

# Petunjuk Penggunaan

## RT-AX53U

**AX-1800 Dual Band WiFi 6 Nirkabel  
Router**



**ASUS**  
IN SEARCH OF INCREDIBLE

ID20292

Edisi Revisi versi 2

Juli 2022

**Hak cipta © 2022 ASUSTek Computers, Inc. Semua Hak Dilindungi Undang-Undang**

Dilarang memproduksi ulang, mengirim, mentranskripsi bagian dari panduan ini, yang tersimpan dalam sistem, termasuk produk dan perangkat lunak yang diuraikan di dalamnya, atau menerjemahkannya ke dalam bahasa apa pun dalam bentuk atau cara apa pun, kecuali sebagai dokumen yang disimpan oleh pembeli untuk keperluan cadangan, tanpa izin tertulis dari ASUSTek Computers, Inc. ("ASUS").

Jaminan Produk atau pelayanan tidak akan di perpanjang jika; (1) produk tersebut diperbaiki, dimodifikasi atau diubah, kecuali seperti perbaikan, modifikasi perubahan tersebut diizinkan secara tertulis oleh ASUS; atau (2) nomor seri produk tersebut rusak atau hilang.

ASUS MENYEDIKAN PANDUAN INI "SEBAGAIMANA ADANYA" TANPA ADA JAMINAN APAPUN, BAIK TERSURAT MAUPUN TERSIRAT, TERMASUK NAMUN TIDAK TERBATAS PADA JAMINAN TERSIRAT ATAU KEADAAN YANG DAPAT DIPERJUALBELIKAN ATAU KESESUAIAN UNTUK TUJUAN TERTENTU. DALAM KONDISI APAPUN ASUS, DIREKSINYA, PEJABAT, KARYAWAN ATAU AGEN-AGENNANYA TIDAK BERTANGGUNG JAWAB ATAS KERUGIAN YANG TIDAK LANGSUNG, KHUSUS, KEBETULAN, ATAU SEBAGAI AKIBAT DARI TERJADINYA SESUATU HAL (TERMASUK KERUGIAN ATAS HILANGNYA KEUNTUNGAN, HILANGNYA BISNIS, HILANGNYA PENGGUNAAN ATAU DATA, GANGGUAN BISNIS DAN SEMACAM ITU) MESKIPUN ASUS TELAH DIBERITAHU TENTANG KEMUNGKINAN KERUSAKAN YANG TIMBUL AKIBAT KECACATAN ATAU KESALAHAN DALAM PANDUAN ATAU PRODUK.

SPESIFIKASI DAN INFORMASI YANG TERKANDUNG DI DALAM PANDUAN INI DISEDIAKAN SEBAGAI INFORMASI SAJA, DAN DAPAT BERUBAH SETIAP SAAT TANPA PEMBERITAHUAN, DAN TIDAK BISA DITAFSIRKAN SEBAGAI KOMITMEN OLEH ASUS. ASUS TIDAK BERTANGGUNG JAWAB ATAU BERKEWAJIBAN ATAS KESALAHAN ATAU KETIDAKTEPATAN YANG MUNGKIN TERJADI DI DALAM PANDUAN INI, TERMASUK PRODUK-PRODUK DAN PERANGKAT LUNAK YANG DIJELASKAN DI DALAMNYA.

Produk dan nama perusahaan yang muncul pada panduan ini mungkin atau bukan merupakan merek dagang terdaftar atau hak cipta dari masing-masing perusahaan, dan digunakan hanya untuk identifikasi atau penjelasan dan manfaat bagi pemilikinya, tanpa ada maksud untuk melanggar.

# Daftar Isi

## 1 Mengenal router nirkabel

1.1	Selamat datang!.....	6
1.2	Isi kemasan .....	6
1.3	Router nirkabel .....	7
1.4	Menentukan posisi router.....	9
1.5	Yang diperlukan.....	10
1.6	Mengkonfigurasi router nirkabel .....	11
1.6.1	Sambungan berkabel .....	12
1.6.2	Sambungan nirkabel .....	13

## 2 Persiapan

2.1	Log in ke GUI Web.....	14
2.2	QIS (Konfigurasi Internet Cepat) dengan deteksi otomatis .....	15
2.3	Menyambung ke jaringan nirkabel .....	19

## 3 Mengkonfigurasi pengaturan General (Umum)

3.1	Menggunakan peta jaringan .....	20
3.1.1	Mengkonfigurasi pengaturan keamanan nirkabel...21	
3.1.2	Mengelola klien jaringan.....	22
3.1.3	Memantau perangkat USB.....	23
3.2	Membuat Guest Network (Jaringan Tamu) .....	26
3.3	AiProtection .....	28
3.3.1	Perlindungan Jaringan.....	29
3.3.2	Mengkonfigurasi Kontrol Orang Tua.....	32
3.4	Menggunakan QoS (Kualitas Layanan) .....	34
3.4.1	Mengelola Bandwidth QoS (Kualitas Layanan) .....	34

# Daftar Isi

3.5	Menggunakan Aplikasi USB.....	37
3.5.1	Menggunakan AiDisk.....	37
3.5.2	Menggunakan Pusat Server.....	39
3.5.3	3G/4G.....	44
<b>4</b>	<b>Mengkonfigurasi pengaturan lanjutan</b>	
4.1	Nirkabel.....	46
4.1.1	Umum.....	46
4.1.2	WPS.....	49
4.1.3	WDS.....	51
4.1.4	Filter MAC Nirkabel.....	53
4.1.5	Pengaturan RADIUS.....	54
4.1.6	Profesional.....	55
4.2	LAN.....	58
4.2.1	IP LAN.....	58
4.2.2	Server DHCP.....	59
4.2.3	Rute.....	61
4.2.4	IPTV.....	62
4.3	WAN.....	63
4.3.1	Sambungan Internet.....	63
4.3.2	Pemicu Port.....	66
4.3.3	Server Virtual/Penerusan Port.....	68
4.3.4	DMZ.....	71
4.3.5	DDNS.....	72
4.3.6	Passthrough NAT.....	73
4.4	IPv6.....	74
4.5	Firewall.....	75
4.5.1	Umum.....	75
4.5.2	Filter URL.....	75
4.5.3	Filter kata kunci.....	76
4.5.4	Filter Layanan Jaringan.....	77

## Daftar Isi

4.6	Administrasi .....	79
	4.6.1 Mode Pengoperasian.....	79
	4.6.2 Sistem.....	80
	4.6.3 Upgrade Firmware .....	81
	4.6.4 Mengembalikan/Menyimpan/Meng-upload Pengaturan .....	81
4.7	Log Sistem .....	82
<b>5</b>	<b>Utilitas</b>	
5.1	Pencarian Perangkat .....	83
5.2	Pengembalian Firmware.....	84
<b>6</b>	<b>Mengatasi Masalah</b>	
6.1	Mengatasi Masalah Mendasar .....	86
6.2	Tanya Jawab .....	89
	<b>Lampiran</b>	
	Layanan dan Dukungan.....	106

# 1 Mengenal router nirkabel

## 1.1 Selamat datang!

Terima kasih atas pembelian Router Nirkabel ASUS RT-AX53U ini! RT-AX53U canggih dan trendi ini dilengkapi dual band 2,4 GHz dan 5 GHz untuk menjalankan streaming HD nirkabel yang tak tertandingi secara bersamaan serta Teknologi Jaringan Ramah Lingkungan ASUS yang menghadirkan solusi hemat daya hingga 70%.

## 1.2 Isi kemasan

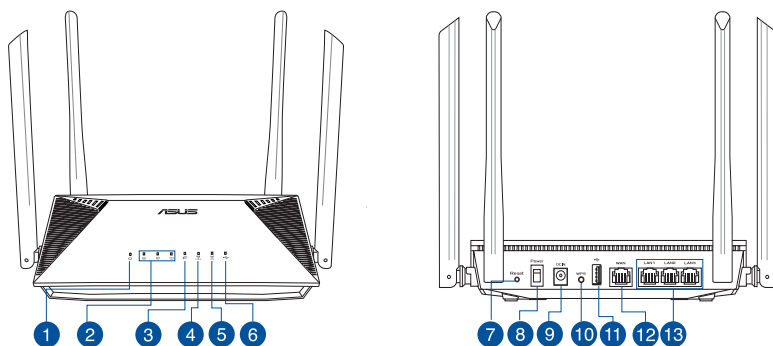
- |  |  |
|--|--|
| <input checked="" type="checkbox"/> Router Nirkabel RT-AX53U | <input checked="" type="checkbox"/> Kabel jaringan (RJ-45) |
| <input checked="" type="checkbox"/> Adaptor daya             | <input checked="" type="checkbox"/> Panduan Ringkas        |

---

### CATATAN:

- Jika salah satu komponen rusak atau tidak ada, hubungi peritel atau ASUS untuk pertanyaan dan dukungan teknis. Lihat daftar Hotline Dukungan ASUS di bagian belakang panduan pengguna ini.
  - Simpan material kemasan awal karena Anda mungkin akan memerlukan layanan jaminan di masa mendatang seperti perbaikan atau penggantian.
-

## 1.3 Router nirkabel



1

### LED Daya

**Mati:** Tidak ada daya.

**Menyala:** Perangkat siap digunakan.

**Berkedip lambat:** Mode Rescue (Penyelamatan).

2

### LED LAN 1~3

**Mati:** Tidak ada aktivitas data atau sambungan fisik.

**Menyala:** Terdapat sambungan fisik ke LAN (local area network).

3

### LED WAN (Internet)

**Merah:** Tidak ada IP atau sambungan fisik.

**Menyala:** Terdapat sambungan fisik ke WAN (wide area network).

4

### LED 2,4 GHz

**Mati:** Tidak ada sinyal 2,4 GHz.

**Menyala:** Nirkabel 2,4 GHz siap digunakan.

**Berkedip:** Mengirim atau menerima data melalui sambungan nirkabel.

5

### LED 5GHz

**Mati:** Tidak ada sinyal 5 GHz.

**Menyala:** Nirkabel 5 GHz siap digunakan.

**Berkedip:** Mengirim atau menerima data melalui sambungan nirkabel.

6

### LED USB 2.0

**Mati:** Tidak ada aktivitas data atau sambungan fisik.

**Menyala:** Dilengkapi koneksi fisik ke perangkat USB.

7

### Tombol atur ulang

Tombol ini akan mengatur ulang atau mengembalikan sistem ke pengaturan default pabrik.

