ยังมีตัวเลือก ในการแสดงผลการจราจรเครือข่ายภายใน 24 ชั่วโมงล่าสุดด้วย



หมายเหตุ: แพคเก็ตจากอินเทอร์เน็ตถูกส่งไปยังอุปกรณ์มีสายและไร้สายเท่านั้น

3.13 การใช้งานผ่าน USB

ฟังก์ชัน การใช้งานผ่าน USB ให้เมื่อย AiDisk (AiDisk), Servers Center (ศูนย์เซิร์ฟเวอร์), Network Printer Server (เน็ตเวิร์กพรินเตอร์เซิร์ฟเวอร์) และ Download Master (ดาวน์โหลดมาสเตอร์)

สำคัญ! ในการใช้ฟังก์ชันของเซิร์ฟเวอร์ คุณจำเป็นต้องเสียบอุปกรณ์เก็บข้อมูล USB เช่น USB ฮาร์ดดิสก์ หรือ USB แฟลชไดรฟ์ เข้ากับพอร์ต USB 3.0 ที่แผงด้านหลังของไวร์เลสเราเตอร์ของคุณ ตรวจสอบให้แน่ใจว่าอุปกรณ์เก็บข้อมูล USB ได้รับการฟอร์แมตและแบ่งพาร์ติชันอย่างเหมาะสม ดูเว็บไซต์ของ ASUS ที่ <http://event.asus.com/2009/networks/disksupport/> สำหรับตารางระบบไฟล์ที่สนับสนุน

USB Application

To remove the hard disk from the router, click the USB icon at the upper right corner of your screen.

- AiDisk**
Share files in the USB disk through the Internet.
- Servers Center**
Setup the UPnP, iTunes, FTP and Network Place (Samba).
- Network Printer Server**
The network printer server supports two methods:
(1) ASUS EZ printer sharing (2) LPR to share printer.
- 3G/4G**
Switch to USB mode to use a 3G/4G USB wireless dongle or Android phone as a USB modem. [Support](#)
- Time Machine**
Enable Time Machine functionality
- Download Master**
PC-free download manager
Install

3.13.1 การใช้ AiDisk

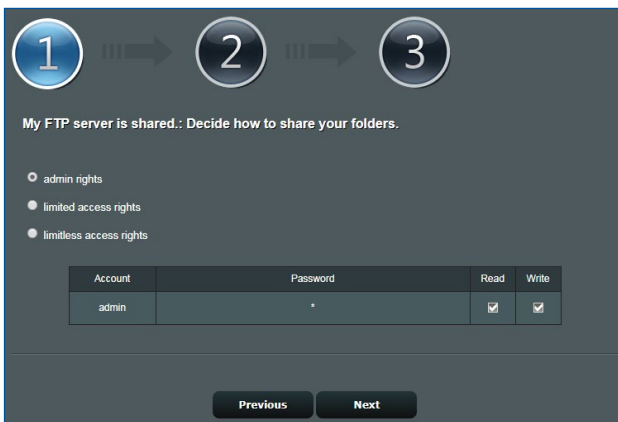
AiDisk ใช้สำหรับแชร์ไฟล์ที่เก็บบนอุปกรณ์ USB ที่เชื่อมต่ออยู่ผ่านอินเทอร์เน็ต นอกจากนี้ AiDisk ยังช่วยคุณในการตั้งค่า ASUS DDNS และ FTP เซิร์ฟเวอร์ด้วย

ในการใช้ AiDisk:

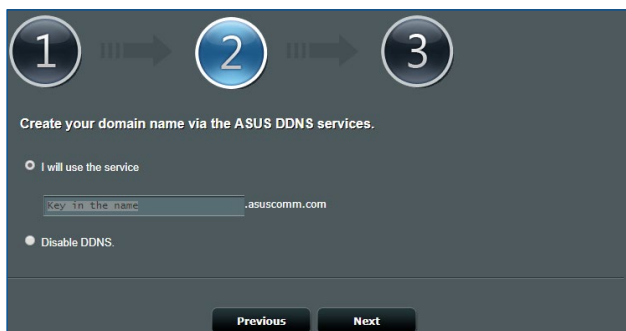
1. จากหน้าต่างระบบเมนูไปที่ **General (ทั่วไป) > USB Application (การใช้งานผ่าน USB)**, จากนั้นคลิกไอคอน AiDisk (AiDisk)
2. จากหน้าจอ Welcome to AiDisk wizard (ยินดีต้อนรับสู่ตัวช่วยสร้าง AiDisk), คลิก **Go (ไป)**



3. เลือกสิทธิ์ในการเข้าถึงที่คุณต้องการกำหนดให้กับไคลเอนต์ที่กำลังเข้าถึงข้อมูลที่แชร์ของคุณ



4. สร้างชื่อโดเมนของคุณผ่านบริการ ASUS DDNS, อ่านเงื่อนไขของบริการ จากนั้นเลือก **I will use the service and accept the Terms of service (ฉันจะใช้บริการและยอมรับในเงื่อนไขของบริการ)** และพิมพ์ชื่อโดเมนของคุณเข้าไป เมื่อทำเสร็จ, คลิก **Next (ถัดไป)**



นอกจากนี้,คุณสามารถเลือก **Skip ASUS DDNS settings (ข้ามการตั้งค่า ASUS DDNS)** จากนั้นคลิก **Next (ถัดไป)** เพื่อข้ามการตั้งค่า DDNS ก็ได้

5. คลิก **Finish (เสร็จ)** เพื่อทำการตั้งค่าให้สมบูรณ์
6. ในการเข้าถึง FTP ไซต์ที่คุณสร้างขึ้น, ให้เปิดเว็บเบราว์เซอร์ หรืออยู่ที่ลิ้น FTP ไคลเอ็นต์ของบริษัทที่สาม และป้อน ftp ลิงค์ (**ftp://<ชื่อโดเมน>.asuscomm.com**) ที่คุณได้สร้างขึ้นมาก่อนหน้า

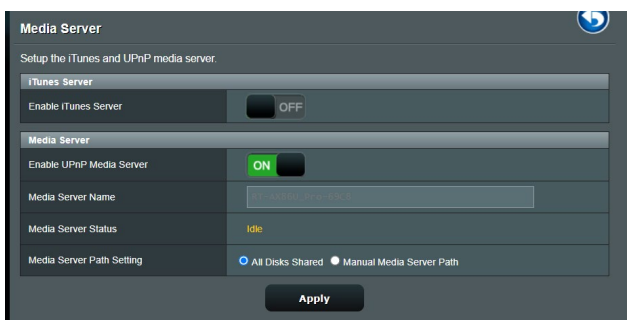
3.13.2 การใช้เซิร์ฟเวอร์เซินเตอร์

เซิร์ฟเวอร์เซินเตอร์ อนุญาตให้คุณแชร์ไฟล์มีเดียจาก USB ดิสก์ผ่านไดเรกทอรี มีเดียเซิร์ฟเวอร์, บริการแชร์มาแชร์ หรือบริการ FTP แชร์ นอกจากนี้ คุณยังสามารถกำหนดค่าการตั้งค่าอื่นๆ สำหรับ USB ดิสก์ในเซิร์ฟเวอร์เซินเตอร์ได้ด้วย

การใช้มีเดียเซิร์ฟเวอร์

ไวร์เลสเราเตอร์ของคุณ อนุญาตให้อุปกรณ์ที่สนับสนุนคุณสมบัติ DLNA สามารถเข้าถึงไฟล์มีเดียมีเดียจาก USB ดิสก์ที่เชื่อมต่ออยู่กับไวร์เลสเราเตอร์ของคุณ

หมายเหตุ: ก่อนที่จะใช้ฟังก์ชัน DLNA มีเดียเซิร์ฟเวอร์, ให้เชื่อมต่ออุปกรณ์ของคุณเข้ากับเครือข่ายของ

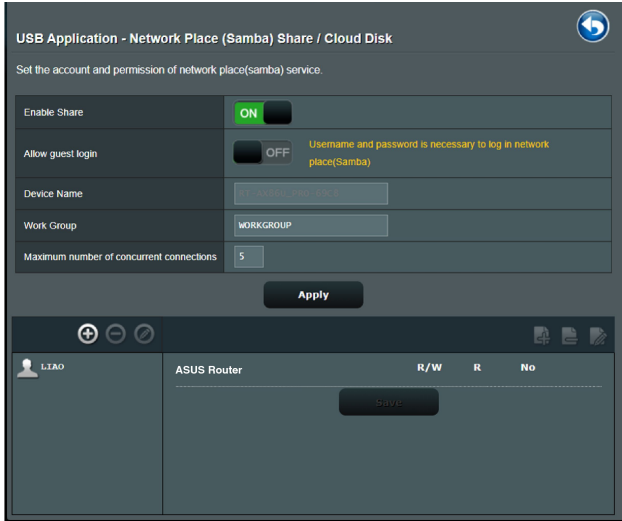


ในการเปิดหน้าการตั้งค่าของมีเดียเซิร์ฟเวอร์ ไปที่ **General (ทั่วไป) > USB Application (การใช้งานผ่าน USB) > Servers Center (ศูนย์เซิร์ฟเวอร์) > Media Server (มีเดียเซิร์ฟเวอร์)**

- **เปิดทำงาน iTunes เซิร์ฟเวอร์:** เลือก เปิด/ปิด เพื่อเปิดทำงาน/ ปิดทำงาน iTunes เซิร์ฟเวอร์
- **เปิดทำงาน UPnP มีเดียเซิร์ฟเวอร์:** เลือก เปิด/ปิด เพื่อเปิดทำงาน/ ปิดทำงาน UPnP มีเดียเซิร์ฟเวอร์
- **สถานะมีเดียเซิร์ฟเวอร์:** แสดงสถานะของมีเดียเซิร์ฟเวอร์
- **Media Server Path Setting (การตั้งค่าพารามิเตอร์มีเดียเซิร์ฟเวอร์):** เลือก All Disks Shared (ดิสก์ทั้งหมดที่แชร์) หรือ Manual Media Server Path (พารามิเตอร์มีเดียเซิร์ฟเวอร์แบบแมนนวล)

การใช้บริการเน็ตเวิร์กเพลส (แชร์มบ้า) แชร์

เน็ตเวิร์กเพลส (แชร์มบ้า) แชร์ อนุญาตให้คุณตั้งค่าบัญชี และการอนุญาตสำหรับบริการแชร์มบ้า




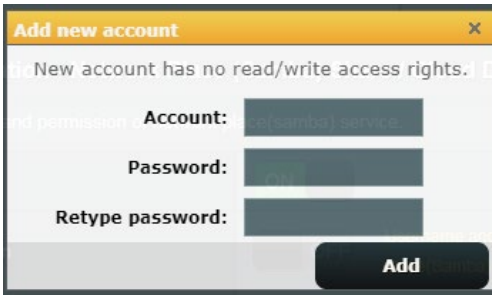
ในการใช้แชร์มบ้าแชร์:

1. จากจากแผงระบบนำทาง ไปที่ **General (ทั่วไป) > USB Application (การใช้งานผ่าน USB) > Servers Center (ศูนย์เซิร์ฟเวอร์) > Network Place (Samba) Share / Cloud Disk (เน็ตเวิร์กเพลส (แชร์มบ้า) แชร์ / คลาวด์ดิสก์)**

หมายเหตุ: เน็ตเวิร์กเพลส (แชร์มบ้า) แชร์ ถูกเปิดทำงานตามค่าเริ่มต้น

2. ปฏิบัติตามขั้นตอนด้านล่าง เพื่อเพิ่ม ลบ หรือแก้ไขบัญชีในการสร้างบัญชีใหม่:

- a) คลิก  เพื่อเพิ่มบัญชีใหม่
- b) ในฟิลด์ **Account (บัญชี)** และ **Password (รหัสผ่าน)**, พิมพ์ชื่อและรหัสผ่านของเน็ตเวิร์กไคลเอนต์ของคุณ, พิมพ์รหัสผ่านซ้ำ เพื่อยืนยัน คลิก **Add (เพิ่ม)** เพื่อเพิ่มบัญชีลงในรายการ

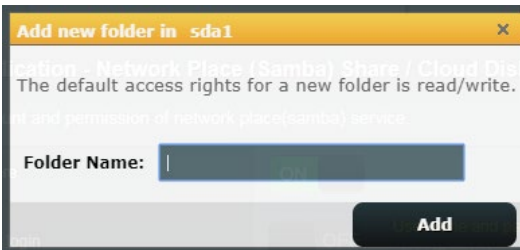


ในการลบบัญชีที่มีอยู่:

- a) เลือกบัญชีที่คุณต้องการลบ
- b) คลิก 
- c) เมื่อระบบถาม, คลิก **Delete (ลบ)** เพื่อยืนยันการลบบัญชี

ในการเพิ่มโฟลเดอร์:

- a) คลิก 
- b) ป้อนชื่อโฟลเดอร์ และคลิก **Add (เพิ่ม)**
โฟลเดอร์ที่คุณสร้างขึ้น จะถูกเพิ่มไปยังรายการโฟลเดอร์



3. จากรายการของโฟลเดอร์, เลือกชนิดของการอนุญาตการเข้าถึงที่คุณต้องการกำหนดสำหรับโฟลเดอร์ที่ต้องการ:

- **R/W:** เลือกตัวเลือกนี้เพื่อกำหนดการเข้าถึงได้ด้วยการอ่าน/เขียน
- **R:** เลือกตัวเลือกนี้เพื่อกำหนดการเข้าถึงได้ด้วยการอ่านเพียงอย่างเดียว
- **No (ไม่):** เลือกตัวเลือกนี้ ถ้าคุณไม่ต้องการแชร์ไฟล์หรือโฟลเดอร์เฉพาะ

4. คลิก **Apply (นำไปใช้)** เพื่อใช้การเปลี่ยนแปลง

การใช้บริการ FTP แชร์

FTP แชร์ เปิดทำงานให้ FTP แชร์ไฟล์จาก USB ดิสก์ไปยังอุปกรณ์อื่น ๆ ผ่านเครือข่ายแลนของคุณ หรือผ่านอินเทอร์เน็ต

สำคัญ:

- ให้แน่ใจว่าคุณถอด USB ดิสก์อย่างปลอดภัย การถอด USB ดิสก์อย่างไม่ถูกต้อง อาจทำให้ข้อมูลเสียหายได้
- ในการถอด USB ดิสก์อย่างปลอดภัย ให้ดูส่วน การถอด USB ดิสก์อย่างปลอดภัย ภายใต **3.1.3 การตรวจสอบแลอุปกรณ์ USB ของคุณ**

USB Application - FTP Share

Set the account and permission of FTP service.

