

TH22958



# USER MANUAL

ROG Rapture GT6

ROG Rapture AX10000 เราเตอร์ตาข่ายเกมมิ่งไฮรเพนดึบความถี่

ASUS

TH22958

การแก้ไขครั้งที่ 1

เดือนธันวาคม 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 ไม่ว่าจะได้ขายจัดแจ้งหรือเป็นหน่วย ซึ่งรวมถึงแต่ไม่จำกัดอยู่เพียงการรับประกัน หรือเงื่อนไขของความสามารถเชิงพาณิชย์ หรือความเข้ากันได้สำหรับวัตถุประสงค์เฉพาะ ไม่ว่าจะได้ในกรณีใดๆ ก็ตาม ASUS กรรมการ เจ้าหน้าที่ พนักงาน หรือตัวแทนของบริษัท ไม่ยอมรับผิดชอบต่อความเสียหายที่เกิดขึ้นโดยอ้อม โดยกรณีพิเศษ โดยไม่ได้ตั้งใจ หรือโดยเป็นผลกระทบตามมา (รวมถึงความเสียหายจากการสูญเสียกำไร การขาดทุนของธุรกิจ การสูญเสียการใช้งานหรือข้อมูล การหยุดชะงักของธุรกิจ และอื่นๆ ในลักษณะเดียวกันนี้) แม้ว่า ASUS จะได้รับทราบถึงความจำเป็นไปของความเสียหายดังกล่าว อันเกิดจากข้อบกพร่องหรือข้อผิดพลาดในคู่มือหรือผลิตภัณฑ์นี้

ข้อกำหนดและข้อมูลต่างๆ ที่ระบุในคู่มือฉบับนี้ เป็นเพียงข้อมูลเพื่อการใช้งานเท่านั้น และอาจเปลี่ยนแปลงได้ตามเวลาที่ผ่านไปโดยไม่ต้องแจ้งให้ทราบ จึงไม่ควรถือเป็นภาระผูกพันของ ASUS ASUS ไม่ขอรับผิดชอบหรือรับผิดชอบข้อผิดพลาด หรือความไม่ถูกต้องใดๆ ที่อาจเกิดขึ้นในคู่มือฉบับนี้ รวมทั้งผลิตภัณฑ์และซอฟต์แวร์ที่ระบุในคู่มือด้วย

ผลิตภัณฑ์และชื่อบริษัทที่ปรากฏในคู่มือนี้อาจเป็น หรือไม่เป็นเครื่องหมายการค้าจดทะเบียน หรือลิขสิทธิ์ของบริษัทที่เป็นเจ้าของ และมีการใช้เฉพาะสำหรับการอ้างอิง หรืออธิบายเพื่อประโยชน์ของเจ้าของเท่านั้น โดยไม่มีการละเมิดใดๆ



# สารบัญ

<b>1</b>	<b>ทำความรู้จัก! ไรเลสเราเตอร์ของคุณ</b>	
1.1	ยินดีต้อนรับ!	7
1.2	สิ่งต่างๆ ในกล่องบรรจุ	7
1.3	ไรเลสเราเตอร์ของคุณ	8
1.4	การวางตำแหน่งเราเตอร์	10
1.5	ความต้องการในการติดตั้ง	11
<b>2</b>	<b>เริ่มต้นการใช้งาน</b>	
2.1	การตั้งค่าเราเตอร์	12
	A. การเชื่อมต่อแบบมีสาย	13
	B. การเชื่อมต่อไร้สาย	14
2.2	การตั้งค่าอินเทอร์เน็ตควอน (QIS) ด้วยการตรวจพบ อัตโนมัติ ...	16
2.3	กำลังเชื่อมต่อไปยังเครือข่ายไร้สายของคุณ	19
<b>3</b>	<b>การกำหนดค่าการตั้งค่าทั่วไป และ ค่าการตั้งค่าขั้นสูง</b>	
3.1	การเข้าระบบไปยังเว็บ GUI	20
3.2	การดูแลระบบ	22
	3.2.1 โหมดการทำงาน	22
	3.2.2 ระบบ	23
	3.2.3 การอัปเดตเฟิร์มแวร์	24
	3.2.4 การกู้คืน/การจัดเก็บ/การอัปโหลดการตั้งค่า	24
3.3	AiCloud 2.0	25
	3.3.1 คลาวด์ดีสก์	26
	3.3.2 เข้าถึงแบบสมาร์ท	28
	3.3.3 AiCloudซิงค์	29
3.4	AiProtection	30
	3.4.1 การกำหนดค่า AiProtection	31
	3.4.2 การบล็อกไซต์ที่ประสงค์ร้าย	33

## สารบัญ

3.4.3	Two-Way IPS .....	34
3.4.4	การป้องกันและการบล็อกอุปกรณ์ที่ติดไวรัส.....	35
3.4.5	การตั้งค่าการควบคุมโดยผู้ปกครอง .....	36
3.5	แดชบอร์ด .....	39
3.6	ไฟร์วอลล์ .....	42
3.6.1	ทั่วไป.....	42
3.6.2	ตัวกรอง URL .....	42
3.6.3	ตัวกรองคำสำคัญ.....	43
3.6.4	ตัวกรองบริการเครือข่าย.....	44
3.6.5	ไฟร์วอลล์ IPv6.....	45
3.7	อัตราเร่งของเกม .....	46
3.7.1	QoS (คุณภาพของการให้บริการ) .....	47
3.7.2	Gear Accelerator.....	48
3.8	เรดาร์เกม .....	49
3.9	เครือข่ายแยก.....	51
3.10	IPv6 .....	53
3.11	LAN .....	54
3.11.1	LAN IP.....	54
3.11.2	DHCP เซิร์ฟเวอร์.....	55
3.11.3	เส้นทาง .....	57
3.11.4	IPTV.....	58
3.12	การใช้แผนที่เครือข่าย .....	59
3.12.1	การตั้งค่าระบบความปลอดภัยไร้สาย .....	59
3.12.2	การจัดการเน็ตเวิร์กเวิลด์ไวด์ของคุณ .....	61
3.12.3	การตรวจดูแลอุปกรณ์ USB ของคุณ .....	62
3.13	โรเฟ่น NAT & ไร้พรไฟล์เกม .....	64
3.14	Smart Connect (การเชื่อมต่ออัจฉริยะ) .....	66
3.14.1	การตั้งค่าการเชื่อมต่ออัจฉริยะ .....	66
3.14.2	Smart Connect Rule (กฎการเชื่อมต่ออัจฉริยะ) .....	67

## สารบัญ

3.15	บันทึกระบบ .....	70
3.16	ตัววิเคราะห์การรับส่งข้อมูล.....	71
3.17	การใช้งานผ่าน USB.....	72
	3.17.1 การใช้ AiDisk .....	73
	3.17.2 การใช้เซิร์ฟเวอร์เซินเตอร์ .....	75
	3.17.3 3G/4G.....	80
3.18	VPN .....	81
	3.18.1 VPN Fusion.....	82
	3.18.2 Instant Guard .....	84
3.19	WAN .....	85
	3.19.1 การเชื่อมต่ออินเทอร์เน็ต .....	85
	3.19.2 Dual WAN (คูอัล WAN) .....	88
	3.19.3 พอร์ตทริกเกอร์.....	89
	3.19.4 เวอร์ชวลเซิร์ฟเวอร์/พอร์ตพอร์เวิร์ดดิ้ง .....	91
	3.19.5 DMZ.....	94
	3.19.6 DDNS.....	95
	3.19.7 NAT ผ่านตลอด .....	96
3.20	WiFi Radar.....	97
	3.20.1 การสำรวจไซต์ WiFi.....	98
	3.20.2 สถิติช่องสัญญาณไร้สาย .....	99
	3.20.3 การแก้ไขปัญหาขั้นสูง .....	99
3.21	ไร้สาย.....	100
	3.21.1 ทั่วไป .....	100
	3.21.2 WPS.....	102
	3.21.3 บรีดจ์ .....	104
	3.21.4 ตัวกรอง MAC ไร้สาย .....	106
	3.21.5 การตั้งค่า RADIUS.....	107
	3.21.6 Professional (มืออาชีพ) .....	108



<b>4</b>	<b>ยูนิตลิต</b>	
4.1	การค้นหาอุปกรณ์.....	112
4.2	การกู้คืนเฟิร์มแวร์.....	113
4.3	การตั้งค่าพรินเตอร์เซิร์ฟเวอร์ของคุณ.....	114
	4.3.1 การแชร์เครื่องพิมพ์ ASUS EZ.....	114
	4.3.2 การใช้ LPR เพื่อแชร์เครื่องพิมพ์.....	118
4.4	ดาวนโหลดมาสเตอร์.....	123
	4.4.1 กฎกำหนดค่าการตั้งค่าการดาวนโหลดบิตทอร์ เรนต์ .....	124
	4.4.2 การตั้งค่า NZB .....	125
<b>5</b>	<b>การแก้ไขปัญหา</b>	
5.1	การแก้ไขปัญหาพื้นฐาน .....	126
5.2	คำถามที่มีการถามบ่อยๆ (FAQs).....	128
	<b>ภาคผนวก</b>	
	ประกาศความปลอดภัย .....	146
	บริการและการสนับสนุน.....	148

# 1 ทำความรู้จัก! ไรร์เลสเราเตอร์ของคุณ

## 1.1 ยินดีต้อนรับ!

ขอบคุณที่ซื้อ เราเตอร์แบบไร้สายสำหรับเล่นเกม ROG Rapture! เราเตอร์ที่ทันสมัยมีดualแบนด์ 2.4GHz, 5GHz-1 และ 5GHz-2 สำหรับการสตรีม HD แบบไร้สายพร้อมกันที่ไม่มีใครเทียบได้; 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

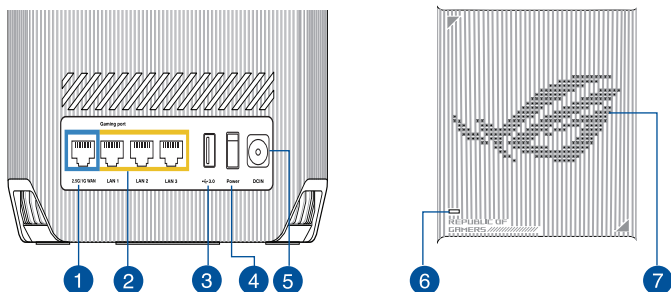
- เราเตอร์แบบไร้สายสำหรับเล่นเกม ROG Rapture
- อะแดปเตอร์พาวเวอร์
- สายเคเบิลเครือข่าย(RJ45)
- คู่มือเริ่มต้นอย่างรวดเร็ว

---

### หมายเหตุ:

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

## 1.3 ไวร์เลสเราเตอร์ของคุณ



- 1 **พอร์ต WAN (อินเทอร์เน็ต) 2.5G/1G**  
เชื่อมต่อสายเคเบิลเครือข่ายเข้ากับพอร์ตนี้ เพื่อสร้างการเชื่อมต่อ WAN 2.5G/1G
- 2 **พอร์ต LAN 1~3**  
เชื่อมต่อสายเคเบิลเครือข่ายเข้ากับพอร์ตเหล่านี้ เพื่อสร้างการเชื่อมต่อ LAN
- 3 **พอร์ต USB 3.2 Gen 1x1**  
เสียบอุปกรณ์ที่รองรับ USB 3.2 Gen 1x1 เช่น ฮาร์ดดิสก์ USB หรือ USB แฟลชไดรฟ์ลงในพอร์ตเหล่านี้
- 4 **สวิตช์เปิด/ปิด**  
กดปุ่มนี้เพื่อเปิดเครื่องหรือปิดเครื่องระบบ
- 5 **พอร์ตเพาเวอร์ (DC เข้า)**  
เสียบอะแดปเตอร์ AC ที่ให้มาเข้ากับพอร์ตนี้ และเชื่อมต่อเราเตอร์ของคุณเข้ากับแหล่งพลังงาน
- 6 **ไฟแสดงสถานะ LED**
  - สีน้ำเงินหยุดนิ่ง: ROG Rapture GT6 ของคุณพร้อมสำหรับการตั้งค่า
  - สีขาวหยุดนิ่ง: ROG Rapture GT6 ของคุณออนไลน์และใช้งานได้ดี
  - สีแดงหยุดนิ่ง: เราเตอร์ ROG Rapture GT6 ของคุณไม่มีการเชื่อมต่ออินเทอร์เน็ต / ภูมิภาคของคุณถูกตัดการเชื่อมต่อจากเราเตอร์
  - สีเหลืองหยุดนิ่ง: สัญญาณระหว่างเราเตอร์ ROG Rapture GT6 และอินเทอร์เน็ต
- 7 **Aura RGB**  
ช่วยให้ผู้ใช้สามารถกำหนดหรือเปิด/ปิด Aura RGB จากแดชบอร์ด



---

## หมายเหตุ

- ใช้เฉพาะอะแดปเตอร์ที่มาพร้อมกับแพคเกจของคุณเท่านั้น  
การใช้อะแดปเตอร์อื่นอาจทำให้อุปกรณ์เสียหาย
- ข้อมูลจำเพาะ:

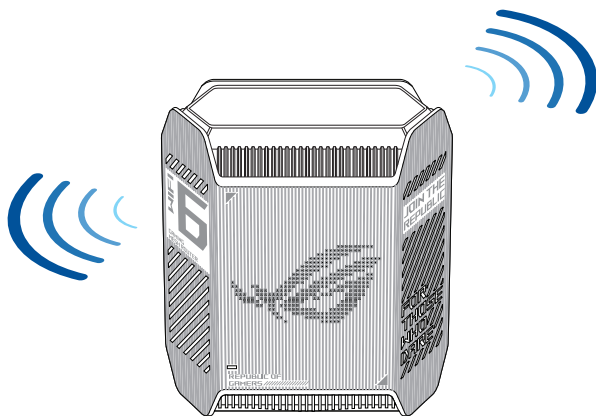
อะแดปเตอร์เพาเวอร์ DC	เอาต์พุต DC: +19V โดยมีกระแสสูงสุด 2.37A เอาต์พุต DC: +19.5V โดยมีกระแสสูงสุด 2.31A		
อุณหภูมิขณะทำงาน	0~40°C	ขณะเก็บรักษา	0~70°C
ความชื้นขณะทำงาน	50~90%	ขณะเก็บรักษา	20~90%

---

## 1.4 การวางตำแหน่งเราเตอร์

เพื่อให้การรับส่งสัญญาณไร้สายระหว่างไวร์เลสเราเตอร์ และอุปกรณ์เครือข่ายที่เชื่อมต่ออยู่มีคุณภาพดีที่สุด ให้แน่ใจว่าคุณ:

- วางไวร์เลสเราเตอร์ในบริเวณศูนย์กลาง เพื่อให้ครอบคลุมพื้นที่ไร้สายมากที่สุดสำหรับอุปกรณ์เครือข่าย
- วางอุปกรณ์ให้ห่างจากวัตถุขวางกันที่เป็นโลหะ และไม่ให้ถูกแสงแดดโดยตรง
- วางอุปกรณ์ให้ห่างจากอุปกรณ์ Wi-Fi 802.11g หรือ 20MHz, อุปกรณ์ต่อพ่วงคอมพิวเตอร์ 2.4GHz, อุปกรณ์บลูทูธ, โทรศัพท์ไร้สาย, หม้อแปลง, มอเตอร์พลังงานสูง, แสงฟลูออเรสเซนต์, เต้าไมโครเวฟ, ตู้เย็น และอุปกรณ์อุตสาหกรรมอื่นๆ เพื่อป้องกันสัญญาณรบกวน หรือสัญญาณสูญหาย
- อัปเดตไปเป็นเฟิร์มแวร์ล่าสุดเสมอ เยี่ยมชมเว็บไซต์ ASUS ที่ <http://www.asus.com> เพื่อรับอัปเดตเฟิร์มแวร์ล่าสุด



## 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
- ด้วยเทคโนโลยี 4K/8K ของไวร์เลสเรเตอร์ อุปกรณ์สนับสนุนสัญญาณไร้สายความถี่ 2.4GHz, 5GHz-1 และ 5GHz-2 พรอมกัน สัมพันธ์ช่วยให้คุณสามารถทำกิจกรรมที่เกี่ยวข้องของกับอินเทอร์เน็ตต่างๆ เช่น การท่องอินเทอร์เน็ต หรือการอ่าน/เขียนข้อความอีเมลโดยใช้แถบความถี่ 2.4GHz ในขณะที่เดียวกับที่กำลังสตรีมวิดีโอเสียง/วิดีโอระดับไฮเดฟฟินิชัน เช่น ภาพยนตร์ หรือเพลงโดยใช้แถบความถี่ 5GHz ไปพรอมๆ กัน
- อุปกรณ์ IEEE 802.11n บางอย่างที่คุณต้องการเชื่อมต่อไปยังเครือข่ายของคุณ อาจสนับสนุนหรือไม่สนับสนุนแถบความถี่ 5GHz สำหรับข้อมูลจำเพาะ ให้ดูคู่มือผู้ใช้ของอุปกรณ์
- สายเคเบิลอีเธอร์เน็ต RJ-45 ซึ่งจะนำไปใช้เพื่อเชื่อมต่ออุปกรณ์เครือข่าย ไม่ควรมีความยาวเกิน 100 เมตร

---

### สำคัญ!

- อะแดปเตอร์ไร้สายบางตัวอาจมีปัญหาการเชื่อมต่อกับ 802.11ax WiFi APs
- หากคุณกำลังประสบกับปัญหา 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:
  - หากคุณกำลังแทนที่เราเตอร์ที่มีอยู่ ให้ตัดการเชื่อมต่ออุปกรณ์เกาจากเครือข่ายของคุณ
  - ถอดสายเคเบิล/สายไฟจากชุดรีโมตที่มีอยู่ของคุณ ถ้ามีเดิมของคุณมีแบตเตอรี่สำรอง ให้ถอดออกด้วย
  - บุตคอมพิวเตอร์ใหม่ (แนะนำ)
- 



#### คำเตือน!

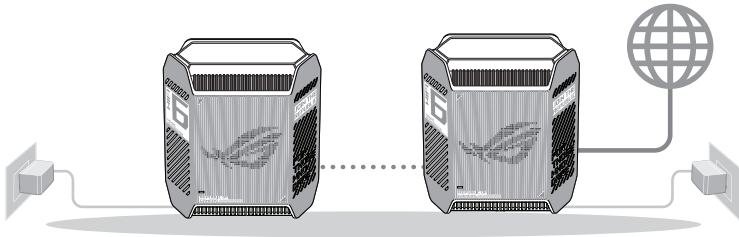
- ต้องเสียบสายไฟเข้ากับเต้ารับที่มีสายดินที่เหมาะสม เชื่อมต่ออุปกรณ์เข้ากับเต้ารับใกล้เคียงที่เขาถึงได้ง่ายเท่านั้น
  - หากอะแดปเตอร์เสียหาย อย่าพยายามซ่อมด้วยตัวเอง ติดต่อช่างเทคนิคซ่อมแซมที่มีคุณสมบัติ หรือร้านค้าของคุณ
  - อย่าใช้สายไฟ อุปกรณ์เสริม หรืออุปกรณ์ต่อพ่วงที่ชำรุดเสียหาย
  - อย่าติดตั้งอุปกรณ์นี้สูงเกิน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

## A. การเชื่อมต่อแบบมีสาย

**หมายเหตุ:** ไร้เลสเราเตอร์ซึ่งคุณสนับสนุนทั้งสายเคเบิลแบบต่อตรง หรือแบบไขว้ เมื่อตั้งค่าการเชื่อมต่อแบบมีสาย

### ในการตั้งค่าเครือข่ายโดยผู้ใช้การเชื่อมต่อแบบมีสาย:

1. เสียบเราเตอร์เข้ากับเต้าเสียบและ เปิดเครื่อง เชื่อมต่อสายเคเบิลเครือข่ายจากคอมพิวเตอร์ไปยัง พอร์ต LAN บนเราเตอร์ของคุณ



2. เว็บ GUI จะเปิดใช้งานโดยอัตโนมัติเมื่อคุณเปิดเว็บเบราว์เซอร์ หากไม่เปิดใช้งานโดยอัตโนมัติ เข้าไปที่ <http://www.asusrouter.com>
3. ตั้งค่ารหัสผ่านสำหรับเราเตอร์ของคุณเพื่อความปลอดภัยจากการเข้าถึงที่ไม่ได้รับอนุญาต

**Login Information Setup**

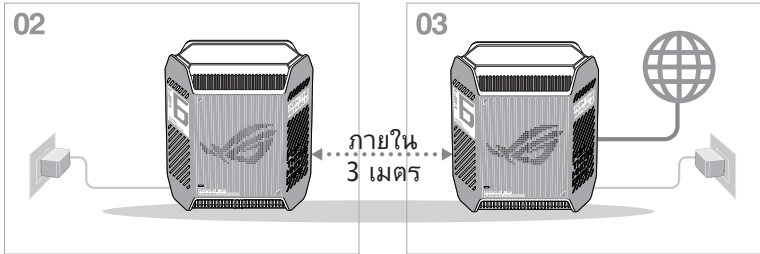
Change the router password to prevent unauthorized access to your ASUS wireless router.

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

## B. การเชื่อมต่อไร้สาย

ในการตั้งค่าเครือข่ายโดยใช้การเชื่อมต่อแบบมีสาย:

1. เสียบเราเตอร์เข้ากับเต้าเสียบและ เปิดเครื่อง



2. เชื่อมต่อกับชื่อเครือข่าย (SSID) ที่แสดงบนฉลากผลิตภัณฑ์ที่ด้านหลังของเราเตอร์ เพื่อการรักษาความปลอดภัยของเครือข่ายที่ดีกว่า เปลี่ยนเป็น SSID ที่มีลักษณะเฉพาะและกำหนดรหัสผ่าน



Wi-Fi Name (SSID): ASUS\_XX\_GT6

\* XX หมายถึงตัวเลขสองหลักสุดท้ายของ MAC แอดเดรส 2.4GHz คุณสามารถค้นหาไดบนฉลากด้านหลังของ GT6



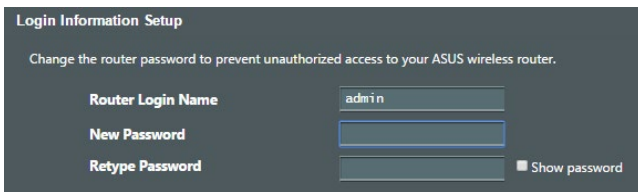
- เมื่อเชื่อมต่อแล้ว เว็บ GUI จะเปิดใช้งานโดยอัตโนมัติเมื่อคุณเปิดเว็บเบราว์เซอร์ หากไม่เปิดใช้งานโดยอัตโนมัติ เข้าไปที่ <http://www.asusrouter.com>
- ตั้งค่ารหัสผ่านสำหรับเราเตอร์ของคุณเพื่อความปลอดภัยจากการเข้าถึงที่ไม่ได้รับอนุญาต

---

#### หมายเหตุ:

- สำหรับรายละเอียดในการเชื่อมต่อเข้ากับเครือข่ายไร้สาย ให้ดูคู่มือผู้ใช้ของอะแดปเตอร์ WLAN
- ในการตั้งค่าระบบความปลอดภัยสำหรับเครือข่ายของคุณ ให้ดูส่วนการตั้งค่าระบบความปลอดภัยไร้สาย

---



Login Information Setup

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

Router Login Name

New Password

Retype Password   Show password

## 2.2 การตั้งค่าอินเทอร์เน็ตด้วย (QIS) ด้วยการตรวจพบอัตโนมัติ

ฟังก์ชัน การตั้งค่าอินเทอร์เน็ตด้วย (QIS) จะแนะนำวิธีการในการตั้งค่าการเชื่อมต่ออินเทอร์เน็ตของคุณอย่างรวดเร็ว

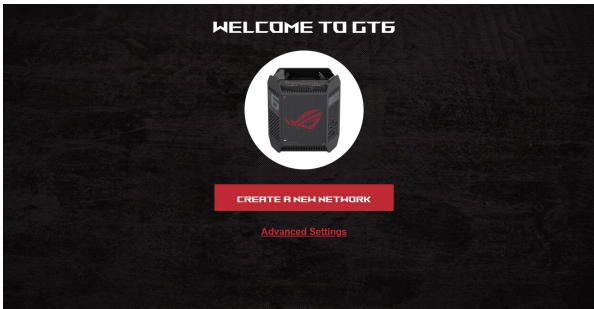
---

**หมายเหตุ:** ในขณะที่ตั้งค่าการเชื่อมต่ออินเทอร์เน็ตเป็นครั้งแรก กดปุ่ม รีเซ็ต 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:

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

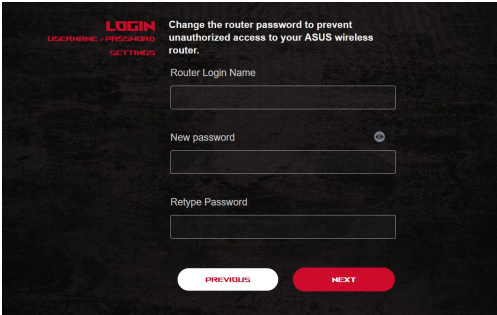
3. กำหนดชื่อเครือข่ายไร้สาย (SSID) และคีย์การป้องกัน สำหรับการเชื่อมต่อไร้สาย 2.4GHz, 5GHz-1 และ 5GHz-2 ของคุณ คลิก **Apply (นำไปใช้)** เมื่อเสร็จ

The screenshot shows the 'WIRELESS SETTINGS' interface. At the top, it says 'Assign a unique name or SSID (Service Set Identifier) to help identify your wireless network.' Below this, there are three sections for configuring different wireless networks:

- 2.4 GHz Network Name (SSID):** A text input field.
- 2.4 GHz Wireless Security:** A dropdown menu with a lock icon.
- 5 GHz-1 Network Name (SSID):** A text input field.
- 5 GHz-1 Wireless Security:** A dropdown menu with a lock icon.
- 5 GHz-2 Network Name (SSID):** A text input field.
- 5 GHz-2 Wireless Security:** A dropdown menu with a lock icon.

At the bottom, there is a checkbox labeled 'Separate 2.4 GHz and 5 GHz' which is checked. Below the checkbox are two buttons: 'PREVIOUS' (white) and 'APPLY' (red).