8

### Tombol daya

Alihkan untuk mengaktifkan atau menonaktifkan sistem.

- 
- 9 Port daya (DCIn)**  
Pasang adaptor AC yang tersedia ke port ini, lalu sambungkan router ke catu daya.

---

  - 10 Tombol WPS**  
Untuk mengaktifkan Wizard WPS, tekan lama tombol ini.

---

  - 11 Port USB 2.0**  
Pasang perangkat USB 2.0 yang kompatibel, misalnya hard disk USB atau flash drive USB ke port.

---

  - 12 Port WAN (Internet)**  
Untuk membuat sambungan WAN, sambungkan kabel jaringan ke port ini.

---

  - 13 Port LAN 1 ~ 3**  
Untuk membuat sambungan LAN, sambungkan kabel jaringan ke port ini.
- 

**CATATAN:**

- Gunakan hanya adapter yang disertakan dalam kemasan. Penggunaan adapter lain dapat merusak perangkat.
- **Kondisi sekitar:**

<b>Adaptor daya DC</b>	Output DC: +12 V dengan arus maks. 1.5 A		
<b>Suhu Pengoperasian</b>	0~40°C	Penyimpanan	0~70°C
<b>Kelembaban Pengoperasian</b>	50~90%	Penyimpanan	20~90%

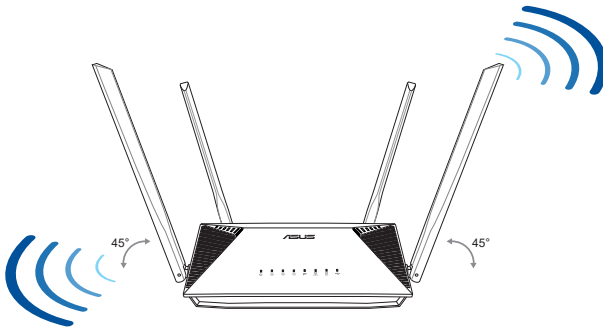
---



## 1.4 Menentukan posisi router

Untuk transmisi sinyal nirkabel terbaik antara router nirkabel dan perangkat jaringan yang tersambung, pastikan Anda:

- Menempatkan router LTE nirkabel di dekat jendela untuk mendapatkan performa upstream nirkabel maksimum berkualitas terbaik dengan stasiun basis LTE.
- Tidak menghalangi perangkat dengan benda logam dan menjauhkannya dari sinar matahari langsung.
- Agar sinyal tidak hilang, jauhkan perangkat ini dari perangkat Wi-Fi 802.11g atau hanya 20 MHz, periferal komputer 2,4 GHz, perangkat Bluetooth, telepon nirkabel, trafo, mesin berat, lampu fluoresen, oven microwave, lemari es, dan peralatan industri lainnya.
- Selalu memperbarui ke firmware terkini. Untuk mendapatkan pembaruan firmware terkini, kunjungi situs web ASUS di <http://www.asus.com>.



## 1.5 Yang diperlukan

Untuk mengkonfigurasi jaringan, Anda memerlukan satu komputer yang memenuhi persyaratan sistem berikut ini:

- Port Ethernet RJ-45 (LAN) (10Base-T/100Base-TX/1000Base-TX)
- Kapabilitas nirkabel IEEE 802.11a/b/g/n/ac/ax
- Layanan TCP/IP terinstal
- Browser Web seperti Microsoft Internet Explorer, Firefox, Apple Safari, atau Google Chrome

---

### CATATAN:

- Jika komputer tidak memiliki kapabilitas nirkabel internal, instal adapter WLAN IEEE 802.11a/b/g/n/ac/ax di komputer untuk menyambung ke jaringan.
  - Dengan teknologi dual band, router nirkabel mendukung sinyal nirkabel 2.4GHz dan 5GHz secara bersamaan. Teknologi ini memungkinkan Anda melakukan aktivitas yang berhubungan dengan Internet seperti berselancar di Internet atau membaca/menulis pesan email menggunakan pita 2.4GHz sambil melakukan streaming file audio/video definisi tinggi, misalnya film maupun musik menggunakan pita 5GHz secara bersamaan.
  - Sebagian perangkat IEEE 802.11n yang akan disambungkan ke jaringan mungkin mendukung atau tidak mendukung pita 5GHz. Untuk informasi rinci, lihat panduan perangkat.
  - Kabel RJ-45 Ethernet yang digunakan untuk menyambungkan perangkat jaringan tidak boleh lebih dari 100 meter.
-

## 1.6 Mengkonfigurasi router nirkabel

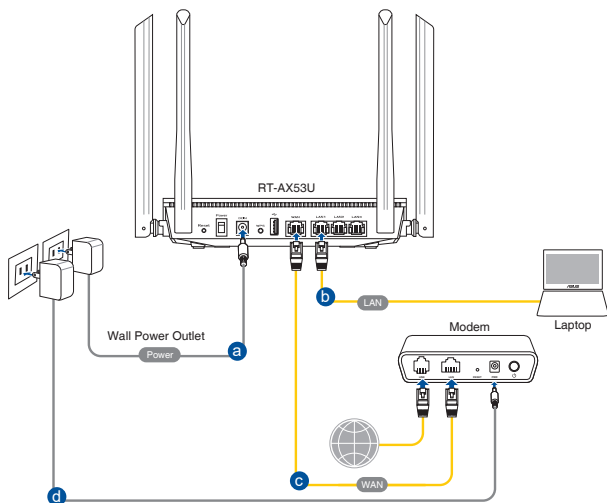
---

### **PENTING!**

- Gunakan sambungan berkabel saat mengkonfigurasi router nirkabel untuk menghindari kemungkinan masalah konfigurasi nirkabel.
  - Sebelum mengkonfigurasi router nirkabel ASUS, lakukan yang berikut:
    - Jika Anda mengganti router yang ada, putuskan sambungannya dari jaringan.
    - Lepas kabel dari modem yang ada. Jika modem memiliki baterai cadangan, keluarkan juga.
    - Jalankan boot ulang komputer (disarankan).
-

## 1.6.1 Sambungan berkabel

**CATATAN:** Router nirkabel Anda mendukung kabel pemasangan lurus dan pemasangan menyalang saat mengkonfigurasi sambungan berkabel.



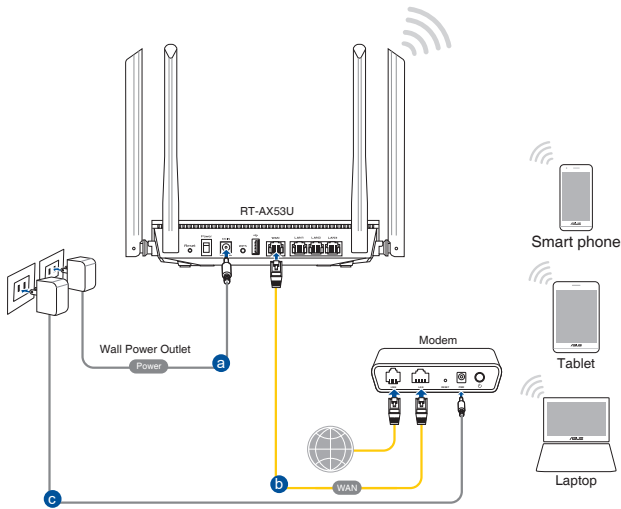
### Untuk mengkonfigurasi jaringan menggunakan sambungan berkabel:

1. Masukkan adaptor AC router nirkabel ke port DCIn, lalu pasang ke catu daya.
2. Menggunakan kabel jaringan yang disertakan, sambungkan komputer ke port LAN router nirkabel.

**PENTING!** Pastikan LED LAN berkedip.

3. Menggunakan kabel jaringan lain, sambungkan modem ke port WAN router nirkabel.
4. Masukkan adaptor AC modem ke port DCIn, lalu pasang ke catu daya.

## 1.6.2 Sambungan nirkabel



### Untuk mengkonfigurasi router nirkabel melalui sambungan nirkabel:

1. Masukkan adaptor AC router nirkabel ke port DCIn, lalu pasang ke catu daya.
2. Menggunakan kabel jaringan yang disertakan, sambungkan modem ke port WAN router nirkabel.
3. Masukkan adaptor AC modem ke port DCIn, lalu pasang ke catu daya.
4. Instal adapter WLAN IEEE 802.11a/b/g/n/ac/ax di komputer.

### CATATAN:

- Untuk rincian tentang cara menyambung ke jaringan nirkabel, lihat panduan pengguna adapter WLAN.
- Untuk mengkonfigurasi pengaturan keamanan jaringan, lihat bagian **3.1.1 Mengkonfigurasi keamanan nirkabel.**

## 2 Persiapan

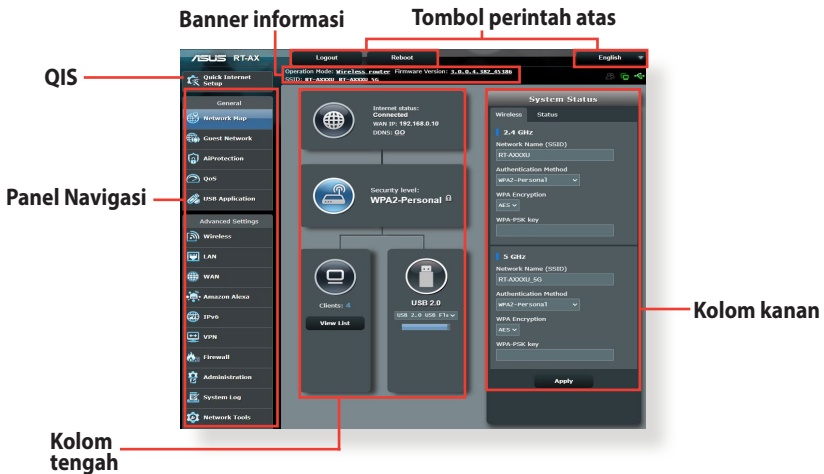
### 2.1 Log in ke GUI Web

Router Nirkabel ASUS menggunakan antarmuka pengguna berbasis Web yang memungkinkan Anda mengkonfigurasi router menggunakan browser Web apapun seperti Internet Explorer, Mozilla Firefox, Apple Safari, atau Google Chrome.

**CATATAN:** Fitur dapat bervariasi untuk setiap versi firmware yang berbeda.

#### Untuk log in ke GUI Web:

1. Buka browser Web, lalu masukkan alamat IP default router nirkabel secara manual: **<http://router.asus.com>**.
2. Pada halaman login, masukkan nama pengguna (**admin**) dan sandi (**admin**) default.
3. GUI router nirkabel memberikan akses ke berbagai pengaturan konfigurasi.