Enable FTP	<input type="checkbox"/> OFF
Enable WAN access	<input type="checkbox"/> OFF
Allow anonymous login	<input type="checkbox"/> OFF Username and password is necessary to log in FTP service.
Enable TLS support	<input checked="" type="radio"/> Yes <input type="radio"/> No
Maximum number of concurrent connections	5
Character set on FTP Server	UTF-8

Apply

LIAO	A8878A175D4A6FD54D2E6 BD6195DB5EF7.asuscomm. com	R/W	W	R	No
------	--	-----	---	---	----

Save

ในการใช้บริการ FTP แชร์:

หมายเหตุ: ตรวจสอบให้แน่ใจว่าคุณตั้งค่า FTP เซิร์ฟเวอร์ของคุณผ่าน AiDisk สำหรับรายละเอียดเพิ่มเติม ในดูส่วน 3.13.1 การใช้ AiDisk

1. จากหน้าต่างระบบเมนู คลิก **General (ทั่วไป) > USB application (การใช้งานผ่าน USB) > Servers Center (ศูนย์เซิร์ฟเวอร์) > FTP Share (FTP แชร์)**
2. จากรายการของโฟลเดอร์, เลือกชนิดของการอนุญาตการเข้าถึงที่คุณต้องการกำหนดสำหรับโฟลเดอร์ที่ต้องการ:
 - **R/W:** เลือกเพื่อกำหนดให้สามารถเข้าถึงด้วยการอ่าน/เขียนสำหรับโฟลเดอร์เฉพาะ
 - **W;** เลือกเพื่อกำหนดให้สามารถเข้าถึงด้วยการเขียนได้ อย่างเดียวสำหรับโฟลเดอร์เฉพาะ
 - **R;** เลือกเพื่อกำหนดให้สามารถเข้าถึงด้วยการอ่านได้ อย่างเดียวสำหรับโฟลเดอร์เฉพาะ
 - **No (ไม่):** เลือกตัวเลือกนี้ ถ้าคุณไม่ต้องการแชร์ไฟล์หรือโฟลเดอร์เฉพาะ
3. คลิก **Apply (นำไปใช้)** เพื่อยืนยันการเปลี่ยนแปลง
4. ในการเข้าถึง FTP เซิร์ฟเวอร์, ให้ป้อน ftp ลิงค์ **ftp://<ชื่อโฮสต์>.asuscomm.com** และชื่อผู้ใช้และรหัสผ่านของคุณบนเว็บเบราว์เซอร์ หรืออยู่ที่ลิต์ FTP ของบริษัทที่สาม

3.13.3 3G/4G

โมเด็ม USB 3G/4G สามารถใช้เชื่อมต่อไปยัง RT-AX88U PRO เพื่ออนุญาตให้เข้าถึงอินเทอร์เน็ตได้

หมายเหตุ: สำหรับรายการของโมเด็ม USB ที่ได้รับการรับรอง โปรดเยี่ยมชมที่:

<http://event.asus.com/2009/networks/3gsupport/>

USB Modem / USB Tethering

Switch to USB mode to use a 3G/4G USB wireless dongle or Android phone as a USB modem.

Basic Config

Enable USB Mode	<input checked="" type="checkbox"/> ON
Select USB Device	Auto
APN Configuration	Auto
Telecommunications Standards	WCDMA (UMTS) / LTE
APN Service(optional)	internet
Dial Number	*99#
Username	
Password	
Authentication	None
PIN code	
USB Adapter	Auto
USB MTU	0

Special Requirement from ISP

Extend the TTL value	<input type="radio"/> Yes <input checked="" type="radio"/> No
Spoof LAN TTL value	<input type="radio"/> Yes <input checked="" type="radio"/> No

ในการตั้งค่าการเข้าถึงอินเทอร์เน็ต 3G/4G:

1. จากหน้าต่างระบบเมนู คลิก **General (ทั่วไป) > USB application (การใช้งาน USB) > 3G/4G**
2. ในฟิลด์ **Enable USB Modem (เปิดทำงานโมเด็ม USB)**, เลือก **Yes (ใช่)**
3. ตั้งค่าข้อมูลต่อไปนี้:
 - **Location (สถานที่):** เลือกสถานที่ของผู้ให้บริการ 3G/4G ของคุณจากรายการแบบดิ่งลง
 - **ISP (ISP):** เลือกผู้ให้บริการอินเทอร์เน็ต (ISP) ของคุณจากรายการแบบดิ่งลง
 - **บริการ APN (ชื่อชุดเชื่อมต่อ) (ใส่หรือไม่ก็ได้):** ติดต่อผู้ให้บริการ 3G/4G ของคุณสำหรับข้อมูลอย่างละเอียด
 - **หมายเลขโทรและรหัส PIN:** หมายเลขการเข้าถึงของผู้ให้บริการ 3G/4G และรหัส PIN สำหรับการเชื่อมต่อ

หมายเหตุ: รหัส PIN อาจแตกต่างกันในผู้ให้บริการรายต่างๆ

- **ชื่อผู้ใช้ / รหัสผ่าน:** ผู้ให้บริการเครือข่าย 3G/4G ของคุณจะให้ชื่อผู้ใช้และรหัสผ่านแก่คุณ
 - **อะแดปเตอร์ USB:** เลือกอะแดปเตอร์ USB 3G / 4G จากรายการแบบดิ่งลง ถ้าคุณไม่แน่ใจถึงรุ่นของอะแดปเตอร์ USB ของคุณ หรือรุ่นของคุณไม่ได้อยู่ในรายการตัวเลือก ให้เลือก **Auto (อัตโนมัติ)**
4. คลิก **Apply (นำไปใช้)**

หมายเหตุ: เราเตอร์จะบูตใหม่เพื่อให้การตั้งค่ามีผล

3.14 WAN

3.14.1 การเชื่อมต่ออินเทอร์เน็ต

หน้าจอ Internet Connection (การเชื่อมต่ออินเทอร์เน็ต) อนุญาตให้คุณกำหนดค่าการตั้งค่าต่างๆ ของชนิดการเชื่อมต่อ WAN ที่หลากหลาย

WAN - Internet Connection

ASUS Router supports several connection types to WAN (wide area network). These types are selected from the dropdown menu beside WAN Connection Type. The setting fields differ depending on the connection type you selected.

Configure the Ethernet WAN settings of ASUS Router.

Basic Config

WAN Connection Type:

Enable WAN: Yes No

Enable NAT: Yes No

Enable UPnP: Yes No

Enable WAN Aggregation: Yes No
WAN Aggregation combines two network connections to increase your WAN speed up to 2Gbps. Connect your router's WAN port and LAN 4 port to your modem's LAN ports (ensure you use two cables with the same specification) [WAN Aggregation FAQ](#)

WAN DNS Setting

DNS Server:

Assign a DNS service to improve security, block advertisement and gain faster performance.

Forward local domain queries to upstream DNS: Yes No

Enable DNS Rebind protection: Yes No

Enable DNSSEC support: Yes No

Prevent client auto DoH:

DNS Privacy Protocol:

DHCP Option

Class Identifier (Option 60):

Client Identifier (Option 61): IAID/DUID

Class Identifier (Option 60):

Client Identifier (Option 61): IAID/DUID

Account Settings

Authentication:

PPP Echo Interval:

PPP Echo Max Failures:

Special Requirement from ISP

Host Name:

MAC Address:

DHCP query frequency:

Extend the TTL value: Yes No

Spoof LAN TTL value: Yes No

ในการกำหนดค่าการตั้งค่าการเชื่อมต่อ WAN:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings** (การตั้งค่าขั้นสูง) > **WAN (WAN)** > **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 ของคุณถ้าเราเตอร์ไม่สามารถ รับ IP แอดเดรสที่ถูกต้อง หรือถ้าคุณไม่แน่ใจถึงชนิดการเชื่อมต่อ WAN
 - **เปิดทำงาน WAN:** เลือก **Yes (ใช่)** เพื่ออนุญาตให้เราเตอร์ เข้าถึงอินเทอร์เน็ต เลือก **No (ไม่)** เพื่อปิดทำงานการเข้าถึง อินเทอร์เน็ต
 - **เปิดทำงาน NAT:** NAT (การแปลเน็ตเวิร์กแอดเดรส) เป็นระบบซึ่ง IP สาธารณะ (WAN IP) หนึ่งตัวถูกใช้ เพื่อให้การเข้าถึงอินเทอร์เน็ตแก่เน็ตเวิร์กไคลเอ็นต์ที่มี IP แอดเดรสส่วนตัวใน LAN IP แอดเดรสส่วนตัวของเน็ตเวิร์กไคล เอ็นต์แต่ละตัวถูกบันทึกในตาราง NAT และถูกใช้เพื่อเปลี่ยน เส้นทางแพคเกจข้อมูลของเขา
 - **เปิดทำงาน UPnP:** UPnP (พลังเอนด์เพลย์สากล) อนุญาตให้คุณควบคุมอุปกรณ์หลายชนิด (เช่น เราเตอร์, โทรทัศน์, ระบบสเตอริโอ, เกมคอนโซล, โทรศัพท์เซลลูลาร์) ผ่านเครือข่ายที่ใช้ IP โดยมีหรือไม่มี การควบคุมจากศูนย์กลาง ผ่านเกตเวย์ก็ได้ UPnP เชื่อมต่อ PC ทุกรูปแบบ โดยให้เครือข่าย ที่ไร้รอยต่อสำหรับการกำหนดค่าจากระยะไกล และการถ่าย โอนข้อมูล เมื่อใช้ UPnP, อุปกรณ์เครือข่ายใหม่จะถูกค้นพบ โดยอัตโนมัติ หลังจากที่เชื่อมต่อไปยังเครือข่ายแล้ว, อุปกรณ์สามารถถูกกำหนดค่าจากระยะไกลเพื่อสนับสนุนแอปพลิเคชัน P2P, เกมอินเทอร์เน็ตแอกทีฟ, การประชุมผ่านวิดีโอ และเว็บหรือพริ๊งค์เฟิร์เวอร์ใด ๆ ไม่เหมือนกับพอร์ตฟอเวิร์ดดิ้ง ซึ่ง เกี่ยวข้องกับการกำหนดค่าการตั้งค่าพอร์ตด้วยตัวเอง, UPnP จะกำหนดค่าเราเตอร์โดยอัตโนมัติ เพื่อให้เราเตอร์ยอมรับการเชื่อมต่อของเขา และส่งค่าขอไปยัง PC ที่เจาะจงบนเครือข่ายแลน โดยตรง

- **เปิดใช้งานการรวม WAN:** การรวม WAN รวมการเชื่อมต่อเครือข่ายสองแหล่งเข้าด้วยกัน เพื่อเพิ่มความเร็ว WAN ของคุณจนถึง 2 Gbps เชื่อมต่อพอร์ต WAN และพอร์ต LAN 4 ของเราเตอร์ของคุณ ไปยังพอร์ต LAN ของโมเด็มของคุณ
- **เชื่อมต่อไปยัง DNS เซิร์ฟเวอร์:** อนุญาตให้เราเตอร์รับ DNS IP แอดเดรสจาก ISP โดยอัตโนมัติ DNS เป็นโพรโตคอลอินเทอร์เน็ต ซึ่งแปลงชื่ออินเทอร์เน็ตไปยัง IP แอดเดรสที่เป็นตัวเลข
- **การยืนยันตัวบุคคล:** รายการนี้อาจถูกกำหนดโดย ISP บางแห่ง ตรวจสอบกับ ISP ของคุณ และกรอกข้อมูลลงไป ถ้าจำเป็น
- **ข้อโหวต:** พิลัดนี้อนุญาตให้คุณใส่ข้อโหวตสำหรับเราเตอร์ของคุณ โดยปกติเป็นความต้องการพิเศษจาก ISP ของคุณ ถ้า ISP ของคุณกำหนดข้อโหวตให้กับคอมพิวเตอร์ของคุณ ให้ป้อนข้อโหวตที่นี่
- **MAC แอดเดรส:** MAC (การควบคุมการเข้าถึงมีเดีย) แอดเดรส เป็นหมายเลขระบุที่ไม่ซ้ำกัน สำหรับอุปกรณ์เครือข่ายของคุณ ISP บางแห่งตรวจสอบ MAC แอดเดรสของอุปกรณ์เครือข่าย ซึ่งเชื่อมต่อไปยังบริการของบริษัท และปฏิเสธอุปกรณ์ที่ไม่รู้จักที่พยายามเชื่อมต่อเข้ามา เพื่อหลีกเลี่ยงปัญหาในการเชื่อมต่อเนื่องจาก MAC แอดเดรสที่ไม่ได้ลงทะเบียน คุณสามารถ:
 - ติดต่อ ISP ของคุณและอัปเดต MAC แอดเดรสที่เชื่อมโยงกับบริการของ ISP ของคุณ
 - โคลน หรือเปลี่ยนแปลง MAC แอดเดรสของ ASUS ไร้สายเราเตอร์ เพื่อให้ตรงกับ MAC แอดเดรสของอุปกรณ์เครือข่ายก่อนหน้า ISP รู้จัก

3.14.2 ดูอัล WAN

ดูอัล WAN อนุญาตให้คุณเลือกการเชื่อมต่อ ISP สองแหล่งไปยังเราเตอร์ของคุณ ซึ่งคือ WAN หลักและ WAN รอง

ในการกำหนดค่าดูอัล WAN:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง) > WAN**
2. ไปที่ฟิลด์ **Dual WAN (ดูอัล WAN)**, เลือก **ON (เปิด)**
3. เลือก **Primary WAN (WAN หลัก)** และ **Secondary WAN (WAN รอง)** ของคุณ ตัวเลือกที่ใช้ได้มี WAN, USB, อีเทอร์เน็ต LAN และ 2.5G WAN
4. เลือก **Fail Over (เฟลโอเวอร์)** หรือ **Load Balance (โหลดบาลานซ์)**
5. คลิก **Apply (นำไปใช้)**

หมายเหตุ: คำอธิบายอย่างละเอียดมีอยู่ที่ FAQ บนเว็บไซต์สนับสนุนของ ASUS ที่ <https://www.asus.com/support/FAQ/1011719>

WAN - Dual WAN

ASUS Router provides Dual WAN support. Select Failover mode to use a secondary WAN for backup network access. Select Load Balance mode to optimize bandwidth, maximize throughput, minimize response time, and prevent data overload for both WAN connections. [Dual WAN FAQ](#)

To enable WAN Aggregation go to the [WAN/Internet Connection page](#)

Basic Config

Enable Dual WAN	<input type="checkbox"/> OFF
Primary WAN	1G WAN ▾
Auto USB Backup WAN	<input checked="" type="radio"/> Yes <input type="radio"/> No

Auto Network Detection

Detailed explanations are available on the [ASUS Support Site FAQ](#), which may help you use this function effectively.