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





**หมายเหตุ:** ชื่อผู้ใช้และรหัสผ่านในการล็อกอินของไวร์เลสเราเตอร์นั้น แตกต่างจากชื่อเครือข่าย 2.4GHz/5GHz-1/5GHz-2 (SSID) และคีย์การป้องกัน ชื่อผู้ใช้ และรหัสผ่านในการล็อกอินของไวร์เลสเราเตอร์ ใช้สำหรับการล็อกอินเข้าไปยังเว็บ GUI ของไวร์เลสเราเตอร์ของคุณ เพื่อกำหนดค่าการตั้งค่าต่างๆ ของไวร์เลสเราเตอร์ของคุณ ชื่อเครือข่าย 2.4GHz/5GHz-1/5GHz-2 (SSID) และคีย์การป้องกัน อนุญาตให้อุปกรณ์ Wi-Fi ล็อกอินและเชื่อมต่อไป ยังเครือข่าย 2.4GHz/5GHz-1/5GHz-2 ของคุณ

## 2.3 กำลังเชื่อมต่อไปยังเครือข่ายไร้สายของคุณ

หลังจากการตั้งค่าไวร์เลสเราเตอร์ของคุณด้วย QIS แล้ว คุณสามารถเชื่อมต่อคอมพิวเตอร์หรืออุปกรณ์สมาร์ตอื่น ๆ 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
  - ดูคู่มือผู้ใช้อุปกรณ์ของคุณสำหรับรายละเอียดเพิ่มเติมในการเชื่อมต่ออุปกรณ์เข้ากับเครือข่ายไร้สายของคุณ
-

# 3 การกำหนดค่าการตั้งค่าทั่วไป และ ค่าการตั้งค่าขั้นสูง

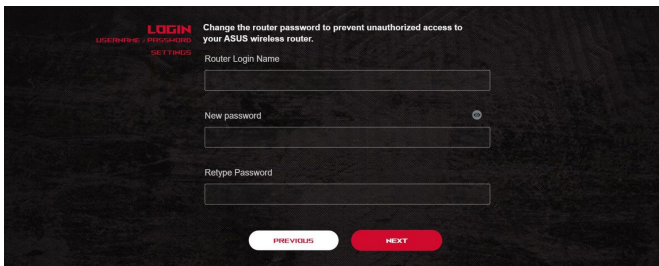
## 3.1 การเข้าระบบไปยังเว็บ GUI

เราเตอร์แบบไร้สายสำหรับเล่นเกม ROG Rapture ของคุณใช้อินเทอร์เฟซผู้ใช้บนเว็บ – ROG Gaming Center ซึ่งจะช่วยให้คุณสามารถควบคุมเครือข่ายโดยรวม พร้อมข้อมูลที่จำเป็นต่อรูเช่น สถานะอุปกรณ์ที่เชื่อมต่อและค่า ping ของเซิร์ฟเวอร์เกมทั่วโลก และเข้าถึงคุณลักษณะการเล่นเกมที่น่าตื่นตาตื่นใจได้ทันที

**หมายเหตุ:** คุณสมบัติอาจแตกต่างกันไปในเวอร์ชันเฟิร์มแวร์ต่างๆ

### ในการเข้าระบบไปยังเว็บ GUI:

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



3. ขณะนี้คุณสามารถใช้เว็บ GUI เพื่อกำหนดค่าการตั้งค่าต่างๆ ของ ASUS ไวร์เลสเราเตอร์ของคุณได้

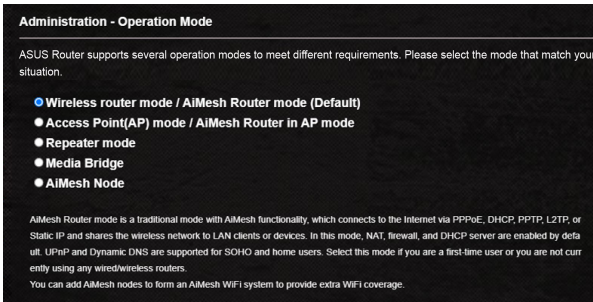


**หมายเหตุ:** ถ้าคุณเข้ามาที่ระบบเว็บ GUI เป็นครั้งแรก คุณจะถูกนำไปยังหน้า การตั้งค่าอินเทอร์เน็ตเดคตัน (QIS) โดยอัตโนมัติ

## 3.2 การดูแลระบบ

### 3.2.1 โหมดการทำงาน

หน้า โหมดการทำงาน อนุญาตให้คุณเลือกโหมดที่เหมาะสมสำหรับเครือข่ายของคุณ



ในการตั้งค่าโหมดการทำงาน:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง) > Administration (การดูแลระบบ) > Operation Mode (โหมดการทำงาน)**

2. เลือกโหมดการทำงานเหล่านี้:

- **โหมดไวร์เลสเราเตอร์ / โหมดAiMesh เราเตอร์ (ค่าเริ่มต้น):** ในโหมดไวร์เลสเราเตอร์, ไวร์เลสเราเตอร์จะเชื่อมต่อไปยังอินเทอร์เน็ต และให้การเข้าถึงอินเทอร์เน็ตไปยังอุปกรณ์ที่ใช้ได้บนเครือข่ายแลนของตัวเอง
- **จุดเข้าใช้งาน (AP) โหมด/ โหมดเราเตอร์ AiMesh ใน AP:** ในโหมดนี้ เราเตอร์จะสร้างเครือข่ายไร้สายบนเครือข่ายที่มีอยู่แล้ว
- **โหมดรีพีตเตอร์:** ในโหมดรีพีตเตอร์ GT6 จะเชื่อมต่อไปยังเครือข่ายไร้สายแบบไร้สายเพื่อขยายพื้นที่การทำงานไร้สายให้ครอบคลุมมากขึ้น ในโหมดนี้ ไฟร์วอลล์, การแชร์ IP และฟังก์ชัน NAT จะถูกปิดทำงาน
- **มีเดียบริดจ์:** การตั้งค่านี้จำเป็นต้องใช้ไวร์เลสเราเตอร์สองตัว เราเตอร์ตัวที่สองจะทำหน้าที่เป็นมีเดียบริดจ์ ซึ่งอุปกรณ์หลายอย่าง เช่น สมาร์ท TV และเกมคอนโซลสามารถเชื่อมต่อผ่านอีเทอร์เน็ตได้



- **โหมด AiMesh:** การตั้งค่านี้ต้องใช้เราเตอร์ ASUS อย่างน้อยสองตัวที่รองรับ AiMesh เปิดใช้งานโหมด AiMesh และลงชื่อเข้าใช้ UI เว็บของเราเตอร์ AiMesh เพื่อค้นหาโหมด AiMesh ที่มีอยู่ในบริเวณใกล้เคียงเพื่อเข้าร่วมระบบ AiMesh ของคุณ ระบบ AiMesh มีสัญญาณครอบคลุมทั่วทั้งบ้านและการจัดการแบบรวมศูนย์

### 3. คลิก **Apply (นำไปใช้)**

**หมายเหตุ:** เราเตอร์จะบูตใหม่เมื่อคุณเปลี่ยนทั้งหมด

## 3.2.2 ระบบ

หน้า **System (ระบบ)** อนุญาตให้คุณกำหนดค่าการตั้งค่าไวร์เลสเราเตอร์ของคุณ

**ในการตั้งค่าระบบ:**

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง)** > **Administration (การดูแลระบบ)** > **System (ระบบ)**
2. คุณสามารถกำหนดค่าการตั้งค่าต่อไปนี้:
  - **เปลี่ยนรหัสผ่านล็อกอินของเราเตอร์:** คุณสามารถเปลี่ยนรหัสผ่านและชื่อล็อกอินของไวร์เลสเราเตอร์ โดยการป้อนชื่อและรหัสผ่านใหม่
  - **โซนเวลา:** เลือกโซนเวลาสำหรับเครือข่ายของคุณ
  - **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
  - **รายการไคลเอ็นต์:** ป้อน WAN IP แอดเดรสของอุปกรณ์เครือข่ายที่อนุญาตให้เข้าถึงยังการตั้งค่าของไวร์เลสเราเตอร์ รายการนี้จะถูกใช้ ถ้าคุณคลิก **Yes (ใช่)** ในรายการ **Only allow specific IP (อนุญาตเฉพาะ IP ที่เจาะจง)**
3. คลิก **Apply (นำไปใช้)**

### 3.2.3 การอัปเดตเฟิร์มแวร์

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

ในการอัปเดตเฟิร์มแวร์:

1. จากหน้าดั่งระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง) > Administration (การดูแลระบบ) > Firmware Upgrade (เฟิร์มแวร์อัปเดต)**
2. ในไฟล์ **New Firmware File (ไฟล์เฟิร์มแวร์ใหม่)**, คลิก **Browse (เรียกดู)** เพื่อค้นหาเฟิร์มแวร์ใหม่ในคอมพิวเตอร์ของคุณ
3. คลิก **Upload (อัปโหลด)**

หมายเหตุ:

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

### 3.2.4 การกู้คืน/การจัดเก็บ/การอัปเดตการตั้งค่า

ในการกู้คืน/จัดเก็บ/อัปเดตการตั้งค่า:

1. จากหน้าดั่งระบบเมนู 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 (จัดเก็บ)**, และคลิก **Save (จัดเก็บ)** ในหน้าต่างดาวน์โหลดไฟล์ เพื่อจัดเก็บไฟล์ระบบลงในพาร์ตที่คุณต้องการ
  - ในการกู้คืนการตั้งค่าระบบก่อนหน้า, คลิก **Browse (เรียกดู)** เพื่อค้นหาไฟล์ระบบที่คุณต้องการกู้คืน, จากนั้นคลิก **Upload (อัปโหลด)**

**สำคัญ!** ถ้าเกิดปัญหาขึ้น ให้อัปเดตเฟิร์มแวร์เวอร์ชันล่าสุด และกำหนดค่าการตั้งค่าใหม่ อย่างไรก็ตามเราเตอร์กลับเป็นการตั้งค่าเริ่มต้น

## 3.3 AiCloud 2.0

AiCloud 2.0 เป็นแอปพลิเคชันบริการคลาวด์ที่อนุญาตให้คุณบันทึกซิงค์ แชร์ และเข้าถึงไฟล์ของคุณ

**AiCloud 2.0**

ASUS AiCloud 2.0 keeps you connected to your data wherever and whenever you have an Internet connection. It links your home network and online storage service and lets you access your data through the AiCloud mobile app on your iOS or Android mobile device or through a personalized web link in a web browser. Now all your data can go where you go.

- Enter AiCloud 2.0 <https://router.asus.com>
- Find FAQs [GO](#)

ANDROID APP ON  
Google play  
Download on the  
App Store

The wireless router is currently using a private WAN IP address.  
This router may be in a multiple-NAT environment, and accessing AiCloud from WAN does not work.

**Cloud Disk**  
Enables USB-attached storage devices to be accessed, streamed or shared through an Internet-connected PC or device.

**Smart Access**  
Enables Network Place (Samba) networked PCs and devices to be accessed remotely. Smart Access can also wake up a sleeping PC.

**AiCloud Sync**  
Enables synchronization of USB-attached storage with cloud services like [ASUS Webstorage](#) and other AiCloud 2.0-enabled networks.

### ในการใช้ AiCloud:

1. จาก Google เพลย์สโตร์ หรือ Apple สโตร์, ดาวน์โหลดและติดตั้งแอป ASUS AiCloud ไปยังอุปกรณ์สมาร์ตของคุณ
2. เชื่อมต่ออุปกรณ์สมาร์ตของคุณเข้ากับเครือข่าย ปฏิบัติตามขั้นตอนเพื่อทำการบวนาการตั้งค่า AiCloud ให้สมบูรณ์

### 3.3.1 คลาวด์ดีสก์

#### ในการสร้างคลาวด์ดีสก์:

1. เสียบอุปกรณ์เก็บข้อมูล USB เข้ากับไวร์เลสเราเตอร์
2. เปิด คลาวด์ดีสก์

**AiCloud 2.0**

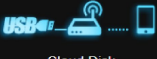


ASUS AiCloud 2.0 keeps you connected to your data wherever and whenever you have an Internet connection. It links your home network and online storage service and lets you access your data through the AiCloud mobile app on your iOS or Android mobile device or through a personalized web link in a web browser. Now all your data can go where you go.

- Enter AiCloud 2.0 <https://router.asus.com>
- Find FAQs [GO](#)

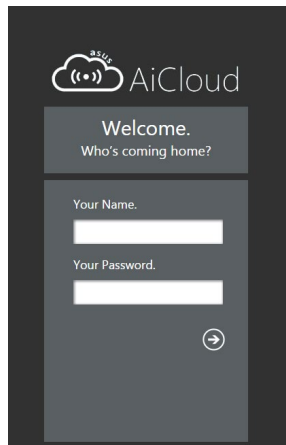
ANDROID APP ON  
Google play

Download on the  
App Store

The wireless router is currently using a private WAN IP address.  
This router may be in a multiple-NAT environment, and accessing AiCloud from WAN does not work.

 <p>Cloud Disk</p>	Enables USB-attached storage devices to be accessed, streamed or shared through an Internet-connected PC or device.	<input type="checkbox"/>
 <p>Smart Access</p>	Enables Network Place (Samba) networked PCs and devices to be accessed remotely. Smart Access can also wake up a sleeping PC.	<input type="checkbox"/>
 <p>AiCloud Sync</p>	Enables synchronization of USB-attached storage with cloud services like <b>ASUS Webstorage</b> and other AiCloud 2.0-enabled networks.	<input type="button" value="GO"/>

3. ไปที่ <http://www.asusrouter.com> และป้อนบัญชีผู้ใช้ของคุณ และรหัสผ่านของเรอูเตอร์ เพื่อให้ได้ประสบการณ์ผู้ใช้ที่ดีกว่า เราแนะนำให้คุณใช้ **Google Chrome** หรือ **Firefox**

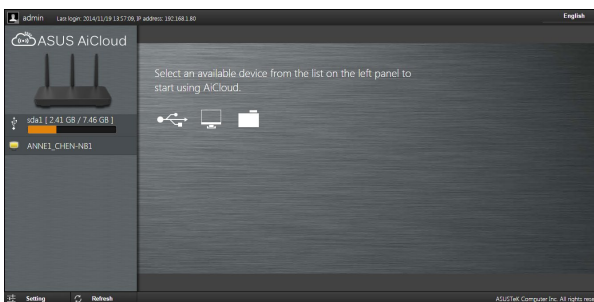


4. ขณะนี้คุณสามารถเริ่มการใช้งานไฟล์บนคลาวด์ได้กับอุปกรณ์ที่เชื่อมต่อกับเครือข่ายใดแล้ว

---

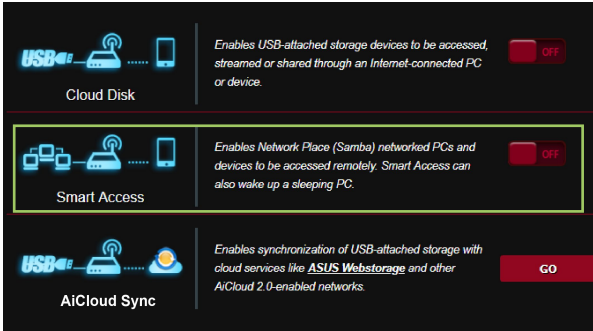
**หมายเหตุ:** ในขณะที่เข้าถึงอุปกรณ์ที่เชื่อมต่ออยู่กับเครือข่าย คุณจำเป็นต้องป้อนชื่อผู้ใช้และรหัสผ่านของอุปกรณ์ด้วยตัวเอง ซึ่งจะไม่ถูกบันทึกโดย AiCloud เนื่องจากเหตุผลด้านความปลอดภัย

---



### 3.3.2 เข้าถึงแบบสมาร์ท

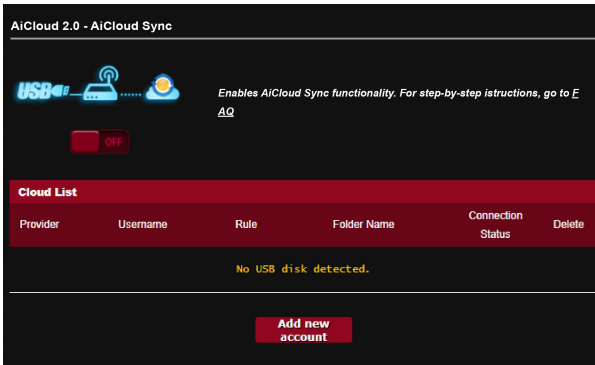
ฟังก์ชัน เข้าถึงแบบสมาร์ท อนุญาตให้คุณเข้าถึงเครื่องข่ายที่บ้านของคุณผ่านชื่อโดเมนของเราเตอร์ของคุณได้



#### หมายเหตุ:

- คุณสามารถสร้างชื่อโดเมนสำหรับเราเตอร์ของคุณด้วย ASUS DDNS สำหรับรายละเอียดเพิ่มเติม โปรดดูส่วน **3.20.6 DDNS**
- ตามค่าเริ่มต้น AiCloud ให้การเชื่อมต่อ HTTPS ที่มีระบบรักษาความปลอดภัย ป้อน [https://\[ชื่อ ASUSDDNS ของคุณ\].asuscomm.com](https://[ชื่อ ASUSDDNS ของคุณ].asuscomm.com) สำหรับการใช้งานคลาวด์ดีสก์ และการเข้าถึงแบบสมาร์ทที่มีความปลอดภัยมาก

### 3.3.3 AiCloudซิงค์

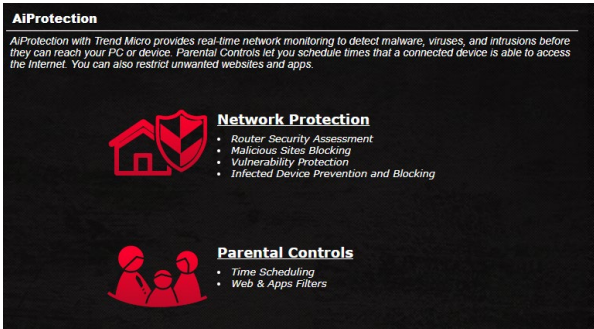


#### ในการใช้ AiCloud ซิงค์:

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

## 3.4 AiProtection

AiProtection มีการตรวจสอบแบบเรียลไทม์ที่ตรวจจับมัลแวร์ ภัยร้าย และ การเข้าถึงที่ไม่ต้องการ นอกจากนี้ยังช่วยกรอง เว็บไซต์และแอปที่ไม่พึงประสงค์ออกไป และอนุญาตให้คุณกำหนด ตารางเวลาที่อุปกรณ์ที่เชื่อมต่อสามารถเข้าถึงอินเทอร์เน็ตได้



**AiProtection**

*AiProtection with Trend Micro provides real-time network monitoring to detect malware, viruses, and intrusions before they can reach your PC or device. Parental Controls let you schedule times that a connected device is able to access the Internet. You can also restrict unwanted websites and apps.*

**Network Protection**

- Router Security Assessment
- Malicious Sites Blocking
- Vulnerability Protection
- Infected Device Prevention and Blocking

**Parental Controls**

- Time Scheduling
- Web & Apps Filters



### 3.4.1 การกำหนดค่า AiProtection

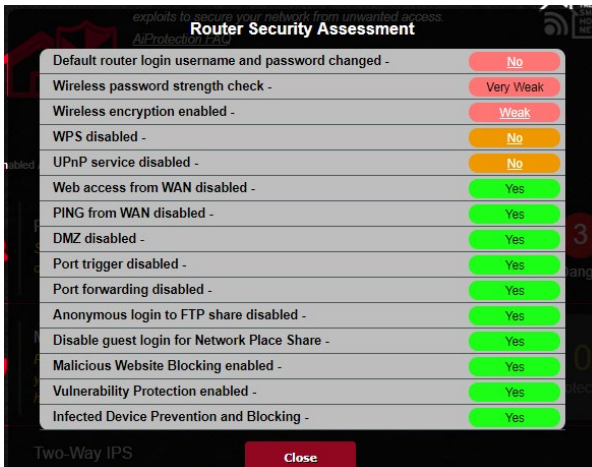
AiProtection ป้องกันการใช้ประโยชน์จากเครือข่าย และป้องกันเครือข่ายของคุณจากการเข้าถึงที่ไม่พึงประสงค์



วิธีการกำหนดค่า AiProtection:

1. จากแผงหน้าทาง ไปที่ **General (ทั่วไป) > AiProtection**
2. จากหน้าหลักของ AiProtection กด คลิที่ **Network Protection (การป้องกันเครือข่าย)**
3. จากแท็บ Network Protection (การป้องกันเครือข่าย) คลิที่ **Scan (สแกน)**

ผลการค้นหาจะแสดงอยู่บนหน้า **Router Security Assessment (การประเมินความปลอดภัยของเราเตอร์)**



**สำคัญ!** รายการที่ทำเครื่องหมายด้วย **Yes (ใช่)** บนหน้า **Router Security Assessment (การประเมินความปลอดภัยของเราเตอร์)** จะถือว่าเป็นปลอดภัย

4. (ทางเลือก) จากหน้า **Router Security Assessment (การประเมินความปลอดภัยของเราเตอร์)** กำหนดค่ารายการที่ทำเครื่องหมายเป็น **No (ไม่)**, **Weak (อ่อน)**, หรือ **Very Weak (อ่อนมาก)** ในการดำเนินการ:
  - a. คลิกที่รายการเพื่อไปที่หน้าการตั้งค่าของรายการ
  - b. จากหน้าการตั้งค่าด้านความปลอดภัยของรายการ ให้กำหนดค่า และทำการเปลี่ยนแปลงที่จำเป็น และคลิก **Apply (นำไปใช้)** เมื่อทำเสร็จ
  - c. ไปที่หน้า **Router Security Assessment (การประเมินความปลอดภัยของเราเตอร์)** และคลิก **Close (ปิด)** เพื่อออกจากหน้า
5. คลิกที่ **OK (ตกลง)** บนข้อความการยืนยัน

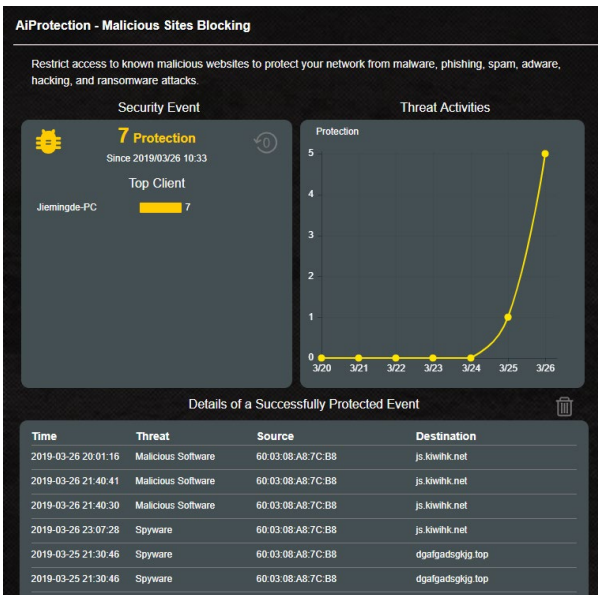
## 3.4.2 การบล็อกเว็บไซต์ที่ประสงค์ร้าย

คุณสมบัตินี้จำกัดการเข้าถึงยังเว็บไซต์ที่ประสงค์ร้ายที่รู้จักในฐานข้อมูลบนคลาวด์ เพื่อการป้องกันที่ปรับปรุงอยู่ตลอดเวลา

หมายเหตุ: ฟังก์ชันนี้จะเปิดใช้งานโดยอัตโนมัติถ้าคุณรัน Router Weakness Scan (สแกนความอ่อนแอของเราเตอร์)

### วิธีการเปิดใช้งานการบล็อกเว็บไซต์ที่ประสงค์ร้าย

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



### 3.4.3 Two-Way IPS

คุณสมบัตินี้แก้ไขปัญหาการโจมตีข้อบกพร่องที่พบทั่วไปภายใน การกำหนดค่าเราเตอร์

หมายเหตุ: ฟังก์ชันนี้จะเปิดใช้งานโดยอัตโนมัติถ้าคุณรัน Router Weakness Scan (สแกนความอ่อนแอของเราเตอร์)

#### วิธีการเปิดใช้งาน Two-Way IPS:

1. จากแผงหน้าทาง ไปที่ **General (ทั่วไป) > AiProtection**
2. จากหน้าหลักของ AiProtection คลิกที่ **Network Protection (การป้องกันเครือข่าย)**
3. จากแผง Two-Way IPS คลิก **ON (เปิด)**



### 3.4.4 การป้องกันและการบล็อกอุปกรณ์ที่ติดไวรัส

คุณสมบัตินี้ป้องกันอุปกรณ์ที่ติดไวรัสไม่ให้ส่งข้อมูลส่วนตัวหรือสถานะที่ติดไวรัสไปยังบุคคลภายนอก

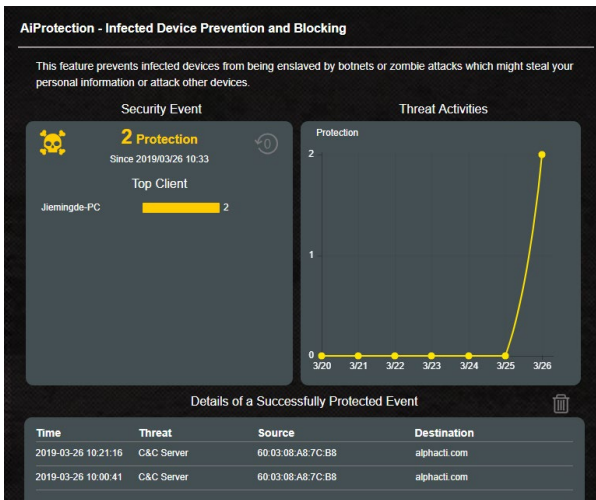
**หมายเหตุ:** ฟังก์ชันนี้จะเปิดใช้งานโดยอัตโนมัติถ้าคุณรัน Router Weakness Scan (สแกนความอ่อนแอของเราเตอร์)

**วิธีการเปิดใช้งานการป้องกันและการปิดกั้นอุปกรณ์ที่ติดไวรัส:**

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

**วิธีการกำหนดค่าการกำหนดลักษณะการแจ้ง:**

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

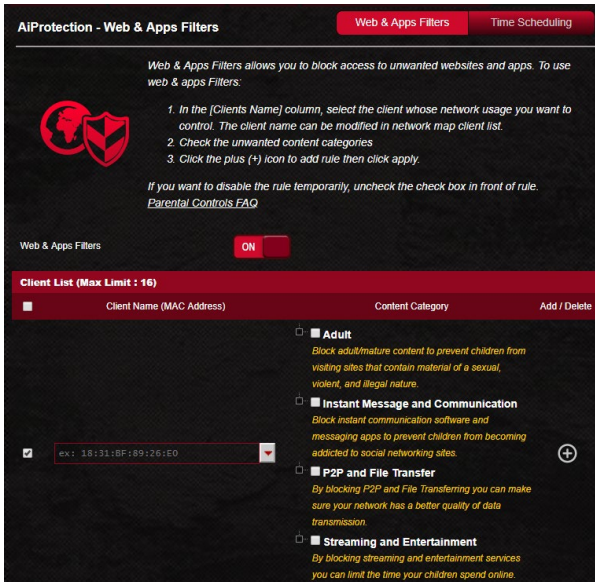


### 3.4.5 การตั้งค่าการควบคุมโดยผู้ปกครอง

การควบคุมโดยผู้ปกครอง อนุญาตให้คุณควบคุมเวลาใช้อินเทอร์เน็ต หรือตั้งคําขีดจำกัดเวลาสำหรับการใช้เครือข่ายของไคลเอ็นต์ได้

วิธีการเปิดใช้งาน Two-Way IPS:


1. จากแผงหน้าทาง ไปที่ **General (ทั่วไป) > AiProtection**
2. จากหน้าหลักของ AiProtection คลิกที่ **Parental Controls (การควบคุมโดยผู้ปกครอง)**



## ตัวกรองเว็บ & แอป

ตัวกรองเว็บ & แอป เป็นคุณสมบัติหนึ่งของการควบคุมโดยผู้ปกครองที่อนุญาตให้คุณบล็อกการเข้าถึงไปยังเว็บไซต์หรือแอปพลิเคชันที่ไม่ต้องการ

วิธีการกำหนดค่าตัวกรองเว็บ & แอป:

1. จากแผงหน้าทาง ไปที่ **General (ทั่วไป) > AiProtection**
2. จากหน้าหลักของ AiProtection คลิกที่ไอคอน **Parental Controls (การควบคุมโดยผู้ปกครอง)** เพื่อไปยังแท็บ Parental Controls (การควบคุมโดยผู้ปกครอง)
3. จากแผง **Web & Apps Filters (งานตัวกรองเว็บ & แอป)** คลิก **ON (เปิด)**
4. เมื่อข้อความข้อตกลงในการอนุญาตให้ใช้งานของผู้ใช้ (EULA) ปรากฏขึ้น คลิก **I agree (ยอมรับ)** เพื่อทำต่อ
5. จากคอลัมน์ **Client List (รายการไอคลเอนด์)** เลือกหรือพิมพ์ชื่อไอคลเอนด์จากรายการแบบดิ่งลงเขาไป
6. 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)**
7. คลิก  เพื่อเพิ่มโปรไฟล์ของไอคลเอนด์
8. คลิก **Apply (นำไปใช้)** เพื่อจัดเก็บการตั้งค่า



## การกำหนดตารางเวลา

การกำหนดเวลาช่วยให้คุณสามารถตั้งค่าขีดจำกัดเวลาสำหรับการใช้งานเครือข่ายของไคลเอนต์หนึ่งได้

**หมายเหตุ:** ให้แน่ใจว่าเวลาระบบของคุณซิงโครไนซ์กับ NTP เซิร์ฟเวอร์

**AiProtection - Time Scheduling** Web & Apps Filters Time Scheduling

Time Scheduling allows you to set up time limits for a specific client's network usage.

1. In the [Clients Name] column, select the client whose network usage you want to control. You may also key in the clients MAC address in the [Clients MAC Address] column.
2. In the [Add / Delete] column, click the plus(+) icon to add the client.
3. In the [Time Management] column, click the edit icon to edit the Active Schedule.
4. Select your time slot with a click. You can hold and drag to extend the duration.
5. Click [OK] to save the settings made.

**Note:**

1. Clients that are added to Parental Controls will have their internet access restricted by default.
2. Please disable NAT Acceleration for more precise scheduling control.

Enable Time Scheduling **ON**

System Time **Sat, May 05 07:53:34 2018**  
\* Reminder: The system time has not been synchronized with an NTP server.  
\* Reminder: The System time zone is different from your locale setting.

**Client List (Max Limit : 16)**

	Client Name (MAC Address)	Time Management	Add / Delete
<input checked="" type="checkbox"/>	ex: 18:31:BF:69:26:E0	-	+

No data in table.