**CATATAN:** Jika log in ke GUI Web untuk pertama kalinya, Anda akan diarahkan ke halaman QIS (Konfigurasi Internet Cepat) secara otomatis.

## 2.2 QIS (Konfigurasi Internet Cepat) dengan deteksi otomatis

Fitur QIS (Konfigurasi Internet Cepat) memandu Anda untuk mengkonfigurasi sambungan Internet dengan cepat.

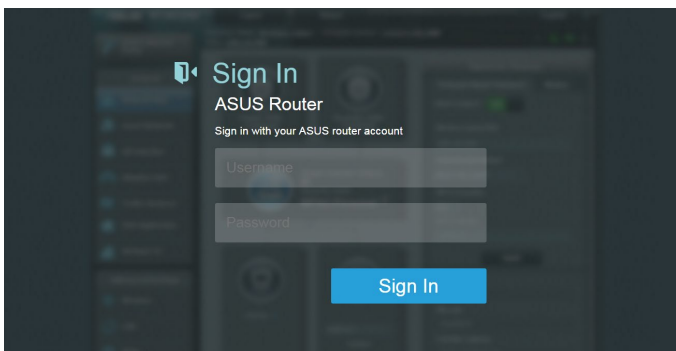
---

**CATATAN:** Saat mengatur sambungan Internet untuk pertama kali, tekan tombol Reset (Atur Ulang) pada router nirkabel untuk mengatur ulang pengaturan default pabrik.

---

### Untuk menggunakan QIS dengan deteksi otomatis:

1. Log in ke GUI Web. Konfigurasi Internet Cepat akan aktif secara otomatis.



---

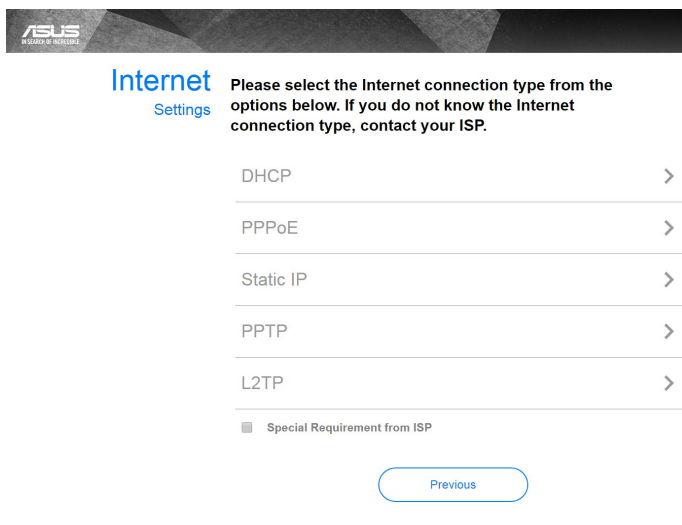
### CATATAN:

- Secara default, nama pengguna dan sandi login untuk GUI Web router nirkabel adalah **admin**. Untuk informasi rinci tentang cara mengubah nama pengguna dan sandi login router nirkabel, lihat bagian **4.6.2 Sistem**.
  - Nama pengguna dan sandi login router nirkabel berbeda dengan nama jaringan (SSID) 2.4GHz/5GHz dan kode keamanan. Nama pengguna dan sandi login router nirkabel memungkinkan Anda login ke Web GUI router nirkabel untuk mengkonfigurasi pengaturan router nirkabel. Nama jaringan (SSID) 2.4GHz/5GHz dan kunci keamanan memungkinkan perangkat Wi-Fi log in serta tersambung ke jaringan 2.4GHz/5GHz.
-

2. Setelah port WAN tersambung, fitur Konfigurasi Ringkas Internet (QIS) pada router nirkabel akan secara otomatis terdeteksi jika jenis sambungan ISP adalah **Dynamic IP (IP Dinamis)**, **PPPoE**, **PPTP**, **L2TP**, dan **Static IP (IP Statis)**. Masukkan informasi yang diperlukan untuk jenis sambungan ISP.

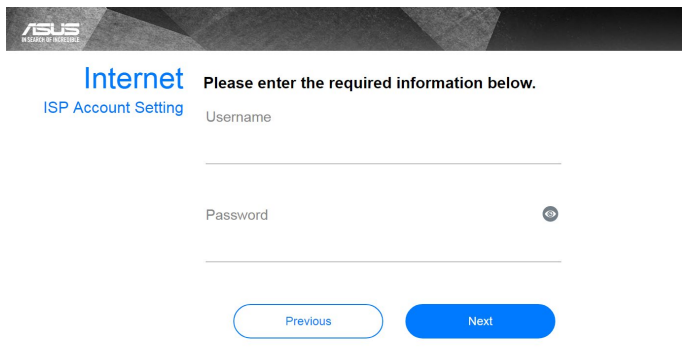
**PENTING!** Dapatkan informasi penting dari ISP tentang jenis sambungan Internet.

untuk IP Otomatis (DHCP)



The screenshot shows the 'Internet Settings' page on an ASUS router. The page title is 'Internet Settings'. Below the title, there is a message: 'Please select the Internet connection type from the options below. If you do not know the Internet connection type, contact your ISP.' There are five radio button options: 'DHCP', 'PPPoE', 'Static IP', 'PPTP', and 'L2TP'. Each option has a right-pointing chevron icon. Below these options is a checkbox labeled 'Special Requirement from ISP'. At the bottom of the page is a 'Previous' button.

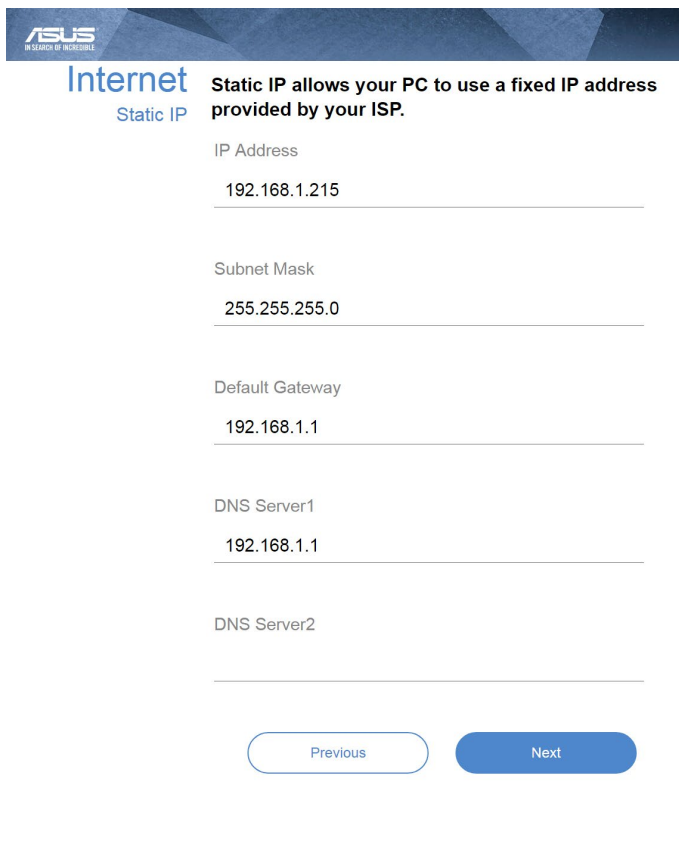
untuk PPPoE, PPTP, dan L2TP



The screenshot shows the 'Internet Account Setting' page on an ASUS router. The page title is 'Internet Account Setting'. Below the title, there is a message: 'Please enter the required information below.' There are two input fields: 'Username' and 'Password'. The 'Password' field has a small eye icon to its right. At the bottom of the page are two buttons: 'Previous' and 'Next'.



## untuk IP Statis



**ASUS**  
IN SEARCH OF INCREDIBLE

### Internet

Static IP

**Static IP allows your PC to use a fixed IP address provided by your ISP.**

IP Address  
192.168.1.215

Subnet Mask  
255.255.255.0

Default Gateway  
192.168.1.1

DNS Server1  
192.168.1.1

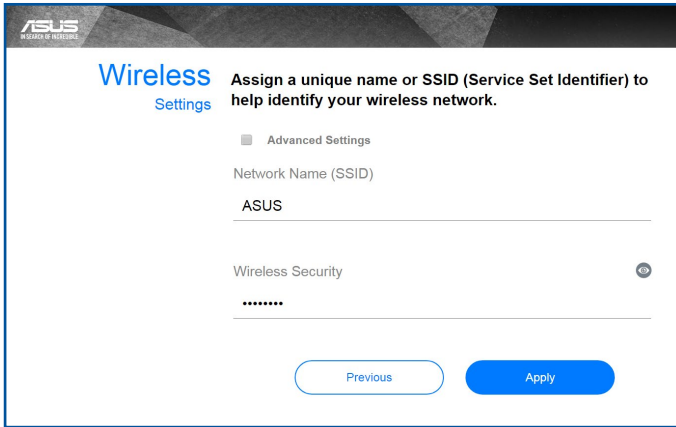
DNS Server2

Previous Next

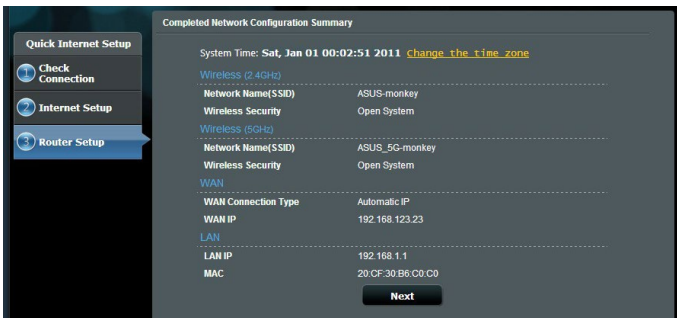
### CATATAN:

- Deteksi otomatis jenis sambungan ISP berjalan saat Anda mengkonfigurasi router nirkabel untuk pertama kalinya atau saat router nirkabel diatur ulang ke pengaturan default.
- Jika QIS gagal mendeteksi jenis sambungan Internet, klik **Skip to manual setting (Lompat ke pengaturan manual)**, lalu konfigurasi pengaturan sambungan secara manual.