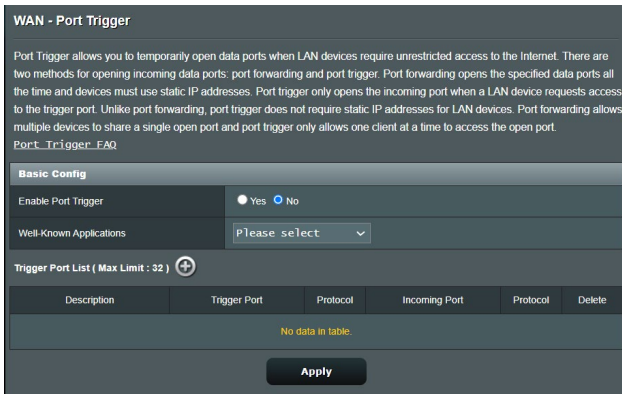
Detect Interval	Every <input type="text" value="3"/> seconds
Internet Connection Diagnosis	When the current WAN fails <input type="text" value="2"/> continuous times, it is deemed a disconnection.
Network Monitoring	<input checked="" type="checkbox"/> DNS Query <input checked="" type="checkbox"/> Ping

Apply

3.14.3 พอร์ตทริกเกอร์

ช่วงพอร์ตทริกเกอร์จะเปิดพอร์ตขาเข้าที่ไม่ได้กำหนดเป็นช่วงเวลาที่จำกัด เมื่อใดก็ตามที่ไคลเอนต์บนเครือข่ายแลนทำการเชื่อมต่อขาออกไปยังพอร์ตที่ระบุ พอร์ตทริกเกอร์จะถูกใช้ในสถานการณ์ต่อไปนี้:

- มีไคลเอนต์ท้องถิ่นมากกว่าหนึ่งเครื่องจำเป็นต้องส่งต่อพอร์ตสำหรับการใช้งานเดียวกันในเวลาที่แตกต่างกัน
- การใช้งานต้องการให้มีพอร์ตขาเข้าเฉพาะที่แตกต่างจากพอร์ตขาออก



ในการตั้งค่าพอร์ตทริกเกอร์:

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

- **ทริกเกอร์พอร์ต:** ระบบทริกเกอร์พอร์ตเพื่อเปิดพอร์ตขาเข้า
- **โปรโตคอล:** เลือกโปรโตคอล, TCP หรือ UDP
- **พอร์ตขาเข้า:** ระบบพอร์ตขาเข้าเพื่อรับข้อมูลขาเข้าจากอินเทอร์เน็ต

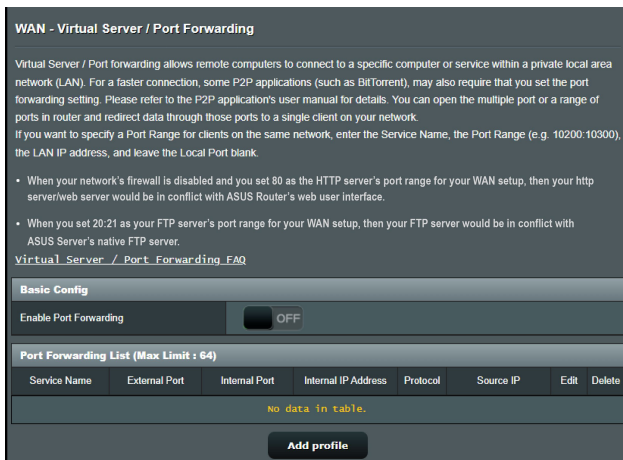
หมายเหตุ:

- ในขณะที่เชื่อมต่อไปยัง IRC เซิร์ฟเวอร์, โคลเอ็นต์ PC ทำการเชื่อมต่อขาออกโดยใช้ช่วงพอร์ตทริกเกอร์ 66660-7000 IRC เซิร์ฟเวอร์ตอบสนองโดยการตรวจสอบข้อมูลผู้ใช้ และสร้างการเชื่อมต่อใหม่ไปยังโคลเอ็นต์ PC โดยใช้พอร์ตขาเข้า
 - ถ้า พอร์ตทริกเกอร์ ถูกปิดทำงาน, เราเตอร์จะตัดการเชื่อมต่อ เนื่องจากไม่สามารถหา PC เครื่องใดที่กำลังขอการเข้าถึง IRC อยู่ เมื่อพอร์ตทริกเกอร์ เปิดทำงาน, เราเตอร์จะกำหนดพอร์ตขาเข้า เพื่อรับข้อมูลขาเข้า พอร์ตขาเข้านี้จะปิดหลังจากถึงช่วงเวลาที่กำหนด เนื่องจากเราเตอร์ไม่แน่ใจว่าเมื่อใดที่แอปพลิเคชันสิ้นสุดการทำงาน
 - พอร์ตทริกเกอร์จริง อนุญาตโคลเอ็นต์เพียงหนึ่งเครื่องในเครือข่ายให้ใช้บริการที่เจาะจง และพอร์ตขาเข้าที่เจาะจงในเวลาเดียวกัน
 - คุณไม่สามารถใช้แอปพลิเคชันเดียวกันเพื่อทริกเกอร์พอร์ตใน PC มากกว่าหนึ่งเครื่องในเวลาเดียวกันได้ เราเตอร์จะส่งต่อพอร์ตกลับไปยังคอมพิวเตอร์เครื่องล่าสุดที่ส่งคำขอ/ทริกเกอร์ไปให้เราเตอร์เท่านั้น
-

3.14.4 เวอร์ชวลเซิร์ฟเวอร์/พอร์ตฟอร์เวิร์ดดิ้ง

พอร์ตฟอร์เวิร์ดดิ้ง เป็นวิธีการเพื่อเปลี่ยนเส้นทางการจราจรเครือข่ายจากอินเทอร์เน็ตไปยังพอร์ตที่เจาะจง หรือช่วงพอร์ตที่เจาะจงไปยังอุปกรณ์บนเครือข่ายแลนของคุณ การตั้งค่าพอร์ตฟอร์เวิร์ดดิ้งบนเราเตอร์ของคุณ อนุญาตให้ PC ที่อยู่นอกเครือข่ายเข้าถึงบริการที่เจาะจงที่มีให้โดย PC ในเครือข่ายของคุณได้

หมายเหตุ: เมื่อพอร์ตฟอร์เวิร์ดดิ้งเปิดทำงาน, ASUS เราเตอร์จะบล็อกการจราจรขาเข้าที่ไม่พึงประสงค์จากอินเทอร์เน็ต และอนุญาตเฉพาะการตอบกลับจากคำขอขาออกจาก LAN เท่านั้น เน็ตเวิร์กโคลเอนด์ไม่สามารถเข้าถึงอินเทอร์เน็ตได้โดยตรง รวมทั้งในทางกลับกันด้วย



ในการตั้งค่าการส่งต่อพอร์ต:

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

2. กำหนดค่าการตั้งค่าต่อไปนี้ดังแสดงด้านล่าง: เมื่อทำเสร็จ, คลิก ON (เปิด)

- **เปิดทำงานพอร์ตพอร์เตอร์ดิ่ง:** เลือก ON (เปิด) เพื่อเปิดใช้งานพอร์ตพอร์เตอร์ดิ่ง
- **รายการเซิร์ฟเวอร์ที่มีชื่อเสียง:** หาชนิดของบริการที่คุณต้องการเข้าถึง
- **รายการเกมที่มีชื่อเสียง:** รายการนี้แสดงพอร์ตที่ต้องการสำหรับเกมออนไลน์ที่เป็นที่นิยมเพื่อให้ทำงานอย่างถูกต้อง
- **FTP เซิร์ฟเวอร์พอร์ต:** หลีกเลี่ยงการกำหนดช่วงพอร์ต 20:21 สำหรับ FTP เซิร์ฟเวอร์ของคุณ เนื่องจากการทำเช่นนี้จะทำให้เกิดข้อขัดแย้งกับการกำหนดเนทีฟ FTP เซิร์ฟเวอร์ของเราเตอร์
- **ข้อบริการ:** ป้อนข้อบริการ
- **ช่วงพอร์ต:** ถ้าคุณต้องการระบุช่วงพอร์ตสำหรับไคลเอนต์บนเครือข่ายเดียวกัน, ป้อน Service Name (ข้อบริการ), 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 พอร์ตที่เจาะจงสามารถถูกใช้โดยแอปพลิเคชันหรือบริการใดๆได้ในแต่ละขณะเวลา ดังนั้น การที่ PC สองตัวพยายามเข้าถึงข้อมูลผ่านพอร์ตเดียวกันในเวลาเดียวกันก็อาจทำให้การทำงานล้มเหลว ตัวอย่างเช่น คุณไม่สามารถตั้งค่าพอร์ตพอร์เตอร์ดิ่ง สำหรับพอร์ต 100 สำหรับ PC สองเครื่องในเวลาเดียวกันได้

- **โกลบอล IP:** ป้อน LAN IP แอดเดรสของโพลีเน็ต

หมายเหตุ: ใช้สวิตช์ IP แอดเดรสสำหรับโพลีเน็ตท้องถิ่น เพื่อให้พอร์ตฟอว์เวิร์ดทำงานอย่างเหมาะสม สำหรับข้อมูล ใหญ่ส่วน **3.10 LAN**

- **โกลบอลพอร์ต:** ป้อนพอร์ตที่เจาะจง เพื่อรับแพคเกจที่ส่งต่อมาจากปลายฟิลต์นี้ให้วางไว้ ถ้าคุณต้องการแพคเกจเข้าให้ถูกเปลี่ยนเส้นทางไปยังช่วงพอร์ตที่ระบุ
- **โปรโตคอล:** เลือกโปรโตคอล ถ้าคุณไม่แน่ใจ เลือก **BOTH (ทั้งคู่)**

ในการตรวจสอบว่าพอร์ตฟอว์เวิร์ดดังกล่าวที่กำหนดค่าสำเร็จหรือไม่:

- ให้แน่ใจว่าเซิร์ฟเวอร์หรือแอปพลิเคชันของคุณถูกตั้งค่าแล้ว และกำลังรันอยู่
- คุณจำเป็นต้องให้โพลีเน็ตอยู่นอก LAN ของคุณแต่มีการเข้าถึงอินเทอร์เน็ต (เรียกว่า “อินเทอร์เน็ตโพลีเน็ต”) โพลีเน็ตนี้ไม่ควรเชื่อมต่อกับ ASUS เราเตอร์
- บนอินเทอร์เน็ตโพลีเน็ต, ใช้ WAN IP ของเราเตอร์ เพื่อเข้าถึงเซิร์ฟเวอร์ ถ้าพอร์ตฟอว์เวิร์ดดังกล่าวที่กำหนดค่าสำเร็จ, คุณควรสามารถเข้าถึงไฟล์หรือแอปพลิเคชันได้

ความแตกต่างระหว่างพอร์ตทริกเกอร์ และพอร์ตฟอว์เวิร์ด:

- พอร์ตทริกเกอร์จะทำงานแม้ว่าไม่มีการตั้งค่า LAN IP แอดเดรสที่เฉพาะเจาะจง ไม่เหมือนกับพอร์ตฟอว์เวิร์ดซึ่งจำเป็นต้องมีสวิตช์ LAN IP แอดเดรส, พอร์ตทริกเกอร์อนุญาตให้ส่งต่อพอร์ตแบบใดนามักโดยใช้เราเตอร์ได้ ช่วงพอร์ตที่กำหนดไว้ล่วงหน้า ถูกกำหนดค่าเพื่อให้ยอมรับการเชื่อมต่อขาเข้าภายในช่วงระยะเวลาที่จำกัด พอร์ตทริกเกอร์อนุญาตให้คอมพิวเตอร์หลายเครื่องรันแอปพลิเคชันที่โดยปกติอาจต้องการให้ส่งต่อพอร์ตเดียวกันไปยัง PC แต่ละเครื่องบนเครือข่ายด้วยตัวเอง
- พอร์ตทริกเกอร์มีความปลอดภัยมากกว่าพอร์ตฟอว์เวิร์ดเนื่องจากพอร์ตขาเข้าไม่ได้เปิดตลอดเวลา พอร์ตเหล่านั้นเปิดเฉพาะเมื่อแอปพลิเคชันทำการเชื่อมต่อขาออกผ่านทริกเกอร์พอร์ตเท่านั้น

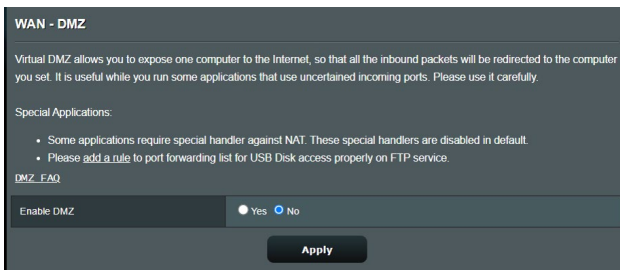
3.14.5 DMZ

เวอรัล DMZ เปิดเผยโคลเอ็นต์หนึ่งเครื่องไปยังอินเทอร์เน็ต ทำให้โคลเอ็นต์นี้รับแพคเกจเข้าทั้งหมดโดยตรงไปยังเครือข่ายแลนของคุณ

โดยปกติ การจราจรเข้าจากอินเทอร์เน็ตถูกทิ้งและเปลี่ยนเส้นทางไปยังโคลเอ็นต์ที่เจาะจงเฉพาะเมื่อพอร์ตฟอร์เวิร์ดตั้ง หรือพอร์ตทริกเกอร์ถูกกำหนดไว้ในเครือข่าย ในการกำหนดค่า DMZ, เน็ตเวิร์กโคลเอ็นต์หนึ่งเครื่องจะรับแพคเกจเข้าทั้งหมด

การตั้งค่า DMZ บนเครือข่ายมีประโยชน์เมื่อคุณต้องการให้พอร์ตขาเข้าเปิด หรือเมื่อคุณต้องการโฮสต์โดเมน เว็บ หรืออีเมล เซิร์ฟเวอร์

ข้อควรระวัง: การเปิดพอร์ตทั้งหมดบนโคลเอ็นต์ไปยังอินเทอร์เน็ต ทำให้เครือข่ายอ่อนแอต่อการโจมตีภายนอก โปรดระมัดระวังความเสี่ยงด้านความปลอดภัยที่เกี่ยวข้องกับการใช้ DMZ



ในการตั้งค่า DMZ:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง) > WAN (WAN) > DMZ (DMZ)**
2. กำหนดค่าการตั้งค่าด้านล่าง: เมื่อทำเสร็จ, คลิก **Apply (นำไปใช้)**
 - **IP แอดเดรสของสถานที่เปิดออก:** บัณฑิต LAN IP แอดเดรสของโคลเอ็นต์ที่จะให้บริการ DMZ และถูกเปิดออกบนอินเทอร์เน็ต ตรวจสอบให้แน่ใจว่าเซิร์ฟเวอร์โคลเอ็นต์มีสแตติก IP แอดเดรส

ในการลบ DMZ:

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

3.14.6 DDNS

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

WAN - DDNS

DDNS (Dynamic Domain Name System) is a service that allows network clients to connect to the wireless router, even with a dynamic public IP address, through its registered domain name. The wireless router is embedded with the ASUS DDNS service and other DDNS services.

If you cannot use ASUS DDNS services, please go to <https://iplookup.asus.com/nslookup.php> to reach your internet IP address to use this service.

The wireless router currently uses a private WAN IP address.
This router may be in the multiple-NAT environment and DDNS service cannot work in this environment.

The host name is successfully registered. You can use "[hostname].asuscomm.com" to access the service in home network from WAN. Use "[hostname].asuscomm.com" to remotely access your network.
Go to Advanced Settings > WAN to configure the port forwarding or DMZ settings to allow other WAN clients to remotely access your network.
If you want to remotely configure the wireless router, go to [here](#).