**Apply**

วิธีการกำหนดค่าตารางเวลา:

1. จากแผงหน้าทาง ไปที่ **General (ทั่วไป) > AiProtection > Parental Controls (การควบคุมโดยผู้ปกครอง) > Time Scheduling (การกำหนดตารางเวลา)**
2. จากแผง **Enable Time Scheduling (เปิดใช้งานการกำหนดตารางเวลา)** คลิก **ON (เปิด)**
3. จากคอลัมน์ **Clients Name (ชื่อไคลเอนต์)** เลือกหรือพิมพ์ชื่อ ไคลเอนต์จากรายการแบบดิ่งลงเข้าไป

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

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



### 3.5 แดชบอร์ด

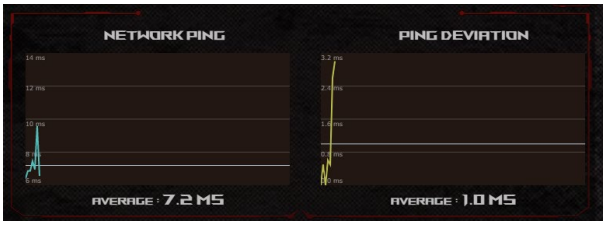
Dash Board (แดชบอร์ด) ช่วยให้คุณสามารถตรวจสอบเครือข่าย การรับส่งข้อมูลแบบเรียลไทม์สำหรับสภาพแวดล้อมเครือข่ายของคุณ และวิเคราะห์ค่า ping เครือข่ายและค่าเบี่ยงเบนของ ping แบบเรียลไทม์



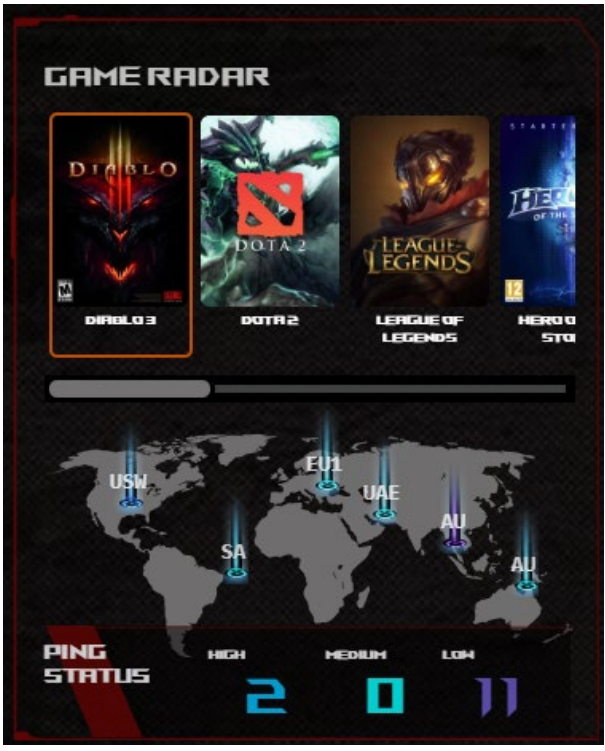
ค่า ping เครือข่ายอ้างอิงกับประสบการณ์การเล่นเกมนออนไลน์ ค่า ping ที่สูงขึ้นหมายถึงเวลาแฝงที่สูงขึ้นสำหรับเกมแบบเรียลไทม์ สำหรับเกมออนไลน์ส่วนใหญ่ ค่า ping เครือข่ายที่น้อยกว่า 99 ms

ถือว่ามึคณภาพดี ถ้าค่า ping เครือข่ายน้อยกว่า 150 ms ถือว่า คณภาพเป็นที่ยอมรับได้ โดยทั่วไปถ้าค่า ping เครือข่ายมากกว่า 150 ms ก็ยากที่จะเล่นเกมได้โดยราบรื่น

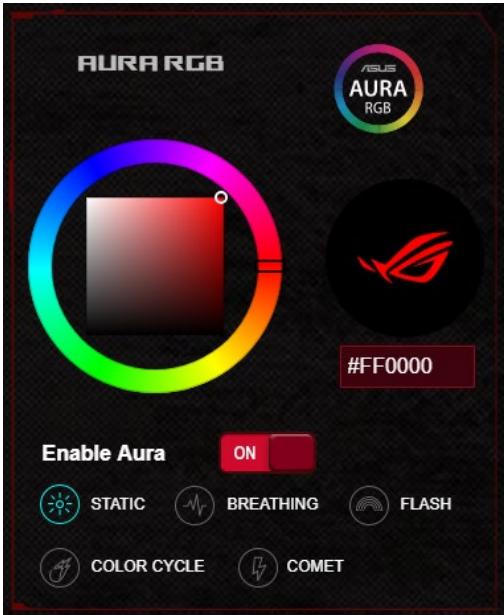
ค่าเบี่ยงเบนของ ping มีความเกี่ยวข้องกับประสบการณ์การเล่น เกมออนไลน์อย่างมาก ด้วยค่าเบี่ยงเบนของ ping ที่สูงขึ้น จะทำให้ การสลับทำได้ง่ายขึ้นเมื่อเล่นเกมออนไลน์ ไม่มีเส้นฐานสำหรับค่า เบี่ยงเบนของ ping ใดๆก็ตาม ค่าเบี่ยงเบนของ ping ที่ต่ำลง จะดีกว่า



- **เรดาร์เกม:** เรดาร์เกมจากแดชบอร์ดช่วยให้คุณสามารถดูเวลา การปิงได้อย่างรวดเร็วสำหรับเซิร์ฟเวอร์เกมทีละบุ



- **Aura RGB:** ช่วยให้ผู้ใช้สามารถกำหนดหรือเปิด/ปิด Aura RGB จากแดชบอร์ด คุณสามารถตั้งค่าสีใดก็ได้และเลือกรูปแบบไฟค้นหาแบบ



## 3.6 ไฟร์วอลล์

ไฟร์วอลล์เราเตอร์สามารถทำหน้าที่เป็นฮาร์ดแวร์ไฟร์วอลล์สำหรับเครือข่ายของคุณได้

---

หมายเหตุ: ตามค่าเริ่มต้น คุณสมบัติไฟร์วอลล์จะเปิดทำงาน

---

### 3.6.1 ท้าไป

ในการตั้งค่าไฟร์วอลล์พื้นฐาน:

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

### 3.6.2 ตัวกรอง URL

คุณสามารถระบุค่าสำคัญหรือเว็บแอดเดรส เพื่อป้องกันการเข้าถึงยัง URL ที่เจาะจงได้

---

หมายเหตุ: ตัวกรอง URL เป็นไปตามการสอบถาม DNS ถ้าเน็ตเวิร์กไคลเอนต์เข้าถึงเว็บไซต์อยู่แล้ว เช่น <http://www.abcxxx.com>, เว็บไซต์จะไม่ถูกล็อก (DNS แคชในระบบเก็บเว็บไซต์ที่เข้าชมก่อนหน้านี้) ในการแก้ไขปัญหานี้ ให้ล้าง DNS แคชก่อนที่จะตั้งค่าตัวกรอง URL

---

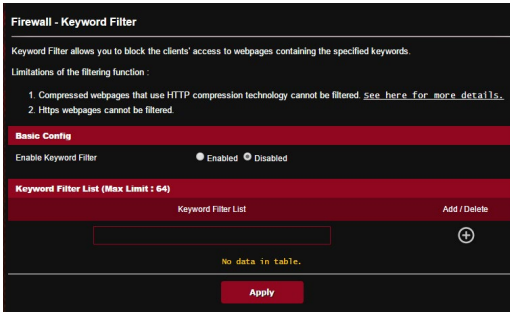
ในการตั้งค่าตัวกรอง URL:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings** (การตั้งค่าขั้นสูง) > **Firewall (ไฟร์วอลล์)** > **URL Filter** (ตัวกรอง URL)

2. บนฟิลต์ **Enable URL Filter** (เปิดทำงานตัวกรอง URL), เลือก **Enabled** (เปิดทำงาน)
3. บ้อน URL และคลิกปุ่ม **+**
4. คลิก **Apply** (นำไปใช้)

### 3.6.3 ตัวกรองคำสำคัญ

ตัวกรองคำสำคัญจะบล็อกการเข้าถึงไปยังเว็บเพจที่ประกอบด้วยคำสำคัญที่ระบุ



ในการตั้งค่าตัวกรองคำสำคัญ:

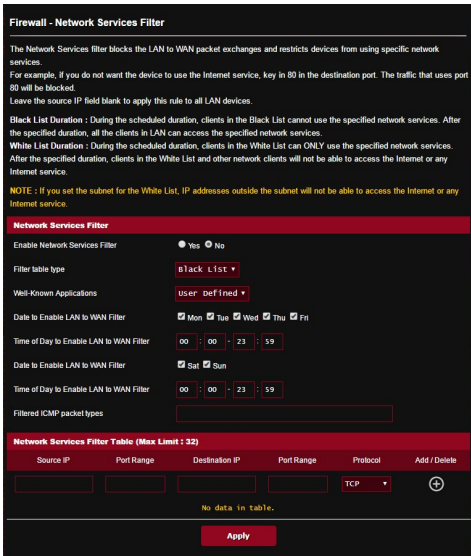
1. จากหน้าตาของระบบเมนู ไปยัง **Advanced Settings** (การตั้งค่าขั้นสูง) > **Firewall** (ไฟรอลล์) > **Keyword Filter** (ตัวกรองคำสำคัญ)
2. บนฟิลต์ **Enable Keyword Filter** (เปิดทำงานตัวกรองคำสำคัญ), เลือก **Enabled** (เปิดทำงาน)
3. บ้อนคำหรือวลี และคลิกปุ่ม **+**
4. คลิก **Apply** (นำไปใช้)

#### หมายเหตุ:

- ตัวกรองคำสำคัญ เป็นไปตามการสอบถาม DNS ถ้าเน็ตเวิร์กโพลเอนด์เข้าถึงเว็บไซต์อยู่แล้ว เช่น <http://www.abcxxx.com>, เว็บไซต์จะไม่ถูกบล็อก (DNS แคลชในระบบเก็บเว็บไซต์ที่เข้าชมก่อนหน้านี้) ในการแก้ไขปัญหานี้ให้ล้าง DNS แคชก่อนที่จะตั้งค่าตัวกรองคำสำคัญ
- เว็บเพจที่มีขนาดโดยใช้การบีบขนาด HTTP ไม่สามารถถูกกรองได้ เพจ HTTPS ยังไม่สามารถถูกบล็อกโดยใช้ตัวกรองคำสำคัญได้เช่นกัน

### 3.6.4 ตัวกรองบริการเครือข่าย

ตัวกรองบริการเครือข่าย บล็อกการแลกเปลี่ยนแพคเกจ LAN ไปยัง WAN และจำกัดเน็ตเวิร์กโพลีโคลเอนต์ไม่ให้เข้าถึงยังบริการเว็บไซต์ที่เจาะจง เช่น Telnet หรือ FTP



ในการตั้งค่าตัวกรองบริการเครือข่าย:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง) > Firewall (ไฟรอลล์) > Network Service Filter (ตัวกรองบริการเครือข่าย)**
2. บนฟิลต์ **Enable Network Services Filter (เปิดทำงานตัวกรองบริการเครือข่าย)**, เลือก **Yes (ใช่)**
3. เลือกชนิดตารางตัวกรอง **Black List (บัญชีดำ)** บล็อกบริการเครือข่ายที่ระบุ **White List (บัญชีขาว)** 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)**

### 3.6.5 ไฟร์วอลล์ IPv6

ตามค่าเริ่มต้น ASUS ไร้เลสเราเตอร์ของคุณจะบล็อกข้อมูลขาเข้าที่ไม่พึงประสงค์ทั้งหมด ฟังก์ชัน ไฟร์วอลล์ IPv6 อนุญาตให้การรับส่งขาเข้าที่มาจากบริการที่ระบุผ่านเข้ามายังเครือข่ายของคุณ

**Firewall - 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 empty 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 Please select ▼

**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 ▼	+

No data in table.

**Apply**

## 3.7 อัตราเร่งของเกม

คุณสมบัตินี้ช่วยให้คุณสามารเปิดใช้ Game Boost ได้ด้วยคลิกเดียว เมื่อเปิดใช้งาน Game Boost GT-AX6000 จะจัดลำดับขั้นแพ็คเก็ตเกมไว้ในลำดับสูงสุดเพื่อให้คุณได้รับประสบการณ์การเล่นเกมที่ดีที่สุด



### Game Boost

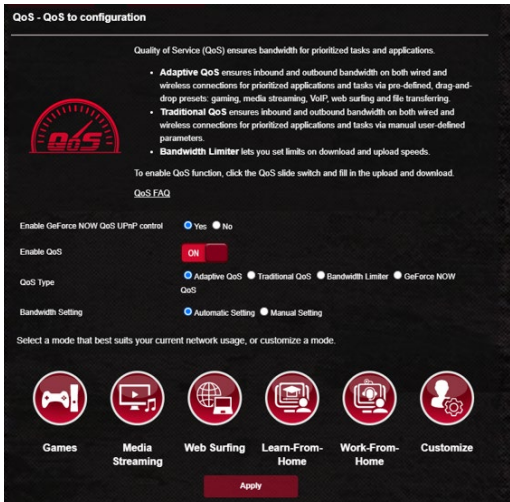
วิธีการเปิดการ Game Boost:

จาก Game Boost เลื่อนแถบเลื่อน Enable Game Boost (เปิดใช้งานมุดเกม) ไปที่ ON (เปิด)



### 3.7.1 QoS (คุณภาพของการให้บริการ)

คุณสมบัตินี้มีไว้สำหรับตรวจสอบแบนด์วิดท์สำหรับงานและแอปพลิเคชันที่มีลำดับความสำคัญสูง



วิธีการเปิดใช้งานฟังก์ชัน QoS:

1. จากแผงหน้าทาง ไปที่ **General (ทั่วไป) > อัตราเร่งของเกม > QoS**
2. จากแผง **Enable QoS (เปิดใช้งาน QoS)** คลิก **ON (เปิด)**
3. เลือกชนิด QoS (อะแดปทีฟ ดั้งเดิม หรือตัวจำกัดแบนด์วิดท์) สำหรับการกำหนดค่าของคุณ

---

**หมายเหตุ:** ดูที่แท็บ QoS สำหรับค่าจำกัดความของชนิด QoS

---

4. คลิก **Automatic Setting (การตั้งค่าอัตโนมัติ)** สำหรับแบนด์วิดท์ที่เหมาะสมที่สุดโดยอัตโนมัติ หรือ **Manual Setting (การตั้งค่าด้วยตนเอง)** เพื่อตั้งค่าการอัปโหลดและดาวน์โหลดแบนด์วิดท์ด้วยตนเอง

---

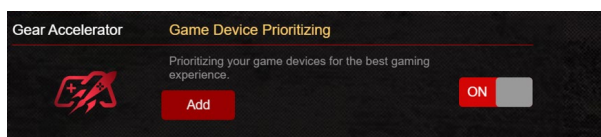
**หมายเหตุ:** รับข้อมูลแบนด์วิดท์จาก ISP ของคุณ นอกจากนี้ คุณสามารถไปที่ <http://speedtest.net> เพื่อตรวจสอบ และรับแบนด์วิดท์ของคุณ

---


5. คลิก **Apply (นำไปใช้)**

## 3.7.2 Gear Accelerator

Gear Accelerator อนุญาตให้คุณจัดลำดับความสำคัญของอุปกรณ์เกมแบบไร้สาย ผ่านแผงควบคุมออนไลน์สำหรับประสบการณ์การเล่นเกมที่ดีที่สุด



ในการกำหนดค่า Gear Accelerator:

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

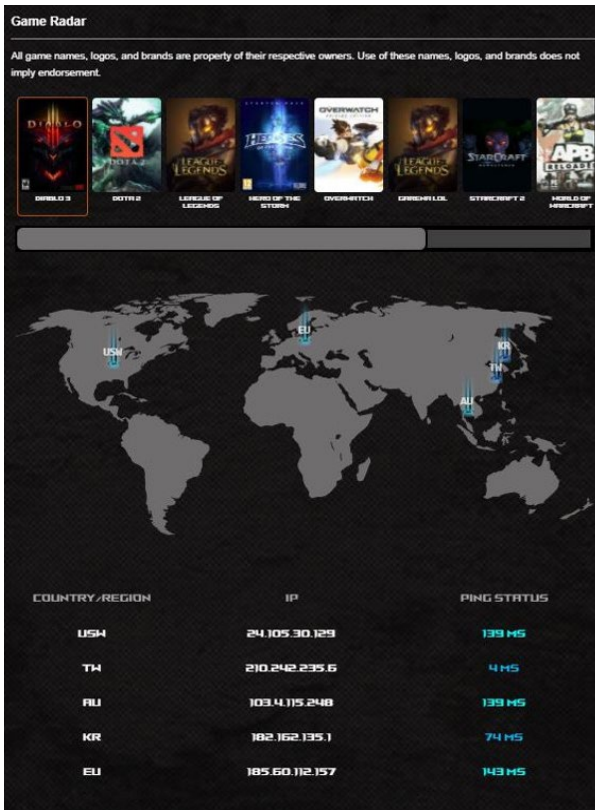
---

หมายเหตุ: ถ้าคุณต้องการลบโปรไฟล์ของไอคอนเอ็นดี คลิก 

---

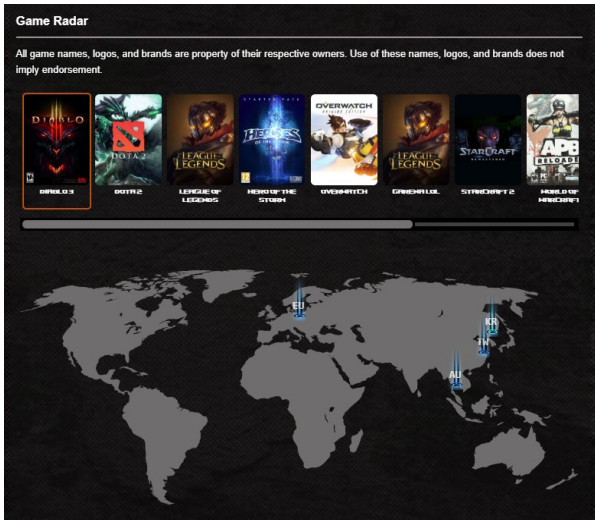
## 3.8 เรดาร์เกม

เกมเรดาร์เป็นเครื่องมือวินิจฉัยที่ช่วยให้คุณสามารถระบุคุณภาพการเชื่อมต่อของเซิร์ฟเวอร์สำหรับเกมที่เฉพาะเจาะจง



### วิธีการใช้เรดาร์เกม

1. จากแผงหน้าทาง ไปที่ **General (ทั่วไป) > Game Radar (เรดาร์เกม)** และเลือกเกมจากรายการเกม



2. ตรวจสอบ **Ping Status (สถานะ ping)** ของแต่ละเซิร์ฟเวอร์
3. สำหรับการเล่นเกมออนไลน์ที่ราบรื่น ให้เลือกเซิร์ฟเวอร์เกมที่มีสถานะ ping ต่ำ

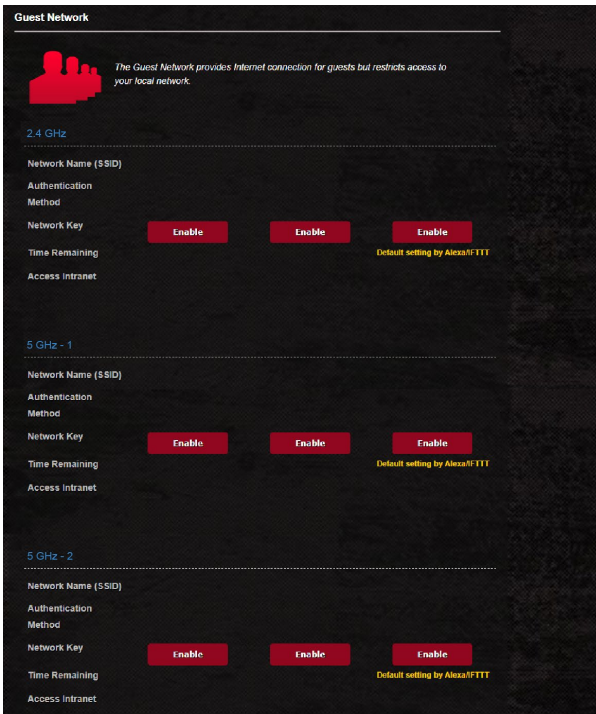
## 3.9 เครือข่ายแขก

เครือข่ายแขก ให้การเชื่อมต่ออินเทอร์เน็ตชั่วคราวแก่ผู้มาเยี่ยมชม ผ่านการเข้าถึง SSID หรือเครือข่ายที่แยกกัน โดยไม่ต้องให้การเข้าถึงไปยังเครือข่ายส่วนตัวของคุณ

หมายเหตุ: GT6 สนับสนุน SSID มากถึง 9 ตัว (2.4GHz 3 ตัว 5GHz-1 3 ตัว และ 5GHz-2 3 ตัว)

ในการสร้างเครือข่ายแขกของคุณ:

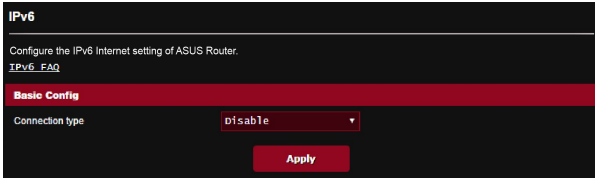
1. จากหน้าดั่งระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง) > Guest Network (เครือข่ายแขก)**
2. บนหน้าจอ Guest Network (เครือข่ายแขก), เลือกแถบความถี่ 2.4GHz 5GHz-1 หรือ 5GHz-2 สำหรับเครือข่ายแขกที่คุณต้องการสร้าง
3. คลิก **Enable (เปิดทำงาน)**



4. ในการเปลี่ยนแปลงการตั้งค่าของแชน ให้คลิกการตั้งค่าของแชนที่คุณต้องการแก้ไข คลิก **Remove (ลบ)** เพื่อลบการตั้งค่าของแชน
5. กำหนดชื่อเครือข่ายไร้สายสำหรับเครือข่ายชั่วคราวของคุณบนพีลด์ ชื่อเครือข่าย (SSID)
6. เลือก วิธีการยืนยันตัวตนบุคคล
7. ถ้าคุณเลือกวิธีการยืนยันตัวตนบุคคล WPA ให้เลือกการเข้ารหัส WPA
8. ระบุ เวลาการเข้าถึง หรือคลิก **Limitless (ไม่จำกัด)**
9. เลือก **Disable (ปิดทำงาน)** หรือ **Enable (เปิดทำงาน)** บนรายการ Access Intranet (เข้าถึงอินเทอร์เน็ต)
10. เมื่อทำเสร็จ, คลิก **Apply (นำไปใช้)**

## 3.10 IPv6

เราเตอร์เราเตอร์นี้สนับสนุน IPv6 แอดเดรสซึ่ง ซึ่งเป็นระบบที่สนับสนุน IP แอดเดรสมากกว่า มาตรฐานหนึ่งยังไม่ค่อยใช้กันอย่างกว้างขวาง ติดต่อ ISP ของคุณถ้าบริการอินเทอร์เน็ตของคุณสนับสนุน IPv6



ในการตั้งค่า IPv6:

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

---

**หมายเหตุ:** โปรดสอบถาม ISP ของคุณเกี่ยวกับข้อมูล IPv6 เฉพาะสำหรับบริการอินเทอร์เน็ตของคุณ

---

## 3.11 LAN

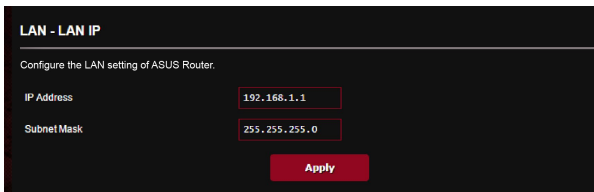
### 3.11.1 LAN IP

หน้าจอ LAN IP อนุญาตให้คุณแก้ไขการตั้งค่า LAN IP ของไวร์เลสเราเตอร์ของคุณ

---

**หมายเหตุ:** การเปลี่ยนแปลงใดๆ ต่อ LAN IP แอดเดรสจะถูกสะท้อนบนการตั้งค่า DHCP

---



LAN - LAN IP

Configure the LAN setting of ASUS Router.

IP Address

Subnet Mask

Apply

ในการปรับเปลี่ยนการตั้งค่า LAN IP:

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



### 3.11.2 DHCP เซิร์ฟเวอร์

ไวร์เลสเราเตอร์ของคุณใช้ DHCP เพื่อกำหนด IP แอดเดรสบนเครือข่ายของคุณโดยอัตโนมัติ คุณสามารถระบุช่วง IP แอดเดรสและลีสท์ใหม่ 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 of NDS server IP and default gateway IP. ASUS Router supports up to 253 IP addresses for your local network.

**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

WINS Server

**Enable Manual Assignment**

Enable Manual Assignment  Yes  No

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

Client Name (MAC Address)	IP Address	Add / Delete
No data in table.		

ในการกำหนดค่า DHCP เซิร์ฟเวอร์:

1. จากหน้าต่างระบบเมนู 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) (วินาที)**, ป้อนเวลาที่ IP แอดเดรสจะ หมดอายุ และไวร์เลสเราเตอร์จะกำหนด IP แอดเดรสใหม่ สำหรับเน็ตเวิร์กไคลเอนต์โดยอัตโนมัติ

---

**หมายเหตุ:**

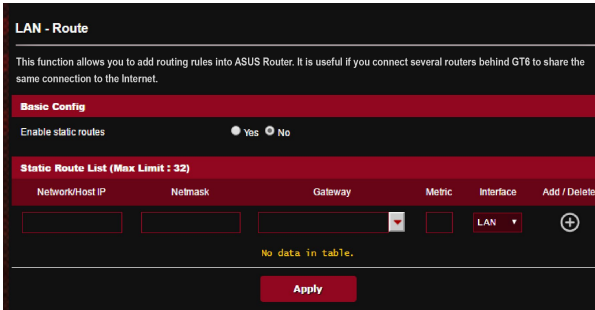
- ASUS แนะนำให้คุณใช้รูปแบบ IP แอดเดรสเป็น 192.168.1.xxx (ซึ่ง xxx สามารถเป็นตัวเลขใดๆ ก็ได้ระหว่าง 2 ถึง 254) ในขณะที่ระบุช่วง IP แอดเดรส
- แอดเดรสเริ่มต้น IP พูล ไม่ควรมีค่ามากกว่าแอดเดรสสิ้นสุด IP พูล

7. ในส่วน **DNS and WINS Server Settings (การตั้งค่า DNS และ WINS เซิร์ฟเวอร์)**, ป้อน DNS เซิร์ฟเวอร์และ WINS เซิร์ฟเวอร์ IP แอดเดรส ถ้าจำเป็น
8. ไวร์เลสเราเตอร์ของคุณยังสามารถกำหนด IP แอดเดรสด้วยตัวเองไปยังอุปกรณ์ต่างๆ บนเครือข่ายได้ด้วย บนฟิลด์ **Enable Manual Assignment (เปิดการทำงานการกำหนดด้วยตัวเอง)**, เลือก **Yes (ใช่)** เพื่อกำหนด IP แอดเดรสให้กับ MAC แอดเดรสเฉพาะบนเครือข่าย คุณสามารถเพิ่ม MAC แอดเดรสได้ถึง 32 รายการไปยังรายการ DHCP สำหรับการกำหนดด้วยตัวเอง



### 3.11.3 เส้นทาง

ถ้าเครือข่ายของคุณใช้ไวร์เลสเราเตอร์มากกว่าหนึ่งตัว คุณสามารถกำหนดค่าตารางเส้นทาง เพื่อแชร์บริการอินเทอร์เน็ตเดียวกันได้

**หมายเหตุ:** เราแนะนำให้คุณอย่าเปลี่ยนการตั้งค่าเส้นทางเริ่มต้น ถ้าคุณ ไม่มีความรูข้สูงเกี่ยวกับตารางเส้นทาง



ในการกำหนดค่าตารางเส้นทาง LAN:

1. จากหน้าต่างระบบเมนู 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)

### 3.11.4 IPTV

เราแนะนำให้ท่านสนับสนุนการเชื่อมต่อไปยังบริการ IPTV ผ่าน ISP หรือ LAN IPTV ให้การตั้งค่าการกำหนดค่าต่างๆ ที่จำเป็นในการตั้งค่า IPTV, VoIP, มัลติคาสติ้ง 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**

LAN1/ LAN2 ▾

**IPTV VoIP Port Settings**

Gaming Ports are set up in LAN1 and LAN2. If you would like to use Gaming Ports, please choose LAN 5/ LAN 6 for your IPTV or VoIP port.

Select ISP Profile: None ▾

Choose IPTV STB Port: None ▾

**Special Applications**

Use DHCP routes: Microsoft ▾

Enable multicast routing (IGMP Proxy): Disable ▾

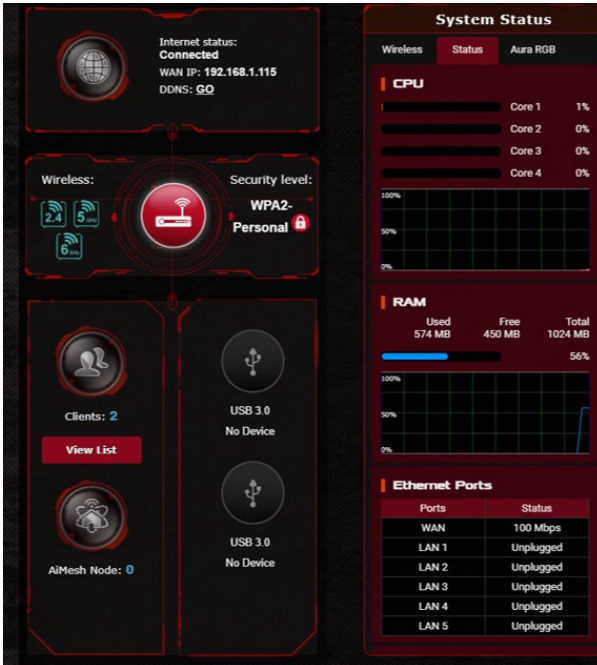
Enable efficient multicast forwarding (IGMP Snooping): Disable ▾

UDP Proxy (Udpxy): 0

Apply

## 3.12 การใช้แผนที่เครือข่าย

แผนที่เครือข่าย อนุญาตให้คุณกำหนดค่าการตั้งค่าระบบป้องกันของเครือข่ายของคุณ, จัดการเน็ตเวิร์กไคลเอนต์ของคุณ และตรวจดูแลอูปกรณ USB ของคุณ



### 3.12.1 การตั้งค่าระบบความปลอดภัยไร้สาย

เพื่อป้องกันเครือข่ายของคุณจากการเข้าถึงโดยไม่ได้รับอนุญาต คุณจำเป็นต้องกำหนดค่าของการตั้งค่าระบบความปลอดภัยของเครือข่ายในการตั้งค่าระบบความปลอดภัยไร้สาย:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings**, (การตั้งค่าขั้นสูง) > **Network Map** (แผนที่เครือข่าย)
2. บนหน้าจอ Network Map (แผนที่เครือข่าย) และภายใต้ **System Status** (สถานะระบบ), คุณสามารถกำหนดค่าต่างๆ ของระบบความปลอดภัยไร้สาย เช่น SSID, ระดับความปลอดภัย และการตั้งค่าการเข้ารหัส

---

หมายเหตุ: คุณสามารถตั้งค่าระบบความปลอดภัยไร้สายที่แตกต่างกันสำหรับแถบความถี่ 2.4GHz, 5GHz-1 และ 5GHz-2 ได้

---

### การตั้งค่าระบบความปลอดภัย 2.4GHz

**2.4 GHz**

Network Name (SSID)  
ASUS Router

Authentication Method  
WPA2-Personal

WPA Encryption  
AES

WPA-PSK key  
\*\*\*\*\*

### การตั้งค่าระบบความปลอดภัย 5GHz-1

**5 GHz-1**

Network Name (SSID)  
admin

Authentication Method  
WPA2-Personal

WPA Encryption  
AES

WPA-PSK key  
\*\*\*\*\*

### การตั้งค่าระบบความปลอดภัย 5GHz-2

**5 GHz-2**

Network Name (SSID)  
admin

Authentication Method  
WPA2-Personal

WPA Encryption  
AES

WPA-PSK key  
\*\*\*\*\*

3. บุนฟิลด์ **Network Name (SSID) (ชื่อเครือข่าย (SSID))**, บอนชื่อที่เป็นเอกลักษณ์สำหรับเครือข่ายไร้สายของคุณ
4. จากรายการ **Authentication Method (วิธีการยืนยันตัวตนบุคคล)** เลือกวิธีการยืนยันตัวตนบุคคลสำหรับเครือข่ายไร้สายของคุณ

ถ้าคุณเลือก WPA-ส่วนตัว หรือ WPA-2 ส่วนตัว เป็นวิธีการยืนยันตัวตนบุคคล ให้พิมพ์ WPA-PSK คีย์ หรือคีย์ผ่านด้านความปลอดภัยเข้าไป

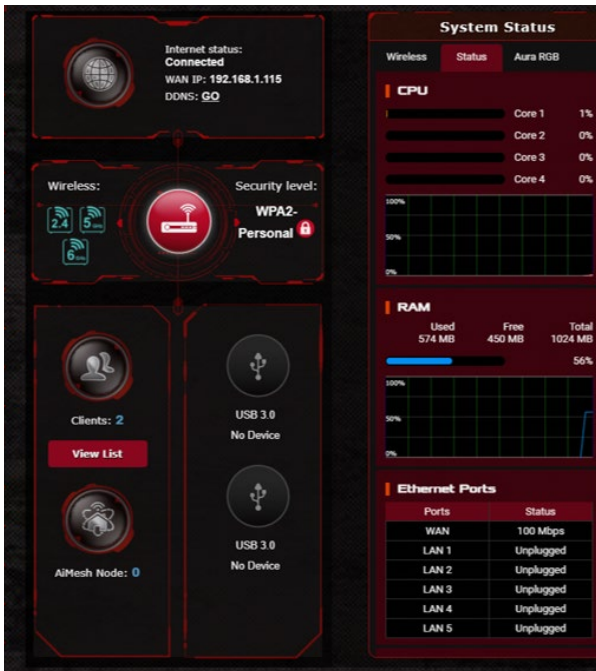
---

**สำคัญ!** มาตรฐาน IEEE 802.11n/ac ห้ามการใช้ไช่ทรพุดกับ WEP หรือ WPA-TKIP เป็นยูนแคสต์ไช่เฟออร์ ถ้าคุณใช้วิธีการเข้ารหัสเหล่านี้ อัตรการรับส่งข้อมูลของคุณจะตกลงเป็นการเชื่อมต้อ IEEE 802.11g 54Mbps