3. Tetapkan nama jaringan (SSID) dan kode keamanan untuk sambungan nirkabel 2,4 GHz dan 5 GHz. Setelah selesai, klik **Apply (Terapkan)**.



4. Pengaturan Internet dan nirkabel akan ditampilkan. Untuk menyelesaikan proses QIS, klik **Next (Berikutnya)**.





5. Baca Tutorial Sambungan Jaringan Nirkabel. Klik **Finish (Selesai)**.

## 2.3 Menyambung ke jaringan nirkabel

Setelah mengkonfigurasi router nirkabel melalui QIS, Anda dapat menyambungkan komputer atau perangkat pintar lainnya ke jaringan nirkabel Anda.

### Untuk menyambung ke jaringan:

1. Di komputer, klik ikon jaringan di bidang pemberitahuan untuk  menampilkan jaringan nirkabel yang tersedia.
2. Pilih jaringan nirkabel yang diinginkan agar dapat tersambung, lalu klik **Connect (Sambungkan)**.
3. Anda mungkin harus memasukkan kunci keamanan jaringan untuk jaringan nirkabel aman. Setelah itu, klik **OK**.
4. Tunggu hingga komputer berhasil tersambung ke jaringan nirkabel. Status sambungan akan ditampilkan dan ikon jaringan menampilkan status tersambung .

---

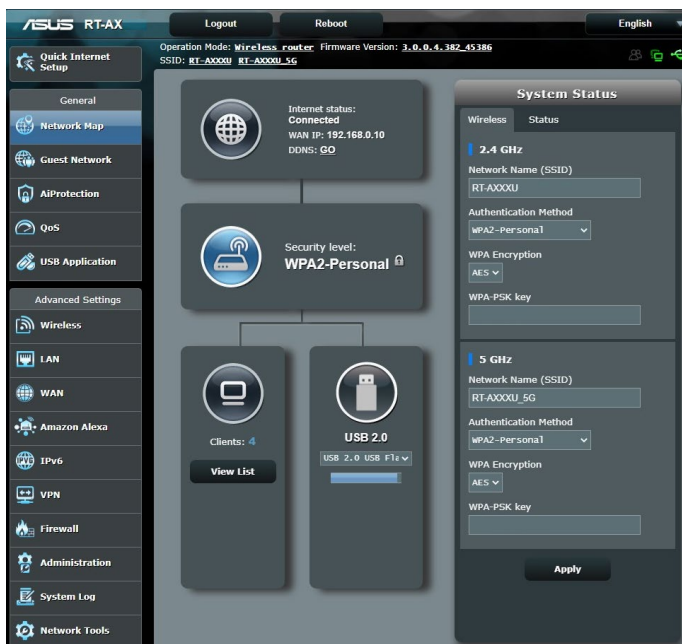
### CATATAN:

- Untuk informasi lebih rinci tentang mengkonfigurasi pengaturan jaringan nirkabel, lihat bab berikutnya.
  - Untuk informasi lebih rinci tentang cara menyambungkannya ke jaringan nirkabel, lihat panduan pengguna perangkat.
-

# 3 Mengkonfigurasi pengaturan General (Umum)

## 3.1 Menggunakan peta jaringan

Network Map (Peta Jaringan) memungkinkan Anda mengkonfigurasi pengaturan keamanan jaringan, mengelola klien jaringan, dan memantau perangkat USB.



### 3.1.1 Mengkonfigurasi pengaturan keamanan nirkabel

Untuk melindungi jaringan nirkabel dari akses tidak sah, Anda harus mengkonfigurasi pengaturan keamanannya.

#### Untuk mengkonfigurasi pengaturan keamanan nirkabel:

1. Dari panel navigasi, buka **General (Umum) > Network Map (Peta Jaringan)**.
2. Di layar Network Map (Peta Jaringan), klik ikon **Status System**. Anda dapat mengkonfigurasi pengaturan keamanan nirkabel seperti nama nirkabel (SSID), tingkat keamanan, dan pengaturan enkripsi.

**CATATAN:** Anda dapat mengkonfigurasi pengaturan keamanan nirkabel yang berbeda untuk pita 2.4GHz dan 5GHz.

#### Pengaturan keamanan 2,4 GHz    Pengaturan keamanan 5 GHz

**System Status**

2.4GHz    5GHz    Status

Network Name (SSID)  
ASUS\_2G

Authentication Method  
WPA2-Personal

WPA Encryption  
AES

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

Apply

LAN IP  
192.168.50.1

PIN code  
12345670

LAN MAC address  
00:00:00:00:00:00

Wireless 2.4GHz MAC address  
00:00:00:00:00:00

**System Status**

2.4GHz    5GHz    Status

Network Name (SSID)  
ASUS\_5G

Authentication Method  
WPA2-Personal

WPA Encryption  
AES

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

Apply

LAN IP  
192.168.50.1

PIN code  
12345670

LAN MAC address  
00:00:00:00:00:00

Wireless 5GHz MAC address  
00:00:00:00:00:00

3. Di kolom **Wireless Name (SSID) (Nama nirkabel (SSID))**, masukkan nama unik untuk jaringan nirkabel.

4. Dari daftar drop down **Enkripsi WEP**, pilih metode enkripsi untuk jaringan nirkabel.

**PENTING!** Standar IEEE 802.11n/ac/ax melarang penggunaan High Throughput dengan WEP atau WPA-TKIP sebagai sandi unicast. Jika Anda menggunakan metode enkripsi ini, maka kecepatan data akan turun ke sambungan IEEE 802.11g 54Mbps.

5. Masukkan kode akses keamanan.
6. Klik **Apply (Terapkan)**.

### 3.1.2 Mengelola klien jaringan

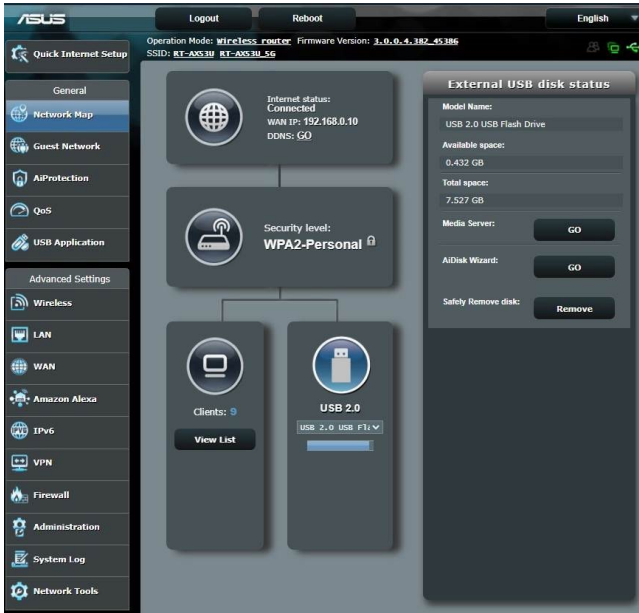


#### Untuk mengelola klien jaringan:

1. Dari panel navigasi, buka tab **General (Umum) > Network Map (Peta Jaringan)**.
2. Di layar Network Map (Peta Jaringan), pilih ikon **Client status (Status klien)** untuk menampilkan informasi klien jaringan.
3. Untuk memblokir akses klien ke jaringan, pilih klien, lalu klik ikon **blokir**.

### 3.1.3 Memantau perangkat USB

Router nirkabel ASUS menyediakan satu port USB untuk menyambungkan perangkat USB atau printer USB agar Anda dapat berbagi file dan printer dengan klien di jaringan.



---

**CATATAN:** Untuk menggunakan fitur ini, Anda harus menyambungkan perangkat penyimpanan USB, misalnya hard disk USB atau flash drive USB ke port USB 3.0/2.0 di panel belakang router nirkabel. Pastikan perangkat penyimpanan USB telah diformat dan dipartisi dengan benar. Lihat Daftar Dukungan Plug-n-Share Disk di <http://event.asus.com/networks/disksupport>.

---

---

**PENTING!** Anda harus terlebih dulu membuat akun bersama sekaligus izin atau hak aksesnya agar klien jaringan lain dapat mengakses perangkat USB melalui situs FTP/utilitas klien FTP server pihak ketiga, Pusat Server, Samba, maupun AiCloud. Untuk informasi lebih rinci, lihat bagian **3.5 Menggunakan Aplikasi USB** dalam panduan pengguna ini.

---

### **Untuk memantau perangkat USB:**

1. Dari panel navigasi, buka tab **General (Umum) > Network Map (Peta Jaringan)**.
2. Di layar Network Map (Peta Jaringan), pilih ikon **Status Disk USB** untuk menampilkan informasi perangkat USB.
3. Pada kolom AiDisk Wizard (Wizard AiDisk), klik **GO (Mulai)** agar dapat mengkonfigurasi server FTP untuk berbagi file Internet.

---

### **CATATAN:**


- Untuk informasi lebih rinci, lihat bagian **3.5.2 Menggunakan Pusat Server** dalam panduan pengguna ini
  - Router nirkabel berfungsi dengan sebagian besar HDD/flash disk USB (kapasitas hingga 2 TB) dan mendukung akses baca-tulis untuk FAT16, FAT32, EXT2, EXT3, serta NTFS.
-

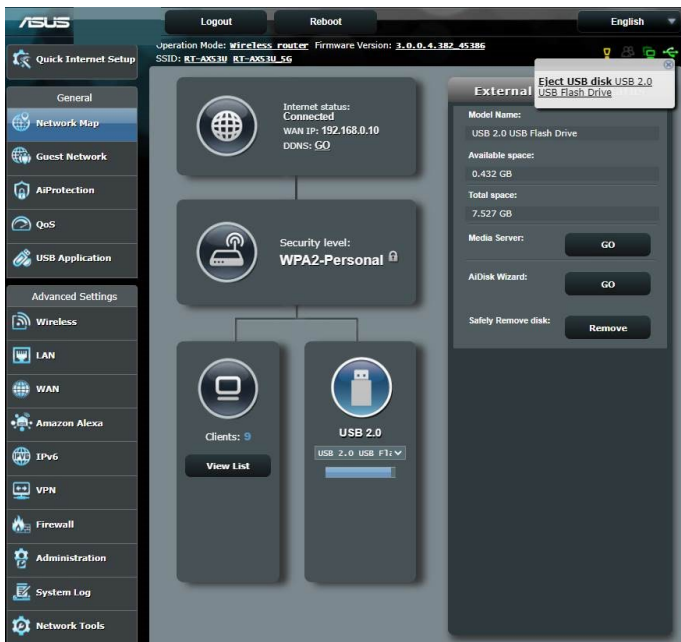


## Melepas disk USB secara aman

**PENTING!** Melepas disk USB secara salah dapat mengakibatkan data rusak.

Untuk melepas disk USB secara aman:

1. Dari panel navigasi, buka tab **General (Umum)** > **Network Map (Peta Jaringan)**.
2. Di sudut kanan atas, klik  > **Eject USB disk (Keluarkan disk USB)**. Bila disk USB berhasil dikeluarkan, status USB akan menampilkan **Unmounted (Dilepas)**.