Enable the DDNS Client	<input checked="" type="radio"/> Yes <input type="radio"/> No
Server	WAN.ASUS.COM <input type="button" value="Deregister"/>
Host Name	A8878A175D4A6F054D2E6BD6195D85EF7.asuscomm.com
DDNS Status	Active
DDNS Registration Result	Registration is successful.
HTTPS/SSL Certificate	<input type="radio"/> Free Certificate from Let's Encrypt <input type="radio"/> Import Your Own Certificate <input checked="" type="radio"/> None

ในการตั้งค่า DDNS:

1. จากหน้าจอรูระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง) > WAN (WAN) > DDNS (DDNS)**
2. กำหนดค่าการตั้งค่าต่อไปนี้ดังแสดงด้านล่าง: เมื่อทำเสร็จ, คลิก **Apply (นำไปใช้)**
 - **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:

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

3.14.7 NAT ผ่านตลอด

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

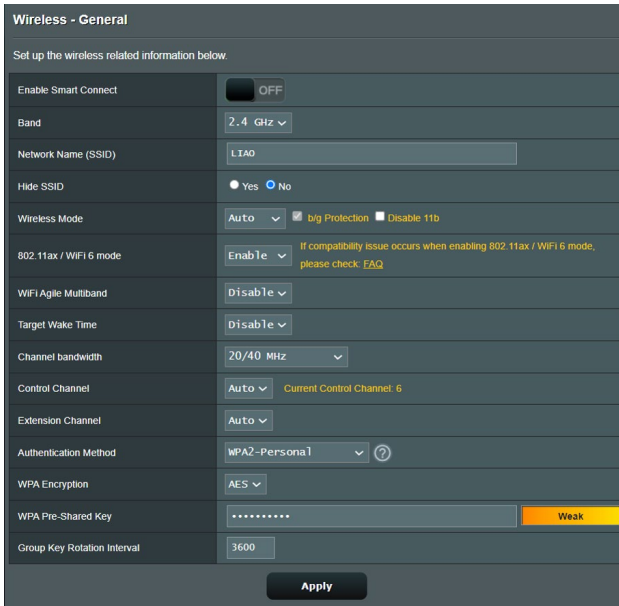
ในการเปิดทำงาน / ปิดทำงานการตั้งค่า NAT ผ่านตลอด ไปที่ **Advanced Settings (การตั้งค่าขั้นสูง) > WAN (WAN) > NAT Passthrough (NAT ผ่านตลอด)** เมื่อทำเสร็จ, คลิก **Apply (นำไปใช้)**

WAN - NAT Passthrough	
Enable NAT Passthrough to allow a Virtual Private Network (VPN) connection to pass through the router to the network clients.	
PPTP Passthrough	Enable
L2TP Passthrough	Enable
IPsec Passthrough	Enable
RTSP Passthrough	Enable
H.323 Passthrough	Enable
SIP Passthrough	Enable
PPPoE Relay	Disable
FTP ALG port	2021
Apply	

3.15 ไร้สาย

3.15.1 ทั่วไป

แท็บ General (ทั่วไป) อนุญาตให้คุณกำหนดค่าการตั้งค่าไร้สายพื้นฐาน



ในการกำหนดค่าการตั้งค่าไร้สายพื้นฐาน:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง) > Wireless (ไร้สาย) > General (ทั่วไป)**
2. เลือก 2.4GHz หรือ 5GHz เป็นแถบความถี่สำหรับเครือข่ายไร้สายของคุณ
3. กำหนดชื่อที่ไม่ซ้ำที่ประกอบด้วยตัวอักษรได้มากถึง 32 ตัวสำหรับ SSID (ตัวระบุชุดบริการ) หรือชื่อเครือข่ายของคุณ เพื่อระบุเครือข่ายไร้สายของคุณ อุปกรณ์ Wi-Fi สามารถหาและเชื่อมต่อไปยังเครือข่ายไร้สายผ่าน SSID ที่คุณกำหนดไว้ SSID บนเมนู เหนือข้อมูลจะถูกอัปเดตทันทีที่ SSID ใหม่ถูกบันทึกไปยังการตั้งค่า

หมายเหตุ: คุณสามารถกำหนด SSID ที่ไม่ซ้ำสำหรับแถบความถี่ 2.4 GHz และ 5GHz

4. ในฟิลด์ **Hide SSID (ซ่อน SSID)**, เลือก **Yes (ใช่)** เพื่อป้องกันอุปกรณ์ไร้สายไม่ให้ตรวจพบ SSID ของคุณ เมื่อฟังก์ชันนี้เปิดทำงาน คุณจำเป็นต้องป้อน SSID ด้วยตัวเองบนอุปกรณ์ไร้สายเพื่อเข้าถึงเครือข่ายไร้สาย
5. เลือกตัวเลือกทั้งหมดไร้สายเหล่านี้ เพื่อหาชนิดของอุปกรณ์ไร้สายที่สามารถเชื่อมต่อไปยังไวร์เลสเราเตอร์ของคุณ:
 - **อัตโนมัติ:** เลือก **Auto (อัตโนมัติ)** เพื่ออนุญาตให้อุปกรณ์ 802.11AC, 802.11n, 802.11g และ 802.11b เชื่อมต่อไปยังไวร์เลสเราเตอร์
 - **ดั้งเดิม:** เลือก **Legacy (ดั้งเดิม)** เพื่ออนุญาตให้อุปกรณ์ 802.11b/g/n เชื่อมต่อไปยังไวร์เลสเราเตอร์ อย่างไรก็ตาม ฮาร์ดแวร์ที่สนับสนุน 802.11n จะรันที่ความเร็วสูงสุด 54Mbps เท่านั้น
 - **เฉพาะ N:** เลือก **N only (เฉพาะ N)** เพื่อเพิ่มสมรรถนะไวร์เลส N ให้สูงที่สุด การตั้งค่านี้ป้องกันไม่ให้อุปกรณ์ 802.11g และ 802.11b เชื่อมต่อไปยังไวร์เลสเราเตอร์
6. เลือกแบนด์วิดธ์ช่องเหล่านี้เพื่อให้ได้ความเร็วการรับส่งข้อมูลสูงขึ้น:
 - 40MHz:** เลือกแบนด์วิดธ์นี้เพื่อเพิ่มผลลัพธ์การส่งผ่านข้อมูลไร้สายให้สูงที่สุด
 - 20MHz (ค่าเริ่มต้น):** เลือกแบนด์วิดธ์นี้ ถ้าคุณพบปัญหาบางอย่างกับการเชื่อมต่อไร้สายของคุณเลือกช่องการทำงาน
7. สำหรับไวร์เลสเราเตอร์ของคุณ เลือก **Auto (อัตโนมัติ)** เพื่ออนุญาตให้ไวร์เลสเราเตอร์เลือกช่องที่มีปริมาณการรบกวนน้อยที่สุดโดยอัตโนมัติ
8. เลือกวิธีการยืนยันตัวตนบุคคลเหล่านี้:
 - **ระบบเปิด:** ตัวเลือกนี้ไม่มีระบบรักษาความปลอดภัยใดๆ
 - **แชร์คีย์:** คุณต้องใช้การเข้ารหัส WEP และป้อนแชร์คีย์อย่างน้อยหนึ่งตัว

- **WPA/WPA2 ส่วนตัว/WPA อัตโนมัติ-ส่วนตัว:** ตัวเลือกนี้ให้ระบบรักษาความปลอดภัยที่แข็งแกร่ง คุณสามารถใช้ WPA (กับ TKIP) หรือ WPA2 (กับ AES) ได้ ถ้าคุณเลือกตัวเลือกนี้ คุณต้องใช้การเข้ารหัส TKIP + AES และป้อนรหัสผ่าน WPA (เน็ตเวิร์คคีย์)
- **WPA/WPA2 เ็นเตอร์ไพรส์/WPA อัตโนมัติ-เอ็นเตอร์ไพรส์:** ตัวเลือกนี้ให้ระบบรักษาความปลอดภัยที่แข็งแกร่งมาก โดยมาพร้อมกับ EAP เซิร์ฟเวอร์ในตัว หรือ RADIUS เซิร์ฟเวอร์ภายนอกด้วยบุคคลแบ็ค-เอ็นด์ภายนอก
- **เรเดี่ยสกับ 802.1x**

หมายเหตุ: ไร้เลสเราเตอร์ของคุณสนับสนุนอัตราการรับส่งข้อมูลสูงที่สุด 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)**

3.15.2 WPS

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

หมายเหตุ: ตรวจสอบให้แน่ใจว่าอุปกรณ์สนับสนุน WPS

Wireless - WPS

WPS (WiFi Protected Setup) provides easy and secure establishment of a wireless network. You can configure WPS here via the PIN code or the WPS button.

Enable WPS	<input checked="" type="checkbox"/>
Current Frequency	2.4 GHz
Connection Status	Idle
Configured	Enabled <input type="button" value="Reset"/> Pressing the reset button resets the network name (SSID) and WPA encryption key.
AP PIN Code	<input type="text" value="51246044"/>

You can easily connect a WPS client to the network in either of these two ways:

- Method1: Click the WPS button on this interface (or press the physical WPS button on the router), then press the WPS button on the client's WLAN adapter and wait for about three minutes to make the connection.
- Method2: Start the client WPS process and get the client PIN code. Enter the client's PIN code on the Client PIN code field and click Start. Please check the user manual of your wireless client to see if it supports the WPS function. If your wireless client does not support the WPS function, you have to configure the wireless client manually and set the same network Name (SSID), and security settings as this router.

WPS Method: Push button Client PIN Code

ในการเปิดทำงาน WPS บนเครือข่ายไร้สายของคุณ:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง) > Wireless (ไร้สาย) > WPS (WPS)**
2. ในฟิลต์ **Enable WPS (เปิดทำงาน WPS)**, เลื่อนตัวเลื่อนไปยัง **ON (เปิด)**
3. ตามค่าเริ่มต้น WPS ใช้ความถี่ 2.4GHz ถ้าคุณต้องการเปลี่ยนความถี่เป็น 5GHz, **ปิด** ฟังก์ชัน WPS, คลิก **Switch Frequency (สลับความถี่)** ในฟิลต์ **Current Frequency (ความถี่ปัจจุบัน)**, จากนั้น **เปิด WPS** อีกครั้ง

หมายเหตุ: WPS สันับสนุนการยืนยันตัวตนด้วยคีย์ของระบบเปิด, WPA-ส่วนตัว และ WPA2-ส่วนตัว WPS ไม่สนับสนุนเครือข่ายไร้สายที่ใช้วิธีการเข้ารหัส แชรค์ย, WPA-เอ็นเตอร์ไพรส์, WPA2-เอ็นเตอร์ไพรส์ และ RADIUS

4. ในฟิลด์ WPS Method (วิธี WPS), เลือก **Push Button (ปุ่มกด)** หรือรหัส **Client PIN (ไคลเอ็นต์ PIN)** ถ้าคุณเลือก **Push Button (ปุ่มกด)**, ไปยังขั้นตอนที่ 5 ถ้าคุณเลือกรหัส **Client PIN (ไคลเอ็นต์ PIN)**, ไปยังขั้นตอนที่ 6
5. ในการตั้งค่า WPS ใ้ดยใช้ปุ่ม WPS ของเราเตอร์, ให้ปฏิบัติตามขั้นตอนเหล่านี้:
 - a. คลิก **Start (เริ่ม)** หรือกดปุ่ม WPS ที่พบที่ด้านหลังของไวร์เลสเราเตอร์
 - b. กดปุ่ม WPS บนอุปกรณ์ไร้สายของคุณ ซึ่งโดยปกติจะมีการระบุด้วยโลโก้ WPS

หมายเหตุ: ตรวจสอบอุปกรณ์ไร้สายของคุณ หรือคู่มือผู้ใช้ของอุปกรณ์สำหรับตำแหน่งของปุ่ม WPS

- c. ไวร์เลสเราเตอร์จะสแกนหาอุปกรณ์ WPS ที่ใช้ได้ ถ้าไวร์เลสเราเตอร์ไม่พบอุปกรณ์ WPS ใดๆ, เครื่องจะสลับไปยังโหมดสแตนด์บาย
6. ในการตั้งค่า WPS ใ้ดยใช้รหัส PIN ของไคลเอ็นต์, ให้ปฏิบัติตามขั้นตอนเหล่านี้:
 - a. คำนรหัส PIN WPS บนคู่มือผู้ใช้ของอุปกรณ์ไร้สายของคุณ หรือบนตัวอุปกรณ์
 - b. ป้อนรหัส PIN ของไคลเอ็นต์บนกล่องข้อความ
 - c. คลิก **Start (เริ่ม)** เพื่อสั่งให้ไวร์เลสเราเตอร์ของคุณเข้าสู่โหมดสำรวจ WPS ตัวแสดงสถานะ LED ของเราเตอร์จะกะพริบ 3 ครั้งอย่างรวดเร็ว จนกระทั่งตั้งค่า WPS สมบูรณ์

3.15.3 บริดจ์

บริดจ์ หรือ WDS (ระบบการกระจายไร้สาย) อนุญาตให้ ASUS ไร้สายเราเตอร์ของคุณเชื่อมต่อไปยังไร้สายแอคเซสพอยต์อีกตัวหนึ่ง โดยป้องกันไม่ให้อุปกรณ์ไร้สายหรือสถานีอื่นๆ เข้าถึง ASUS ไร้สายเราเตอร์ของคุณ ระบบนี้อาจเรียกว่าเป็นไร้สายรีพีตเตอร์ก็ได้ ซึ่ง ASUS ไร้สายเราเตอร์ของคุณสื่อสารกับแอคเซสพอยต์อีกตัวหนึ่ง และอุปกรณ์ไร้สายอื่นๆ

Wireless - Bridge

Bridge (or named WDS - Wireless Distribution System) function allows your ASUS Router to connect to an access point wirelessly. WDS may also be considered a repeater mode.

Note:

The function only support [Open System/NONE, Open System/WEP] security authentication method. To set up the corresponding authentication method, please select Legacy as your wireless mode first. [Click Here](#) to modify. Please refer to this [FAQ](#) for more details.

To enable WDS to extend the wireless signal, please follow these steps :

1. Select [WDS Only] or [Hybrid] mode and add MAC address of APs in Remote AP List.
2. Ensure that this wireless router and the AP you want to connect to use the same channel.
3. Key in the remote AP mac in the remote AP list and open the remote AP's WDS management interface, key in the this router's MAC address.
4. To get the best performance, please go to Advanced Settings > Wireless > General and assign the same channel bandwidth, control channel, and extension channel to every router in the network.

You are currently using the Auto channel bandwidth. [Click Here](#) to modify.
You are currently using the Auto channel. [Click Here](#) to modify.

Basic Config

2.4 GHz MAC	<input type="text" value="C8:7F:54:12:69:C8"/>
5 GHz MAC	<input type="text" value="C8:7F:54:12:69:CC"/>
Band	<input type="text" value="2.4 GHz"/>
AP Mode	<input type="text" value="AP On ly"/>
Connect to APs in list	<input type="radio"/> Yes <input checked="" type="radio"/> No

Remote AP List (Max Limit : 4)

Remote AP List	Add / Delete
<input type="text"/>	<input type="button" value="⊕"/>
No data in table.	

ในการตั้งค่าไร้สายบริดจ์:


1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง) > Wireless (ไร้สาย) > WDS**
2. เลือกแถบความถี่สำหรับไร้สายบริดจ์
3. ในฟิลด์ **AP Mode (โหมด AP)**, เลือกระหว่างตัวเลือกต่อไปนี้:
 - **AP เท่านั้น:** ปิดทำงานฟังก์ชันไร้สายบริดจ์

- **WDS เท่านั้น:** เปิดทำงานคุณสมบัติไวร์เลสบริดจ์ แต่ป้องกันไม่ให้อุปกรณ์ไร้สาย/สถานีอื่นเชื่อมต่อไปยังเราเตอร์
- **ไอบริด:** เปิดทำงานคุณสมบัติไวร์เลสบริดจ์ และอนุญาตให้อุปกรณ์ไร้สาย/สถานีอื่นเชื่อมต่อไปยังเราเตอร์ได้

หมายเหตุ: ในโหมดไอบริด, อุปกรณ์ไร้สายที่เชื่อมต่ออยู่กับ ASUS ไวร์เลสเราเตอร์ จะได้รับความเร็วการเชื่อมต่อเพียงครึ่งหนึ่งของแอดเซสพอยต์เท่านั้น

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

หมายเหตุ: ช่องที่ใช้ได้ แตกต่างกันไปตามประเทศหรือภูมิภาค

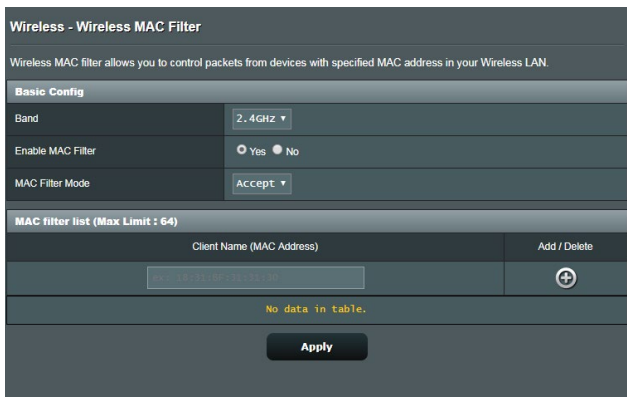
6. บนรายการ รีโมท AP, ป้อน MAC แอดเดรส และคลิกปุ่ม **Add (เพิ่ม)**  เพื่อป้อน MAC แอดเดรสของแอดเซสพอยต์ที่ใช้ได้อื่นๆ