---

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

### 3.12.2 การจัดการเน็ตเวิร์กไคลเอนต์ของคุณ



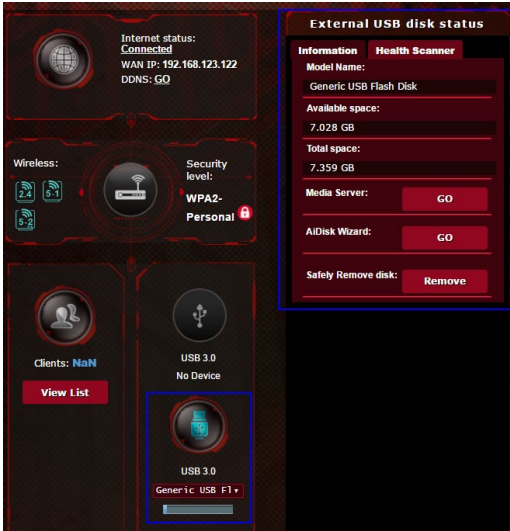
Internet	Icon	Clients Name	Clients IP Address	Clients MAC Address	Interface	Tx Rate (Mbps)	Rx Rate (Mbps)	Access Time
		android(Sony)	192.168.3.116	08:00:14:15:31:42	CA	433.3	40.5	02:10:155
		MIUI11_Plat...	192.168.3.203	E0:13:10:1E:42:0D		330	33.5	02:33:02
		AAL300616-NB2	192.168.3.240	50:46:15:01:64:15:84		-	-	-

ในการจัดการเน็ตเวิร์กไคลเอนต์ของคุณ:

1. จากหน้าตาของระบบเมนู ไปยัง **Advanced Settings**, (การตั้งค่าขั้นสูง) > **Network Map** (แผนที่เครือข่าย)
2. บนหน้าจอ **Network Map** (แผนที่เครือข่าย), เลือกไอคอน **Clients** (ไคลเอนต์) เพื่อแสดงข้อมูลเกี่ยวกับเน็ตเวิร์กไคลเอนต์ของคุณ
3. คลิก **View List** (มุมมองรายการ) ด้านล่างไอคอน **Clients** (ไคลเอนต์) เพื่อแสดงไคลเอนต์ทั้งหมด
4. เพื่อบล็อกการเข้าถึงของไคลเอนต์ไปยังเครือข่ายของคุณ, ให้เลือกไคลเอนต์ และคลิก ไอคอน เปิดล็อก

### 3.12.3 การตรวจสอบอุปกรณ์ USB ของคุณ

ASUS ไรร์เลสเราเตอร์ให้พอร์ต USB มาสองพอร์ต สำหรับเชื่อมต่ออุปกรณ์ USB หรือเครื่องพิมพ์ USB เพื่ออนุญาตให้คุณแชร์ไฟล์และเครื่องพิมพ์กับไคลเอนต์ต่างๆ ในเครือข่ายของคุณ



#### หมายเหตุ:

- ในการใช้คุณสมบัตินี้ คุณจำเป็นต้องเสียอุปกรณ์เก็บข้อมูล USB เช่น USB ฮาร์ดดิสก์ หรือ USB แฟลชไดรฟ์ เข้ากับพอร์ต USB 3.0/2.0 ที่แผงด้านหลังของไรร์เลสเราเตอร์ของคุณ ตรวจสอบให้แน่ใจว่าอุปกรณ์เก็บข้อมูล USB ได้รับการฟอร์แมตและแบ่งพาร์ติชันอย่างเหมาะสม ดูรายการสนับสนุนผลิตภัณฑ์แอ็นด์แชร์ดิสก์ที่ <http://event.asus.com/networks/disksupport>
- พอร์ต USB สนับสนุน USB ไดรฟ์สองตัว หรือเครื่องพิมพ์หนึ่งเครื่องและ USB ไดรฟ์อีกหนึ่งตัวในเวลาเดียวกัน

**สำคัญ!** แรกสุด คุณจำเป็นต้องสร้างบัญชีสำหรับแชร์ และกำหนดสิทธิ์การอนุญาต/การเข้าถึง เพื่ออนุญาตให้เน็ตเวิร์กไคลเอนต์อื่นๆ สามารถเข้าถึงอุปกรณ์ USB ของคุณผ่าน FTP ไรต์/ยูทิลิตี้ FTP ไคลเอนต์ของบริษัทอื่น, เซิร์ฟเวอร์เซิร์ฟเวอร์, แซมบ้า หรือ AiCloud สำหรับรายละเอียดเพิ่มเติม ให้อ่านส่วน 3.17 การใช้งานผ่าน USB และ 3.3 AiCloud 2.0 ในคู่มือผู้ใช้



## ในการตรวจดูแลอุปกรณ์ USB ของคุณ:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (Tetapan Lanjutan) > Network Map (แผนที่เครือข่าย)**
2. บนหน้าจอ Network Map (แผนที่เครือข่าย), เลือกไอคอน **USB Disk Status (สถานะ USB ดิสก์)** เพื่อแสดงข้อมูลของอุปกรณ์ USB ของคุณ
3. บนฟลุต, AiDisk Wizard (ตัวช่วยสร้าง AiDisk), คลิก **GO (ไป)** เพื่อตั้งค่า FTP เซิร์ฟเวอร์สำหรับการแชร์ไฟล์อินเทอร์เน็ต


### หมายเหตุ:

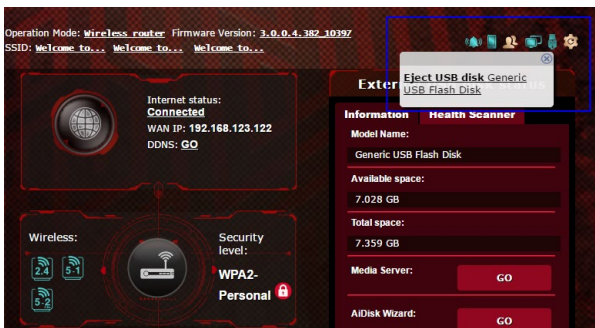
- สำหรับรายละเอียดเพิ่มเติม ให้ดูส่วน **3.17.2 การใช้เซิร์ฟเวอร์เซนต์ ออร์** ในคู่มือผู้ใช้ฉบับนี้
- ไวร์เลสเราเตอร์ทำงานกับ USB แฟลชดิสก์/HDD ขนาดใหญ่ (สูงสุด 2TB) และสนับสนุนการอ่าน-เขียนสำหรับระบบ FAT16, FAT32, NTFS และ HFS+

## การถอด USB ดิสก์อย่างปลอดภัย

**สำคัญ!** การถอด USB ดิสก์อย่างไม่ถูกต้อง อาจทำให้ข้อมูลเสียหายได้

## ในการถอด USB ดิสก์อย่างปลอดภัย:

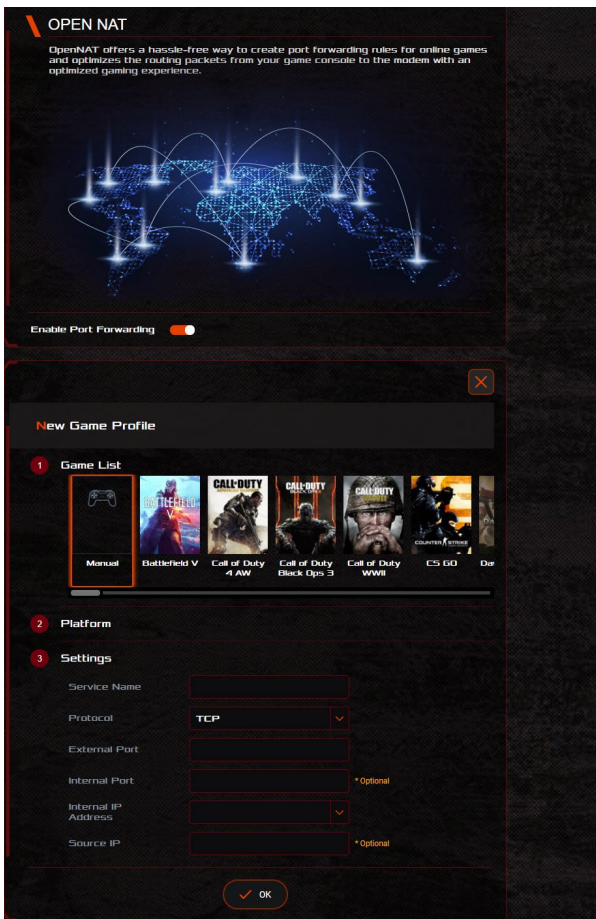
1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (Tetapan Lanjutan) > Network Map (แผนที่เครือข่าย)**
2. ที่มุมขวาบน, คลิก  > **Eject USB disk (ถอด USB ออก)** เมื่อ USB ถูกถอดสำเร็จแล้ว, สถานะ USB จะแสดงคำว่า **Unmounted (เลิกเมตแล้ว)**



### 3.13 ropicpen NAT & ropicpenไฟล้เกม

ropicpen NAT เป็นวิธีที่ไม่ง่ายยากในการสร้างกฎพอร์ตฟอร์เวิร์ด ดิ่งสำหรับเกมออนไลน์ และเพิ่มประสิทธิภาพเราดิ่งแพ็กเก็ตเกิดจาก คอนโซลเกมของคุณไปยังโม่เดิม ซึ่งให้ประสบการณ์การเล่นเกมที่ดีที่สุด

เมื่อเล่นเกม PC หรือเกมคอนโซลอาจมีปัญหการเชื่อมต่อ เนื่องจากการดิ่งค่า ISP หรือเราเตอร์ในสภาพแวดล้อมของคุณ เช่น NAT และบล็อกพอร์ต ropicpenไฟล้เกมช่วยให้หมั่นใจได้ว่า เราเตอร์เกม ROG Rapture ไม้ได้บล็อกการเชื่อมต่อเกม



## ในการกำหนดค่าโอเพ่น NAT

1. จากหน้าต่างระบบเมนู ไปที่ **General (ทั่วไป) > Open NAT (โอเพ่น NAT)**
2. เลือก **Enable Port Forwarding (เปิดใช้งานการส่งต่อพอร์ต)**
3. จาก **Game List (รายการเกม)** เลือกเกมของคุณ และทำการตั้งค่าพื้นฐานให้สมบูรณ์
4. คลิก **OK (ตกลง)**

## 3.14 Smart Connect (การเชื่อมต่ออัจฉริยะ)

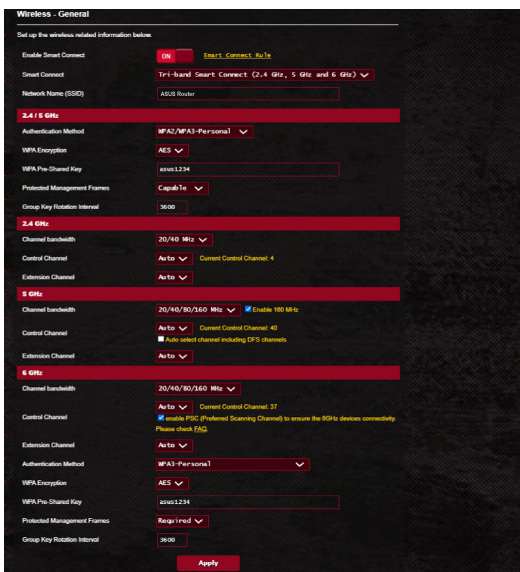
การเชื่อมต่ออัจฉริยะ ได้รับการออกแบบเพื่อเปลี่ยนเส้นทางโคลเ็นต์ไปยังหนึ่งในคลื่นวิทยุ 3 อย่าง (2.4 GHz, 5 GHz-1 และ 5 GHz-2) เพื่อปรับปรุงอัตราการรับส่งข้อมูลไร้สายโดยรวมให้สูงที่สุด

### 3.14.1 การตั้งค่าการเชื่อมต่ออัจฉริยะ

คุณสามารถเปิดทำงานการเชื่อมต่ออัจฉริยะได้จากเว็บ GUI ด้วยสองวิธีการต่อไปนี้:

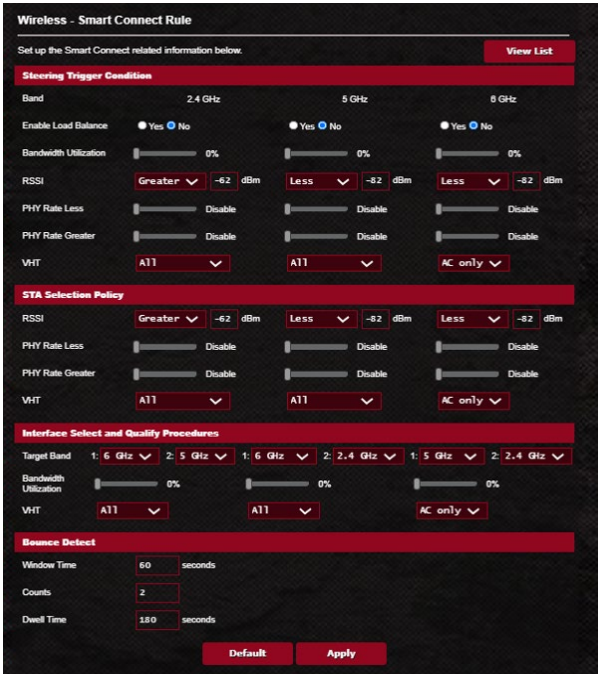
- **ผ่านหน้าจอไร้สาย**

1. บนเว็บเบราว์เซอร์ของคุณ ป้อน IP แอดเดรสเริ่มต้นของไวร์เลสเราเตอร์แบบแมนนวล: <http://www.asusrouter.com>
2. บนหน้าเข้าสู่ระบบ ให้ป้อนชื่อผู้ใช้เริ่มต้น (**admin**) และรหัสผ่าน (**admin**) และคลิก **OK (ตกลง)** หน้า QIS จะเปิดโดยอัตโนมัติ
3. จากหน้าต่างระบบเมนู ไปยังแท็บ **Advanced Settings (การตั้งค่าขั้นสูง) > Wireless (ไร้สาย) > General (ทั่วไป)**
4. เลื่อนตัวเลื่อนไปยัง **ON (เปิด)** ในฟิลด์ **Enable Smart Connect (เปิดทำงานการเชื่อมต่ออัจฉริยะ)** ฟังก์ชันนี้จะเชื่อมต่อโคลเ็นต์ในเครือข่ายของคุณไปยังแถบความถี่ที่เหมาะสมโดยอัตโนมัติ เพื่อให้ได้ความเร็วสูงที่สุด



### 3.14.2 Smart Connect Rule (กฎการเชื่อมต่ออัจฉริยะ)

ASUSWRT ให้การตั้งค่าเงื่อนไขเริ่มต้น เพื่อทริกเกอร์การสลับ นอกจากนี้ คุณยังสามารถเปลี่ยนเงื่อนไขทริกเกอร์ตามสภาพแวดล้อมเครือข่ายของคุณได้ด้วย ในการเปลี่ยนแปลงการตั้งค่าไปที่แท็บ **Smart Connect Rule (กฎการเชื่อมต่ออัจฉริยะ)** บนหน้าจอ **Network Tools (เครื่องมือเครือข่าย)**

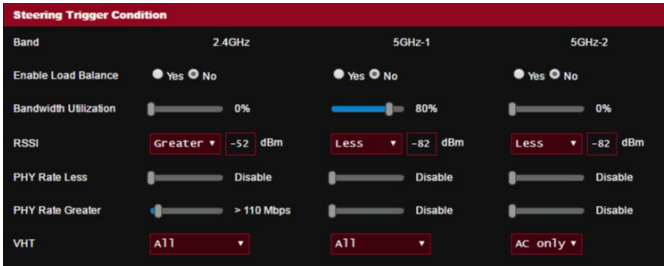


การควบคุมกฎการเชื่อมต่ออัจฉริยะ ถูกแบ่งออกเป็น 4 ส่วน:

- เงื่อนไขทริกเกอร์สำหรับการเปลี่ยนเส้นทาง
- นโยบายการเลือก STA
- การเลือกอินเทอร์เฟซ และขั้นตอนการผ่านคุณสมบัติ
- การตรวจสอบการตีกลับ

## เงื่อนไขที่ทริกเกอร์สำหรับการเปลี่ยนเส้นทาง

ชุดของการควบคุมนี้ ตั้งค่าเงื่อนไขเพื่อเริ่มการเปลี่ยนเส้นทาง ความถี่



- การใช้แบนด์วิดธ์

เมื่อแบนด์วิดธ์ใช้เกินเปอร์เซ็นต์นี้ การเปลี่ยนเส้นทางจะเริ่มต้นขึ้น เอกสารของ

- Enable Load Balance (เปิดทำงานโหลดบาลานซ์)

ตัวเลือกนี้ควบคุมโหลดบาลานซ์

- RSSI (RSSI)

ถ้าระดับสัญญาณที่ได้รับของไคลเอนต์ที่เกี่ยวข้องใด ๆ ตรงตามเงื่อนไขนี้ การเปลี่ยนเส้นทางจะถูกทริกเกอร์

- PHY Rate Less / PHY Rate Greater (อัตรา PHY น้อยลง / อัตรา PHY มากขึ้น)

ตัวควบคุมเหล่านี้กำหนดอัตราการลิงค์ STA ซึ่งทริกเกอร์การเปลี่ยนเส้นทางความถี่

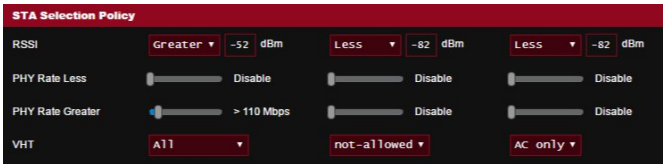
- VHT (VHT)

ตัวควบคุมนี้กำหนดว่า 802.11ac และไคลเอนต์ที่ไม่ใช่ ac จะถูกจัดการอย่างไร

- **ALL (ทั้งหมด)** (ค่าเริ่มต้น) หมายถึงไคลเอนต์ทุกชนิดสามารถทริกเกอร์การเปลี่ยนเส้นทางได้
- **AC only (AC เท่านั้น)** หมายถึงไคลเอนต์ต้องสนับสนุน 802.11ac จึงจะเปลี่ยนเส้นทางทริกเกอร์ได้
- **Not-allowed (ไม่อนุญาต)** หมายถึงเฉพาะไคลเอนต์ที่ไม่ใช่ 802.11ac จึงจะทริกเกอร์การเปลี่ยนเส้นทางได้ เช่น 802.11a/b/g/n

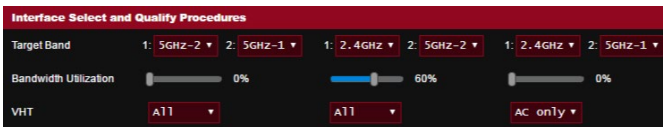
## STA Selection Policy (นโยบายการเลือก STA)

ทันทีที่การเปลี่ยนเส้นทางถูกทริกเกอร์ ASUSWRT จะดำเนินการตามนโยบายการเลือก STA เพื่อเลือกไคลเอนต์ (STA) ที่จะถูกเปลี่ยนเส้นทางไปยังแถบความถี่ที่เหมาะสมที่สุด



## Interface Select and Qualify Procedures (การเลือกอินเทอร์เฟซ และขั้นตอนการผ่านคุณสมบัติ)

ตัวควบคุมเหล่านี้กำหนดสถานที่ซึ่งไคลเอนต์ที่เปลี่ยนเส้นทางจะสิ้นสุด ตัวควบคุม Target Band (แถบความถี่เป้าหมาย) ระบุทางเลือกแรกและทางเลือกที่สองของเป้าหมายการเปลี่ยนเส้นทาง ไคลเอนต์ที่มีเงื่อนไขตรงตามนโยบายการเลือก STA สำหรับความถี่วิทยุ จะถูกเปลี่ยนเส้นทางไปยังเป้าหมายแรก ถ้า Bandwidth Utilization (การใช้แบนด์วิดท์) ของความถี่วิทยุ มีค่าน้อยกว่าค่าที่กำหนดไว้ ไม่เช่นนั้น ไคลเอนต์จะถูกส่งไปยังคลื่นวิทยุ Target Band (ความถี่เป้าหมาย) ที่สอง



## Bounce Detect (การตรวจสอบการตกลับ)

ตัวควบคุมชุดนี้ กำหนดว่าไคลเอนต์สามารถถูกเปลี่ยนเส้นทางได้บ่อยเพียงใด ทั้งนี้เพื่อป้องกัน ไม่ให้ไคลเอนต์เปลี่ยนไป ๆ มา ๆ อย่างต่อเนื่อง อย่างไรก็ตาม ตัวเลือกนี้ไม่ป้องกันไคลเอนต์ไม่ให้ตัดการเชื่อมต่อเอง หรือนับตัวเองเป็นการตกลับถ้าไคลเอนต์ทำเอง แต่ละไคลเอนต์สามารถถูกเปลี่ยนเส้นทางได้ N ครั้ง ภายในช่วงเวลาที่กำหนด เมื่อถึงขีดจำกัดจำนวนครั้งแล้ว ไคลเอนต์จะไม่ถูกเปลี่ยนเส้นทางอีกใน Dwell Time (เวลาอยู่นิ่ง)



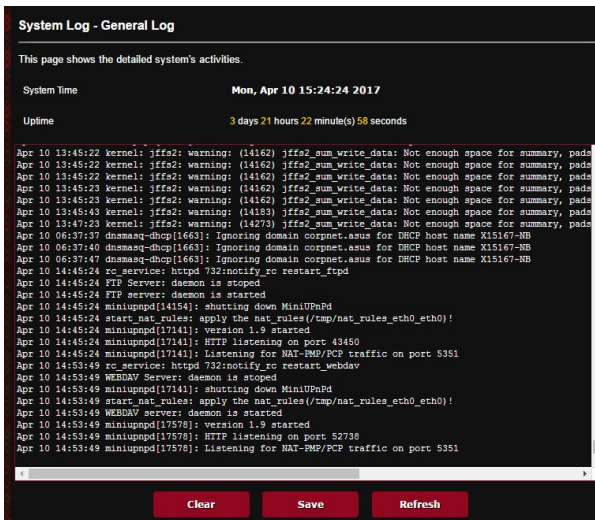
## 3.15 บันทึกกระบบ

บันทึกกระบบ ประกอบด้วยกิจกรรมต่างๆ ของเครือข่ายที่บันทึกไว้

หมายเหตุ: บันทึกกระบบ รีเซ็ตเมื่อเราเตอร์ถูกบูตใหม่ หรือปิดเครื่อง

ในการดูบันทึกกระบบของคุณ:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง) > System Log (บันทึกกระบบ)**
2. คุณสามารถดูกิจกรรมเครือข่ายของคุณในแถบเหล่านี้ได้:
  - บันทึกทั่วไป
  - บันทึกที่ไร้สาย
  - DHCP ลิส
  - IPv6
  - ตารางเราต้ง
  - พอร์ตฟอว์เวิร์ดต้ง
  - 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 'Mon, Apr 10 15:24:24 2017' and the 'Uptime' is '3 days 24 hours 22 minute(s) 58 seconds'. The log entries are as follows:

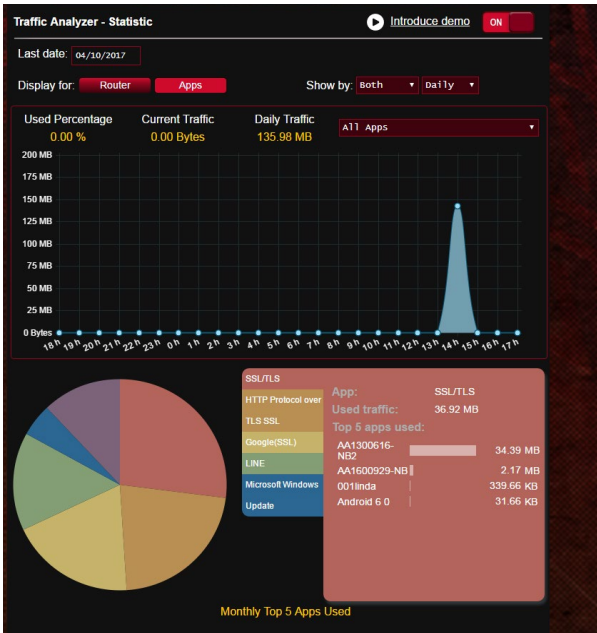
```
Apr 10 13:45:22 kernel: jffs2: warning: (14162) jffs2_sum_write_data: Not enough space for summary, paid
Apr 10 13:45:22 kernel: jffs2: warning: (14162) jffs2_sum_write_data: Not enough space for summary, paid
Apr 10 13:45:22 kernel: jffs2: warning: (14162) jffs2_sum_write_data: Not enough space for summary, paid
Apr 10 13:45:23 kernel: jffs2: warning: (14162) jffs2_sum_write_data: Not enough space for summary, paid
Apr 10 13:45:43 kernel: jffs2: warning: (14183) jffs2_sum_write_data: Not enough space for summary, paid
Apr 10 13:47:23 kernel: jffs2: warning: (14213) jffs2_sum_write_data: Not enough space for summary, paid
Apr 10 06:37:57 dnsmasq-dhcp[1663]: Ignoring domain corpnet.asu for DHCP host name X15167-NB
Apr 10 06:37:40 dnsmasq-dhcp[1663]: Ignoring domain corpnet.asu for DHCP host name X15167-NB
Apr 10 06:37:47 dnsmasq-dhcp[1663]: Ignoring domain corpnet.asu for DHCP host name X15167-NB
Apr 10 14:45:24 rc_service: httpd %32:snofiy_rc restart_ftpd
Apr 10 14:45:24 FTP Server: daemom is stopped
Apr 10 14:45:24 FTP server: daemom is started
Apr 10 14:45:24 miniupnpd[14154]: shutting down MiniUPnPd
Apr 10 14:45:24 start_nat_rules: apply the nat_rules(/tmp/nat_rules_eth0_eth0)!
Apr 10 14:45:24 miniupnpd[17141]: version 1.9 started
Apr 10 14:45:24 miniupnpd[17141]: HTTP listening on port 43450
Apr 10 14:53:49 rc_service: httpd %32:snofiy_rc restart_webdav
Apr 10 14:53:49 WEBDAV Server: daemom is stopped
Apr 10 14:53:49 miniupnpd[17141]: shutting down MiniUPnPd
Apr 10 14:53:49 start_nat_rules: apply the nat_rules(/tmp/nat_rules_eth0_eth0)!
Apr 10 14:53:49 WEBDAV server: daemom is started
Apr 10 14:53:49 miniupnpd[17578]: version 1.9 started
Apr 10 14:53:49 miniupnpd[17578]: HTTP listening on port 52738
Apr 10 14:53:49 miniupnpd[17578]: Listening for NAT-FM/FCP traffic on port 5351
```

At the bottom of the log window, there are three buttons: 'Clear', 'Save', and 'Refresh'.