## 3.2 Membuat Guest Network (Jaringan Tamu)

Guest Network (Jaringan Tamu) menyediakan konektivitas Internet melalui akses ke SSID atau jaringan terpisah tanpa memberikan akses ke jaringan pribadi Anda kepada pengunjung sementara.

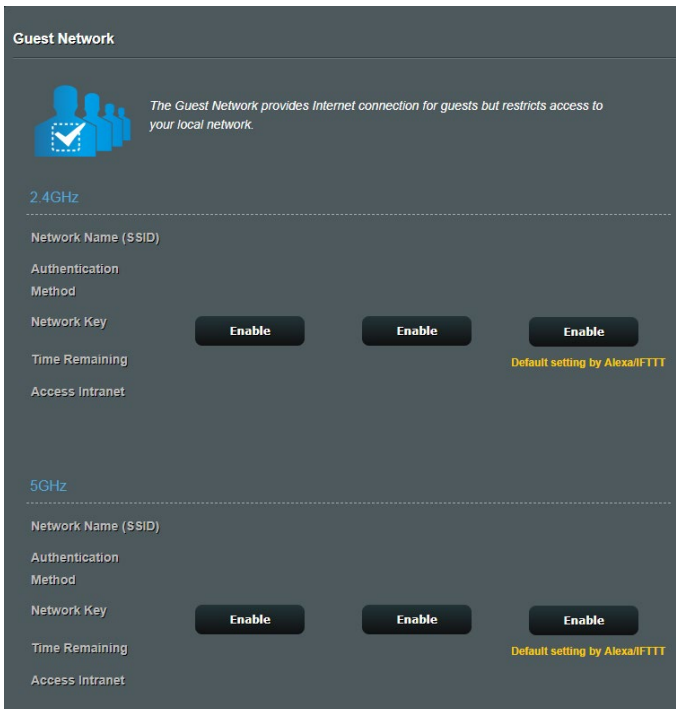
---

**CATATAN:** RT-AX53U mendukung hingga enam SSID (tiga SSID 2.4 GHz dan tiga SSID 5 GHz).

---

### Untuk membuat jaringan tamu:

1. Dari panel navigasi, buka **General (Umum) > Guest Network (Jaringan Tamu)**.
2. Pada layar Guest Network (Jaringan Tamu), pilih pita frekuensi 2.4 Ghz atau 5 Ghz untuk jaringan tamu yang akan dibuat.
3. Klik **Enable (Aktifkan)**.



4. Untuk mengkonfigurasi pilihan tambahan, klik **Modify (Modifikasikan)**.

The screenshot displays the 'Guest Network' configuration page. At the top, there is a header 'Guest Network' and a blue icon of people with a checkmark. Below the icon is a descriptive text: 'The Guest Network provides Internet connection for guests but restricts access to your local network.' The interface is divided into two sections: '2.4GHz' and '5GHz'. Each section contains a table of settings and two 'Enable' buttons. The '2.4GHz' section has settings: Network Name (SSID) 'ASUS\_2G\_Guest', Authentication Method 'Open System', Network Key 'None', Time Remaining 'Unlimited access', and Access Intranet 'off'. The '5GHz' section has settings: Network Name (SSID) 'ASUS\_5G\_Guest', Authentication Method 'Open System', Network Key 'None', Time Remaining 'Unlimited access', and Access Intranet 'off'. A 'Remove' button is located below each table. A yellow note at the bottom right of each section reads 'Default setting by Alexa/IFTTT'.

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

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

5. Klik **Yes (Ya)** pada layar **Enable Guest Network (Aktifkan Jaringan Tamu)**.
6. Tetapkan nama nirkabel untuk jaringan sementara pada bidang **Network Name (SSID) [Nama Jaringan (SSID)]**.
7. Pilih **Authentication Method (Metode Otentikasi)**.
8. Pilih metode **Encryption (Enkripsi)**.
9. Tentukan **Access time (Waktu akses)** atau pilih **Limitless (Tanpa Batas)**.
10. Pilih **Disable (Nonaktifkan)** atau **Enable (Aktifkan)** pada item **Access Intranet (Intranet Akses)**.
11. Setelah selesai, klik **Apply (Terapkan)**.

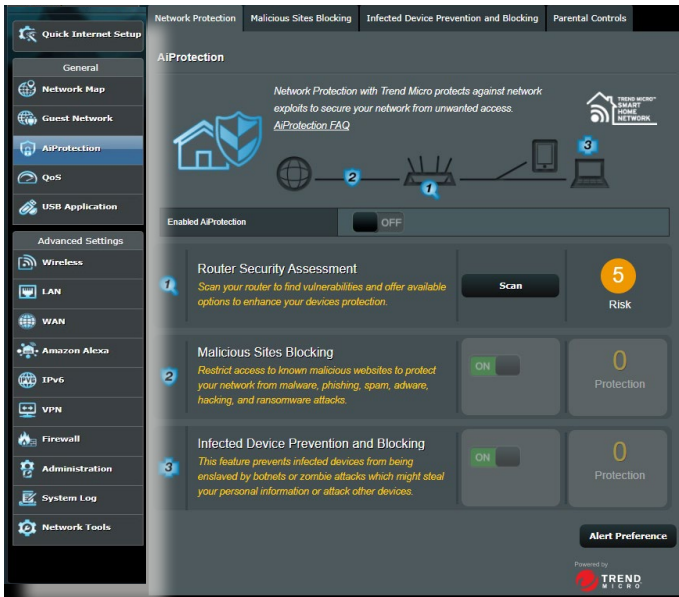
### 3.3 AiProtection

AiProtection melakukan pemantauan real-time yang dapat mendeteksi malware, spyware, dan akses yang tidak diinginkan. Selain itu, fitur ini juga menyaring situs web dan aplikasi yang tidak diinginkan serta memungkinkan penjadwalan akses perangkat ke Internet.



### 3.3.1 Perlindungan Jaringan

Perlindungan Jaringan mencegah eksploitasi jaringan dan mengamankan jaringan Anda dari akses yang tidak diinginkan.

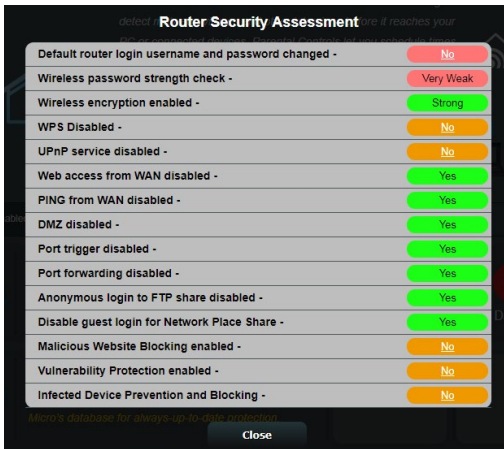


### Mengonfigurasi Perlindungan Jaringan

Untuk mengonfigurasi Perlindungan Jaringan:

1. Dari panel navigasi, klik tab **General (Umum) > AiProtection**.
2. Dari halaman utama **AiProtection**, klik **Network Protection (Perlindungan Jaringan)**.
3. Dari tab **Network Protection (Perlindungan Jaringan)**, klik **Scan (Pindai)**.

Setelah pemindaian selesai, utilitas akan menampilkan hasilnya di halaman **Router Security Assessment (Penilaian Keamanan Router)**.



**PENTING!** Item yang bertanda **Yes (Ya)** di halaman **Router Security Assessment (Penilaian Keamanan Router)** dianggap memiliki status **safe (aman)**. Sedangkan, penyesuaian konfigurasi sangat disarankan untuk item yang bertanda **No, Weak (Tidak, Lemah)**, atau **Very Weak (Sangat Lemah)**.

4. (Opsional) Dari halaman **Router Security Assessment (Penilaian Keamanan Router)**, konfigurasi item yang bertanda **No, Weak, or Very Weak (Tidak, Lemah, atau Sangat Lemah)** secara manual. Untuk melakukannya:

a. Klik item.

**CATATAN:** Saat Anda mengklik item, utilitas akan menampilkan halaman pengaturan item.

- b. Dari halaman pengaturan keamanan item, lakukan konfigurasi dan buat perubahan yang diperlukan, lalu klik **Apply (Terapkan)** jika sudah selesai.
  - c. Kembali ke halaman **Router Security Assessment (Penilaian Keamanan Router)**, lalu klik **Close (Tutup)** untuk keluar dari halaman.
5. Untuk mengonfigurasi pengaturan keamanan secara otomatis, klik **Secure Your Router (Amankan Router Anda)**.
6. Saat ada pesan yang muncul, klik **OK (Oke)**.

## Pemblokiran Situs Web Berbahaya

Fitur ini membatasi akses ke situs web berbahaya yang sudah tercatat dalam pusat data cloud guna memberikan perlindungan mutakhir.

---

**CATATAN:** Fungsi ini otomatis aktif saat Anda menjalankan **Router Weakness Scan (Pemindaian Kelemahan Router)**.

---

### Pemblokiran Situs Web Berbahaya:

1. Dari panel navigasi, klik tab **General (Umum) > AiProtection**.
2. Dari halaman utama **AiProtection**, klik **Network Protection (Perlindungan Jaringan)**.
3. Dari panel **Malicious Sites Blocking (Pemblokiran Situs Web Berbahaya)**, klik **ON (Aktifkan)**.

## Pemblokiran dan Pembatasan Perangkat Terinfeksi

Fitur ini mencegah perangkat yang terinfeksi mengirimkan informasi personal atau status terinfeksi ke pihak eksternal.

---

**CATATAN:** Fungsi ini otomatis aktif saat Anda menjalankan **Router Weakness Scan (Pemindaian Kelemahan Router)**.

---

### Pemblokiran dan Pembatasan Perangkat Terinfeksi:

1. Dari panel navigasi, klik tab **General (Umum) > AiProtection**.
2. Dari halaman utama **AiProtection**, klik **Network Protection (Perlindungan Jaringan)**.
3. Dari panel **Infected Device Prevention and Blocking (Pembatasan dan Pemblokiran Perangkat Terinfeksi)**, klik **ON (AKTIFKAN)**.