หมายเหตุ: แอดเซสพอยต์ใดๆ ที่เพิ่มไปยังรายการ ควรอยู่บนช่องควบคุมเดียวกันกับ ASUS ไวร์เลสเราเตอร์

7. คลิก **Apply (นำไปใช้)**

3.15.4 ตัวกรอง MAC ไร้สาย

ตัวกรอง MAC ไร้สาย ให้การควบคุมแพคเกจที่ส่งไปยัง MAC (การควบคุมการเข้าถึงสื่อ) แอดเดรสที่ระบุบนเครือข่ายไร้สายของคุณ

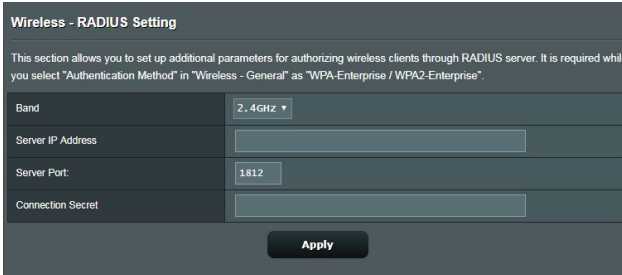


ในการตั้งค่าตัวกรอง MAC ไร้สาย:

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

3.15.5 การตั้งค่า RADIUS

การตั้งค่า RADIUS (บริการผู้ใช้ที่รเข้าเพื่อยืนยันตัวบุคคลระยะไกล) ให้ระบบป้องกันขั้นพิเศษเมื่อคุณเลือก WPA-เอ็นเตอร์ไพรส์, WPA2-เอ็นเตอร์ไพรส์ หรือ Radius กับ 802.1x เป็นโหมดการยืนยันตัวบุคคลของคุณ



ในการตั้งค่า RADIUS ไร้สาย:

1. ให้แน่ใจว่าโหมดการยืนยันตัวบุคคลของไวร์เลสเราเตอร์ถูกตั้งค่าเป็น WPA-เอ็นเตอร์ไพรส์, WPA2-เอ็นเตอร์ไพรส์ หรือ Radius กับ 802.1x

หมายเหตุ: โปรดดูส่วน 3.15.1 ทั่วไป สำหรับการกำหนดค่าโหมดการยืนยันตัวบุคคลของไวร์เลสเราเตอร์ของคุณ

2. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง) > Wireless (ไร้สาย) > 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)**

3.15.6 Professional (มืออาชีพ)

หน้าจอ Professional (มืออาชีพ) ให้ตัวเลือกการกำหนดค่าขั้นสูง

หมายเหตุ: เราแนะนำให้ผู้ใช้ค่าเริ่มต้นบนหน้านี้

Setting	Value
Band	2.4 GHz
Enable Radio	Yes
Enable wireless scheduler	No
Set AP Isolated	No
Roaming assistant	Enable
Disconnect clients with RSSI lower than	-70 dBm
Bluetooth Coexistence	Disable
Enable IGMP Snooping	Enable
Multicast Rate(Mbps)	Auto
Preamble Type	Long
AMPDU RTS	Enable
RTS Threshold	2347
DTIM Interval	1
Beacon Interval	100
Enable TX Bursting	Enable
Enable WMM	Enable
Enable WMM No-Acknowledgement	Disable
Enable WMM APSD	Enable
Optimize AMPDU aggregation	Disable
Modulation Scheme	Up to MCS 11 (NitroQAM/1024-QAM)
Airtime Fairness	Disable
Multi-User MIMO	Enable
OFDMA/802.11ax MU-MIMO	Disable
Explicit Beamforming	Enable
Universal Beamforming	Enable
Tx power adjustment	Performance

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) คลิกที่แต่ละเฟรมเพื่อเปลี่ยนการตั้งค่าของชั่วโมงในสัปดาห์ต่าง 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
- **อัตราการลัดดาสด (Mbps):** เลือกอัตราการส่งข้อมูลลัดดาสด หรือคลิก **Disable (ปิดทำงาน)** เพื่อปิดการส่งข้อมูลเดี่ยวพร้อมกัน

- **ประเภทพร็แฮมเบิล:** ประเภทพร็แฮมเบิล กำหนดความยาวของเวลาที่เราเตอร์ใช้สำหรับ CRC (ตรวจสอบความซ้ำซ้อนแบบวงกลม) CRC เป็นวิธีในการตรวจสอบข้อผิดพลาดระหว่างการส่งข้อมูล เลือก **Short (สั้น)** สำหรับเครือข่ายไร้สายที่ยังไม่มีการจราจรเครือข่ายสูง เลือก **Long (ยาว)** ถ้าเครือข่ายไร้สายของคุณประกอบด้วยอุปกรณ์ไร้สายรุ่นเก่า หรือแบบดั้งเดิม
- **ขีดจำกัด RTS:** เลือกค่าที่ต่ำกว่าสำหรับขีดจำกัด RTS (ค่าขอให้ส่ง) เพื่อปรับปรุงการสื่อสารไร้สายในเครือข่ายไร้สายที่ยังไม่มีการจราจรเครือข่ายสูง และอุปกรณ์ไร้สายจำนวนมาก
- **ช่วง DTIM:** ช่วง DTIM (ข้อความระบุการจราจรที่ส่ง) หรืออัตราการส่งข้อมูล คือช่วงเวลาก่อนที่สัญญาณจะถูกส่งไปยังอุปกรณ์ไร้สายในโหมดสลิป เพื่อเป็นการระบวามีแพคเก็ตข้อมูลที่รอการส่ง ค่าเริ่มต้นคือ 3 มิลลิวินาที
- **ช่วงเวลานับคอน:** ช่วงเวลานับคอน คือเวลาระหว่าง DTIM หนึ่งกับตัวถัดไป ค่าเริ่มต้นคือ 100 มิลลิวินาที ลดค่าช่วงเวลานับคอนลง สำหรับการเชื่อมต่อไร้สายที่ไม่มีเสถียรภาพ หรือสำหรับอุปกรณ์โรมมิ่ง
- **เปิดทำงาน TX เวิร์สดี:** เปิดทำงาน TX เวิร์สดี ช่วยปรับปรุงความเร็วการส่งข้อมูลระหว่างไวเลสเราเตอร์ และอุปกรณ์ 802.11g
- **เปิดทำงาน WMM APSD:** เปิดทำงาน WMM APSD (Wi-Fi มีลต์มีเดีย การส่งการประหยัดพลังงานอัตโนมัติ) เพื่อปรับปรุงการจัดการพลังงานระหว่างอุปกรณ์ไร้สายต่างๆ เลือก **Disable (ปิดทำงาน)** เพื่อปิด WMM APSD

4 ยูทิลิตี้

หมายเหตุ:

- ดาวน์โหลดและติดตั้งยูทิลิตี้ของไวร์เลสเราเตอร์จากเว็บไซต์ ASUS:
- การสำรวจอุปกรณ์ v1.4.7.1 ที่ https://www.asus.com/Networking/RT-AX88U_PRO/HelpDesk_Download/
- การอัปเดตเฟิร์มแวร์ v1.9.0.4 ที่ https://www.asus.com/Networking/RT-AX88U_PRO/HelpDesk_Download/
- ยูทิลิตี้เครื่องพิมพ์ของ Windows v1.0.5.5 ที่ <http://dlcdnnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Printer.zip>
- ยูทิลิตี้เหล่านี้ไม่ได้รับการสนับสนุนบน MAC OS

4.1 การค้นหาอุปกรณ์

Device Discovery (การค้นหาอุปกรณ์) เป็นยูทิลิตี้ ASUS WLAN ซึ่งทำหน้าที่ตรวจสอบหาอุปกรณ์ ASUS ไวร์เลส เราเตอร์ และอนุญาตให้คุณตั้งค่าคอนฟิกอุปกรณ์

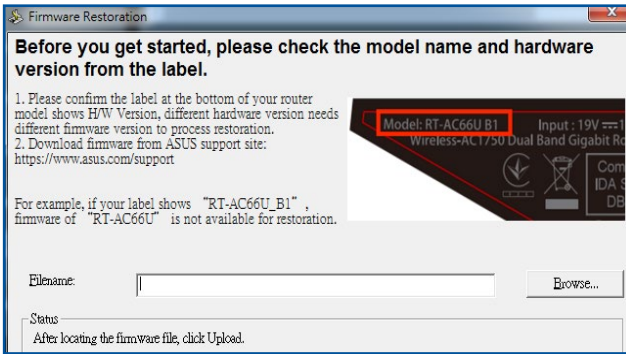
ในการเปิดยูทิลิตี้ การค้นหาอุปกรณ์:

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

หมายเหตุ:เมื่อคุณตั้งค่าเราเตอร์เป็นโหมดแอดเดสส์พอยต์, คุณจำเป็นต้องใช้ การสำรวจอุปกรณ์ เพื่อรับ IP แอดเดรสของเราเตอร์

4.2 การกู้คืนเฟิร์มแวร์

การกู้คืนเฟิร์มแวร์ ถูกใช้บน ASUS ไร้สาย เราเตอร์ หลังจากที่ทำกรอัปเดตเฟิร์มแวร์ล้มเหลว ยุทิลิตีนี้จะอัปโหลดไฟล์เฟิร์มแวร์ไปยังเราเตอร์ ระยะเวลาการจะใช้เวลาประมาณ 3 ถึง 4 นาที



สำคัญ: ปิดโหมดช่วยเหลือน ก่อนที่จะใช้ยูทิลิตี การกู้คืนเฟิร์มแวร์

หมายเหตุ: คุณสมบัตินี้ไม่ได้รับการสนับสนุนบน MAC OS

ในการเปิดโหมดช่วยเหลือน และใช้ยูทิลิตี การกู้คืนเฟิร์มแวร์:

1. ถอดปลั๊กเราเตอร์จากแหล่งพลังงาน
2. กดปุ่มกู้คืน ที่แผงด้านหลังค้างไว้ ในขณะที่เสียบปลั๊กเราเตอร์ที่เราเตอร์กลับเข้าไป ยังแหล่งพลังงาน ปลอบปุ่มกู้คืน เมื่อ LED เพาเวอร์ที่แผงด้านหลังกะพริบซ้ำๆ ซึ่งเป็นการ ระบุว่าเราเตอร์อยู่ในโหมดช่วยเหลือน

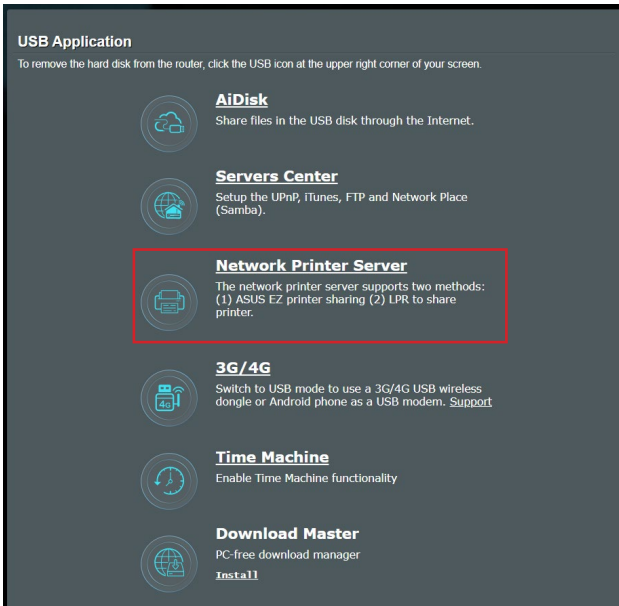
3. ตั้งค่าสแตตติก IP บนคอมพิวเตอร์ของคุณ และใช้สิ่งต่อไปนี้เพื่อตั้งค่าการตั้งค่า TCP/IP ของคุณ:
IP แอดเดรส: 192.168.1.x
ซับเน็ต มาสก์: 255.255.255.0
4. จากเดสก์ทอปของคอมพิวเตอร์ของคุณ, คลิก **Start (เริ่ม) > All Programs (โปรแกรมทั้งหมด) > ASUS Utility (ยูทิลิตี้ ASUS) > Wireless Router (ไวร์เลส เราเตอร์) > Firmware Restoration (การกู้คืนเฟิร์มแวร์)**
5. คลิก **Browse (เรียกดู)** เพื่อเลือกไฟล์เฟิร์มแวร์ จากนั้นคลิก **Upload (อัปโหลด)**

หมายเหตุ: นี่ไม่ใช่ยูทิลิตี้สำหรับอัปเดตเฟิร์มแวร์ และไม่สามารถใช้กับ ASUS ไวร์เลสเราเตอร์ที่ทำงานได้ คุณต้องทำการอัปเดตเฟิร์มแวร์ตามปกติผ่านอินเทอร์เน็ตเบราว์เซอร์ ดู **บทที่ 3: การกำหนดค่าการตั้งค่าทั่วไป และ ค่าการตั้งค่าขั้นสูง** สำหรับรายละเอียดเพิ่มเติม

4.3 การตั้งค่าพรินเตอร์เซิร์ฟเวอร์ของคุณ

4.3.1 การแชร์เครื่องพิมพ์ ASUS EZ

ยู่ทิลิตี้การแชร์เครื่องพิมพ์ ASUS EZ อนุญาตให้คุณเชื่อมต่อเครื่องพิมพ์ USB เข้ากับพอร์ต USB ของไวร์เลสเราเตอร์ของคุณ และตั้งค่าพรินต์เซิร์ฟเวอร์ การทำเช่นนี้ ทำให้เน็ตเวิร์กไคลเอนต์ของคุณสามารถพิมพ์และสแกนไฟล์แบบไร้สายได้



หมายเหตุ: ฟังก์ชันพรินต์เซิร์ฟเวอร์ได้รับการสนับสนุนบน Windows® 10/11

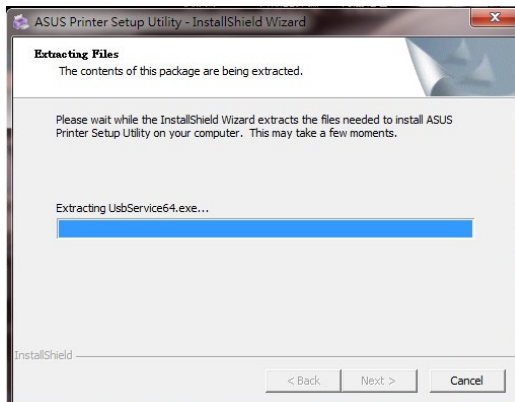
ในการตั้งค่าโหมดการแชร์เครื่องพิมพ์ EZ:

1. จากหน้าต่างระบบเมนู ไปยัง **General (ทั่วไป) > USB Application (การใช้งานผ่าน USB) > Network Printer Server (เน็ตเวิร์กพรินเตอร์เซิร์ฟเวอร์)**
2. คลิก **Download Now (ดาวน์โหลดเดี๋ยวนี้)**! เพื่อดาวน์โหลดชุดยูทิลิตี้เน็ตเวิร์กพรินเตอร์

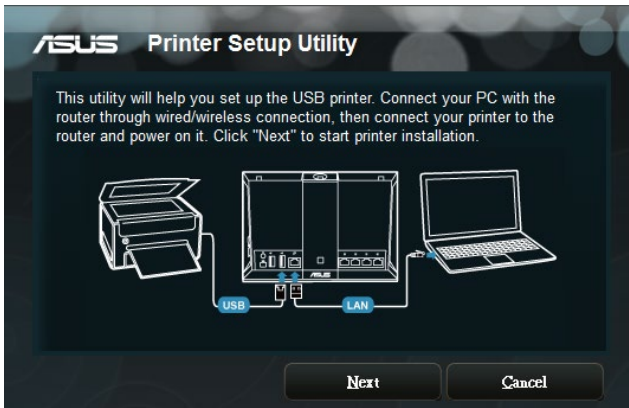


หมายเหตุ: ยูทิลิตี้เน็ตเวิร์กพรินเตอร์ ได้รับการสนับสนุนบน Windows® 10/11 เท่านั้น ในการติดตั้งยูทิลิตี้บน Mac OS, เลือก **ใช้โปรโตคอล LPR สำหรับการแชร์เครื่องพิมพ์**