### 3.16 ตัววิเคราะห์การรับส่งข้อมูล

ตัววิเคราะห์การรับส่งข้อมูลจะช่วยให้คุณสามารถดูข้อมูลเกี่ยวกับสิ่งที่เกิดขึ้นในเครือข่ายของคุณเป็นรายวัน รายสัปดาห์ หรือรายเดือนได้อย่างรวดเร็ว ช่วยให้คุณสามารถดูการใช้แบนด์วิดธ์ของผู้ใช้แต่ละราย หรืออุปกรณ์ หรือแอปพลิเคชันที่ใช้ช่วยลดปัญหาเรื่องคอขวดในการเชื่อมต่ออินเทอร์เน็ตของคุณได้ นอกจากนี้ ยังเป็นวิธีที่ยอดเยี่ยมในการตรวจสอบการใช้อินเทอร์เน็ตหรือกิจกรรมของผู้ใช้



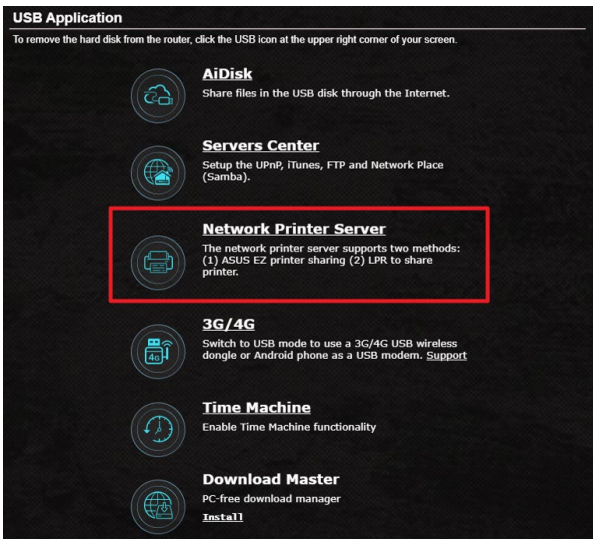
วิธีการกำหนดค่าตัววิเคราะห์การรับส่งข้อมูล:

1. จากแผงหน้าทาง ไปที่ **General (ทั่วไป) > Traffic Analyzer (ตัววิเคราะห์การรับส่งข้อมูล)**
2. จากหน้าหลักของตัววิเคราะห์การรับส่งข้อมูล ให้เปิดสถิติตัววิเคราะห์การรับส่งข้อมูล
3. เลือกวันที่มีแผนภูมิที่คุณต้องการแสดง
4. บนฟิลต์ แสดงสำหรับ เลือก Router (เราเตอร์) หรือ Apps (แอป) เพื่อแสดงข้อมูลการรับส่ง
5. บนฟิลต์ Show by (แสดงโดย) เลือกวิธีการที่คุณต้องการจะแสดงข้อมูลการรับส่ง

## 3.17 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 แฟลชไดรฟ์เข้ากับพอร์ต USB 3.0 ที่แผงด้านหลังของไวร์เลสเราเตอร์ของคุณ ตรวจสอบให้แน่ใจว่าอุปกรณ์เก็บข้อมูล USB ได้รับการฟอร์แมตและแบ่งพาร์ติชันอย่างเหมาะสม ดูเว็บไซต์ของ ASUS ที่ <http://event.asus.com/2009/networks/disksupport/> สำหรับตารางระบบไฟล์ที่สนับสนุน

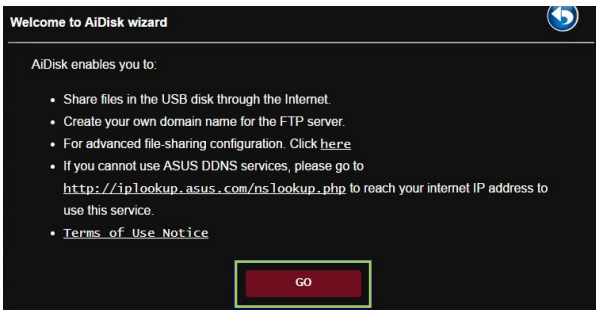


### 3.17.1 การใช้ AiDisk

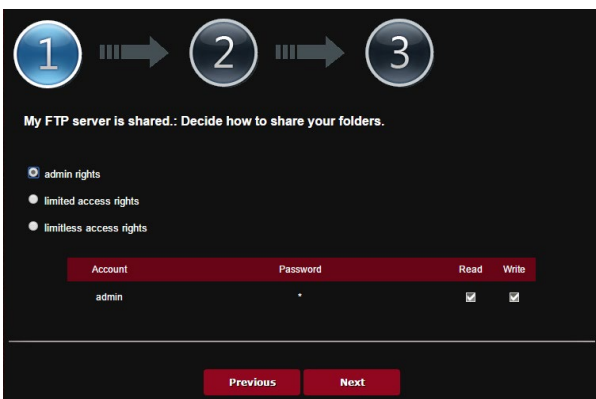
AiDisk ใช้สำหรับแชร์ไฟล์ที่เก็บบนอุปกรณ์ USB ที่เชื่อมต่ออยู่ผ่านอินเทอร์เน็ต นอกจากนี้ AiDisk ยังช่วยคุณในการตั้งค่า ASUS DDNS และ FTP เซิร์ฟเวอร์ด้วย

#### ในการใช้ AiDisk:

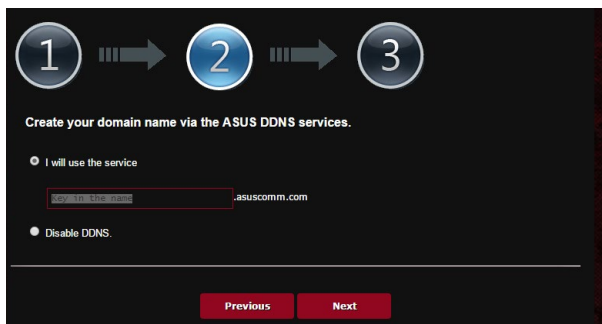
1. จากหน้าต่างระบบเมนู ไปที่ **Advanced Settings (การตั้งค่าขั้นสูง) > USB Application (การใช้งานผ่าน USB)**, จากนั้นคลิกไอคอน AiDisk (AiDisk)
2. จากหน้าจอ Welcome to AiDisk wizard (ยินดีต้อนรับสู่ตัวช่วยสร้าง AiDisk), คลิก **Go (ไป)**



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 (ขามการตั้งค่า ASUS DDNS)** จากนั้นคลิก **Next (ถัดไป)** เพื่อขามการตั้งค่า DDNS ก็ได้

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

## 3.17.2 การใช้เซิร์ฟเวอร์เซินเตอร์

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

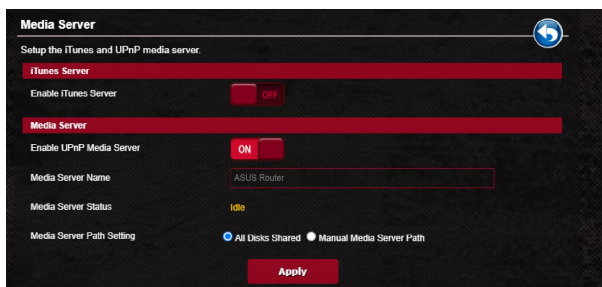
### การใช้มีเดียเซิร์ฟเวอร์

ไวร์เลสเราเตอร์ของคุณ อนุญาตให้อุปกรณ์ที่สนับสนุนคุณสมบัตื UpnP สามารถเข้าถึงไฟล์มีเดียมีเดียจาก USB ดิสก์ที่เชื่อมต่ออยู่ กับไวร์เลสเราเตอร์ของคุณ

---

**หมายเหตุ:** ก่อนที่จะใช้ฟังก์ชัน UpnP มีเดียเซิร์ฟเวอร์, ให้เชื่อมต่อ อุปกรณ์ของคุณเข้ากับเครือข่ายของ

---

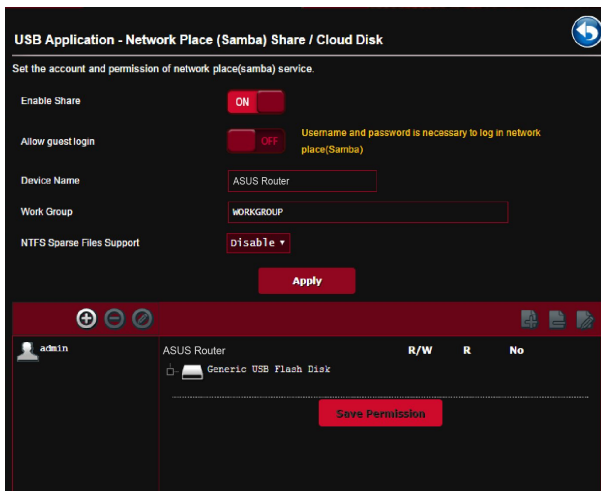


ในการเปิดหน้าการตั้งค่าของมีเดียเซิร์ฟเวอร์ ไปที่ **Advanced Settings (การตั้งค่าขั้นสูง) > USB Application (การใช้งานผ่าน USB) > Media Server (มีเดียเซิร์ฟเวอร์)**

- **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 (การตั้งค่าพารมีเดียเซิร์ฟเวอร์):** เลือก All Disks Shared (ดิสก์ทั้งหมดที่แชร์) หรือ Manual Media Server Path (พารมีเดียเซิร์ฟเวอร์แบบแมนนวล)

## การใช้บริการเน็ตเวิร์กเพลส (แชร์มบ้า) แชร์

เน็ตเวิร์กเพลส (แชร์มบ้า) แชร์ อนุญาตให้คุณตั้งค่าบัญชี และการอนุญาตสำหรับบริการแชร์มบ้า



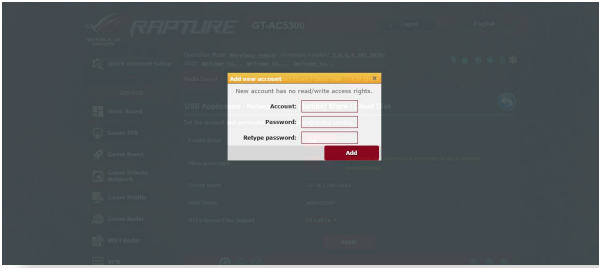
### ในการใช้แชร์มบ้าแชร์:

1. จากจอกับแผงระบบหน้าทาง ไปที่ **Advanced Settings** (การตั้งค่าขั้นสูง) > **USB Application** (การใช้งานผ่าน USB) > **Network Place (Samba) Share / Cloud Disk** (เน็ตเวิร์กเพลส (แชร์มบ้า) แชร์ / คลาวดิสก์)

หมายเหตุ: เน็ตเวิร์กเพลส (แชร์มบ้า) แชร์ ถูกเปิดทำงานตามค่าเริ่มต้น

2. ปฏิบัติตามขั้นตอนด้านล่าง เพื่อเพิ่ม ลบ หรือแก้ไขบัญชี  
ในการสร้างบัญชีใหม่:

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

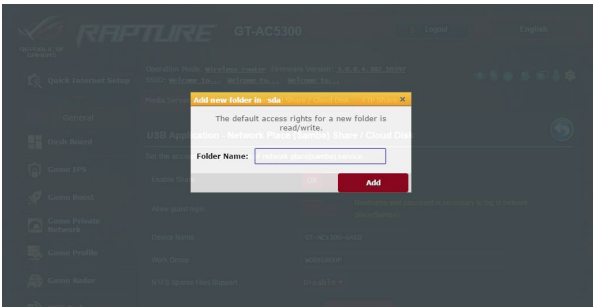


ในการลบบัญชีที่มีอยู่:

- 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

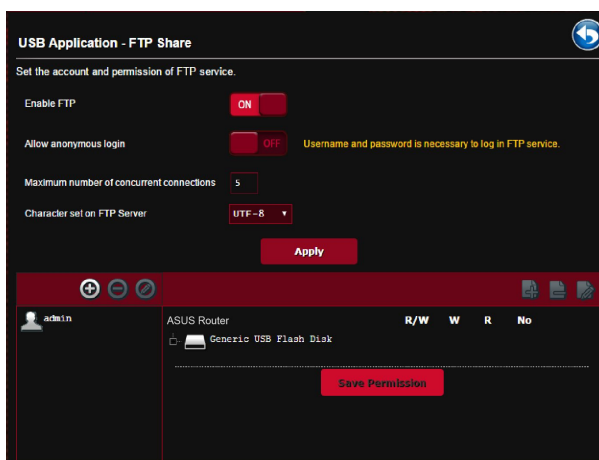
4. คลิก **Apply (นำไปใช้)** เพื่อใช้การเปลี่ยนแปลง

## 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 ภายใต้อินเทอร์เฟซ 3.12.3 การตรวจสอบอุปกรณ์ USB ของคุณ



## ในการใช้บริการ FTP แชร์:

หมายเหตุ: ตรวจสอบให้แน่ใจว่าคุณตั้งค่า FTP เซิร์ฟเวอร์ของคุณผ่าน AiDisk สำหรับรายละเอียดเพิ่มเติม ให้อ่านส่วน 3.17.1 การใช้ AiDisk



1. จากหน้าต่างระบบเมนู คลิก **Advanced Settings** (การตั้งค่าขั้นสูง) > **USB application** (การใช้งานผ่าน USB) > **FTP Share (FTP แชร์)**
2. จากรายการของโพลเดอร์, เลือกชนิดของกฎอนุญาตการเข้าถึงที่คุณต้องการกำหนดสำหรับโพลเดอร์ที่ต้องการ:
  - **R/W:** เลือกเพื่อกำหนดให้สามารถเข้าถึงด้วยการอ่าน/เขียนสำหรับโพลเดอร์เฉพาะ
  - **W:** เลือกเพื่อกำหนดให้สามารถเข้าถึงด้วยการเขียนได้อย่างเดียวสำหรับโพลเดอร์เฉพาะ
  - **R:** เลือกเพื่อกำหนดให้สามารถเข้าถึงด้วยการอ่านได้อย่างเดียวสำหรับโพลเดอร์เฉพาะ
  - **No (ไม่):** เลือกตัวเลือกนี้ ถ้าคุณไม่ต้องการแชร์ไฟล์หรือโพลเดอร์เฉพาะ
3. ถ้าต้องการ, คุณสามารถตั้งค่า **Allow anonymous login** (อนุญาตให้ล็อกอินโดยไม่เปิดเผยชื่อ) เป็น **ON** (เปิด)
4. ในฟิลด์ **Maximum number of concurrent connections** (จำนวนมากที่สุดของการเชื่อมต่อพร้อมกัน) ป้อนจำนวนของอุปกรณ์ที่สามารถเชื่อมต่อไปยัง FTP แชร์ เซิร์ฟเวอร์ใดพร้อมกัน
5. คลิก **Apply (นำไปใช้)** เพื่อยืนยันการเปลี่ยนแปลง
6. ในการเข้าถึง FTP เซิร์ฟเวอร์, ให้ป้อน ftp ลิงค์ **ftp:// <ชื่อโฮสต์>.asuscomm.com** และชื่อผู้ใช้และรหัสผ่านของคุณบนเว็บเบราว์เซอร์ หรืออยู่ที่ลิต์ FTP ของบริษัทที่สาม

### 3.17.3 3G/4G

โมเด็ม USB 3G/4G สามารถใช้เชื่อมต่อไปยัง GT6 เพื่ออนุญาตให้เข้าถึงอินเทอร์เน็ตได้

---

**หมายเหตุ:** สำหรับรายการของโมเด็ม USB ที่ได้รับการรับรอง โปรดเยี่ยมชมที่: <http://event.asus.com/2009/networks/3gsupport/>

---

**ในการตั้งค่าการเข้าถึงอินเทอร์เน็ต 3G/4G:**

1. จากหน้าต่างระบบเมนู คลิก **Advanced Settings (การตั้งค่าขั้นสูง) > USB application (การใช้งาน USB) > 3G/4G (3G/4G)**
2. นฟิลด์ **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):** คัดต่อผู้ให้บริการ 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)**

---

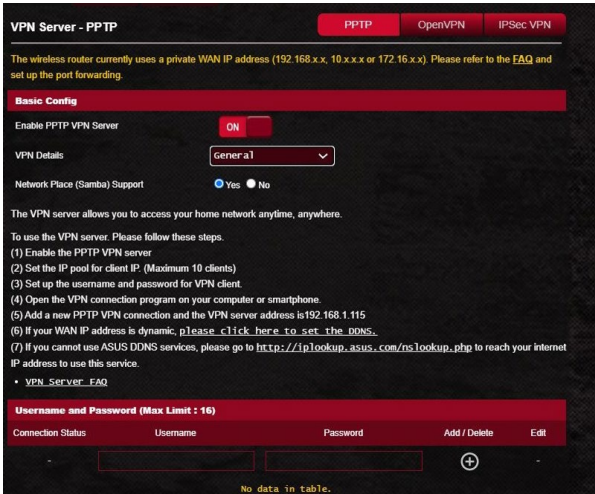
**หมายเหตุ:** เราเตอร์จะบูตใหม่เพื่อให้การตั้งค่ามีผล

---

## 3.18 VPN

เครือข่ายส่วนตัวเสมือน (VPN) มีการเชื่อมต่อที่ปลอดภัยไปยังคอมพิวเตอร์ หรือเครือข่ายระยะไกลโดยใช้เครือข่ายสาธารณะ เช่น อินเทอร์เน็ต

**หมายเหตุ:** ก่อนที่จะตั้งค่าการเชื่อมต่อ VPN, คุณจำเป็นต้องมี IP แอดเดรสหรือชื่อโดเมนของ VPN เซิร์ฟเวอร์



วิธีการตั้งค่าการเข้าถึงไปยัง VPN เซิร์ฟเวอร์:

1. จากแผงหน้าทาง ไปที่ **General (ทั่วไป) > VPN**
2. บนฟิลต์ **Enable PPTP VPN Server (เปิดใช้งาน PPTP VPN เซิร์ฟเวอร์)** คลิก **ON (เปิด)**
3. บนรายการ **VPN Details (รายละเอียด)** เลือก **Advanced Settings (การตั้งค่าขั้นสูง)** เพื่อกำหนดค่าการตั้งค่า VPN ขั้นสูง เช่น การสนับสนุนการออกอากาศ, การยืนยันตัวบุคคล, การเข้ารหัส MPPE และช่วง IP แอดเดรสของไคลเอ็นต์
4. บนฟิลต์ **Network Place (Samba) Support (สนับสนุนเน็ตเวิร์กเพลส (แชร์มบ้า))**, เลือก **Yes (ใช่)**
5. ป้อนชื่อผู้ใช้และรหัสผ่านสำหรับการเข้าถึง VPN เซิร์ฟเวอร์  
คลิก **+**
6. คลิก **Apply (นำไปใช้)**

### 3.18.1 VPN Fusion

VPN Fusion ช่วยให้คุณสามารถเชื่อมต่อกับเซิร์ฟเวอร์ VPN หลายเครื่องพร้อมกันและกำหนดอุปกรณ์ไคลเอนต์ให้เชื่อมต่อกับช่องทางการเชื่อมต่อ VPN ที่ต่างกัน อุปกรณ์บางอย่างเช่นกล่อง Set-top box, สมาร์ททีวี และเครื่องเล่น Blu-ray ไม่รองรับซอฟต์แวร์ VPN คุณสมบัตินี้จะให้สิทธิ์การเข้าถึง VPN ไปยังอุปกรณ์ดังกล่าวในเครือข่ายภายในบ้าน โดยไม่ต้องติดตั้งซอฟต์แวร์ VPN ขณะที่สมาร์ทโฟนของคุณยังคงเชื่อมต่ออินเทอร์เน็ตที่ไม่ใช่ VPN สำหรับนักเล่นเกม การเชื่อมต่อ VPN จะตอบโต้การโจมตี DDoS เพื่อป้องกันมิให้เกมพีซีหรือสตรีมของคุณถูกตัดการเชื่อมต่อจากเซิร์ฟเวอร์เกม นอกจากนี้ การสร้างการเชื่อมต่อ VPN ยังสามารถเปลี่ยนที่อยู่ IP ของคุณไปยังพื้นที่ที่เซิร์ฟเวอร์เกมตั้งอยู่เพื่อปรับปรุงเวลาการปิงของคุณในเซิร์ฟเวอร์เกม

**VPN - VPN Fusion**

VPN Fusion allows you to connect to multiple VPN servers simultaneously and assign your client devices to connect to different VPN tunnels. Some devices like set-top boxes, smart TVs and Blu-ray players do not support VPN software. This feature provides VPN access to such devices in a home network without having to install VPN software, while your smartphone remains connected to Internet not VPN.

For Gamer, VPN connection counteracts DDoS attacks to prevent your PC game or your stream from disconnecting with game servers. Building a VPN connection also can simply change your IP address to the region where the game server is located, to improve your ping to game servers.

To start, please follow the steps below:

1. Click the "+" button beside Server List to add a new VPN tunnel.
2. Activate the VPN connection you created in Server List.
3. Click the "+" button beside Exception List and select the online client you want to configure.
4. Assign a VPN connection to the client device, and click OK.
5. Activate the VPN policy in Exception List, and click Apply at the bottom of the page.

**VPN Fusion FAQ**

**Server List ( Max Limit : 16 )** (+)

Allows you to create VPN connection profiles. The max number of concurrent active VPN connections is 4.

Default	Status	Connection Name	VPN type	Activate	Editor
<input checked="" type="checkbox"/>	connected		Internet		

No data in table.

**Exception List ( Max Limit : 64 )** (+)



You can add VPN policies to the exception list, so that different client devices can connect to different VPN tunnels.

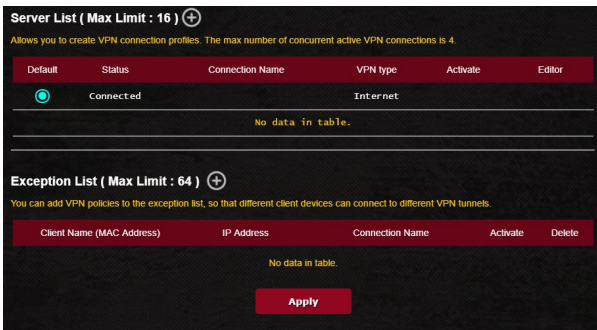
Client Name (MAC Address)	IP Address	Connection Name	Activate	Delete
---------------------------	------------	-----------------	----------	--------

No data in table.

Apply

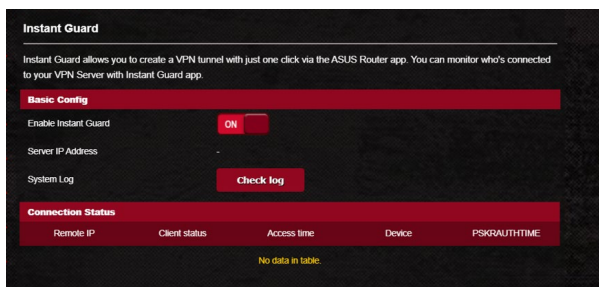
ในการเริ่มต้น ให้ทำตามขั้นตอนด้านล่าง:

1. คลิกปุ่ม  ข้าง **Server List (รายชื่อเซิร์ฟเวอร์)** เพื่อเพิ่มช่องทางการเชื่อมต่อ VPN ใหม่
2. เปิดใช้งานการเชื่อมต่อ VPN ที่คุณสร้างในรายชื่อเซิร์ฟเวอร์
3. คลิกปุ่ม  ข้าง **Exception List (รายการข้อยกเว้น)** และเลือกไอคอนอินเทอร์เน็ตที่คุณต้องการกำหนดค่า
4. กำหนดการเชื่อมต่อ VPN กับอุปกรณ์ไอคอนเน็ตแล้วคลิก **OK (ตกลง)**
5. เปิดใช้งานนโยบาย VPN ใน **Exception List (รายการข้อยกเว้น)** และคลิก **Apply (ปรับใช้)** ที่ด้านล่างของหน้า



## 3.18.2 Instant Guard

Instant Guard เรียกใช้เซิร์ฟเวอร์ VPN ส่วนตัวของคุณเองบนเราเตอร์ของคุณเอง เมื่อคุณใช้โหม่งค์ VPN ข้อมูลทั้งหมดของคุณจะผ่านเซิร์ฟเวอร์ ด้วย Instant Guard คุณสามารถควบคุมเซิร์ฟเวอร์ของคุณเองได้ทั้งหมด ทำให้เป็นโซลูชันที่ปลอดภัยที่สุดเท่าที่จะเป็นไปได้



## 3.19 WAN

### 3.19.1 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: Automatic IP ▾

Enable WAN:  Yes  No

Enable NAT:  Yes  No

Enable UPnP: UPnP FAQ  Yes  No

**WAN DNS Setting**

Connect to DNS Server automatically:  Yes  No

**Account Settings**

Authentication: None ▾

Host-Uniq (Hexadecimal):

**Special Requirement from ISP**

Host Name:

MAC Address:

DHCp query frequency: Aggressive Mode ▾

Extend the TTL value:  Yes  No

Spoof LAN TTL value:  Yes  No

ในการกำหนดค่าการตั้งค่าการเชื่อมต่อ WAN:

1. จากหน้าตาของระบบเมนู ไปยัง **Advanced Settings** (การตั้งค่าขั้นสูง) > **WAN (WAN)** > **Internet Connection** (การเชื่อมต่ออินเทอร์เน็ต)
2. กำหนดค่าการตั้งค่าต่อไปนี้ดังแสดงด้านล่าง: เมื่อทำเสร็จ, คลิก **Apply** (นำไปใช้)
  - **ชนิดการเชื่อมต่อ WAN:** เลือกชนิดผู้ให้บริการอินเทอร์เน็ตของคุณ ทางเลือกต่างๆ คือ **Automatic IP (IP อัตโนมัติ)**, **PPPoE (PPPoE)**, **PPTP (PPTP)**, **L2TP (L2TP)** หรือ **fixed IP (IP คงที่)** ปรึกษา ISP ของคุณถ้าเราเตอร์ไม่สามารถรับ IP แอดเดรสที่ถูกต้อง หรือถ้าคุณไม่แน่ใจถึงชนิดการเชื่อมต่อ WAN

- **เปิดทำงาน WAN:** เลือก **Yes (ใช่)** เพื่ออนุญาตให้เราเตอร์เข้าถึงอินเทอร์เน็ต เลือก **No (ไม่)** เพื่อปิดทำงานการเข้าถึงอินเทอร์เน็ต
- **เปิดทำงาน NAT:** NAT (การแปลเน็ตเวิร์กแอดเดรส) เป็นระบบซึ่ง IP สาธารณะ (WAN IP) หนึ่งตัวถูกใช้ เพื่อให้การเข้าถึงอินเทอร์เน็ตแก่เน็ตเวิร์กไคลเอ็นต์ที่มี IP แอดเดรสส่วนตัวใน LAN IP แอดเดรสส่วนตัวของเน็ตเวิร์กไคลเอ็นต์แต่ละตัวถูกบันทึกในตาราง NAT และถูกใช้เพื่อเปลี่ยนเส้นทางแพคเกจข้อมูลขาเข้า
- **เปิดทำงาน UPnP:** UPnP (พลังก์แอนด์เพลย์สากล) อนุญาตให้คุณควบคุมอุปกรณ์หลายชนิด (เช่น เราเตอร์, โพรเซสเซอร์, ระบบสแตนด์บาย, เกมคอนโซล, โทรศัพท์เซลลูลาร์) ผ่านเครือข่ายที่ใช้ IP โดยมีหรือไม่มี การควบคุมจากศูนย์กลางผ่านเทคโนโลยี UPnP เชื่อมต่อ PC ทุกรูปแบบ โดยให้เครือข่ายที่ไร้รอยต่อสำหรับการกำหนดค่าจากระยะไกล และการถ่ายโอนข้อมูล เมื่อใช้ UPnP, อุปกรณ์เครือข่ายใหม่จะถูกค้นพบโดยอัตโนมัติ หลังจากที่เชื่อมต่อไปยังเครือข่ายแล้ว, อุปกรณ์สามารถถูกกำหนดค่าจากระยะไกลเพื่อสนับสนุนแอปพลิเคชัน P2P, เกมอินเทอร์เน็ตแอกทีฟ, การประชุมผ่านวิดีโอ และเว็บหรือฟร็อกซ์เฟียร์เวอร์ไต ไม่เหมือนกับพอร์ตฟอเวิร์ตติ้ง ซึ่งเกี่ยวข้องกับการกำหนดค่าการตั้งค่าพอร์ตด้วยตัวเอง, UPnP จะกำหนดค่าเราเตอร์โดยอัตโนมัติ เพื่อให้เราเตอร์ยอมรับการเชื่อมต่อขาเข้า และส่งค่าขอไปยัง PC ที่เจาะจงบนเครือข่ายแลนโดยตรง
- **เชื่อมต่อไปยัง DNS เซิร์ฟเวอร์:** อนุญาตให้เราเตอร์นี้รับ DNS IP แอดเดรสจาก ISP โดยอัตโนมัติ DNS เป็นโอสต์บนอินเทอร์เน็ต ซึ่งแปลชื่ออินเทอร์เน็ตไปยัง IP แอดเดรสที่เป็นตัวเลข
- **การยืนยันตัวตนบุคคล:** รายการนี้อาจถูกกำหนดโดย ISP บางแห่ง ตรวจสอบกับ ISP ของคุณ และกรอกข้อมูลลงไป ถ้าจำเป็น
- **ข้อโอสต์:** ฟิลต์นี้อนุญาตให้คุณใส่ข้อโอสต์สำหรับเราเตอร์ของคุณ โดยปกติเป็นความต้องการพิเศษจาก ISP ของคุณ ถ้า ISP ของคุณกำหนดข้อโอสต์ให้กับคอมพิวเตอร์ของคุณ ให้ป้อนข้อโอสต์ที่นี้



- **MAC แอดเดรส:** MAC (การควบคุมการเข้าถึงมีเดีย) แอดเดรส เป็นหมายเลขระบุที่ไม่ซ้ำกัน สำหรับ อุปกรณ์เครือข่ายของคุณ ISP บางแห่งตรวจสอบแล MAC แอดเดรสของอุปกรณ์เครือข่าย ซึ่งเชื่อมต่อไปยังบริการของบริษัท และปฏิเสธอุปกรณ์ที่ไม่รู้จักที่พยายามเชื่อมต่อเข้ามา เพื่อหลีกเลี่ยงปัญหาในการเชื่อมต่อเนื่องจาก MAC แอดเดรสที่ไม่ได้ลงทะเบียน คุณสามารถ:
  - ติดต่อ ISP ของคุณและอัปเดต MAC แอดเดรสที่เชื่อมโยงกับบริการของ ISP ของคุณ
  - โคลน หรือเปลี่ยนแปลง MAC แอดเดรสของ ASUS ไรต์เวร์เรเตอร์ เพื่อให้ตรงกับ MAC แอดเดรสของอุปกรณ์เครือข่ายก่อนหน้านี้ ISP รู้จัก
- **DHCP query frequency (ความถี่การสอบถาม DHCP):** เปลี่ยนการตั้งค่าช่วงการค้นหา DHCP เพื่อหลีกเลี่ยงการทำให้ DHCP เซิร์ฟเวอร์โอเวอร์โหลด

### 3.19.2 Dual WAN (คูอัล WAN)

ASUS ไร้สายเราเตอร์ของคุณ สนับสนุนการทำงานของคูอัล WAN คุณสามารถตั้งค่าคุณสมบัติคูอัล WAN ไปเป็น 2 โหมดนี้:

- **Failover Mode (โหมดเฟลโอเวอร์):** เลือกโหมดนี้เพื่อใช้ WAN รอง เป็นการเข้าถึงเครือข่ายสำรอง
- **Load Balance Mode (โหมดโหลดบาลานซ์):** เลือกโหมดนี้เพื่อปรับค่าแบนด์วิดท์ให้เหมาะสมที่สุด ลดเวลาตอบสนองให้ต่ำที่สุด และป้องกันไม่ให้ข้อมูลโอเวอร์โหลด สำหรับการเชื่อมต่อ WAN หลักและรอง

**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 connection.

**Basic Config**

Enable Dual WAN  ON

Primary WAN

Secondary WAN

Dual WAN Mode   Allow failback

**Auto Network Detection**

Detect Interval  seconds

Failover Execution Time Continuous  times (= 60 seconds) detect network failed.