### Preferensi Peringatan:

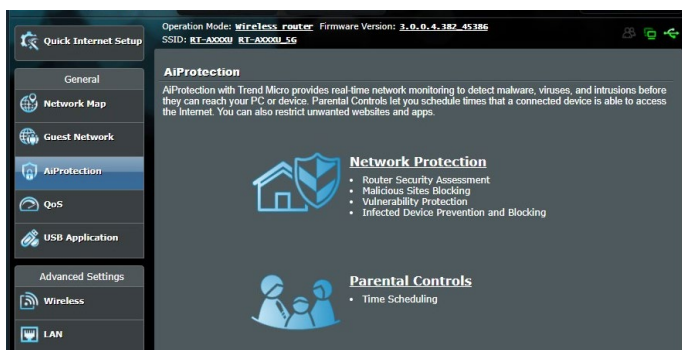
1. Dari panel **Infected Device Prevention and Blocking (Pembatasan dan Pemblokiran Perangkat Terinfeksi)**, klik **Alert Preference (Preferensi Peringatan)**.
  2. Pilih atau masukkan e-mail penyedia, akun e-mail, dan kata sandi, lalu klik **Apply (Terapkan)**.
-

### 3.3.2 Mengkonfigurasi Kontrol Orang Tua

Kontrol Orang Tua memungkinkan Anda mengontrol waktu akses Internet. Pengguna dapat menetapkan batas waktu penggunaan jaringan klien.

#### Untuk membuka halaman utama Kontrol Orang Tua:

1. Dari panel navigasi, klik tab **General (Umum) > AiProtection**.
2. Dari halaman utama **AiProtection**, klik tab **Parental Controls (Kontrol Orang Tua)**.

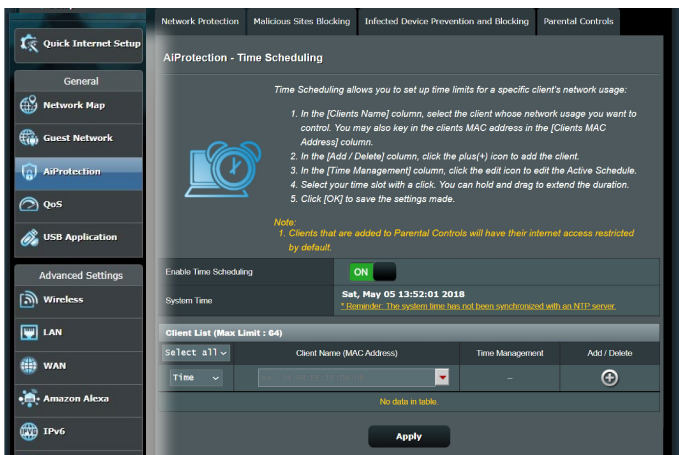




## Penjadwalan Waktu

Penjadwalan Waktu memungkinkan Anda mengatur batas waktu penggunaan jaringan klien.


**CATATAN:** Pastikan sistem waktu Anda telah disesuaikan dengan server NTP.



### Untuk mengonfigurasi Penjadwalan Waktu:

1. Dari panel navigasi, klik tab **General (Umum)** > **AiProtection** > **Parental Controls (Kontrol Orang Tua)** > **Time Scheduling (Penjadwalan Waktu)**.
2. Dari panel **Enable Time Scheduling (Aktifkan Penjadwalan Waktu)**, klik **ON (Aktifkan)**.
3. Dari kolom **Client Name (Nama Klien)**, pilih atau masukkan nama klien dari daftar kotak drop down.

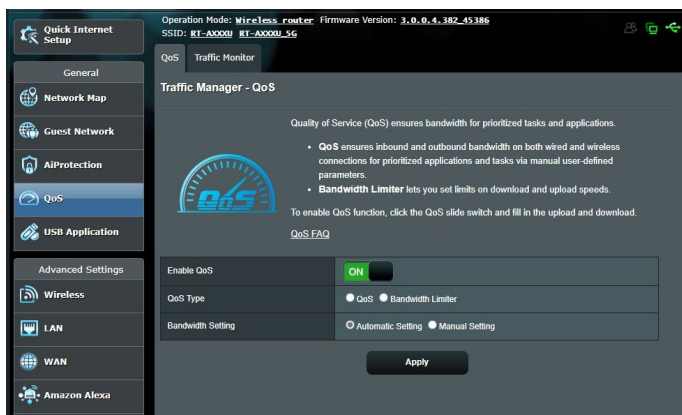
**CATATAN:** Anda juga dapat memasukkan MAC address (Alamat MAC) klien pada kolom **Client MAC Address (Alamat MAC Klien)**. Pastikan nama klien tidak menggunakan karakter khusus atau spasi karena dapat mengakibatkan router tidak berfungsi normal.

4. Klik  untuk menambahkan profil klien.
5. Untuk menyimpan pengaturan, klik **Apply (Terapkan)**.

## 3.4 Menggunakan QoS (Kualitas Layanan)

### 3.4.1 Mengelola Bandwidth QoS (Kualitas Layanan)

Fitur Quality of Service (Kualitas Layanan) memungkinkan Anda menetapkan prioritas bandwidth dan mengelola lalu lintas jaringan.



#### Untuk mengkonfigurasi QoS:

1. Dari panel navigasi, klik tab **General (Umum) > QoS**.
2. Klik **ON (Aktif)** untuk mengaktifkan QoS. Isi kolom bandwidth upload dan download.

---

**CATATAN:** Dapatkan informasi bandwidth dari ISP.

---

3. Klik **Apply (Terapkan)**.

---

**CATATAN:** User Specify Rule List (Daftar Aturan yang Ditentukan Pengguna) digunakan untuk pengaturan lanjutan. Jika Anda ingin memprioritaskan aplikasi jaringan dan layanan jaringan tertentu, pilih **User-defined QoS rules (Aturan QoS yang ditetapkan pengguna)** atau **User-defined Priority (Prioritas yang ditetapkan pengguna)** dari daftar dropdown di sudut kanan atas.

---

4. Pada halaman **user-defined QoS rules (aturan QoS yang ditetapkan pengguna)**, terdapat empat jenis layanan online default: penelusuran web, HTTPS, dan transfer file. Tentukan layanan pilihan, isi **Source IP or MAC (IP Sumber atau MAC)**, **Destination Port (Port Tujuan)**, **Protocol (Protokol)**, **Transferred (Ditransfer)** dan **Priority (Prioritas)**, lalu klik **Apply (Terapkan)**. Informasi akan dikonfigurasi di layar aturan QoS.
- 

#### **CATATAN:**

- Untuk mengisi IP sumber atau MAC, Anda dapat:
    - a) Memasukkan alamat IP tertentu, misalnya "192.168.122.1".
    - b) Memasukkan alamat IP dalam satu subnet atau dalam persediaan IP yang sama, misalnya "192.168.123.\*", atau "192.168.\*.\*"
    - c) Memasukkan semua alamat IP sebagai "\*.\*.\*.\*" atau mengosongkan bidang tersebut.
    - d) Format alamat MAC adalah enam kelompok dua digit heksadesimal, dipisahkan oleh titik dua (:), dalam urutan transmisi (misalnya, 12:34:56:aa:bc:ef)
  - Untuk rentang sumber atau port tujuan, Anda dapat:
    - a) Memasukkan port tertentu, misalnya "95".
    - b) Memasukkan port dalam kisaran, misalnya "103:315", ">100", atau "<65535".
  - Kolom **Transferred (Ditransfer)** berisi informasi tentang lalu lintas upstream dan downstream (lalu lintas jaringan keluar dan masuk) untuk satu bagian. Dalam kolom ini, Anda dapat mengatur batas lalu lintas jaringan (dalam KB) untuk layanan tertentu agar menghasilkan prioritas khusus untuk layanan yang ditetapkan pada port tertentu. Misalnya, jika dua klien jaringan, PC 1 dan PC 2 mengakses Internet (ditetapkan di port 80), namun PC 1 melampaui batas lalu lintas jaringan karena tugas download, PC 1 akan memperoleh prioritas lebih rendah. Jika tidak ingin menetapkan batas lalu lintas, biarkan kosong.
-

5. Pada halaman **User-defined Priority (Prioritas yang ditetapkan pengguna)**, Anda dapat memprioritaskan aplikasi jaringan atau perangkat menjadi lima tingkat dari daftar dropdown **user-defined QoS rules (aturan QoS yang ditetapkan pengguna)**. Berdasarkan tingkat prioritas, Anda dapat menggunakan metode berikut untuk mengirim paket data:
  - Ubah urutan paket jaringan upstream yang dikirim ke Internet.
  - Dalam tabel **Upload Bandwidth (Bandwidth Upload)**, tetapkan **Minimum Reserved Bandwidth (Bandwidth Cadangan Minimum)** dan **Maximum Bandwidth Limit (Batas Bandwidth Maksimum)** untuk beberapa aplikasi jaringan dengan tingkat prioritas berbeda. Persentase menunjukkan tingkat bandwidth upload yang tersedia untuk aplikasi jaringan tertentu.

---

**CATATAN:**

- Paket dengan prioritas rendah akan diabaikan untuk memastikan transmisi paket prioritas tinggi.
- Dalam tabel **Download Bandwidth (Bandwidth Download)**, tetapkan **Maximum Bandwidth Limit (Batas Bandwidth Maksimum)** untuk beberapa aplikasi jaringan dalam urutan yang sesuai. Prioritas paket upstream yang lebih tinggi akan mengakibatkan paket downstream prioritas lebih tinggi.
- Jika tidak ada paket yang dikirim dari aplikasi prioritas tinggi, maka kecepatan transmisi penuh pada sambungan Internet akan tersedia untuk paket dengan prioritas rendah.

- 
6. Tetapkan paket prioritas tertinggi. Untuk memastikan pengalaman bermain game online tanpa gangguan, Anda dapat menetapkan ACK, SYN, dan ICMP sebagai paket prioritas tertinggi.

---

**CATATAN:** Pastikan untuk mengaktifkan QoS terlebih dulu dan menetapkan batas tingkat upload maupun download.

---

## 3.5 Menggunakan Aplikasi USB

Fungsi Aplikasi USB menyediakan submenu AiDisk, Pusat Server, Server Printer Jaringan, dan Download Master.