3. อื่นซิปไฟล์ที่ดาวน์โหลดมา และคลิกไอคอน Printer (เครื่องพิมพ์) เพื่อรันโปรแกรมตั้งค่าเน็ตเวิร์กพรินเตอร์



- ทำตามขั้นตอนบนหน้าจอเพื่อตั้งค่าฮาร์ดแวร์ของคุณ, จากนั้นคลิก **Next** (ถัดไป)

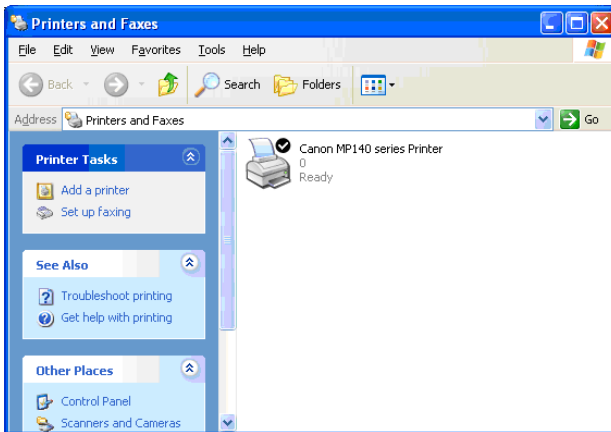


- รอเป็นเวลาสองสามนาที เพื่อให้การตั้งค่าเริ่มต้นเสร็จ คลิก **Next** (ถัดไป)
- คลิก **Finish** (เสร็จสิ้น) เพื่อทำการติดตั้งให้สมบูรณ์

7. ทำตามขั้นตอนของ Windows® OS เพื่อติดตั้งไดรเวอร์เครื่องพิมพ์



8. หลังจากทำการติดตั้งไดรเวอร์ของเครื่องพิมพ์สมบูรณ์แล้ว ขณะนี้เน็ตเวิร์กที่เคเบิลเอ็นตักก็สามารถใช้เครื่องพิมพ์ได้

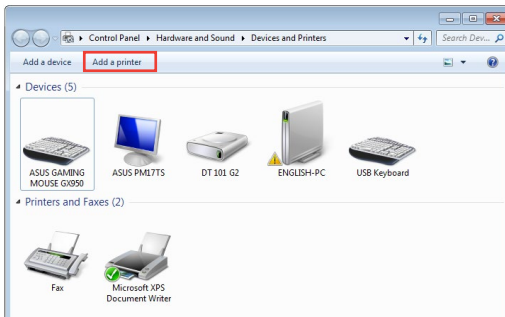


4.3.2 การใช้ LPR เพื่อแชร์เครื่องพิมพ์

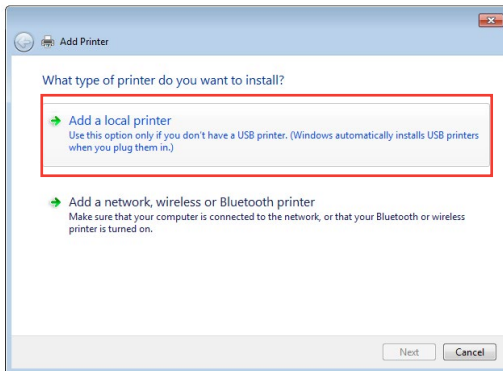
คุณสามารถแชร์เครื่องพิมพ์ของคุณกับคอมพิวเตอร์อื่นๆ ที่รันระบบปฏิบัติการ Windows® และ MAC ได้โดยใช้ LPR/LPD (Line Printer Remote/Line Printer Daemon)

การแชร์เครื่องพิมพ์ LPR ของคุณ ในการแชร์เครื่องพิมพ์ LPR ของคุณ:

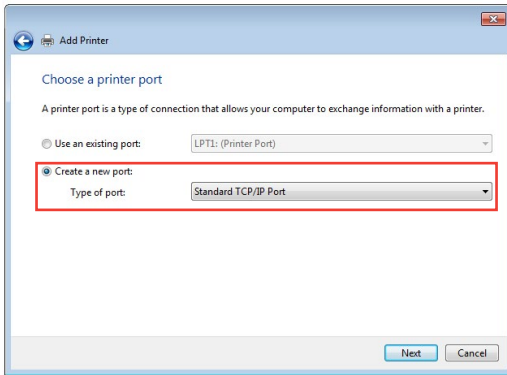
1. จากเดสก์ทอป Windows®, คลิก **Start (เริ่ม) > Devices and Printers (อุปกรณ์และเครื่องพิมพ์) > Add a printer (เพิ่มเครื่องพิมพ์)** เพื่อรัน **Add Printer Wizard (ตัวช่วยสร้างเพิ่มเครื่องพิมพ์)**



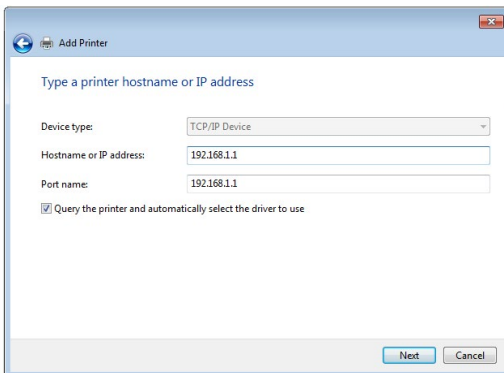
2. เลือก **Add a local printer (เพิ่มเครื่องพิมพ์ในเครื่อง)** จากนั้นคลิก **Next (ถัดไป)**



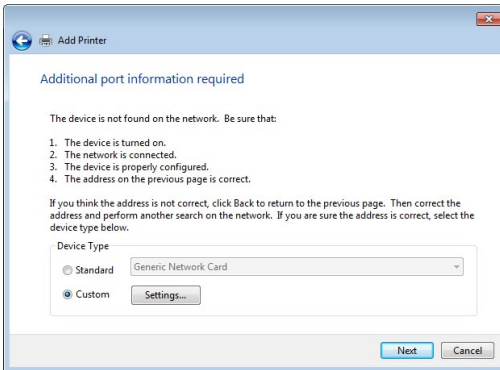
3. เลือก **Create a new port (สร้างพอร์ตใหม่)** จากนั้นตั้งค่า **Type of Port (ชนิดของพอร์ต)** เป็น **Standard TCP/IP Port (พอร์ต TCP/IP มาตรฐาน)** คลิก **New port (พอร์ตใหม่)**



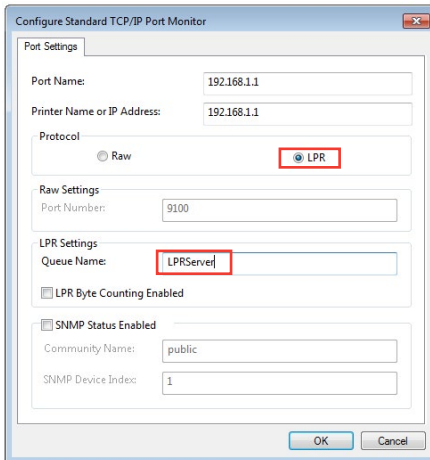
4. ในฟิลด์ **Hostname or IP address (ชื่อโฮสต์หรือ IP แอดเดรส)**, ป้อน IP แอดเดรสของไวร์เลสเราเตอร์ จากนั้นคลิก **Next (ถัดไป)**



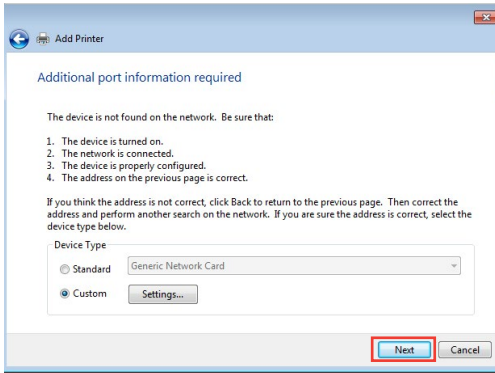
5. เลือก Custom (กำหนดเอง) จากนั้นคลิก Settings (การตั้งค่า)



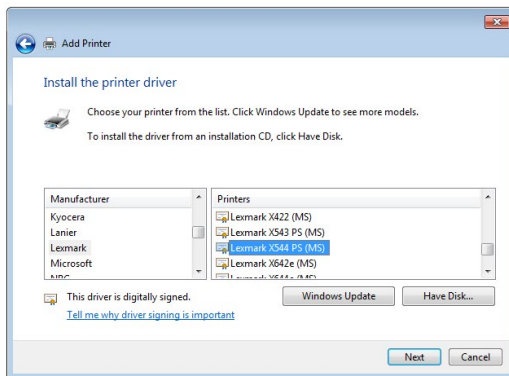
6. ตั้งค่า Protocol (โพรโทคอล) เป็น LPR (LPR) ในฟิลด์ Queue Name (ชื่อคิว), ป้อน LPRServer จากนั้นคลิก OK (ตกลง) เพื่อทำต่อ



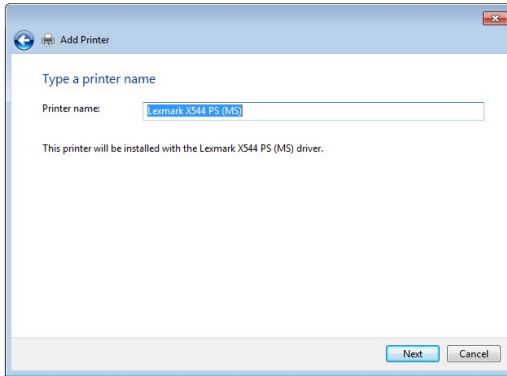
7. คลิก **Next (ถัดไป)** เพื่อทำการตั้งค่าพอร์ต TCP/ IP มาตรฐานให้เสร็จ



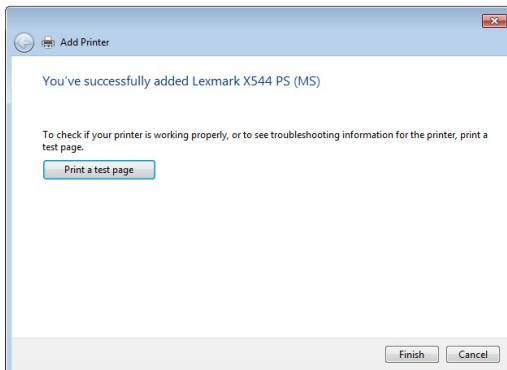
8. ติดตั้งไดรเวอร์เครื่องพิมพ์จากรายการรุ่นของผู้จำหน่าย ถ้าเครื่องพิมพ์ของคุณไม่ได้อยู่ในรายการ, คลิก **Have Disk (มีดิสก์)** เพื่อติดตั้งไดรเวอร์เครื่องพิมพ์ของคุณจาก CD-ROM หรือไฟล์



9. คลิก **Next** (ถัดไป) เพื่อยอมรับชื่อเริ่มต้นสำหรับเครื่องพิมพ์



10. คลิก **Finish** (เสร็จสิ้น) เพื่อทำการติดตั้งให้สมบูรณ์



4.4 ดาวนั้โหลดมาสเตอร์

ดาวนั้โหลดมาสเตอร์ เป็นยูทิลิตี้ที่ช่วยคุณดาวนั้โหลดไฟล์ต่างๆ แมกระทั้งในขณะที่โหนดบูคหรืออุปกรณ์อื่นๆ ปิดเครื่องอยู่

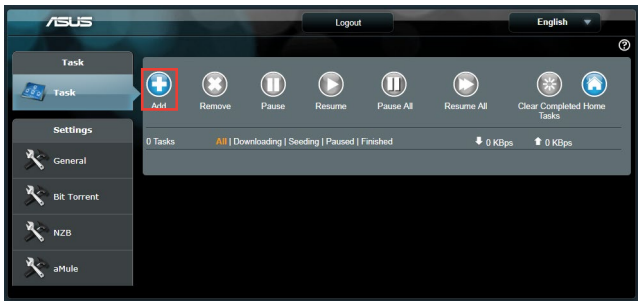
หมายเหตุ: คุณจำเป็นต้องมีอุปกรณ์ USB เชื่อมต่ออยู่กับไวร์เลสเราเตอร์ เพื่อใช้ดาวนั้โหลดมาสเตอร์

ในการใช้ดาวนั้โหลดมาสเตอร์:

1. คลิก **General (ทั่วไป) > USB Application (การใช้งานผ่าน USB) > Download Master (ดาวนั้โหลดมาสเตอร์)** เพื่อดาวนั้โหลดและติดตั้งยูทิลิตี้โดยอัตโนมัติ

หมายเหตุ: ถ้าคุณมี USB ใดรูปมากกว่าหนึ่งตัว, ให้เลือกอุปกรณ์ USB ที่คุณต้องการดาวนั้โหลดไฟล์ไปยัง

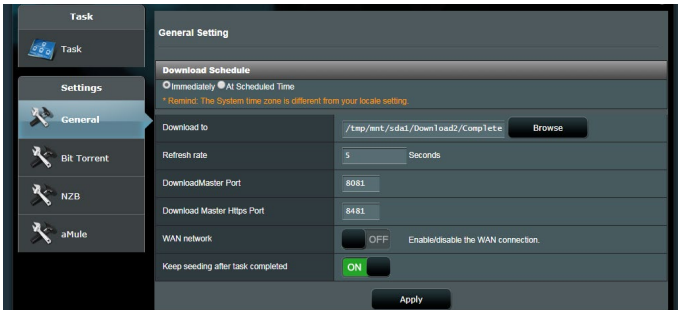
2. หลังจากที่กระบวนการดาวนั้โหลดเสร็จ, คลิกไอคอน Download Master (ดาวนั้โหลดมาสเตอร์) เพื่อเริ่มการไชยูทิลิตี้
3. คลิก **Add (เพิ่ม)** เพื่อเพิ่มงานดาวนั้โหลด



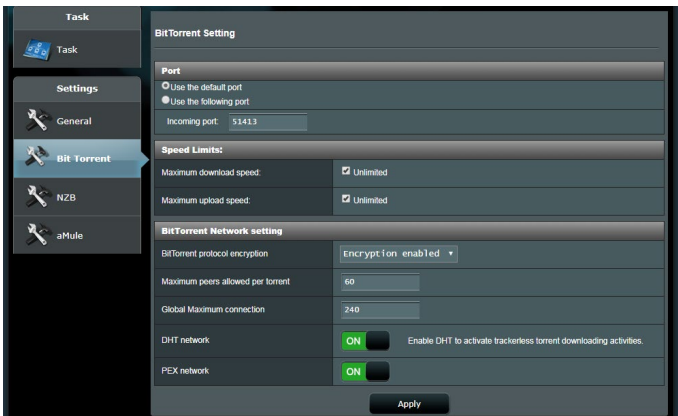
4. เลือกชนิดการดาวนั้โหลด เช่น บิตทอรัเร็นต์, HTTP หรือ FTP ให้ไฟล์บิตทอรัเร็นต์ หรือ URL เพื่อเริ่มการดาวนั้โหลด

หมายเหตุ: สำหรับรายละเอียดเกี่ยวกับบิตทอรัเร็นต์, ให้อ่านส่วน 4.4.1 การกำหนดค่าการตั้งค่าการดาวนั้โหลดบิตทอรัเร็นต์