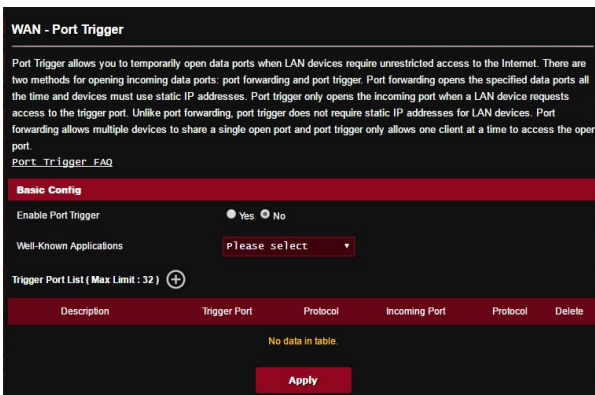
Enable Ping to Internet  Yes  No

**Apply**

### 3.19.3 พอร์ตทริกเกอร์



ช่วงพอร์ตทริกเกอร์รั้ง จะเปิดพอร์ตขาเข้าที่ไม่ได้กำหนดเป็นช่วงเวลาที่จำกัด เมื่อใดก็ตามที่โคลเอ็นต์บนเครือข่ายแลนทำการเชื่อมต่อขาออกไปยังพอร์ตที่ระบุ พอร์ตทริกเกอร์รั้งถูกใช้ในสถานการณ์ต่อไปนี้:

- มีโคลเอ็นต์ที่ท้องถิ่นมากกว่าหนึ่งเครื่องจำเป็นต้องส่งต่อพอร์ตสำหรับการใช้งานเดียวกันในเวลาที่แตกต่างกัน
- การใช้งานต้องการให้มีพอร์ตขาเข้าเฉพาะที่แตกต่างจากพอร์ตขาออก



ในการตั้งค่าพอร์ตทริกเกอร์:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง) > WAN (WAN) > Port Trigger (พอร์ตทริกเกอร์)**
2. บนฟิลด์ **Enable Port Trigger (เปิดทำงานพอร์ตทริกเกอร์)** ทำเครื่องหมายที่ **Yes (ใช่)**
3. บนฟิลด์ **Well-Known Applications (แอปพลิเคชันที่เป็นที่รู้จัก)** เลือกเกม และบริการบนเว็บที่เป็นที่นิยมเพื่อเพิ่มไปยังรายการ Port Trigger (พอร์ตทริกเกอร์)
4. บนตาราง **Trigger Port List (รายการพอร์ตทริกเกอร์)** ป้อนข้อมูลต่อไปนี้เข้าไป:
  - **คำอธิบาย:** ป้อนชื่อหรือคำอธิบายสั้นๆ สำหรับบริการ

- **ทริกเกอร์พอร์ต:** ระบุทริกเกอร์พอร์ตเพื่อเปิดพอร์ตขาเข้า
  - **โปรโตคอล:** เลือกโปรโตคอล, TCP หรือ UDP
  - **พอร์ตขาเข้า:** ระบุพอร์ตขาเข้าเพื่อรับข้อมูลขาเข้าจากอินเทอร์เน็ต
5. คลิก **Add (เพิ่ม)**  เพื่อป้อนข้อมูลพอร์ตทริกเกอร์ไปยังรายการ คลิกปุ่ม **Delete (ลบ)**  เพื่อลบรายการพอร์ตทริกเกอร์จากรายการ
6. เมื่อทำเสร็จ, คลิก **Apply (นำไปใช้)**

---

**หมายเหตุ:**

- ในขณะที่เชื่อมต่อไปยัง IRC เซิร์ฟเวอร์, คอมพิวเตอร์ PC ทำการเชื่อมต่อขาออกโดยใช้ช่วงพอร์ตทริกเกอร์ 66660-7000 IRC เซิร์ฟเวอร์ตอบสนองโดยการตรวจสอบชื่อผู้ใช้และสร้างการเชื่อมต่อใหม่ไปยังคอมพิวเตอร์ PC โดยใช้พอร์ตขาเข้า
  - ถ้า พอร์ตทริกเกอร์ ถูกปิดทำงาน, เราเตอร์จะตัดการเชื่อมต่อ เนื่องจากไม่สามารถหาว่า PC เครื่องใดที่กำลังขอการเข้าถึง IRC อยู่ เมื่อ พอร์ตทริกเกอร์เปิดทำงาน, เราเตอร์จะกำหนดพอร์ตขาเข้า เพื่อรับข้อมูลขาเข้า พอร์ตขาเข้านี้จะปิดหลังจากถึงเวลาที่กำหนด เนื่องจากเราเตอร์ไม่แน่ใจว่าเมื่อใดที่แอปพลิเคชันสิ้นสุดการทำงาน
  - พอร์ตทริกเกอร์จึงอนุญาตคอมพิวเตอร์เพียงหนึ่งเครื่องในเครือข่ายให้ใช้บริการที่เจาะจง และพอร์ตขาเข้าที่เจาะจงในเวลาเดียวกัน
  - คุณไม่สามารถใช้แอปพลิเคชันเดียวกันเพื่อทริกเกอร์พอร์ตใน PC มากกว่าหนึ่งเครื่องในเวลาเดียวกันได้ เราเตอร์จะส่งต่อพอร์ตกลับไปไปยังคอมพิวเตอร์เครื่องล่าสุดที่ส่งคำขอ/ทริกเกอร์ไปให้เราเตอร์แทน
-

### 3.19.4 เวย์รซอลเซิร์ฟเวอร์/พอร์ตฟอร์เวิร์ดดิ้ง

พอร์ตฟอร์เวิร์ดดิ้ง เป็นวิธีการเพื่อเปลี่ยนเส้นทางการจราจร เครือข่ายจากอินเทอร์เน็ตไปยังพอร์ตที่เจาะจง หรือช่วงพอร์ตที่เจาะจงไปยังอุปกรณ์บนเครือข่ายแลนของคุณ การตั้งค่าพอร์ตฟอร์เวิร์ดดิ้งบนเราเตอร์ของคุณ อนุญาตให้ PC ที่อยู่นอกเครือข่ายเข้าถึงบริการที่เจาะจงที่มีให้โดย PC ในเครือข่ายของคุณได้

**WAN - Virtual Server / Port Forwarding**

Virtual Server / Port forwarding allows remote computers to connect to a specific computer or service within a private local area network (LAN). For a faster connection, some P2P applications (such as BitTorrent), may also require that you set the port forwarding setting. Please refer to the P2P application's user manual for details. You can open the multiple port or a range of ports in router and redirect data through those ports to a single client on your network.

If you want to specify a Port Range for clients on the same network, enter the Service Name, the Port Range (e.g. 10200-10300), the LAN IP address, and leave the Local Port empty.

- When your network's firewall is disabled and you set 80 as the HTTP server's port range for your WAN setup, then your http server/web server would be in conflict with ASUS Router's web user interface.
- When you set 20:21 as your FTP server's port range for your WAN setup, then your FTP server would be in conflict with ASUS Server's native FTP server.

[Virtual Server / Port Forwarding FAQ](#)

**Basic Config**

Enable Port Forwarding  Yes  No

Famous Server List

FTP Server Port

**Port Forwarding List (Max Limit : 32)**

Service Name	Source Target	Port Range	Local IP	Local Port	Protocol	Add / Delete
					TCP	+

No data in table.

**Apply**

ในการตั้งค่าการส่งต่อพอร์ต:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง) > WAN (WAN) > แท็บ Virtual Server / Port Forwarding (เวย์รซอลเซิร์ฟเวอร์ / พอร์ตฟอร์เวิร์ดดิ้ง)**
2. บนฟิลต์ **Enable Port Forwarding (เปิดทำงานพอร์ตฟอร์เวิร์ดดิ้ง)** ทำเครื่องหมายที่ **Yes (ใช่)**
3. บนฟิลต์ **Famous Server List (รายการเซิร์ฟเวอร์ที่มีชื่อเสียง)** เลือกชนิดของบริการที่คุณต้องการเข้าถึง
4. บนฟิลต์ **Famous Game List (รายการเกมที่มีชื่อเสียง)** เลือกเกมที่เป็นที่นิยมที่คุณต้องการเข้าถึง รายการนี้แสดงพอร์ตที่ต้องการสำหรับเกมออนไลน์ที่เป็นที่นิยมเพื่อให้ทำงานอย่างถูกต้อง

## 5. บนตาราง **Port Forwarding List** (รายการพอร์ต พอร์ตเวิร์ตติ้ง) ป้อนข้อมูลต่อไปนี้เข้าไป:

- **ชื่อบริการ:** ป้อนชื่อบริการ
- **ช่วงพอร์ต:** ถ้าคุณต้องการระบุช่วงพอร์ตสำหรับโหนดบนเครือข่ายเดียวกัน, ป้อน Service Name (ชื่อบริการ), Port Range (ช่วงพอร์ต) (เช่น 10200:10300), LAN IP address (LAN IP แอดเดรส), และปล่อยให้ Local Port (พอร์ตในเครื่อง) ว่าง ช่วงพอร์ตโดยอ้อมมีรูปแบบต่างๆ 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 ซึ่งแต่ละพอร์ตถูกกำหนดหมายเลขพอร์ตและงานที่เจาะจงไว้ ตัวอย่างเช่น พอร์ต 80 ใช้สำหรับ HTTP พอร์ตที่เจาะจงสามารถถูกใช้โดยแอปพลิเคชันหรือบริการเดียวได้ในแต่ละช่วงเวลา ดังนั้น การที่ PC สองตัวพยายามเข้าถึงข้อมูลผ่านพอร์ตเดียวกันในเวลาเดียวกันก็อาจทำให้การทำงานล้มเหลว ตัวอย่างเช่น คุณไม่สามารถตั้งค่าพอร์ตพอร์ตเวิร์ตติ้งสำหรับพอร์ต 100 สำหรับ PC สองเครื่องในเวลาเดียวกันได้

- **โหนด IP:** ป้อน LAN IP แอดเดรสของโหนดเอ็นดี

---

**หมายเหตุ:** ใช้สแตติก IP แอดเดรสสำหรับโหนดเอ็นดีท้องถิ่น เพื่อให้พอร์ตพอร์ตเวิร์ตติ้งทำงานอย่างเหมาะสม สำหรับข้อมูล ใหญ่ส่วน **3.11 LAN**

- **โหนดพอร์ต:** ป้อนพอร์ตที่เจาะจง เพื่อรับแพคเกจที่ส่งต่อมาจากปลายทางนี้ให้วางไว้ ถ้าคุณต้องการแพคเกจขาเข้าให้ถูกเปลี่ยนเส้นทางไปยังช่วงพอร์ตที่ระบุ
- **โปรโตคอล:** เลือกโปรโตคอล ถ้าคุณไม่แน่ใจ เลือก **BOTH** (ทั้งคู่)

6. คลิก **Add (เพิ่ม)**  เพื่อป้อนข้อมูลพอร์ตทริกเกอร์ไปยังรายการ คลิกปุ่ม **Delete (ลบ)**  เพื่อลบรายการพอร์ตทริกเกอร์จากรายการ

7. เมื่อทำเสร็จ, คลิก Apply (นำไปใช้)

**ในการตรวจสอบว่าพอร์ตฟอร์เวิร์ดตั้งถูกกำหนดค่าสำเร็จหรือไม่:**

- ให้แน่ใจว่าเซิร์ฟเวอร์หรือแอปพลิเคชันของคุณถูกตั้งค่าแล้วและกำลังรันอยู่
- คุณจำเป็นต้องให้ไคลเอ็นต์อยู่นอก LAN ของคุณแต่มีการเข้าถึงอินเทอร์เน็ต (เรียกว่า “อินเทอร์เน็ตไคลเอ็นต์”) ไคลเอ็นต์นี้ไม่ควรเชื่อมต่ออยู่กับ ASUS เราเตอร์
- บนอินเทอร์เน็ตไคลเอ็นต์, ใช้ WAN IP ของเราเตอร์เพื่อเข้าถึงเซิร์ฟเวอร์ ถ้าพอร์ตฟอร์เวิร์ดตั้งถูกตั้งค่าสำเร็จ, คุณควรสามารถเข้าถึงไฟล์หรือแอปพลิเคชันใด

**ความแตกต่างระหว่างพอร์ตทริกเกอร์ และพอร์ตฟอร์เวิร์ดตั้ง:**

- พอร์ตทริกเกอร์จะทำงานแม้ว่าไม่มีการตั้งค่า LAN IP แอดเดรสที่เฉพาะเจาะจง ไม่เหมือนกับพอร์ตฟอร์เวิร์ดตั้งซึ่งจำเป็นต้องมีสแตติก LAN IP แอดเดรส, พอร์ตทริกเกอร์อนุญาตให้ส่งต่อพอร์ตแบบไดนามิกโดยใช้เราเตอร์ใด ช่วงพอร์ตที่กำหนดไว้ล่วงหน้า ถูกกำหนดค่าเพื่อให้ยอมรับการเชื่อมต่อขาเข้าภายในช่วงระยะเวลาที่จำกัด พอร์ตทริกเกอร์อนุญาตให้คอมพิวเตอร์หลายเครื่องรันแอปพลิเคชันที่โดยปกติอาจต้องการให้ส่งต่อพอร์ตเดียวกันไปยัง PC แต่ละเครื่องบนเครือข่ายด้วยตัวเอง
- พอร์ตทริกเกอร์มีความปลอดภัยมากกว่าพอร์ตฟอร์เวิร์ดตั้งเนื่องจากพอร์ตขาเข้าไม่ได้เปิดตลอดเวลา พอร์ตเหล่านี้เปิดเฉพาะเมื่อแอปพลิเคชันทำการเชื่อมต่อขาออกผ่านทริกเกอร์พอร์ตเท่านั้น

### 3.19.5 DMZ

เวอรัล DMZ เปิดเผยโคลเอ็นต์หนึ่งเครื่องไปยังอินเทอร์เน็ต ทำให้โคลเอ็นต์นี้รับแพคเก็ตขาเข้าทั้งหมดโดยตรงไปยังเครือข่ายแลนของคุณ

โดยปกติ การจราจรขาเข้าจากอินเทอร์เน็ตถูกทิ้งและเปลี่ยนเส้นทางไปยังโคลเอ็นต์ที่เจาะจงเฉพาะเมื่อพอร์ตฟอร์เวิร์ดดิ้ง หรือพอร์ตทริกเกอร์ถูกกำหนดค่าไว้บนเครือข่าย ในการกำหนดค่า DMZ, เน็ตเวิร์กโคลเอ็นต์หนึ่งเครื่องจะรับแพคเก็ตขาเข้าทั้งหมด

การตั้งค่า DMZ บนเครือข่ายมีประโยชน์เมื่อคุณต้องการให้พอร์ตขาเข้าเปิด หรือเมื่อคุณต้องการโฮสต์โดเมน เว็บ หรืออีเมลเซิร์ฟเวอร์

---

**ข้อควรระวัง:** การเปิดพอร์ตทั้งหมดบนโคลเอ็นต์ไปยังอินเทอร์เน็ต ทำให้เครือข่ายอ่อนแอต่อการโจมตีภายนอก โปรดระมัดระวังความเสี่ยงด้านความปลอดภัยที่เกี่ยวข้องกับการใช้ DMZ

---

#### ในการตั้งค่า DMZ:

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

#### ในการลบ DMZ:

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



### 3.19.6 DDNS

การตั้งค่า DDNS (ไดนามิก DNS) อนุญาตให้คุณเข้าถึงเราเตอร์จากภายนอกเครือข่ายของคุณผ่านบริการ ASUS DDNS ที่ให้มา 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 [http://iplookup.asus.com/rs\\_lookup.php](http://iplookup.asus.com/rs_lookup.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.

Enable the DDNS Client  Yes  No

Server **WWW.ASUS.COM**

Host Name Key in the name **asuscomm.com**

DDNS Status **Inactive**

HTTPS/SSL Certificate  Free Certificate from Let's Encrypt  Import Your Own Certificate  None

**Apply**

ในการตั้งค่า DDNS:

1. จากหน้าตัวระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง) > WAN (WAN) > DDNS (DDNS)**
2. กำหนดค่าการตั้งค่าต่อไปนี้ดังแสดงด้านล่าง: เมื่อทำเสร็จ, คลิก **Apply (นำไปใช้)**
  - **เปิดทำงาน DDNS ใดคลเอ็นต์:** 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 กรอกฟิลด์ชื่อผู้ใช้หรืออีเมลแอดเดรส และรหัสผ่าน หรือ DDNS คีย์
  - **เปิดทำงานอักขระตัวแทน:** เปิดทำงานอักขระตัวแทนถ้าบริการ DDNS จำเป็นต้องใช้

---

## หมายเหตุ:

บริการ DDNS จะไม่ทำงานภายใต้เงื่อนไขเหล่านี้:

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

### 3.19.7 NAT ผ่านตลอด

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

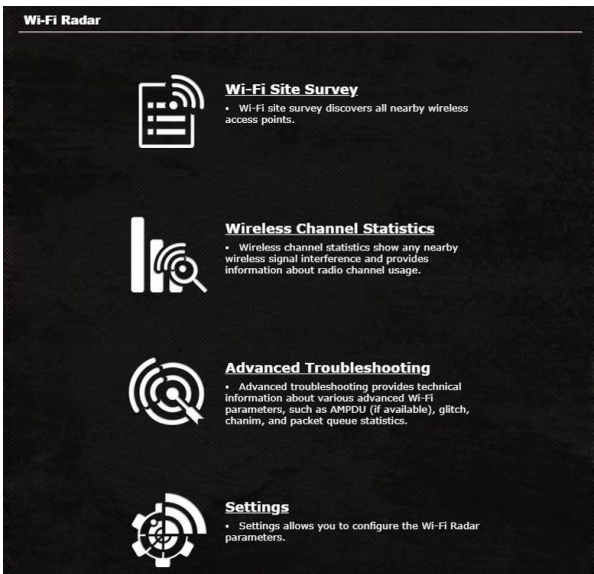
ในการเปิดทำงาน / ปิดทำงานการตั้งค่า NAT ผ่านตลอด ไปที่ **Advanced Settings (การตั้งค่าขั้นสูง) > WAN (WAN) > NAT Passthrough (NAT ผ่านตลอด)** เมื่อทำเสร็จ, คลิก **Apply (นำไปใช้)**

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
<b>Apply</b>	

## 3.20 WiFi Radar

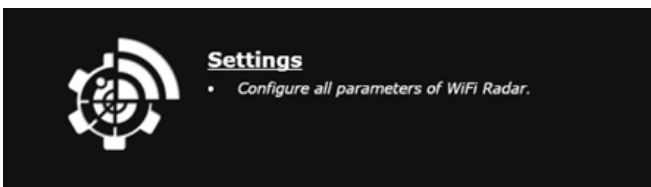
Wi-Fi Radar ซึ่งเป็นเครื่องมือวิเคราะห์ขั้นสูงสำหรับเครือข่ายไร้สายของคุณ จะลึกลงไปในช่องสัญญาณและข้อมูลแพ็คเก็ตสำหรับการแก้ไขปัญหา

**หมายเหตุ:** การเปิดใช้งาน WiFi Radar อาจส่งผลให้ประสิทธิภาพไร้สายลดลง เปิดใช้งาน Wi-Fi Radar เฉพาะเมื่อจำเป็น



วิธีการใช้ WiFi Radar:

1. จากแผงหน้าทาง ไปที่ **General (ทั่วไป) > WiFi Radar** ไปที่ **Settings (การตั้งค่า)** และกำหนดค่าพารามิเตอร์ WiFi Radar ทั้งหมด



2. คลิก **Start Data Collection** (เริ่มการเก็บรวบรวมข้อมูล) และกำหนดตารางเวลาสำหรับการเก็บรวบรวมข้อมูล
3. คลิก **Submit** (ส่ง) หลังจากคุณตั้งค่าพารามิเตอร์ทั้งหมด

The screenshot shows the 'Settings' page for InSSIDer, specifically the 'Configure parameters of WiFi Radar' section. It includes options for 'Sample Interval' (5, 10, 15, 20 seconds), 'Start/Stop Data Collection' (with a 'Start Data Collection' button), 'Database Size' (2 MB), and a list of 'Counters' to be monitored. A 'Submit' button is at the bottom right.

**Sample Interval:** 5 Second, 10 Second, 15 Second, 20 Second

**Start/Stop Data Collection:** Start Data Collection button, Start collecting data every (Sunday to Saturday), From 12:00 AM to 12:00 AM

**Database Size:** 2 MB

**Counters:** Channel Statistics, Channel Statistics, No CTS catches, Bad PLCP, Bad FCS, Packet Requested, Packet Stored, Packet Dropped, Packet Retired, Queue Utilization, Queue Length Precedence, Data Throughput, Physical Rate, CTS Fail, Retry Drop, PS Busy, Acked

**Export Database:** Download Database File, Save Database to File button

[http://inSSIDer.com/configure.asp?Web\\_Feb\\_22\\_2017\\_11:52:14 GMT+0800 \(ไต้หวันเวลา\)](http://inSSIDer.com/configure.asp?Web_Feb_22_2017_11:52:14 GMT+0800 (ไต้หวันเวลา))

## 3.20.1 การสำรวจไซต์ WiFi

การสำรวจเว็บไซต์ WiFi ช่วยให้ค้นหาเครือข่ายไร้สายในสภาพแวดล้อมของคุณ



### 3.20.2 สถิติช่องสัญญาณไร้สาย

คุณสมบัตินี้จะแสดงการใช้ช่องสัญญาณของทุกแถบความถี่และสถิติการกระจายข้อมูลของช่องสัญญาณในสภาพแวดล้อมของคุณ



### 3.20.3 การแก้ไขปัญหาขั้นสูง

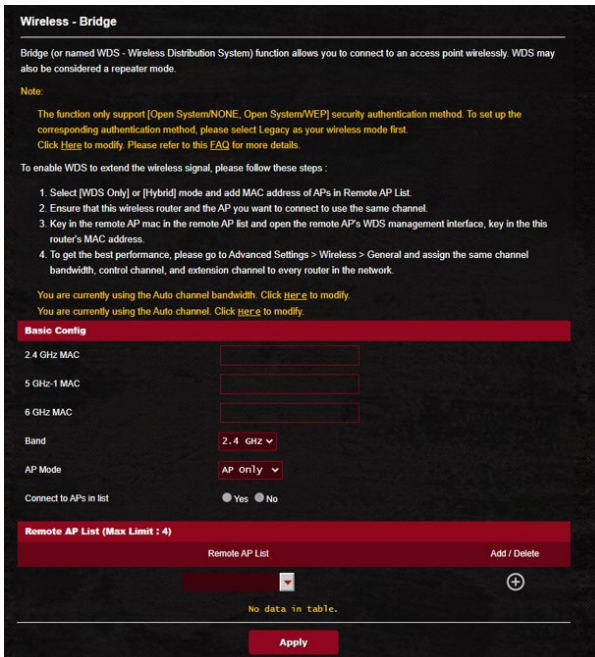
คุณสมบัตินี้จะแสดงสถิติการขัดข้องของ WiFi ในสภาพแวดล้อมของคุณ



# 3.21 ไร้สาย

## 3.21.1 ทั่วไป

แท็บ General (ทั่วไป) อนุญาตให้คุณกำหนดค่าการตั้งค่าไร้สายพื้นฐาน



ในการกำหนดค่าการตั้งค่าไร้สายพื้นฐาน:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง) > Wireless (ไร้สาย) > General (ทั่วไป)**
2. เลือก 2.4GHz, 5GHz-1 หรือ 5GHz-2 เป็นแถบความถี่สำหรับเครือข่ายไร้สายของคุณ
3. ถ้าคุณต้องการใช้ฟังก์ชัน เชื่อมต่อแบบอัตโนมัติ ให้เลื่อนตัวเลื่อนไปที่ **ON (เปิด)** ในฟิลด์ **Enable Smart Connect (เปิดทำงานการเชื่อมต่อแบบอัตโนมัติ)** ฟังก์ชันนี้จะเชื่อมต่อไคลเอนต์ในเครือข่ายของคุณไปยังแถบความถี่ที่เหมาะสม 2.4GHz, 5GHz-1 หรือ 5GHz-2 เพื่อให้ได้ความเร็วสูงสุดโดยอัตโนมัติ

- กำหนดชื่อที่ไม่ซ้ำที่ประกอบด้วยตัวอักษรได้มากถึง 32 ตัวสำหรับ SSID (ตัวระบุชุดบริการ) หรือชื่อเครือข่ายของคุณ เพื่อระบุเครือข่ายไร้สายของคุณ อุปกรณ์ Wi-Fi สามารถหาและเชื่อมต่อไปยังเครือข่ายไร้สายผ่าน SSID ที่คุณกำหนดไว้ SSID บนแบนเนอร์ขอมูลจะถูกลบออกทันทีที่ SSID ใหม่ถูกบันทึกไปยังการตั้งค่า

---

**หมายเหตุ:** คุณสามารถกำหนด SSID ที่ไม่ซ้ำสำหรับแถบความถี่ 2.4 GHz, 5GHz-1 และ 5GHz-2

---

- ในฟิลด์ **Hide SSID (ซ่อน SSID)**, เลือก **Yes (ใช่)** เพื่อป้องกันอุปกรณ์ไร้สายใหม่ให้ตรวจพบ SSID ของคุณ เมื่อฟังก์ชันนี้เปิดทำงาน คุณจำเป็นต้องป้อน SSID ด้วยตัวเองบนอุปกรณ์ไร้สายเพื่อเข้าถึงเครือข่ายไร้สาย
- เลือกตัวเลือกทั้งหมดไร้สายเหล่านี้ เพื่อหาชนิดของอุปกรณ์ไร้สายที่สามารถเชื่อมต่อไปยังไวร์เลสเราเตอร์ของคุณ:
  - **อัตโนมัติ:** เลือก **Auto (อัตโนมัติ)** เพื่ออนุญาตให้อุปกรณ์ 802.11ac, 802.11n, 802.11g และ 802.11b เชื่อมต่อไปยังไวร์เลสเราเตอร์
  - **เฉพาะ N:** เลือก **N only (เฉพาะ N)** เพื่อเพิ่มสมรรถนะไวร์เลส N ให้สูงที่สุด การตั้งค่านี้ป้องกันไม่ให้อุปกรณ์ 802.11g และ 802.11b เชื่อมต่อไปยังไวร์เลสเราเตอร์
  - **ดั้งเดิม:** เลือก **Legacy (ดั้งเดิม)** เพื่ออนุญาตให้อุปกรณ์ 802.11b/g/n เชื่อมต่อไปยังไวร์เลสเราเตอร์ อย่างไรก็ตาม อัตราแบริ์ที่สนับสนุน 802.11n จะรั้นที่ความเร็วสูงที่สุด 54Mbps เท่านั้น
- เลือกช่องการทำงานสำหรับไวร์เลสเราเตอร์ของคุณ เลือก **Auto (อัตโนมัติ)** เพื่ออนุญาตให้ไวร์เลสเราเตอร์เลือกช่องที่มีปริมาณการรบกวนน้อยที่สุดโดยอัตโนมัติ
- เลือกแบนด์วิดธ์ของช่องเพื่อให้ได้ความเร็วการรับส่งข้อมูลสูงขึ้น
- เลือกวิธีการยืนยันตัวตนบุคคล
- เมื่อทำเสร็จ, คลิก **Apply (นำไปใช้)**

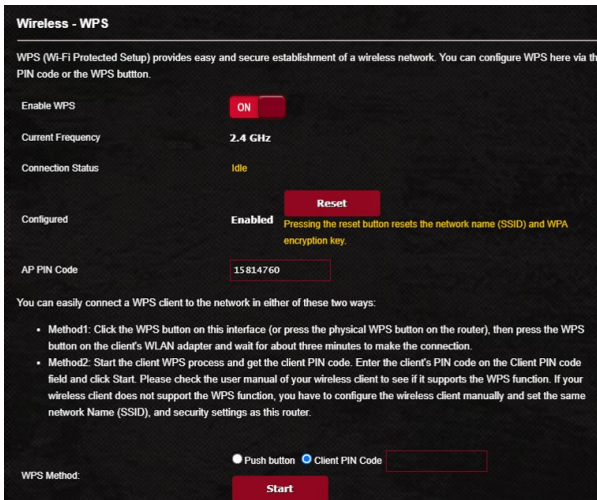
## 3.21.2 WPS

WPS (การตั้งค่า WiFi ที่มีการป้องกัน) เป็นมาตรฐานด้านความปลอดภัยไร้สาย ที่อนุญาตให้คุณเชื่อมต่ออุปกรณ์ต่างๆ ไปยังเครือข่ายไร้สายอย่างง่ายดาย คุณสามารถกำหนดค่าฟังก์ชัน WPS ด้วยรหัส PIN หรือปุ่ม WPS

---

**หมายเหตุ:** ตรวจสอบให้แน่ใจว่าอุปกรณ์สนับสนุน WPS

---



ในการเปิดทำงาน WPS บนเครือข่ายไร้สายของคุณ:

1. จากหน้าค่าตั้งระบบเมนู 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 สนับสนุนการยืนยันตัวตนของคุณของระบบเปิด, WPA/WPA2-ส่วนตัว WPS ไม่สนับสนุนเครือข่ายไร้สายที่ใช้วิธีการเข้ารหัสแอสซิงโครนัส, WPA-เอ็นเตอร์ไพรส์, WPA2-เอ็นเตอร์ไพรส์ และ RADIUS

---



4. ในฟิลด์ WPS Method (วิธี WPS), เลือก **Push button (ปุ่มกด)** หรือ **Client PIN Code (รหัส 4 หลัก PIN)** ถ้าคุณเลือก **Push button (ปุ่มกด)**, ไปยังขั้นตอนที่ 5 ถ้าคุณเลือก **Client PIN Code (รหัส 4 หลัก PIN)**, ไปยังขั้นตอนที่ 6
5. ในการตั้งค่า WPS โดยใช้ปุ่ม 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 โดยใช้รหัส PIN ของไคลเอ็นต์, ให้ปฏิบัติตามขั้นตอนเหล่านี้:
  - a. คำนวณรหัส PIN WPS บนคู่มือผู้ใช้ของอุปกรณ์ไร้สายของคุณ หรือบนตัวอุปกรณ์
  - b. ป้อนรหัส PIN ของไคลเอ็นต์บนกล่องข้อความ
  - c. คลิก **Start (เริ่ม)** เพื่อสั่งให้ไวร์เลสเราเตอร์ของคุณเข้าสู่โหมดสำรวจ WPS ตัวแสดงสถานะ LED ของเราเตอร์จะกะพริบ 3 ครั้งอย่างรวดเร็ว จนกระทั่งตั้งค่า WPS สมบูรณ์

### 3.21.3 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 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	FC:34:197:27:6A:11:0
5 GHz-1 MAC	FC:34:197:27:6A:11:4
8 GHz MAC	FC:34:197:27:6A:11:8
Band	2.4 GHz
AP Mode	AP Only
Connect to APs in list	<input checked="" type="radio"/> Yes <input type="radio"/> No

**Remote AP List (Max Limit : 4)**

Remote AP List	Add / Delete
No data in table.	