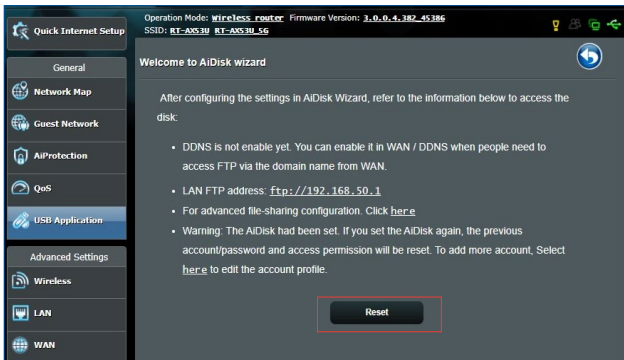
**PENTING!** Untuk menggunakan fungsi server, Anda harus memasang perangkat penyimpanan USB, misalnya hard disk USB atau flash drive USB, di port USB 3.0 di bagian belakang panel router nirkabel. Pastikan perangkat penyimpanan USB telah diformat dan dipartisi dengan benar. Untuk tabel dukungan sistem file, kunjungi situs web ASUS di <http://event.asus.com/2009/networks/disksupport/>.

### 3.5.1 Menggunakan AiDisk

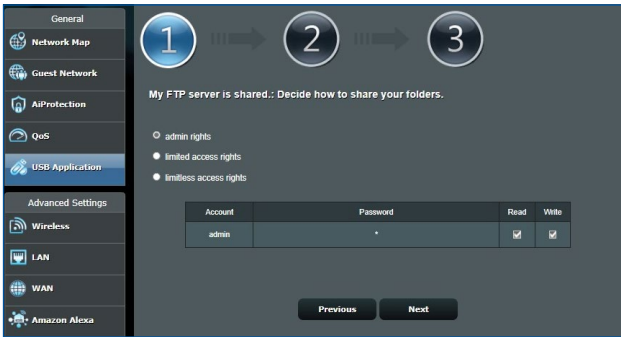
AiDisk dapat digunakan untuk berbagi file yang tersimpan di perangkat USB yang tersambung melalui Internet. AiDisk juga akan membantu Anda mengkonfigurasi DDNS ASUS dan server FTP.

**Untuk menggunakan AiDisk:**

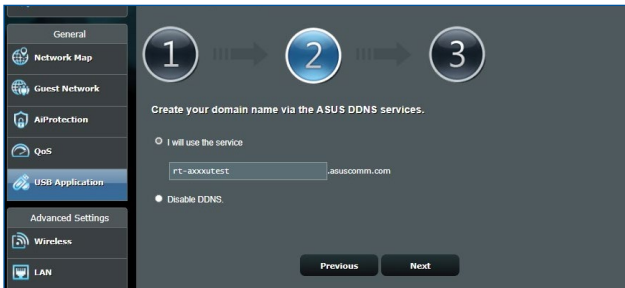
1. Dari panel navigasi, buka **General (Umum) > USB Application (Aplikasi USB)**.
2. Dari layar Welcome to AiDisk wizard (Selamat datang di wizard AiDisk), klik **Reset (Mengatur ulang)**.



3. Pilih hak akses yang akan ditetapkan ke klien yang mengakses data bersama.



4. Buat nama domain melalui layanan DDNS ASUS, baca Persyaratan Layanan, lalu pilih **I will use the service and accept the Terms of service (Saya akan menggunakan layanan ini dan menerima Persyaratan Layanan)** dan masukkan nama domain. Setelah selesai, klik **Next (Berikutnya)**.



Anda juga dapat memilih **Skip ASUS DDNS settings (Lewati pengaturan DDNS ASUS)**, lalu mengklik **Next (Berikutnya)** untuk melewati pengaturan DDNS.

5. Untuk menyelesaikan pengaturan, klik **Finish (Selesai)**.
6. Untuk mengakses situs FTP yang Anda buat, buka browser web atau utilitas klien FTP pihak ketiga, lalu masukkan link ftp (**ftp://<domain name>.asuscomm.com**) yang sebelumnya dibuat.

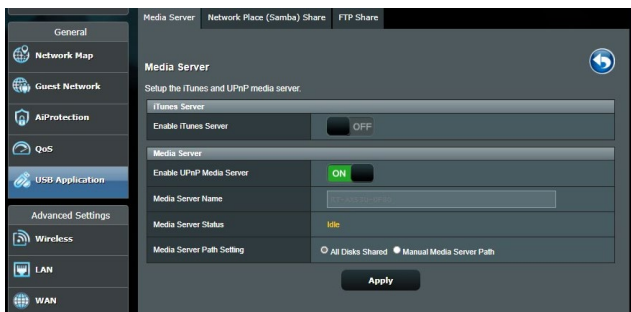
### 3.5.2 Menggunakan Pusat Server

Pusat Server dapat digunakan untuk berbagi file media dari disk USB melalui direktori Server Media, layanan berbagi Samba, atau layanan berbagi FTP. Anda juga dapat mengkonfigurasi pengaturan lainnya untuk disk USB di Pusat Server.

#### Menggunakan Server Media

Router nirkabel ini memungkinkan perangkat yang didukung DLNA mengakses file multimedia dari disk USB yang tersambung ke router nirkabel.

**CATATAN:** Sebelum menggunakan fungsi Server Media DLNA, sambungkan perangkat ke jaringan RT-AX53U.

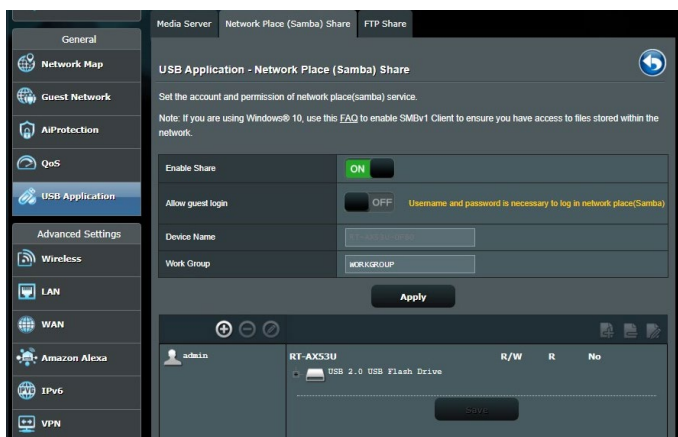


Untuk membuka halaman pengaturan Server Media, buka tab **General (Umum) > USB Application (Aplikasi USB) > Servers Center (Pusat Server) > Media Server (Server Media)**. Untuk keterangan kolom, lihat:

- **Enable iTunes Server (Aktifkan Server iTunes):** Untuk mengaktifkan/menonaktifkan Server iTunes, pilih ON/OFF (Aktif/Tidak Aktif).
- **Media Server Status (Status Server Media):** Menampilkan status server media.
- **Media Server Path Setting (Pengaturan Jalur Server Media):** Pilih **All Disks Shared (Semua Disk Bersama)** atau **Manual Media Server Path (Jalur Server Media Manual)**.

## Menggunakan Layanan Berbagi Lokasi Jaringan (Samba)

Berbagi Lokasi Jaringan (Samba) memungkinkan Anda mengkonfigurasi akun dan izin untuk layanan Samba.




### Untuk menggunakan berbagi Samba:

1. Dari panel navigasi, buka tab **General (Umum) > USB Application (Aplikasi USB) > Servers Center (Pusat Server) > Berbagi Lokasi Jaringan (Samba)**.

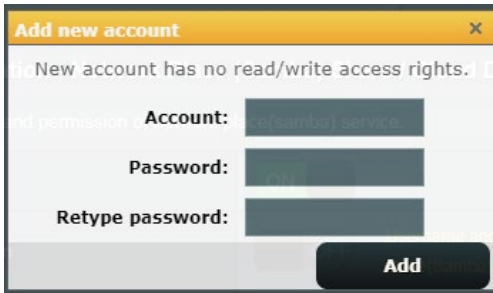
**CATATAN:** Berbagi Lokasi Jaringan (Samba) akan diaktifkan secara default.

2. Ikuti langkah-langkah di bawah ini untuk menambah, menghapus, atau mengubah akun.


### Untuk membuat akun baru:

- a) Klik  untuk menambah akun baru.
- b) Pada kolom **Account (Akun)** dan **Password (Sandi)**, masukkan nama dan sandi klien jaringan. Masukkan ulang sandi untuk mengkonfirmasi. Klik **Add (Tambah)** untuk menambahkan akun ke daftar.




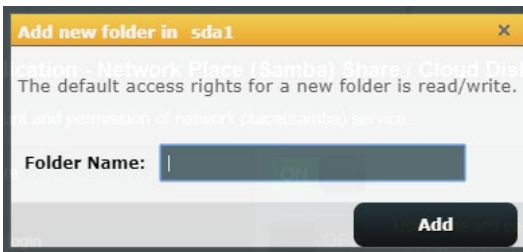


### Untuk menghapus akun yang ada:

- Pilih akun yang akan dihapus.
- Klik .
- Saat ditampilkan, klik **Delete (Hapus)** untuk mengkonfirmasi penghapusan akun.

### Untuk menambah folder:

- Klik .
- Masukkan nama folder, lalu klik **Add (Tambah)**. Folder yang Anda buat akan ditambahkan ke daftar folder.



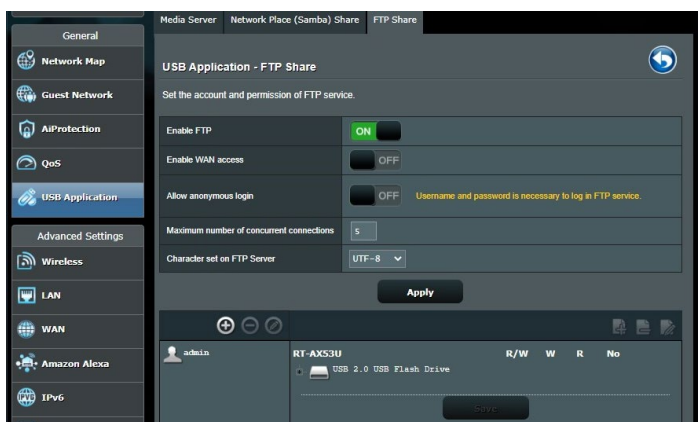
- Dari daftar folder, pilih jenis izin akses yang akan ditetapkan untuk folder tertentu:
  - R/W**: Gunakan pilihan ini untuk menetapkan akses baca/tulis.
  - R**: Gunakan pilihan ini untuk menetapkan akses hanya baca.
  - No (Tidak)**: Gunakan pilihan ini jika Anda tidak ingin berbagi folder file tertentu.
- Untuk menerapkan perubahan, klik **Apply (Terapkan)**.