5. ใช้หน้าจอเมนูเพื่อกำหนดค่าการตั้งค่าขั้นสูง



4.4.1 การกำหนดค่าการตั้งค่าการดาวน์โหลดบิตทอร์เรนต์

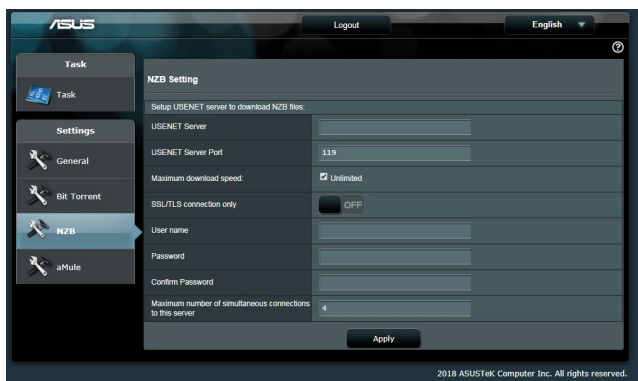


ในการกำหนดค่าการตั้งค่าการดาวน์โหลดบิตทอร์เรนต์:

1. จากหน้าจอเมนูของดาวน์โหลดมาสเตอร์, คลิก **Bit Torrent (บิตทอร์เรนต์)** เพื่อเปิดหน้า **Bit Torrent Setting (การตั้งค่าบิตทอร์เรนต์)**
2. เลือกพอร์ตที่เจาะจงสำหรับงานดาวน์โหลดของคุณ
3. เพื่อป้องกันการติดขัดของเครือข่าย, คุณสามารถจำกัดความเร็วการอัปเดตและดาวน์โหลดสูงสุดได้ภายใต้ **Speed Limits (ขีดจำกัดความเร็ว)**
4. คุณสามารถจำกัดจำนวนของพีร์ที่อนุญาตมากที่สุด และเปิดทำงานหรือปิดทำงานการเซารหัสไฟล์ระหว่างการดาวน์โหลดได้

4.4.2 การตั้งค่า NZB

คุณสามารถตั้งค่า USENET เซิร์ฟเวอร์ให้ดาวน์โหลดไฟล์ NZB ได้หลังจากที่ป้อนการตั้งค่า USENET, เลือก **Apply** (นำไปใช้)



5 การแก้ไขปัญหา

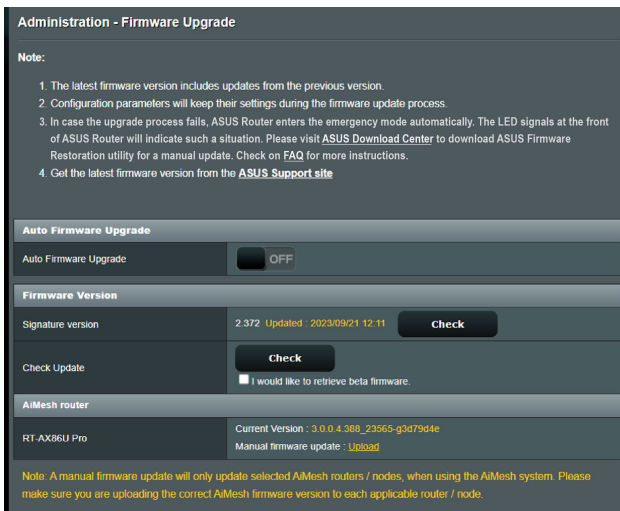
บทนี้ให้วิธีแก้ไขปัญหาคือคุณอาจพบกับเราเตอร์ของคุณ ถ้าคุณพบปัญหาที่ไม่ได้กล่าวถึงในบทนี้ ให้เยี่ยมชมเว็บไซต์สนับสนุนของ ASUS ที่: <https://www.asus.com/support> สำหรับข้อมูลผลิตภัณฑ์เพิ่มเติม และรายละเอียดการติดต่อฝ่ายสนับสนุนด้านเทคนิคของ ASUS

5.1 การแก้ไขปัญหาพื้นฐาน

ถ้าคุณมีปัญหากับเราเตอร์ของคุณ ให้ลองขั้นตอนพื้นฐานในส่วนนี้ก่อนที่จะมองหาวิธีการแก้ไขปัญหาเพิ่มเติม

อัปเดตเฟิร์มแวร์ไปเป็นเวอร์ชันล่าสุด

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



2. ถ้ามีเฟิร์มแวร์ล่าสุด ให้เยี่ยมชมเว็บไซต์ทั่วโลกของ ASUS ที่ <https://www.asus.com/Networking/RT-AX88U-PRO/HelpDesk/> เพื่อดาวน์โหลดเฟิร์มแวร์ล่าสุด
3. จากหน้า **Firmware Version (Laiteohjelmiston versio)**, คลิก **Check (ตรวจสอบ)** เพื่อค้นหาไฟล์เฟิร์มแวร์

4. คลิก **Upload (อัปโหลด)** เพื่ออัปเดตเฟิร์มแวร์

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

ตรวจสอบว่าการตั้งค่าไร้สายบนคอมพิวเตอร์ของคุณตรงกับค่าของเตอร์ของคุณ

- เมื่อคุณเชื่อมต่อคอมพิวเตอร์ของคุณไปยังเราเตอร์แบบไร้สาย, ให้แน่ใจว่า SSID (ชื่อเครือข่ายไร้สาย), วิธีการเข้ารหัส และรหัสผ่านนั้นถูกต้อง

ตรวจสอบว่าการตั้งค่าเครือข่ายของคุณถูกต้องหรือไม่

- ใ้คลิกปุ่มแต่ละตัวบนเครือข่ายควรมี IP แอดเดรสที่ถูกต้อง ASUS แนะนำให้ผู้ใช้ DHCP เซิร์ฟเวอร์ของเราเตอร์เพื่อกำหนด IP แอดเดรสให้กับคอมพิวเตอร์ต่างๆ บนเครือข่ายของคุณ
- ผู้ให้บริการเคเบิลโมเด็มบางราย จำเป็นต้องให้คุณใช้ MAC แอดเดรสของคอมพิวเตอร์ที่ลงทะเบียนครั้งแรกในบัญชี คุณสามารถดู MAC แอดเดรสในเว็บ GUI, **Network Map (แผนที่เครือข่าย) > หน้า Clients (ไคลเอนต์)**, และวางตัวชี้เมาส์เหนืออุปกรณ์ของคุณใน **Client Status (สถานะไคลเอนต์)**

The dashboard displays the following information:

- Internet status:** Connected
WAN IP: 192.168.66.8
DDNS: [GO](#)
- Security level:** WPA2-Personal
- Client status:**
 - Online: 0
 - Wired (1): 1
- Client List:**

Device	IP Address	MAC Address
Jiewing-PC	192.168.58.129	00:00:00:00:00:00
- Other Status:**
 - Clients: 1 (with [View List](#) button)
 - AiMesh Node: 0
 - USB 3.0: No Device (two instances)

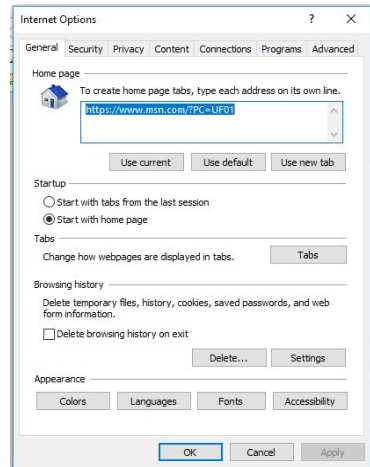
5.2 คำถามที่มีการถามบ่อยๆ (FAQs)

ฉันไม่สามารถเข้าถึง GUI ของเราเตอร์โดยใช้เว็บเบราว์เซอร์ได้

- ถ้าคอมพิวเตอร์ของคุณเป็นแบบมีสาย ให้ตรวจสอบการเชื่อมต่อสายเคเบิลอีเธอร์เน็ต และสถานะ LED ตามที่อธิบายในส่วนก่อนหน้า
- ตรวจสอบให้แน่ใจว่าคุณใช้ข้อมูลการล็อกอินที่ถูกต้อง ชื่อล็อกอินและรหัสผ่านเริ่มต้นคือ "admin/admin" ตรวจสอบให้แน่ใจว่าปุ่ม Caps Lock ถูกปิดการทำงานในขณะที่คุณป้อนข้อมูลการล็อกอิน
- ลบคุกกี้และไฟล์ในเว็บเบราว์เซอร์ของคุณ สำหรับ Internet Explorer ปฏิบัติตามขั้นตอนเหล่านี้:

1. เปิดเว็บ Explorer, จากนั้นคลิก **Tools (เครื่องมือ) > Internet Options (ตัวเลือกอินเทอร์เน็ต)**

2. บนแท็บ **General (ทั่วไป)**, คลิก **Delete (ลบ)** ภายใต้ **Browsing history (ประวัติการเบราว์เซอร์)** เลือก **Temporary Internet files and website files (ไฟล์อินเทอร์เน็ตชั่วคราวและไฟล์เว็บไซต์)** รวมถึง **Cookies and website data (ข้อมูลคุกกี้และเว็บไซต์)** จากนั้นคลิกที่ **Delete (ลบ)**



หมายเหตุ:

- คำสั่งสำหรับการลบคุกกี้และไฟล์นั้นแตกต่างกันในเว็บเบราว์เซอร์แต่ละตัว
- ปิดการทำงานการตั้งค่าพร็อกซีเซิร์ฟเวอร์, ยกเลิกการเชื่อมต่อแบบวิธรเขา และตั้งค่า TCP/IP ให้อัตโนมัติสำหรับ IP แอดเดรสที่อยู่อัตโนมัติสำหรับรายละเอียดเพิ่มเติม ใหดูบทที่ 1 ของคู่มือผู้ใช้ฉบับนี้
- ให้แน่ใจว่าคุณใช้สายเคเบิลอีเธอร์เน็ต CAT5e หรือ CAT6

📶 โคลเอ็นต์ไม่สามารถสร้าง การเชื่อมต่อไร้สายกับ เราเตอร์ได้

หมายเหตุ: ถ้าคุณกำลังมีปัญหาในการเชื่อมต่อไปยังเครือข่าย 5GHz, ตรวจสอบให้แน่ใจว่าอุปกรณ์ไร้สายของคุณสนับสนุนความถี่ 5GHz หรือมีความสามารถแบบดual-band

- **อยู่นอกพื้นที่ทำงาน:**
 - ย้ายเราเตอร์ให้เข้าใกล้ไวร์เลส ๒ โคลเอ็นต์ มากขึ้น
 - พยายามปรับเสถียรภาพของเราเตอร์ไปยังทิศทางที่ดีที่สุดตามทฤษฎีไวใน ส่วน 1.4 การวางตำแหน่งเราเตอร์ของคุณ
- **DHCP เซิร์ฟเวอร์ถูกปิดการทำงาน:**
 1. เปิดเว็บ GUI ไปที่ **General (ทั่วไป) > Network Map (แผนที่เครือข่าย) > Clients (๒ โคลเอ็นต์)** และค้นหาอุปกรณ์ที่คุณต้องการเชื่อมต่อไปยังเราเตอร์
 2. ถ้าคุณไม่สามารถพบอุปกรณ์ใน **Network Map (แผนที่เครือข่าย)**, ให้ไปที่ **Advanced Settings (การตั้งค่าขั้นสูง) > LAN (LAN) > รายการ DHCP Server (DHCP เซิร์ฟเวอร์), Basic Config (การกำหนดค่าพื้นฐาน)**, เลือก **Yes (ใช่)** บน **Enable the DHCP Server (เปิดทำงาน DHCP เซิร์ฟเวอร์)**

LAN - DHCP Server

DHCP (Dynamic Host Configuration Protocol) is a protocol for the automatic configuration used on IP networks. The DHCP server can assign each client an IP address and inform the client of the DNS server IP and default gateway IP. ASUS Router supports up to 253 IP addresses for your local network.
Manually Assigned IP around the DHCP list FAQ

Basic Config

Enable the DHCP Server Yes No

ASUS Router's Domain Name

IP Pool Starting Address

IP Pool Ending Address

Lease time

Default Gateway

DNS and WINS Server Setting

DNS Server 1

DNS Server 2

Advertise router's IP in addition to user-specified DNS Yes No

WINS Server

Manual Assignment

Enable Manual Assignment Yes No

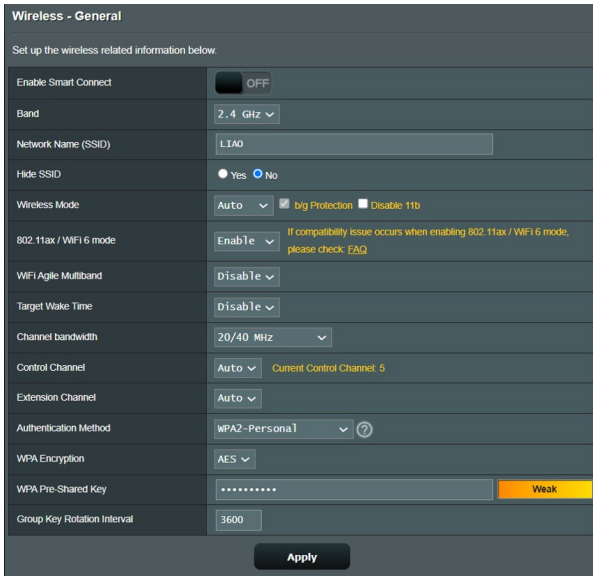
Manually Assigned IP around the DHCP list (Max Limit : 64)

Client Name (MAC Address)	IP Address	DNS Server (Optional)	Host Name (Optional)	Add / Delete
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="⊕"/>

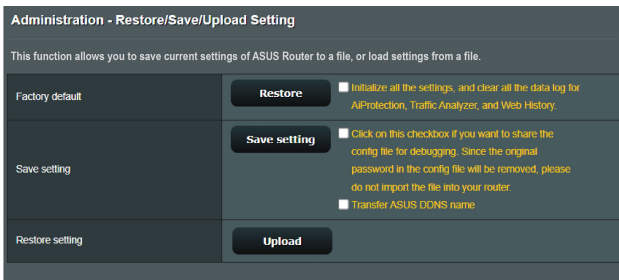
No data in table.