**Apply**

ในการตั้งค่าไร้สายบริดจ์:

1. จากหน้าต่างระบบเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง) > Wireless (ไร้สาย) > WDS (ระบบการกระจายไร้สาย)**
2. เลือกแถบความถี่สำหรับไร้สายบริดจ์

3. ในฟิลด์ **AP Mode (โหมด AP)**, เลือกระหว่างตัวเลือกต่อไปนี้:

- **AP เท่านั้น:** ปิดทำงานฟังก์ชันไวร์เลสบริดจ์
- **WDS เท่านั้น:** เปิดทำงานคุณสมบัติไวร์เลสบริดจ์ แต่ป้องกันไม่ให้อุปกรณ์ไร้สาย/สถานีอื่นเชื่อมต่อไปยังเราเตอร์
- **ไฮบริด:** เปิดทำงานคุณสมบัติไวร์เลสบริดจ์ และอนุญาตให้อุปกรณ์ไร้สาย/สถานีอื่นเชื่อมต่อไปยังเราเตอร์ได้

---

**หมายเหตุ:** ในโหมดไฮบริด, อุปกรณ์ไร้สายที่เชื่อมต่ออยู่กับ ASUS ไวร์เลสเราเตอร์ จะได้รับความเร็วการเชื่อมต่อเพียงครึ่งหนึ่งของแอดเซสพอยด์เท่านั้น

---

4. ในฟิลด์ **Connect to APs in list (เชื่อมต่อไปยัง AP ในรายการ)**, คลิก **Yes (ใช่)** ถ้าคุณต้องการเชื่อมต่อไปยังแอดเซสพอยด์ในรายการรีโมท AP


5. ตามค่าเริ่มต้น ช่องการทำงาน/การควบคุมสำหรับไวร์เลสบริดจ์ ถูกตั้งค่าเป็น **Auto (อัตโนมัติ)** เพื่ออนุญาตให้เราเตอร์เลือกช่องที่มีปริมาณการรบกวนน้อยที่สุดโดยอัตโนมัติ

คุณสามารถแก้ไข **Control Channel (ช่องควบคุม)** จาก **Advanced Settings (การตั้งค่าขั้นสูง) > Wireless (ไร้สาย) > General (ทั่วไป)**

---

**หมายเหตุ:** ช่องที่ใช้ได้ แตกต่างกันไปตามประเทศหรือภูมิภาค

---

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

---

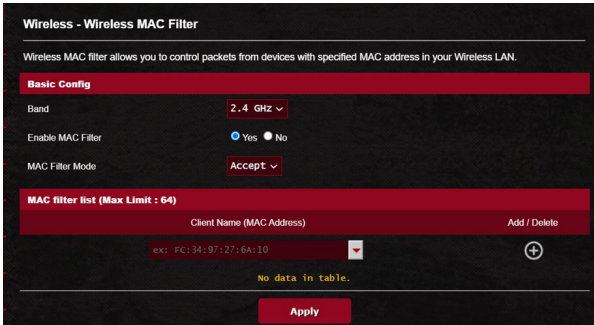
**หมายเหตุ:** แอดเซสพอยด์ใดๆ ที่เพิ่มไปยังรายการ ควรอยู่บนช่องควบคุมเดียวกันกับ ASUS ไวร์เลสเราเตอร์

---

7. คลิก **Apply (นำไปใช้)**

### 3.21.4 ตัวกรอง MAC ไร้สาย

ตัวกรอง MAC ไร้สาย ให้การควบคุมแพคเกจที่ส่งไปยัง MAC (การควบคุมการเข้าถึงสื่อ) แอดเดรสที่ระบุบนเครือข่ายไร้สายของคุณ

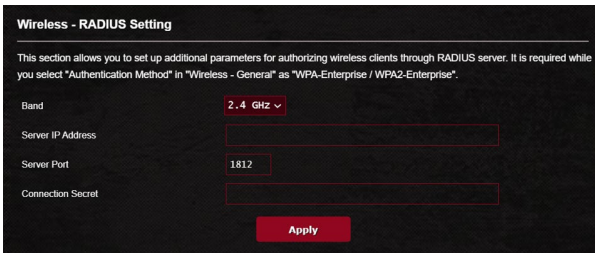


ในการตั้งค่าตัวกรอง MAC ไร้สาย:

1. จากหน้าจอรูขุมล้อมเมนู ไปยัง **Advanced Settings (การตั้งค่าขั้นสูง) > Wireless (ไร้สาย) > Wireless MAC Filter (ตัวกรอง MAC ไร้สาย)**
2. เลือกแถบความถี่
3. ทำเครื่องหมายที่ **Yes (ใช่)** ในฟิลด์ **Enable Mac Filter (เปิดทำงานตัวกรอง Mac)**
4. 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
5. บนรายการตัวกรอง MAC, คลิกปุ่ม **Add (เพิ่ม)**  และพิมพ์ MAC แอดเดรสของอุปกรณ์ไร้สายเข้าไป
6. คลิก **Apply (นำไปใช้)**

### 3.21.5 การตั้งค่า RADIUS

การตั้งค่า RADIUS (บริการผู้ใช้ที่โทรเข้าเพื่อยืนยันตัวตนบุคคลระยะไกล) ให้ระบบป้องกันขั้นพิเศษเมื่อคุณเลือก WPA-เอ็นเตอร์ไพรส์, WPA2-เอ็นเตอร์ไพรส์ หรือ Radius กับ 802.1x เป็นโหมดการยืนยันตัวตนบุคคลของคุณ



#### ในการตั้งค่า RADIUS ไร้สาย:

1. ให้แน่ใจว่าโหมดการยืนยันตัวตนบุคคลของไวร์เลสเราเตอร์ถูกตั้งค่าเป็น WPA-เอ็นเตอร์ไพรส์, หรือ WPA2-เอ็นเตอร์ไพรส์

หมายเหตุ: โปรดดูส่วน 3.21.1 ทั่วไป สำหรับการกำหนดค่าโหมดการยืนยันตัวตนบุคคลของไวร์เลสเราเตอร์ของคุณ

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 **Server Port (พอร์ตของเซิร์ฟเวอร์)** ให้พิมพ์พอร์ตของเซิร์ฟเวอร์เข้าไป
6. ในฟิลด์ **Connection Secret (ความลับการเชื่อมต่อ)**, กำหนดรหัสผ่านเพื่อเข้าถึง RADIUS เซิร์ฟเวอร์ของคุณ
7. คลิก **Apply (นำไปใช้)**

## 3.21.6 Professional (มืออาชีพ)

หน้าจอ Professional (มืออาชีพ) ให้ตัวเลือกการกำหนดค่าขั้นสูง

หมายเหตุ: เราแนะนำให้ผู้ใช้ค่าเริ่มต้นบนหน้านี้

Setting	Value	Notes
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
Hide SSID	No	
Wireless Mode	Auto	big Protection
802.11ax / Wi-Fi 6 mode	Enable	If compatibility issue occurs when enabling 802.11ax / Wi-Fi 6 mode, please check FAQ
Wi-Fi Agile Multiband	Disable	
Target Wake Time	Disable	
Bluetooth Coexistence	Disable	
Enable KMP Snooping	Enable	
Multicast Rate(Mbps)	Auto	
Preamble Type	Long	
AMPOU RTS	Enable	
RTS Threshold	2347	
DTIM Interval	1	
Beacon Interval	100	
Enable TX Dursling	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)	
Airline Fairness	Disable	
Multi-User MIMO	Disable	
OFDMA/802.11ax MU-MIMO	Disable	
Explicit Beamforming	Enable	
Universal Beamforming	Enable	
Tx power adjustment	Performance	

ในหน้าจอ Professional Settings (การตั้งค่าแบบมืออาชีพ), คุณสามารถกำหนดค่าต่อไปนี้:

- **ความถี่:** เลือกแถบความถี่ซึ่งการตั้งค่าแบบมืออาชีพจะถูกนำไปใช้ยัง

- **เปิดทำงานวิทยุ:** เลือก **Yes (ใช่)** เพื่อเปิดทำงานเครือข่ายไร้สาย เลือก **No (ไม่)** เพื่อปิดทำงานเครือข่ายไร้สาย
- **เปิดใช้ตัวกำหนดเวลาแบบไร้สาย:** เลือก **Yes (ใช่)** เพื่อเปิดใช้งานและกำหนดค่าตัวกำหนดตารางเวลาไร้สาย เลือก **No (ไม่)** เพื่อปิดใช้งานตัวกำหนดตารางเวลาไร้สาย
  - **วันที่เพื่อเปิดทำงานวิทยุ (วันธรรมดา):** คุณสามารถระบุว่าเป็นวันที่ใดของสัปดาห์ที่จะให้เครือข่ายไร้สายเปิดทำงาน
  - **เวลาของวันเพื่อเปิดทำงานวิทยุ:** คุณสามารถระบุช่วงเวลาเมื่อเครือข่ายไร้สายเปิดทำงานระหว่างสัปดาห์
  - **วันที่เพื่อเปิดทำงานวิทยุ (สุดสัปดาห์):** คุณสามารถระบุว่าเป็นวันที่ใดของสุดสัปดาห์ที่จะให้เครือข่ายไร้สายเปิดทำงาน
  - **เวลาของวันเพื่อเปิดทำงานวิทยุ:** คุณสามารถระบุช่วงเวลาเมื่อเครือข่ายไร้สายเปิดทำงานระหว่างสุดสัปดาห์
- **ตั้งค่า AP ที่แยกกัน:** รายการ Set AP isolated (ตั้งค่า AP ที่แยกกัน) ป้องกันอุปกรณ์ไร้สายบนเครือข่ายของคุณไม่ให้สื่อสารซึ่งกันและกัน คุณสมบัตินี้มีประโยชน์ ถ้ามีแขกจำนวนมากเข้ามาใช้หรือออกจากเครือข่ายของคุณบ่อยๆ เลือก **Yes (ใช่)** เพื่อเปิดทำงานคุณสมบัตินี้ หรือเลือก **No (ไม่)** เพื่อปิดทำงาน
- **Roaming assistant (ผู้ช่วยโรมมิ่ง):** ในการกำหนดค่าเครือข่ายที่เกี่ยวข้องกับแอคเซสพอยต์หลายตัว หรือไวร์เลส รีพีตเตอร์ บางครั้งโหนดเอ็นดีไร้สายไม่สามารถเชื่อมต่อไปยัง AP ที่มีโดยอัตโนมัติได้ เนื่องจากกำลังเชื่อมต่อง่ายกับไวร์เลสเราเตอร์หลักอยู่ เปิดทำงานการตั้งค่านี้ เพื่อให้โหนดเอ็นดีจะตัดการเชื่อมต่อจากไวร์เลสเราเตอร์หลักถ้าความแรงสัญญาณอยู่ต่ำกว่าขีดจำกัดที่เฉพาะเจาะจง และเชื่อมต่อไปยังสัญญาณที่แรงกว่า
- **Enable IGMP Snooping (เปิดทำงาน IGMP สนุบปิ้ง):** การเปิดทำงานฟังก์ชันนี้ อนุญาตให้ IGMP (โพรโตคอลการจัดการกลุ่มอินเทอร์เน็ต) ถูกตรวจสอบระหว่างอุปกรณ์ต่างๆ และปรับการจราจรมัลติแคสต์ไร้สายให้ดีที่สุด
- **อัตราบิตเดิศาจ (Mbps):** เลือกอัตราการส่งข้อมูลบิตเดิศาจหรือคลิก **Disable (ปิดทำงาน)** เพื่อปิดการส่งข้อมูลเดี่ยวพร้อมกัน
- **ประเภทพีแอมบีล:** ประเภทพีแอมบีลกำหนดความยาวของเวลาที่เราเตอร์ใช้สำหรับ CRC (ตรวจสอบความซ้ำซ้อนแบบวงกลม) CRC เป็นวิธีในการตรวจสอบข้อผิดพลาดระหว่างการส่งข้อมูล เลือก **Short (สั้น)** สำหรับเครือข่ายไร้สายที่มุ่งให้มีการจราจรเครือข่าย

ข้างสูง เลือก **Long (ยาว)** ถ้าเครือข่ายไร้สายของคุณประกอบด้วยอุปกรณ์ไร้สายรุ่นเก่า หรือแบบดั้งเดิม

- **AMPDU RTS (AMPDU RTS):** การเปิดทำงานฟังก์ชันนี้ อนุญาตให้สร้างกลุ่มของเฟรมก่อนที่จะถูกส่งออกไป และใช้ RTS สำหรับทุก AMPDU สำหรับการสื่อสารระหว่างอุปกรณ์ 802.11g และ 802.11b
- **RTS Threshold (ขีดจำกัด RTS):** เลือกค่าที่ต่ำกว่าสำหรับขีดจำกัด RTS (ค่าขอให้ส่ง) เพื่อปรับปรุงการสื่อสารไร้สายในเครือข่ายไร้สายที่ยุง ซึ่งมีการจราจรเครือข่ายสูง และอุปกรณ์ไร้สายจำนวนมาก
- **ช่วง DTIM:** ช่วง DTIM (ข้อความระบุงการจราจรที่ส่ง) หรืออัตราการส่งขอมูล คือช่วงเวลา ก่อนที่สัญญาณจะถูกส่งไปยังอุปกรณ์ไร้สายในโหมดสลิป เพื่อเป็นการระบุงว่ามีแพคเก็ตขอมูลที่รอการส่ง คาเริ่มต่นคือ 3 มิลลิวินาที
- **ช่วงเวลามีค่อน:** ช่วงเวลามีค่อน คือเวลาระหว่าง DTIM หนึ่งกับตัวถัดไป คาเริ่มต่นคือ 100 มิลลิวินาที ลดคาช่วงเวลามีค่อนลง สำหรับการเชื่อมต่อไร้สายที่ไม่มีเสถียรภาพ หรือสำหรับอุปกรณ์โรมมิ่ง
- **เปิดทำงาน TX เวิร์สดี้ง:** เปิดทำงาน TX เวิร์สดี้ง ช่วยปรับปรุงความเร็วการส่งขอมูลระหว่างไวรเลสเราเตอร์ และอุปกรณ์ 802.11g
- **เปิดทำงาน WMM APSD:** เปิดทำงาน WMM APSD (Wi-Fi มัลติมีเดีย การส่งการประหยัดพลังงานอัตโนมัติ) เพื่อปรับปรุงการจัดการพลังงานระหว่างอุปกรณ์ไร้สายต่างๆ เลือก **Disable (ปิดทำงาน)** เพื่อปิด WMM APSD
- **Reducing USB 3.0 interference (การลดการรบกวน USB 3.0):** การเปิดทำงานฟังก์ชันนี้ เพื่อใหม่ั่นใจว่าสมรรถนะการทำงานไร้สายจะดีที่สุดบนแถบความถี่ 2.4 GHz การปิดทำงานคณสมบัตินี้จะเพิ่มความเร็ุงการส่งขอมูลของพอร์ต USB 3.0 และอาจส่งผลกระทบต่อประสิทธิภาพการทำงานไร้สายของความถี่ 2.4 GHz
- **Optimize AMPDU aggregation (เพิ่มประสิทธิภาพการรวม AMPDU):** ปรับจำนวนสูงสุดของ MPDU ใน AMPDU ให้เหมาะสมที่สุด และหลีกเลี่ยงแพคเก็ตที่จะสูญหาย หรือเสียหายระหว่างการรับส่งขอมูลในช่องไร้สายที่ม่กมีขอมัดพลาด
- **Turbo QAM (เทอร์โบ QAM):** การเปิดทำงานฟังก์ชันนี้ อนุญาตให้ส่นบส่นน 256-QAM (MCS.8/9) บนความถี่ 2.4GHz เพื่อให้ได้ระยะและอัตราการส่งผ่านที่ดีกวาบนความถี่นั้น



- **Airtime Fairness (ความสมดุลแอร์ต้าวม)**: ด้วยตัวเลือกความสมดุลแอร์ต้าวม ความเร็วของเครือข่ายไม่ได้ถูกกำหนดโดยการจราจรที่ช้าที่สุด ความสมดุลแอร์ต้าวม อนุญาตให้การส่งข้อมูลทั้งหมดทำงานด้วยความเร็วตามศักยภาพที่สูงที่สุด โดยการจัดสรรเวลาที่เท่ากันระหว่างโหนดเอ็นดีต่างๆ
- **Explicit Beamforming (เอ็กซพลิต บีมฟอร์มมิง)**: ทั้งอะแดปเตอร์ WLAN และเราเตอร์ของโหนดเอ็นดี สนับสนุนเทคโนโลยีบีมฟอร์มมิง เทคโนโลยีนี้อนุญาตให้อุปกรณ์เหล่านี้สื่อสารการประมาณช่องทาง และทิศทางเปลี่ยนเส้นทางซึ่งกันและกัน เพื่อปรับปรุงความเร็วในการดาวน์โหลดและการอัปโหลดให้ดีขึ้น
- **Universal Beamforming (ยูนิเวอร์ซัลบีมฟอร์มมิง)**: สำหรับไวเลสอะแดปเตอร์รุ่นเก่าที่ไม่สนับสนุนบีมฟอร์มมิง เราเตอร์จะประมาณช่องทาง และกำหนดทิศทางเปลี่ยนเส้นทางให้ เพื่อปรับปรุงความเร็วการดาวน์โหลด

## 4 ยูทิลิตี้

---

### หมายเหตุ:

- ดาวน์โหลดและติดตั้งยูทิลิตี้ของไวร์เลสเราเตอร์จากเว็บไซต์ ASUS:
- การสำรวจอุปกรณ์ v1.4.7.1 ที่ <http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Discovery.zip>
- การกู้คืนเฟิร์มแวร์ v1.9.0.4 ที่ <http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Rescue.zip>
- ยูทิลิตี้เครื่องพิมพ์ของ Windows v1.0.5.5 ที่ <http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Printer.zip>
- ยูทิลิตี้เหล่านี้ไม่ได้รับการสนับสนุนบน MAC OS

---

### 4.1 การค้นหาอุปกรณ์

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

ในการเปิดยูทิลิตี้ การค้นหาอุปกรณ์:

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

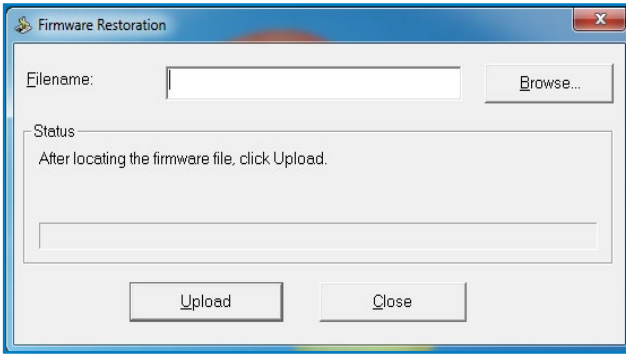
---

**หมายเหตุ:** เมื่อคุณตั้งค่าเราเตอร์เป็นโหมดแอดแอดเดสส์พอยต์, คุณจำเป็นต้องใช้ การสำรวจอุปกรณ์ เพื่อรับ IP แอดเดรสของเราเตอร์

---

## 4.2 การกู้คืนเฟิร์มแวร์

การกู้คืนเฟิร์มแวร์ ถูกใช้บน ASUS ไร้สาย เราเตอร์ หลังจากที่ทำกรอัปเดตเฟิร์มแวร์ล้มเหลว ยูทิลิตีนี้จะอัปโหลดไฟล์เฟิร์มแวร์ไปยังไร้สาย เราเตอร์ กระบวนการจะใช้เวลาประมาณ 3 ถึง 4 นาที



---

**สำคัญ:** ปิดโหมดช่วยเหลือน ก่อนที่จะใช้ยูทิลิตี การกู้คืนเฟิร์มแวร์

---

**หมายเหตุ:** คุณสมบัตินี้ไม่ได้รับการสนับสนุนบน MAC OS

---

**ในการเปิดโหมดช่วยเหลือน และใช้ยูทิลิตี การกู้คืนเฟิร์มแวร์:**

1. ถอดปลั๊กไร้สายเราเตอร์จากแหล่งพลังงาน
2. กดปุ่มกู้คืน ที่แผงด้านหลังค้างไว้ ในขณะที่ยกนั้นก็เสียบปลั๊กไร้สายเราเตอร์กลับเข้าไป ยังแหล่งพลังงาน ปลอบปุ่มกู้คืน เมื่อ LED เพาเวอร์ที่แผงด้านหลังกะพริบซ้ำๆ ซึ่งเป็นการ ระบุว่าไร้สายเราเตอร์อยู่ในโหมดช่วยเหลือน
3. ตั้งค่าสแตติก IP บนคอมพิวเตอร์ของคุณ และใช้สิ่งต่อไปนี้เพื่อตั้งค่าการตั้งค่า TCP/IP ของคุณ:

**IP แอดเดรส:** 192.168.1.x

**ซับเน็ต มาสก:** 255.255.255.0

4. จากเดสก์ทอปของคอมพิวเตอร์ของคุณ, คลิก **Start (เริ่ม) > All Programs (โปรแกรมทั้งหมด) > ASUS Utility (ยูทิลิตี ASUS)**

## GT6 Wireless Router (GT6 ไร้เลส เราเตอร์) > Device Discovery (การค้นห อุปกรณ์)

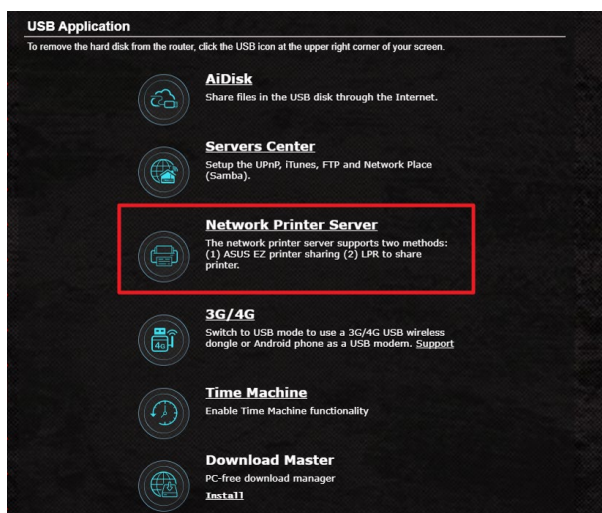
5. คลิก **Browse (เรียกดู)** เพื่อเลือกไฟล์เฟิร์มแวร์ จากนั้นคลิก **Upload (อัปโหลด)**

**หมายเหตุ:** นี่ไม่ใช่ยูทิลิตี้สำหรับอัปเดตเฟิร์มแวร์ และไม่สามารถใช้กับ ASUS ไร้เลสเราเตอร์ที่ทำงานได้ คุณต้องทำการอัปเดตเฟิร์มแวร์ ตามปกติผ่านอินเทอร์เฟซบนเว็บ ดู **บทที่ 3: การกำหนดค่าการตั้งค่าทั่วไป และ การตั้งค่าขั้นสูง** สำหรับรายละเอียดเพิ่มเติม

## 4.3 การตั้งค่าพรินเตอร์เซิร์ฟเวอร์ของคุณ

### 4.3.1 การแชร์เครื่องพิมพ์ ASUS EZ

ยูทิลิตี้การแชร์เครื่องพิมพ์ ASUS EZ อนุญาตให้คุณเชื่อมต่อเครื่องพิมพ์ USB เข้ากับพอร์ต USB ของไร้เลสเราเตอร์ของคุณ และตั้งค่าพรินต์เซิร์ฟเวอร์ การทำเช่นนี้ ทำให้เน็ตเวิร์กโคเลเอ็นต์ของคุณสามารถพิมพ์และสแกนไฟล์แบบไร้สายได้



---

หมายเหตุ: ฟังก์ชันพรินต์เซิร์ฟเวอร์ได้รับการสนับสนุนบน Windows® 7/8/8.1/10

---

### ในการตั้งค่าโหมดการแชร์เครื่องพิมพ์ EZ:

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

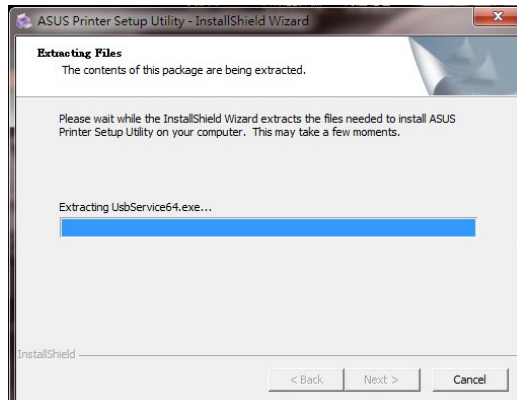


---

หมายเหตุ: ยูทิลิตี้เน็ตเวิร์กพรินเตอร์ ได้รับการสนับสนุนบน Windows® 7/8/8.1/10 เท่านั้น ในการติดตั้งยูทิลิตี้บน Mac OS, เลือก **ใช้โปรโตคอล LPR** สำหรับการแชร์เครื่องพิมพ์

---

3. อินซ์ิปไฟล์ที่ดาวน์โหลดมา และคลิกไอคอน **Printer (เครื่องพิมพ์)** เพื่อรันโปรแกรมตั้งค่าเน็ตเวิร์กพรินเตอร์



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

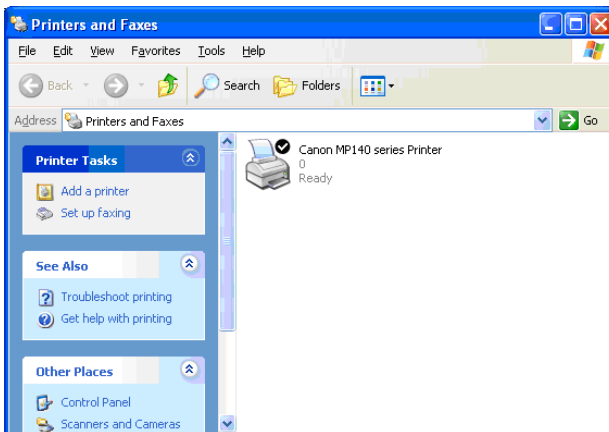


- รอเป็นเวลาสองสามนาที เพื่อให้การตั้งค่าเริ่มต้นเสร็จ คลิก **Next (ถัดไป)**
- คลิก **Finish (เสร็จสิ้น)** เพื่อทำการติดตั้งให้สมบูรณ์

## 7. ทำตามขั้นตอนของ Windows® OS เพื่อติดตั้งไดรเวอร์เครื่องพิมพ์



## 8. หลังจากทำการติดตั้งไดรเวอร์ของเครื่องพิมพ์สมบูรณ์แล้ว ขณะนี้เน็ตเวิร์กไคลเอนต์ก็สามารถใช้เครื่องพิมพ์ได้

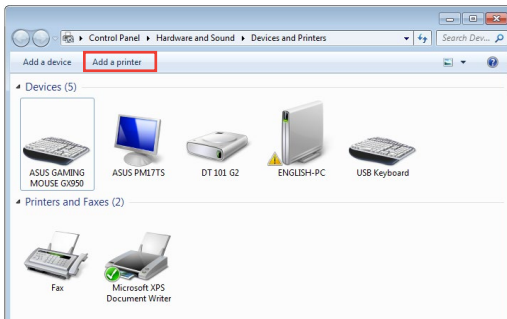


### 4.3.2 การใช้ LPR เพื่อแชร์เครื่องพิมพ์

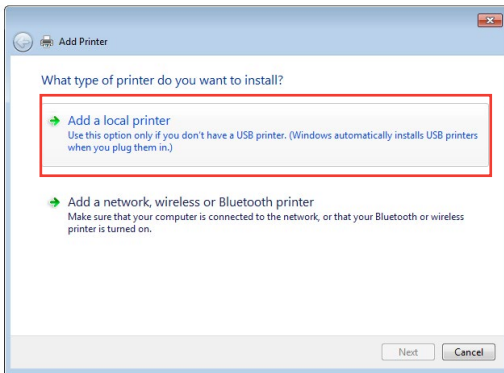
คุณสามารถแชร์เครื่องพิมพ์ของคุณกับคอมพิวเตอร์อื่นๆ ที่รันระบบปฏิบัติการ Windows® และ MAC ได้โดยใช้ LPR/LPD (Line Printer Remote/Line Printer Daemon)

#### 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)**

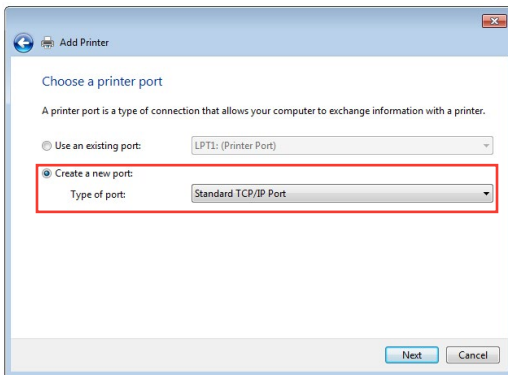


2. เลือก **Add a local printer (เพิ่มเครื่องพิมพ์ในเครื่อง)** จากนั้นคลิก **Next (ถัดไป)**

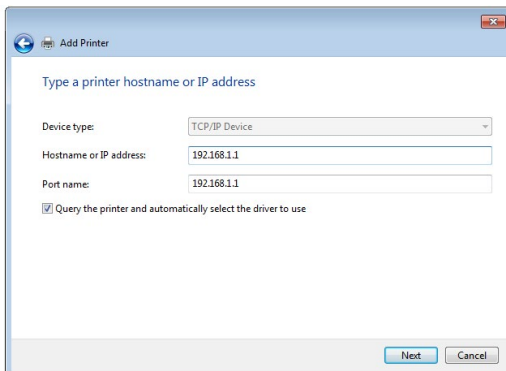




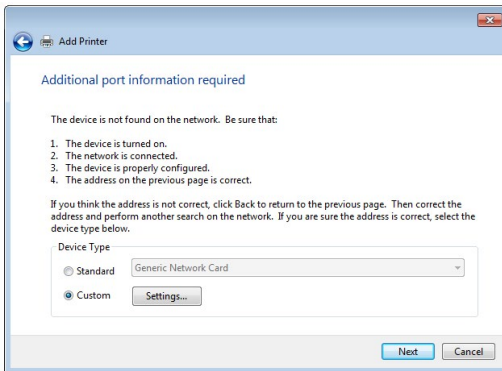
3. เลือก **Create a new port (สร้างพอร์ตใหม่)** จากนั้นตั้งค่า **Type of Port (ชนิดของพอร์ต)** เป็น **Standard TCP/IP Port (พอร์ต TCP/IP มาตรฐาน)** คลิก **Next (ถัดไป)**



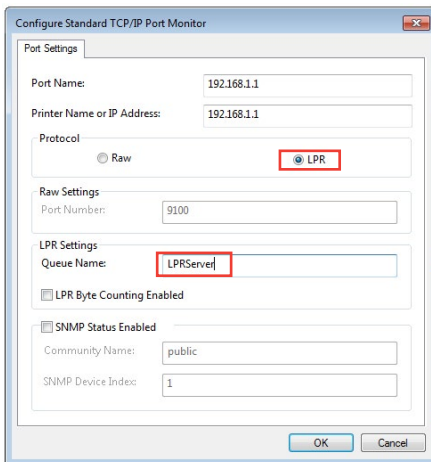
4. ในฟิลด์ **Hostname or IP address (ชื่อโฮสต์หรือ IP แอดเดรส)**, ป้อน IP แอดเดรสของไวร์เลสเราเตอร์ จากนั้นคลิก **Next (ถัดไป)**



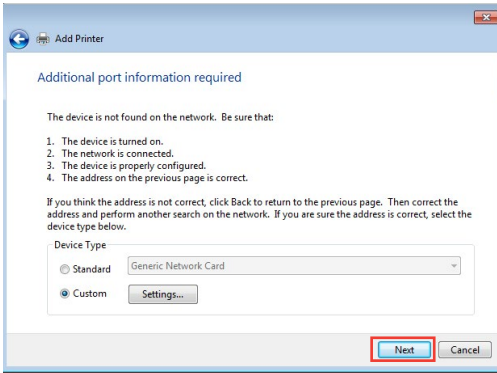
## 5. เลือก Custom (กำหนดเอง) จากนั้นคลิก Settings (การตั้งค่า)



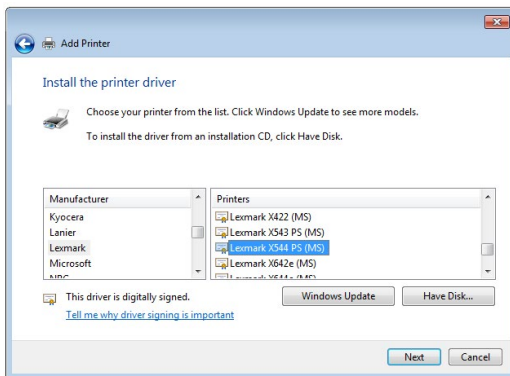
## 6. ตั้งค่า Protocol (โพรโทคอล) เป็น LPR (LPR) ในฟิลด์ Queue Name (ชื่อคิว), ป้อน LPRServer จากนั้นคลิก OK (ตกลง) เพื่อทำต่อ



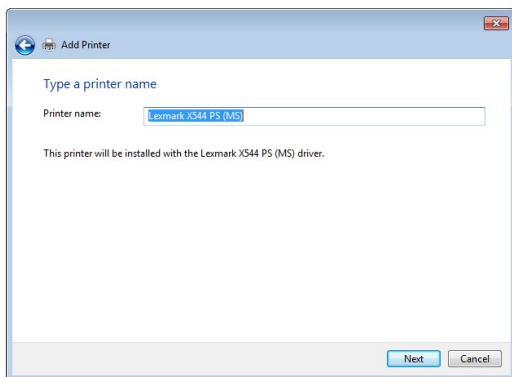
7. คลิก **Next (ถัดไป)** เพื่อทำการตั้งค่าพอร์ต TCP/ IP มาตรฐานให้เสร็จ



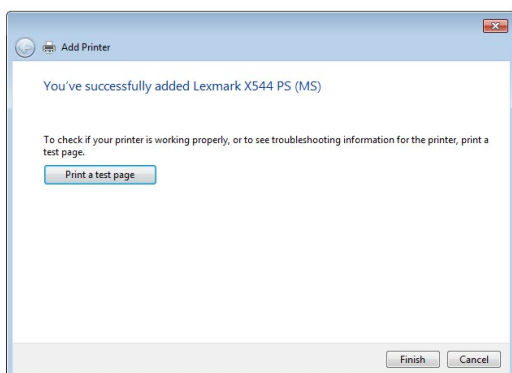
8. ติดตั้งไดรเวอร์เครื่องพิมพ์จากรายการรุ่นของผู้จำหน่าย ถ้าเครื่องพิมพ์ของคุณไม่ได้อยู่ในรายการ, คลิก **Have Disk (มีดิสก์)** เพื่อติดตั้งไดรเวอร์เครื่องพิมพ์ของคุณจาก CD-ROM หรือไฟล์



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



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



## 4.4 ดาวน์โหลดมาสเตอร์

ดาวน์โหลดมาสเตอร์ เป็นยูทิลิตี้ที่ช่วยคุณดาวน์โหลดไฟล์ต่างๆ แม้กระทั่งในขณะที่เน็ตบุคหรืออุปกรณ์อื่นๆ ปิดเครื่องอยู่

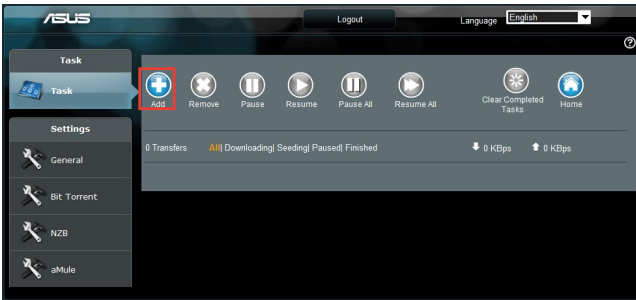
**หมายเหตุ:** คุณจำเป็นต้องมีอุปกรณ์ USB เชื่อมต่ออยู่กับไวร์เลสเราเตอร์ เพื่อใช้ดาวน์โหลดมาสเตอร์

**ในการใช้ดาวน์โหลดมาสเตอร์:**

1. คลิก **Advanced Settings** (การตั้งค่าขั้นสูง) > **USB Application** (การใช้งานผ่าน USB) > **Download Master** (ดาวน์โหลดมาสเตอร์) เพื่อดาวน์โหลดและติดตั้งยูทิลิตี้โดยอัตโนมัติ

**หมายเหตุ:** ถ้าคุณมี USB ใดตัวมากกว่าหนึ่งตัว, ให้เลือกอุปกรณ์ USB ที่คุณต้องการดาวน์โหลดไฟล์ไปยัง

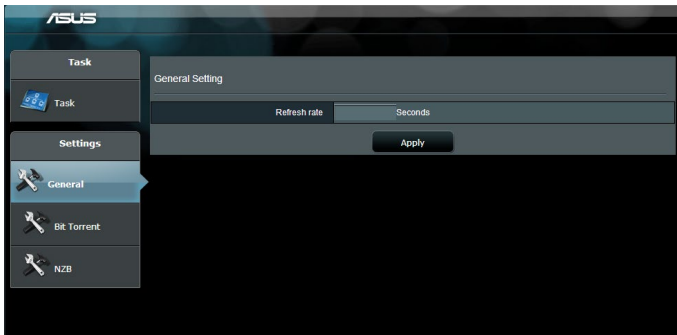
2. หลังจากที่กระบวนการดาวน์โหลดเสร็จ, คลิกไอคอน **Download Master** (ดาวน์โหลดมาสเตอร์) เพื่อเริ่มการใชยยูทิลิตี้
3. คลิก **Add** (เพิ่ม) เพื่อเพิ่มงานดาวน์โหลด



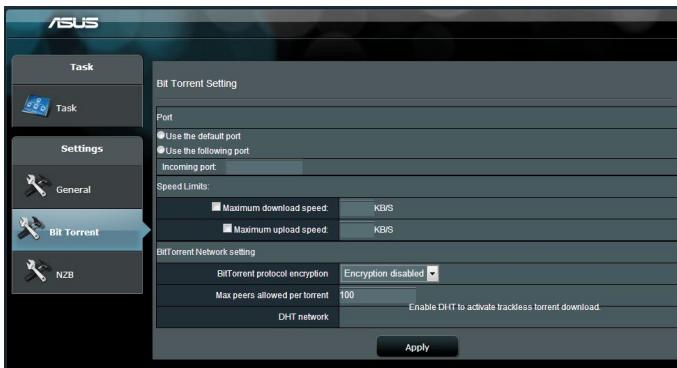
4. เลือกชนิดการดาวน์โหลด เช่น บิตทอว์เร็นต์, HTTP หรือ FTP ให้ไฟล์บิตทอว์เร็นต์ หรือ URL เพื่อเริ่มการดาวน์โหลด

**หมายเหตุ:** สำหรับรายละเอียดเกี่ยวกับบิตทอว์เร็นต์, ให้อ่านส่วน 4.4.1 การกำหนดค่าการตั้งค่าการดาวน์โหลดบิตทอว์เร็นต์

## 5. ใช้หน้าจอเมนูเพื่อกำหนดค่าการตั้งค่าขั้นสูง



### 4.4.1 การกำหนดค่าการตั้งค่าการดาวน์โหลดบิตทอร์เรนต์

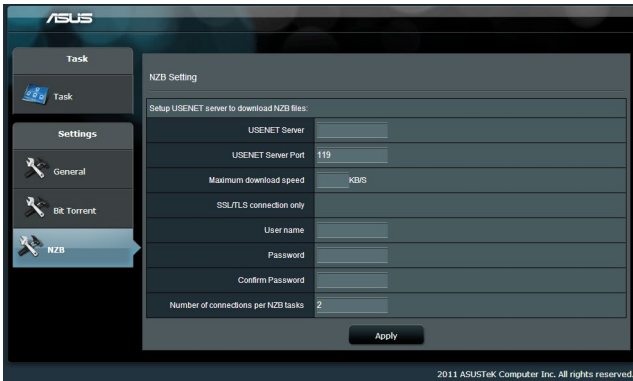


#### ในการกำหนดค่าการตั้งค่าการดาวน์โหลดบิตทอร์เรนต์:

1. จากหน้าจอเมนูของดาวน์โหลดมาสเตอร์, คลิก **Bit Torrent (บิตทอร์เรนต์)** เพื่อเปิดหน้า **Bit Torrent Setting (การตั้งค่าบิตทอร์เรนต์)**
2. เลือกพอร์ตที่จะจองสำหรับงานดาวน์โหลดของคุณ
3. เพื่อป้องกันการติดขัดของเครือข่าย, คุณสามารถจำกัดความเร็วการอัปโหลดและดาวน์โหลดสูงสุดได้ภายใต้ **Speed Limits (ขีดจำกัดความเร็ว)**
4. คุณสามารถจำกัดจำนวนของเพียร์ที่อนุญาตมากที่สุด และเปิดทำงานหรือปิดทำงานการเซิร์ฟเวอร์ระหว่างการดาวน์โหลดได้

## 4.4.2 การตั้งค่า NZB

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



## 5 การแก้ไขปัญหา

บทนี้ให้วิธีแก้ไขปัญหาที่คุณอาจพบกับเราเตอร์ของคุณ 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://rog.asus.com/networking/rog-rapture-GT6-model/helpdesk\\_download](https://rog.asus.com/networking/rog-rapture-GT6-model/helpdesk_download) เพื่อดาวน์โหลดเฟิร์มแวร์ล่าสุด
3. จากหน้า **Firmware Upgrade** (เฟิร์มแวร์อัปเดต), คลิก **Browse** (เรียกดู) 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



## ตรวจสอบว่าสายเคเบิลอีเธอร์เน็ตของคุณเสียบอย่างเหมาะสมหรือไม่

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

## ตรวจสอบว่าการตั้งค่าไร้สายบนคอมพิวเตอร์ของคุณตรงกับค่าของเตอร์ของคุณ

- เมื่อคุณเชื่อมต่อคอมพิวเตอร์ของคุณไปยังเราเตอร์แบบไร้สาย, ให้แน่ใจว่า SSID (ชื่อเครือข่ายไร้สาย), วิธีการเข้ารหัส และรหัสผ่านนั้นถูกต้อง

## ตรวจสอบว่าการตั้งค่าเครือข่ายของคุณถูกต้องหรือไม่

- โคลเอ็นต์แต่ละตัวบนเครือข่ายควรมี IP แอดเดรสที่ถูกต้อง ASUS แนะนำให้คุณใช้ DHCP เซิร์ฟเวอร์ของเราเตอร์เพื่อกำหนด IP แอดเดรสให้กับคอมพิวเตอร์ต่างๆ บนเครือข่ายของคุณ
- ผู้ให้บริการเคเบิลโมเด็มบางราย จำเป็นต้องให้คุณใช้ MAC แอดเดรสของคอมพิวเตอร์ที่ลงทะเบียนครั้งแรกในบัญชี คุณสามารถดู MAC แอดเดรสในเว็บ GUI, **Network Map (แผนที่เครือข่าย) > หน้า Clients (ไคลเอ็นต์)**, และวางตัวชี้เมาส์เหนืออุปกรณ์ของคุณใน **Client Status (สถานะไคลเอ็นต์)**



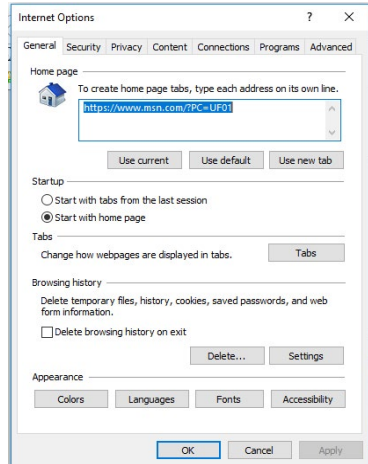
## 5.2 คำถามที่มีการถามบ่อยๆ (FAQs)

### 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, ยกเลิกการเชื่อมต่อแบบพีทูพีทู และตั้งค่า TCP/IP ให้รับ IP แอดเดรสโดยอัตโนมัติ สำหรับรายละเอียดเพิ่มเติม ให้อ่านที่ 1 ของคู่มือผู้ใช้ฉบับนี้
- ให้แน่ใจว่าคุณใช้สายเคเบิลอีเธอร์เน็ต CAT5e หรือ CAT6

# โคลเอนต์ไม่สามารถสร้าง การเชื่อมต่อไร้สายกับ เราเตอร์ได้

หมายเหตุ: ถ้าคุณกำลังมีปัญหาในการเชื่อมต่อไปยังเครือข่าย 5Ghz, ตรวจสอบให้แน่ใจว่าอุปกรณ์ไร้สายของคุณสนับสนุนความถี่ 5Ghz หรือมีความสามารถแบบดualแบนด์

- **อยู่นอกพื้นที่ทำงาน:**
  - ย้ายเราเตอร์ให้เข้าใกล้ไวร์เลส โคลเอนต์ มากขึ้น
- **DHCP เซิร์ฟเวอร์ถูกปิดการทำงาน:**
  1. เปิดเว็บ GUI ไปที่ **Advanced Settings (การตั้งค่าขั้นสูง) > Network Map (แผนที่เครือข่าย) > Clients (โคลเอนต์)** 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 informs the client of the of NDS server IP and default gateway IP. ASUS Router supports up to 253 IP addresses for your local network.

**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

WINS Server

**Enable Manual Assignment**

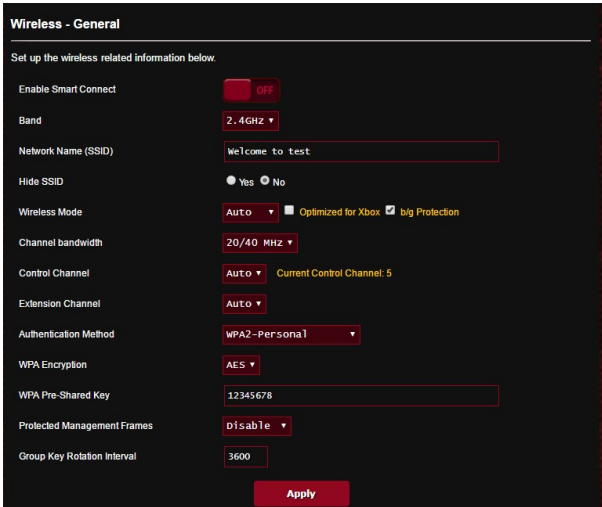
Enable Manual Assignment  Yes  No

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

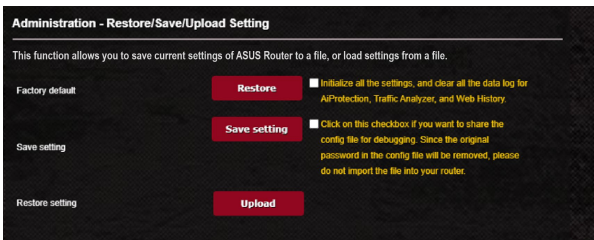
Client Name (MAC Address)	IP Address	Add / Delete
ex: 2C:4D:54:E8:64:E0	<input type="text"/>	<input type="button" value="⊕"/>

No data in table.

- 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 ใดหรือไม่ ในการดำเนินการ, เปิดเว็บ GUI และไปที่ **Advanced Settings (การตั้งค่าขั้นสูง) > Network Map (แผนที่เครือข่าย)**, และตรวจสอบ **Internet status (สถานะอินเทอร์เน็ต)**
- ถ้าเราเตอร์ของคุณไม่สามารถเชื่อมต่อไปยัง WAN IP แอดเดรสของ ISP ใด, ให้ลองเริ่มเครือข่ายของคุณใหม่ ตามที่อธิบายในหัวข้อ **เริ่มเครือข่ายของคุณใหม่ในลำดับต่อไป** ภายใต้อาการแก้ไขปัญหาพื้นฐาน



- อุปกรณ์ถูกบล็อกผ่านฟังก์ชัน **Parental Control (การควบคุมโดยผู้ปกครอง)** ไปที่ **General (ทั่วไป) > AiProtection > Parental Controls (การควบคุมโดยผู้ปกครอง)** และดูว่าอุปกรณ์อยู่ในรายการหรือไม่ ถ้าอุปกรณ์ถูกแสดงอยู่ภายใต้ **Client Name (ชื่อไคลเอนต์)**, ให้ลบอุปกรณ์ออก โดยใช้ปุ่ม **Delete (ลบ)** หรือปรับ การตั้งค่าการจำกัดการเวลา
- ถ้ายังคงเข้าถึงอินเทอร์เน็ตไม่ได้, ให้ลองบูตคอมพิวเตอร์ของคุณใหม่ และตรวจสอบ IP แอดเดรส และเกตเวย์แอดเดรสของเครือข่าย
- ตรวจสอบไฟแสดงสถานะบนโมเด็มเดิม ADSL และไวร์เลส เราเตอร์ ถ้า LED WAN บนไวร์เลสเราเตอร์ไม่ติด, ให้ตรวจสอบว่าสายเคเบิลทั้งหมดเสียบอยู่อย่างเหมาะสมหรือไม่

## คุณลืม SSID (ชื่อเครือข่าย) หรือรหัสผ่านเครือข่าย

- ตั้งค่า SSID และคีย์การเข้ารหัสใหม่ ผ่านการเชื่อมต่อแบบมีสาย (สายเคเบิลอีเทอร์เน็ต) 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)**

ค่าต่อไปนี้เป็นค่าเริ่มต้นจากโรงงาน:

ชื่อผู้ใช้:	admin
รหัสผ่าน:	admin
เปิดทำงาน DHCP:	ใช่ (ถ้าเสียบสายเคเบิล WAN)
IP แอดเดรส:	http://www.asusrouter.com (หรือ 192.168.50.1)
ชื่อโดเมน:	(ว่าง)
ซับเน็ต มาสก์:	255.255.255.0
DNS เซิร์ฟเวอร์ 1:	192.168.50.1
DNS เซิร์ฟเวอร์ 2:	(ว่าง)
SSID (2.4GHz):	ASUS_XX_2G
SSID (5GHz-1):	ASUS_XX_5GHz-1
SSID (5GHz-2):	ASUS_XX_5GHz-2

### การอัปเดตเฟิร์มแวร์ล่าสุด

เปิดโหมดช่วยเหลือ และรันยูทิลิตี้ การกู้คืนเฟิร์มแวร์ ดูส่วน 4.2 การกู้คืนเฟิร์มแวร์ เกี่ยวกับการใช้ยูทิลิตี้ การกู้คืนเฟิร์มแวร์

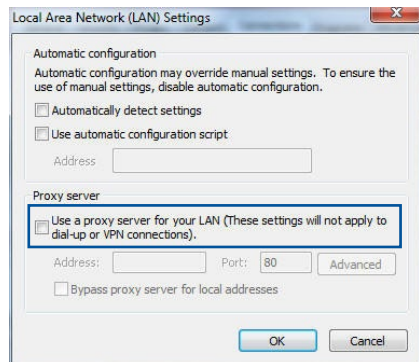
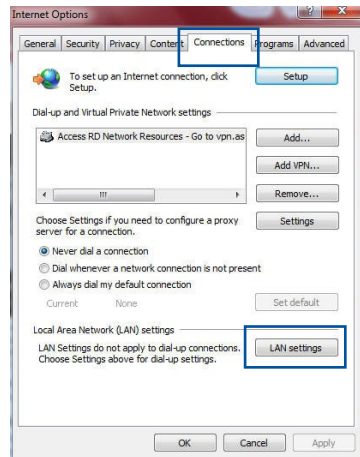
# ไม่สามารถเข้าถึงเว็บ GUI

ก่อนที่จะกำหนดค่าไวร์เลสเราเตอร์ของคุณ ให้ทำขั้นตอนตามที่อธิบายในส่วนนี้ สำหรับโพรเซสเซอร์คอมพิวเตอร์และเน็ตเวิร์กไคลเอ็นต์ของคุณ

## A. ปิดทำงานพร็อกซีเซิร์ฟเวอร์ ถ้าเปิดทำงานอยู่

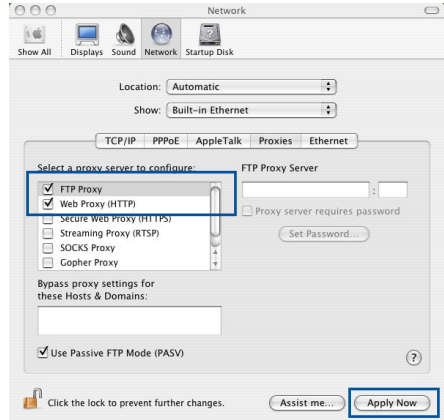
### Windows®

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

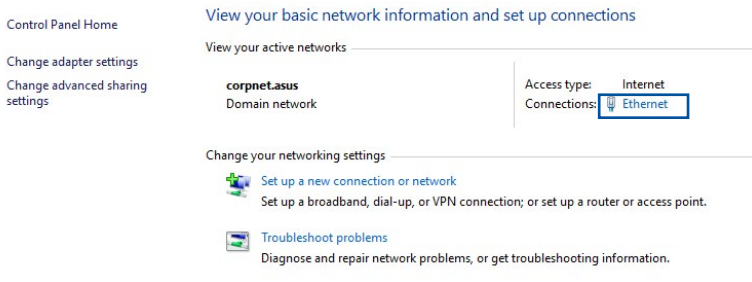


**หมายเหตุ:** คุณควรสมมติวิธีใช้ของเบราว์เซอร์ของคุณ สำหรับรายละเอียดเกี่ยวกับการปิดทำงานพร็อกซีเซิร์ฟเวอร์

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

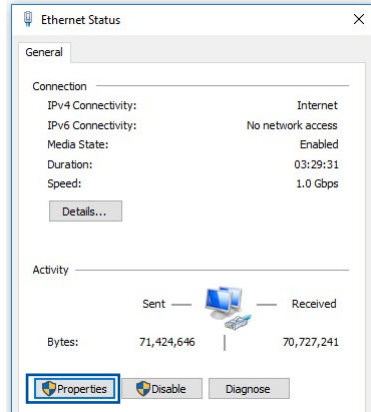
### Windows®

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

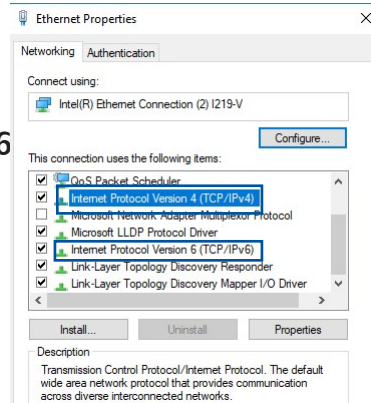




2. คลิกที่ **Properties** (คุณสมบัติ) เพื่อแสดง หน้าตาทางคุณสมบัติอีเทอร์เน็ต



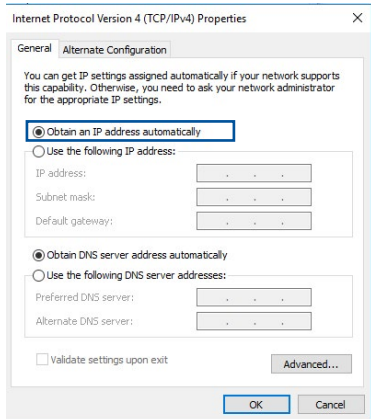
3. เลือก **Internet Protocol Version 4 (TCP/IPv4)** (อินเทอร์เน็ตโปรโตคอลเวอร์ชัน4 (TCP/IPv4)) หรือ **Internet Protocol Version 6 (TCP/IPv6)** (อินเทอร์เน็ตโปรโตคอลเวอร์ชัน6 (TCP/IPv6)), จากหน้าต่าง **Properties** (คุณสมบัติ)




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

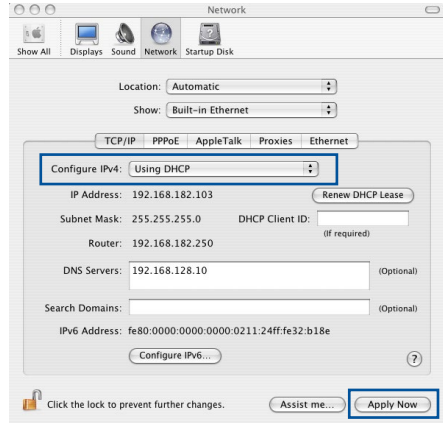
เพื่อรับการตั้งค่า IPv6 IP โดยอัตโนมัติ, ทำเครื่องหมายที่ **Obtain an IPv6 address automatically** (รับ IPv6 แอดเดรสโดยอัตโนมัติ)

5. คลิก **OK** (ตกลง) เมื่อทำเสร็จ



## MAC OS

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

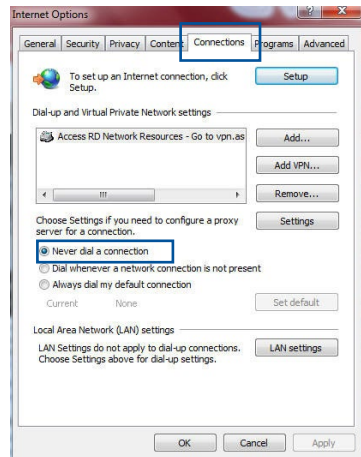


**หมายเหตุ:** คู่มือใช้ของระบบปฏิบัติการของคุณ และคุณสมบัติที่สนับสนุน สำหรับรายละเอียดเกี่ยวกับการกำหนดค่า TCP/IP ของคอมพิวเตอร์ของคุณ

## C. เปิดการทำงานเครือข่ายแบบโทรเข้า

### Windows®

1. คลิก **Start (เริ่ม) > Internet Explorer (อินเทอร์เน็ต เอ็กพลอเรอร์)** เพื่อเปิดเบราว์เซอร์
2. คลิก **Tools (เครื่องมือ) > Internet options (ตัวเลือกอินเทอร์เน็ต) > Connections (การเชื่อมต่อ)** (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  
ชั้นพื้นฐานเสมอ ซึ่งรวมถึงแต่ไม่จำกัดเฉพาะสิ่งต่อไปนี้



### คำเตือน!

- ต้องเสียบสายไฟเข้ากับเต้ารับที่มีสายดินที่เหมาะสม  
เชื่อมต่ออุปกรณ์เข้ากับเต้ารับที่ปลอดภัยซึ่งเข้าถึงได้ง่ายเท่านั้น
- 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 และอุโมงค์
- การรบกวนอุปกรณ์ทางการแพทย์ รักษาระยะห่างขั้นต่ำอย่างน้อย  
15 ซม. (6 นิ้ว) ระหว่างอุปกรณ์ทางการแพทย์ที่ฝังและผลิตภัณฑ์  
ASUS เพื่อลดความเสี่ยงของการรบกวน
- กรณการใช้ผลิตภัณฑ์ ASUS  
ในสถานะการรับสัญญาณที่ดีที่สุดเพื่อลดระดับรังสีให้เหลือน้อยที่สุด
- เก็บอุปกรณ์ให้ห่างจากสตรีมเมอร์และช่องท้องส่วนล่างของวัยรุ่น
- อยู่ใกล้ผลิตภัณฑ์นี้หากสามารถสังเกตเห็นข้อบกพร่องที่มองเห็น  
ได้ หรือเปียก เสียหาย หรือดัดแปลง ขอรับบริการเพื่อขอความ  
ช่วยเหลือ



## คำเตือน!

- อย่าวางบนพื้นผิวทำงานที่ไม่สม่ำเสมอ หรือไม่มั่นคง เข้า
- อย่าวางหรือทำสิ่งของของหล่นทับด้านบนของผลิตภัณฑ์  
หลีกเลี่ยงการทำให้ผลิตภัณฑ์ถูกกระแทกทางกล เช่น การบด  
การตัด การเจาะหรือการฉีกเป็นชิ้นเล็กชิ้นน้อย
- ห้ามแยกชิ้นส่วน เปิด อบรมโคโรเวฟ เผา ทาสี หรือผลักวัตถุ  
แปลกปลอมใดๆ เข้าไปในผลิตภัณฑ์นี้
- ดูแผ่นป้ายระบุกำลังไฟฟ้าใต้ผลิตภัณฑ์ของคุณ  
และตรวจดูใหม่ในใจว่าจะแต่บูเตอรเพาเวอร์ของคุณมีกำลังไฟฟ้า  
สอดคล้องกับระดับกำลังไฟฟ้านี้
- เก็บผลิตภัณฑ์ให้ห่างจากแหล่งไฟและความร้อน
- อย่าให้สัมผัสกับ หรือใช้ในบริเวณที่อยู่ใกล้ของเหลว ฝน  
หรือความชื้น อย่าใช้ผลิตภัณฑ์ในระหว่างพายุไฟฟ้า
- เชื่อมต่อวงจรเอาต์พุต PoE ของผลิตภัณฑ์นี้กับเครือข่าย  
PoE โดยเฉพาะ โดยไม่ต้องกำหนดเส้นทางไปยังสิ่งอำนวยความสะดวก  
ระดมภายนอก
- เพื่อป้องกันอันตรายจากไฟฟ้าช็อต ให้ถอดสายพาวเวอร์ออก  
จากเตาเสียบไฟฟ้า ก่อนที่จะเคลื่อนย้ายระบบ
- ใช้เฉพาะอุปกรณ์เสริมที่ได้รับการรับรองจากผู้ผลิตอุปกรณ์  
เท่านั้นจึงจะสามารถใช้งานร่วมกับรุ่นนี้ได้ การใช้อุปกรณ์เสริม  
ประเภทอื่นอาจทำให้การรับประกันเป็นโมฆะหรือฝ่าฝืน  
กฎข้อบังคับและกฎหมายท้องถิ่น และอาจก่อให้เกิดความเสี่ยง  
ด้านความปลอดภัย ติดต่อผู้ค้าปลีกในพื้นที่ของคุณเพื่อ  
สอบถามอุปกรณ์เสริมที่ได้รับอนุญาต
- การใช้ผลิตภัณฑ์นี้ในลักษณะที่ไม่แนะนำในคำแนะนำที่ระบุไว้  
อาจส่งผลให้เกิดความเสี่ยงต่อการเกิดเพลิงไหม้หรือการบาดเจ็บ  
ส่วนบุคคล

## บริการและการสนับสนุน

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