Apply

- 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/อัปโหลด)** และคลิก **Restore (กู้คืน)**

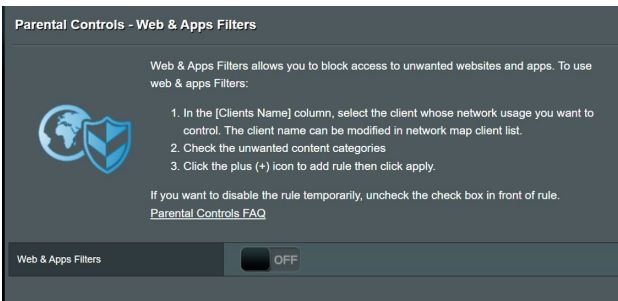


ไม่สามารถเข้าถึงอินเทอร์เน็ตได้

- ตรวจสอบว่าเราเตอร์ของคุณสามารถเชื่อมต่อไปยัง WAN IP แอดเดรสของ ISP ใดหรือใหม่ ในการดำเนินการ, เปิดเว็บ GUI และไปที่ **General (ทั่วไป) > Network Map (แผนที่เครือข่าย)** และตรวจสอบ **Internet status (สถานะอินเทอร์เน็ต)**
- ถ้าเราเตอร์ของคุณไม่สามารถเชื่อมต่อไปยัง WAN IP แอดเดรสของ ISP ใด, ให้ลองเริ่มเครือข่ายของคุณใหม่ ตามที่อธิบายในส่วน **เริ่มเครือข่ายของคุณใหม่ในลำดับต่อไป** ภายใต การแก้ไขปัญหาพื้นฐาน



- อุปกรณ์ถูกบล็อกผ่านฟังก์ชัน **Parental Control (การควบคุมโดยผู้ปกครอง)** ไปที่ **General (ทั่วไป) > Parental Controls (การควบคุมโดยผู้ปกครอง)** และดูว่าอุปกรณ์อยู่ในรายการหรือไม่ ถ้าอุปกรณ์ถูกแสดงอยู่ภายใต้ **Client Name (ชื่อไคลเอนต์)**, ให้ลบอุปกรณ์ออก โดยใช้ปุ่ม **Delete (ลบ)** หรือปรับ การตั้งค่าการจัดการเวลา



- ถ้ายังคงเข้าถึงอินเทอร์เน็ตไม่ได้, ให้ลองบูตคอมพิวเตอร์ของคุณใหม่ และตรวจสอบ IP แอดเดรส และเกตเวย์แอดเดรสของเครือข่าย
- ตรวจสอบไฟแสดงสถานะบนโมเด็ม ADSL และไวร์เลส เราเตอร์ ถ้า LED WAN บนไวร์เลสเราเตอร์ไม่ติด, ให้ตรวจสอบว่าสายเคเบิลทั้งหมดเสียบอยู่อย่างเหมาะสมหรือไม่

คุณลิม 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/อัปโหลด)**, และคลิก **Restore (กู้คืน)** บัญชีและรหัสผ่านการล็อกอินเริ่มต้นเป็น "admin" ทั้งสองอย่าง

วิธีการกู้คืนระบบกลับเป็นการ ตั้งค่าเริ่มต้น

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

การอัปเดตเฟิร์มแวร์ลิมเหลว

เปิดโหมดช่วยเหลือ และเรียนรู้ทีละขั้นตอน การกู้คืนเฟิร์มแวร์ ดูส่วน 4.2 การกู้คืนเฟิร์มแวร์ เกี่ยวกับการใช้ยูทิลิตี้ การกู้คืนเฟิร์มแวร์

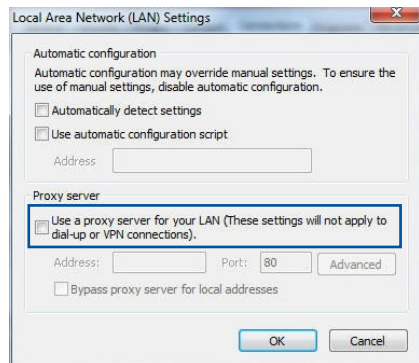
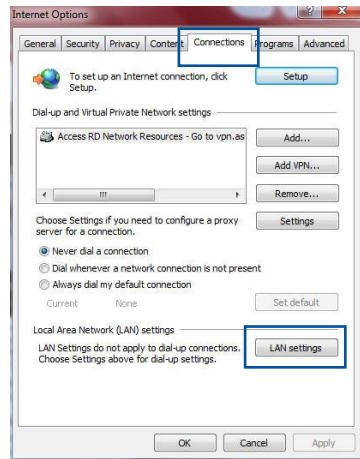
ไม่สามารถเข้าถึงเว็บ GUI

ก่อนที่จะกำหนดค่าไวร์เลสเราเตอร์ของคุณ ให้ทำขั้นตอนตามที่อธิบายในส่วนนี้ สำหรับบ็อกซ์คอมพิวเตอร์และเน็ตเวิร์กโคลเอ็นด์ของคุณ

A. ปิดทำงานพร็อกซีเซิร์ฟเวอร์ ถ้าเปิดทำงานอยู่

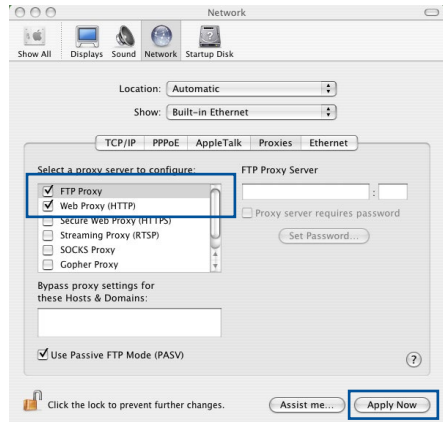
Windows®

1. คลิก **Start (เริ่ม) > Internet Explorer (อินเทอร์เน็ต เอ็กซ์พลอเรอร์)** เพื่อเปิดเบราว์เซอร์
2. คลิก **Tools (เครื่องมือ) > Internet options (ตัวเลือกอินเทอร์เน็ต) > 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)** เมื่อเสร็จ



MAC OS

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

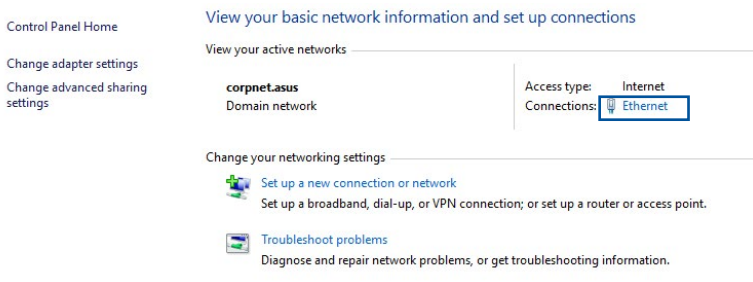


หมายเหตุ: คุณควรสมัครวิธีใช้ของเบราว์เซอร์ของคุณ สำหรับรายละเอียดเกี่ยวกับการปิดทำงานพร็อกซีเซิร์ฟเวอร์

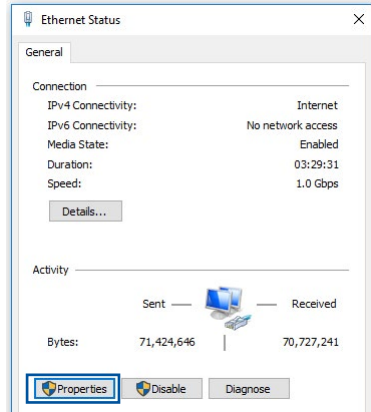
B. ตั้งค่าการตั้งค่า TCP/IP เป็น Automatically obtain an IP address (รับที่อยู่ IP โดยอัตโนมัติ)

Windows®

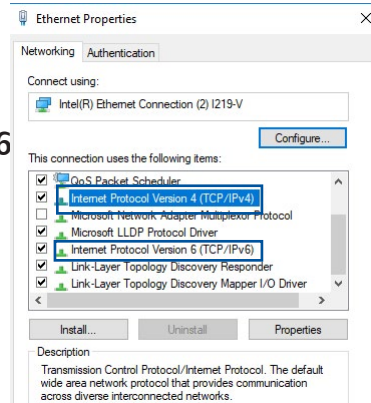
1. คลิก **Start (เริ่ม)** > **Control Panel (แผงควบคุม)** > **Network and Sharing Center (เครือข่ายและศูนย์การใช้ร่วมกัน)**, จากนั้นคลิกที่การเชื่อมต่อเครือข่ายเพื่อแสดงหน้าต่างสถานะ



2. คลิกที่ **Properties** (คุณสมบัติ) เพื่อแสดง หน้าตาทางคุณสมบัติอีเทอร์เน็ต



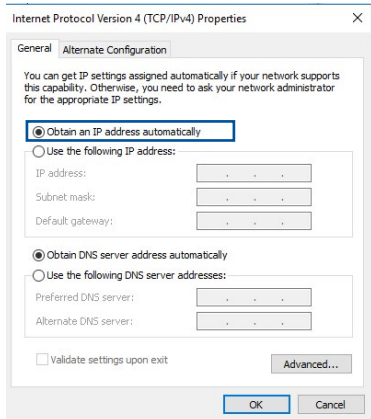
3. เลือก **Internet Protocol Version 4 (TCP/IPv4)** (อินเทอร์เน็ตโปรโตคอลเวอร์ชัน4 (TCP/IPv4)) หรือ **Internet Protocol Version 6 (TCP/IPv6)** (อินเทอร์เน็ตโปรโตคอลเวอร์ชัน6 (TCP/IPv6)), จากนั้นคลิก **Properties** (คุณสมบัติ)




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

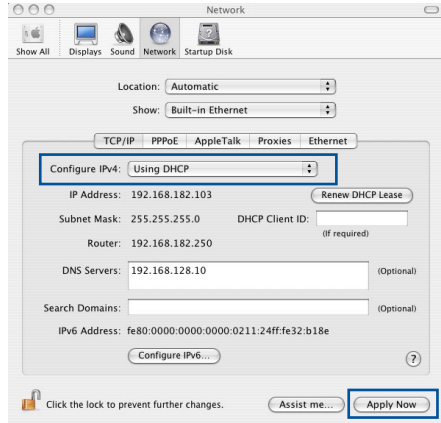
เพื่อรับการตั้งค่า IPv6 IP โดยอัตโนมัติ, ทำเครื่องหมายที่ **Obtain an IPv6 address automatically** (รับ IPv6 แอดเดรสโดยอัตโนมัติ)

5. คลิก **OK** (ตกลง) เมื่อทำเสร็จ



MAC OS

1. คลิกไอคอนแอปเปิล  ที่อยู่บนบริเวณมุมซ้ายบนของหน้าจอ
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

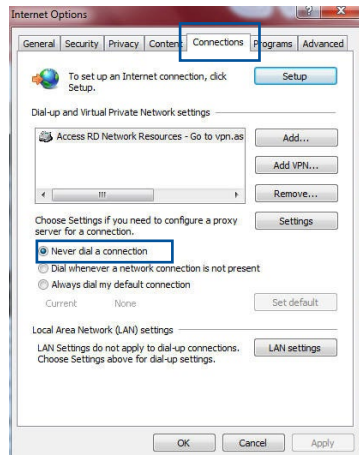


หมายเหตุ: คู่มือใช้ของระบบปฏิบัติการของคุณ และคุณสมบัติที่สนับสนุนสำหรับรายละเอียดเกี่ยวกับการกำหนดค่า TCP/IP ของคอมพิวเตอร์ของคุณ

C. เปิดการทำงานเครือข่ายแบบโทรเข้า

Windows®

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



หมายเหตุ: คุณคุณสมบัติวิธีใช้ของเบราว์เซอร์ของคุณ สำหรับรายละเอียดเกี่ยวกับการปิดการทำงานการเชื่อมต่อแบบโทรเข้า

ภาคผนวก

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

ประกาศความปลอดภัย

เมื่อใช้ผลิตภัณฑ์นี้ ให้ปฏิบัติตามข้อควรระวังด้านความปลอดภัย
ขั้นพื้นฐานเสมอ ซึ่งรวมถึงแต่ไม่จำกัดเฉพาะสิ่งต่อไปนี้



คำเตือน!

- ต้องเสียบสายไฟเข้ากับเต้ารับที่มีสายดินที่เหมาะสม
เชื่อมต่ออุปกรณ์เข้ากับเต้ารับใกล้เคียงที่เข้าถึงได้ง่ายเท่านั้น
- หากอะแดปเตอร์เสียหาย อย่าพยายามซ่อมด้วยตัวเอง
ติดต่อช่างเทคนิคซ่อมแซมที่มีคุณสมบัติ หรือร้านค้าของคุณ
- อย่าใช้สายไฟ อุปกรณ์เสริม หรืออุปกรณ์ต่อพ่วงที่ชำรุดเสียหาย
- อย่าติดตั้งอุปกรณ์นี้สูงเกิน 2 เมตร
- ใช้ผลิตภัณฑ์นี้ในสภาพแวดล้อมที่มีอุณหภูมิสิ่งแวดล้อมระหว่าง
0°C (32°F) ถึง 40°C (104°F)
- อ่านคู่มือและช่วงอุณหภูมิการใช้งานที่ระบุไว้ก่อนใช้ผลิตภัณฑ์
- ให้ความใส่ใจเป็นพิเศษกับความปลอดภัยส่วนบุคคลเมื่อใช้
อุปกรณ์นี้ในสนามบิน โรงพยาบาล บิมน้ำมัน และอุโมงค์รถ
- การรบกวนอุปกรณ์ทางการแพทย์ รักษาระยะห่างขั้นต่ำอย่างน้อย
15 ซม. (6 นิ้ว) ระหว่างอุปกรณ์ทางการแพทย์ที่ฝังและผลิตภัณฑ์
ASUS เพื่อลดความเสี่ยงของการรบกวน
- กรุณาใช้ผลิตภัณฑ์ ASUS
ในสภาวะการรับสัญญาณที่ดีเพื่อลดระดับรังสีให้เหลือน้อยที่สุด
- เก็บอุปกรณ์ให้ห่างจากสตรีมเมอร์และช่องท้องส่วนล่างของวัยรุ่น
- อย่าใช้ผลิตภัณฑ์นี้หากสามารถสังเกตเห็นข้อบกพร่องที่มองเห็น
ได้ หรือเปียก เสียหาย หรือดัดแปลง ขอรับบริการเพื่อขอความ
ช่วยเหลือ



คำเตือน!

- อย่าวางบนพื้นผิวทำงานที่ไม่สม่ำเสมอ หรือไม่มั่นคง เข้า
- อย่าวางหรือทำสิ่งของหล่นทับด้านบนของผลิตภัณฑ์
หลีกเลี่ยงการทำให้ผลิตภัณฑ์ถูกกระแทกทางกล เช่น การบิด
การตัด การเจาะหรือการฉีกเป็นชิ้นเล็กชิ้นน้อย
- ห้ามแยกชิ้นส่วน เปิด อบอุ่นโครงเวฟ เผา ทาสี หรือผลักวัตถุ
แปลกปลอมมใด ๆ เข้าไปในผลิตภัณฑ์นี้
- ดูแผ่นป้ายระบุกำลังไฟฟ้าใต้ผลิตภัณฑ์ของคุณ
และตรวจสอบให้แน่ใจว่าจะแต่บ้เตอร์เพาเวอร์ของคุณมีกำลังไฟฟ้า
สอดคล้องกับระดับกำลังไฟฟ้านี้
- เก็บผลิตภัณฑ์ให้ห่างจากแหล่งไฟและความร้อน
- อย่าให้สัมผัสกับ หรือใช้ในบริเวณที่อยู่ใกล้ของเหลว ฝน
หรือความชื้น อย่าใช้ผลิตภัณฑ์ในระหว่างพายุไฟฟ้า
- เชื่อมต่อวงจรเอาต์พุต PoE ของผลิตภัณฑ์นี้กับเครือข่าย
PoE โดยเฉพาะ โดยไม่ต้องกำหนดเส้นทางไปยังสิ่งอำนวยความสะดวก
สะดวกภายนอก
- เพื่อป้องกันอันตรายจากไฟฟ้าช็อต ให้ถอดสายเพาเวอร์ออก
จากเต้าเสียบไฟฟ้า ก่อนที่จะเคลื่อนย้ายระบบ
- ใช้เฉพาะอุปกรณ์เสริมที่ได้รับการรับรองจากผู้ผลิตอุปกรณ์
เท่านั้นจึงจะสามารถใช้งานร่วมกับรุ่นนี้ได้ การใช้อุปกรณ์เสริม
ประเภทอื่นอาจทำให้การรับประกันเป็นโมฆะหรือฝ่าฝืน
กฎข้อบังคับและกฎหมายท้องถิ่น และอาจก่อให้เกิดความเสี่ยง
ด้านความปลอดภัย ติดต่อผู้ค้าปลีกในพื้นที่ของคุณเพื่อ
สอบถามอุปกรณ์เสริมที่ได้รับอนุญาต
- การใช้ผลิตภัณฑ์นี้ในลักษณะที่ไม่แนะนำในคำแนะนำที่ระบุไว้
อาจส่งผลให้เกิดความเสี่ยงต่อการเกิดเพลิงไหม้หรือการบาดเจ็บ
แก่ส่วนบุคคล

บริการและการสนับสนุน

เยี่ยมชมเว็บไซต์หลายภาษาของเราที่
<https://www.asus.com/support/>