## Menggunakan Layanan Berbagi FTP

Berbagi FTP memungkinkan server FTP berbagi file dari disk USB ke perangkat lain melalui jaringan area lokal atau Internet.

### PENTING!

- Pastikan Anda melepas disk USB dengan aman. Melepas disk USB secara salah dapat mengakibatkan kerusakan data.
- Untuk melepas disk USB dengan aman, lihat bagian **Melepas disk USB dengan aman** dalam **3.1.3 Memantau perangkat USB**.



### Untuk menggunakan layanan Berbagi FTP:

**CATATAN:** Pastikan Anda telah mengkonfigurasi server FTP melalui AiDisk. Untuk informasi lebih rinci, lihat bagian **3.5.1 Menggunakan AiDisk**.

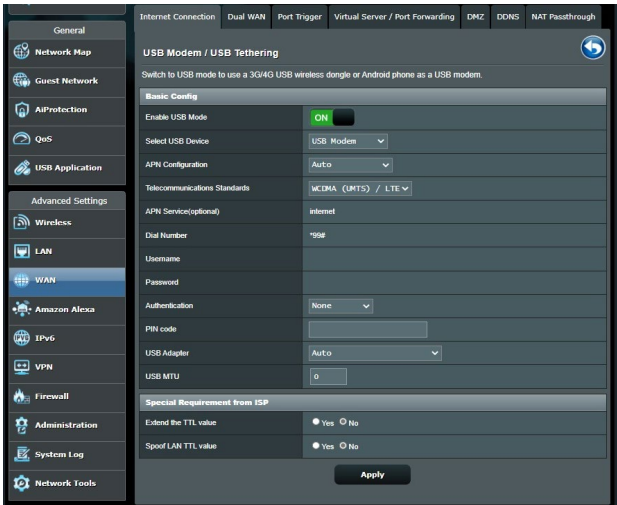
1. Dari panel navigasi, klik tab **General (Umum) > USB Application (Aplikasi USB) > Servers Center (Pusat Server) > FTP Share (Berbagi FTP)**.
2. Dari daftar folder, pilih jenis hak akses yang akan ditetapkan untuk folder tertentu:
  - **R/W:** Pilih agar dapat menetapkan akses baca/tulis untuk folder tertentu.

- **W:** Pilih agar dapat menetapkan akses hanya tulis untuk folder tertentu.
  - **R:** Pilih agar dapat menetapkan akses hanya baca untuk folder tertentu.
  - **No (Tidak):** Gunakan pilihan ini jika Anda tidak ingin berbagi folder tertentu.
3. Untuk mengkonfirmasi perubahan, klik **Apply (Terapkan)**.
  4. Untuk mengakses server FTP, masukkan link ftp **ftp://<hostname>.asuscomm.com** serta nama pengguna dan sandi di browser web atau utilitas FTP pihak ketiga.

### 3.5.3 3G/4G

Modem USB 3G/4G dapat disambungkan ke RT-AX53U untuk memungkinkan akses Internet.

**CATATAN:** Untuk daftar modem USB terverifikasi, kunjungi:  
<http://event.asus.com/2009/networks/3gsupport/>



## Untuk mengkonfigurasi akses Internet 3G/4G:

1. Dari panel navigasi, klik **General (Umum) > USB Application (Aplikasi USB) > 3G/4G**.
2. Pada bidang **Enable USB Mode (Aktifkan Mode USB)**, pilih **ON (Aktifkan)**.
3. Tetapkan sebagai berikut:
  - **Pilih Perangkat USB:** Pilih lokasi penyedia layanan 3G/4G dari daftar dropdown.
  - **Konfigurasi APN:** Untuk informasi rinci, hubungi penyedia layanan 3G/4G Anda.
  - **Standar Telekomunikasi:** Pilih ISP (Penyedia Layanan Internet) dari daftar dropdown.
  - **Nomor Panggilan dan kode PIN:** Nomor akses penyedia layanan 3G/4G dan kode PIN untuk sambungan.

---

**CATATAN:** Kode PIN dari berbagai penyedia dapat bervariasi.

---

- **Nama pengguna/Sandi:** Nama pengguna dan sandi akan diberikan oleh operator jaringan 3G/4G.
  - **Adapter USB:** Pilih adapter USB 3G/4G dari daftar dropdown. Jika tidak yakin dengan model adapter USB atau model tidak tercantum dalam pilihan, pilih **Auto (Otomatis)**.
4. Klik **Apply (Terapkan)**.

---

**CATATAN:** Router akan menjalankan boot ulang agar pengaturan dapat diterapkan.

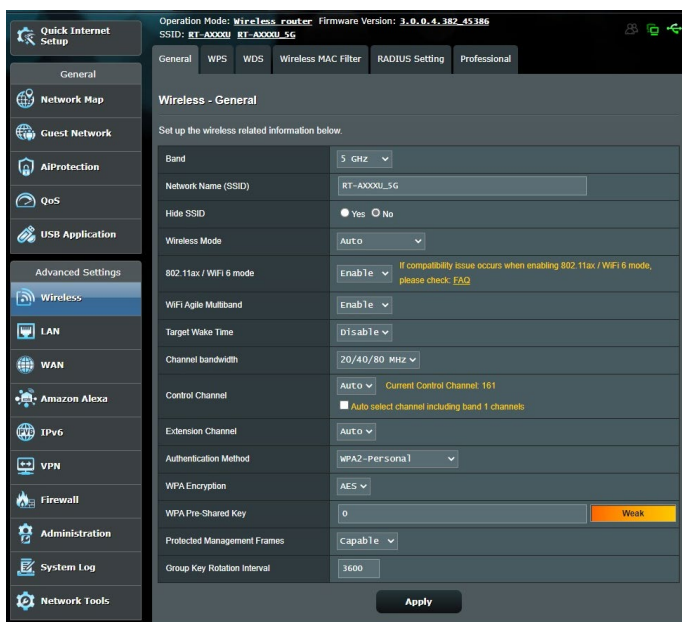
---

# 4 Mengkonfigurasi pengaturan lanjutan

## 4.1 Nirkabel

### 4.1.1 Umum

Tab General (Umum) dapat digunakan untuk mengkonfigurasi pengaturan dasar nirkabel.



## Untuk mengkonfigurasi pengaturan dasar nirkabel:

1. Dari panel navigasi, buka tab **Advanced Settings (Pengaturan Lanjutan) > Wireless (Nirkabel) > General (Umum)**.
2. Atur konfigurasi dasar nirkabel untuk band frekuensi 2,4 GHz atau 5 GHz.
3. Pada kolom SSID, tetapkan nama unik yang berisi maksimal 32 karakter untuk SSID (Service Set Identifier) atau nama jaringan untuk mengidentifikasi jaringan nirkabel. Perangkat Wi-Fi dapat mengidentifikasi dan menyambung ke jaringan nirkabel melalui SSID yang ditetapkan. SSID pada banner informasi akan diperbarui setelah SSID baru disimpan ke pengaturan.

---

**CATATAN:** Anda dapat menetapkan SSID unik untuk pita frekuensi 2.4 GHz dan 5GHz.

---

4. Pada kolom **Hide SSID (Sembunyikan SSID)**, pilih **Yes (Ya)** agar perangkat nirkabel tidak mendeteksi SSID. Setelah fungsi ini diaktifkan, Anda harus memasukkan SSID secara manual di perangkat nirkabel untuk mengakses jaringan nirkabel.
5. Pada kolom **Wireless Mode (Mode Nirkabel)**, gunakan pilihan mode nirkabel untuk menentukan jenis perangkat nirkabel yang dapat disambungkan ke router nirkabel:
  - **Auto (Otomatis):** Pilih **Auto (Otomatis)** agar perangkat 802.11AX, 802.11AC, 802.11n, 802.11g, dan 802.11b dapat tersambung ke router nirkabel.
  - **Legacy (Versi Sebelumnya):** Pilih **Legacy (Versi Sebelumnya)** agar perangkat 802.11b/g/n dapat tersambung ke router nirkabel. Namun perangkat keras yang pada dasarnya mendukung 802.11n hanya akan berjalan pada kecepatan maksimum 54 Mbps.
  - **Hanya N:** Pilih N only (Hanya N) untuk memaksimalkan performa N nirkabel. Pengaturan ini mencegah perangkat 802.11g dan 802.11b tersambung ke router nirkabel.

6. Pada kolom Channel bandwidth (Bandwidth saluran), pilih bandwidth saluran untuk mengakomodasi kecepatan transmisi yang lebih tinggi:
  - **40 MHz:** Pilih bandwidth ini untuk memaksimalkan throughput nirkabel radio 2,4 GHz.
  - **20 MHz (default):** Pilih bandwidth ini jika Anda mengalami masalah pada sambungan nirkabel.
7. Pilih saluran pengoperasian untuk router nirkabel. Pilih **Auto (Otomatis)** agar router nirkabel dapat secara otomatis memilih saluran dengan jumlah interferensi paling sedikit.
8. Pada kolom Authentication Method (Metode Otentikasi), pilih dari metode otentikasi berikut:
  - **Sistem Terbuka:** Pilihan ini tidak dilengkapi fitur keamanan.
  - **WPA/WPA2/WPA3-Pribadi/WPA Pribadi Otomatis:** Pilihan ini dilengkapi fitur keamanan yang kuat. Anda dapat menggunakan WPA (dengan TKIP), WPA2 (dengan AES) atau WPA3. Jika pilihan ini digunakan, Anda harus menggunakan enkripsi TKIP+AES dan memasukkan frasa WPA (kunci jaringan).
  - **WPA/WPA2/WPA3 Perusahaan/WPA Perusahaan Otomatis:** Pilihan ini dilengkapi fitur keamanan yang sangat kuat dan server EAP terintegrasi atau server otentikasi backend RADIUS eksternal.

---

**CATATAN:** Router nirkabel Anda mendukung kecepatan transmisi maksimum 54Mbps saat **Wireless Mode (Mode Nirkabel)** ditetapkan ke **Auto (Otomatis)** dan metode enkripsi adalah **WEP** atau **TKIP**.

---

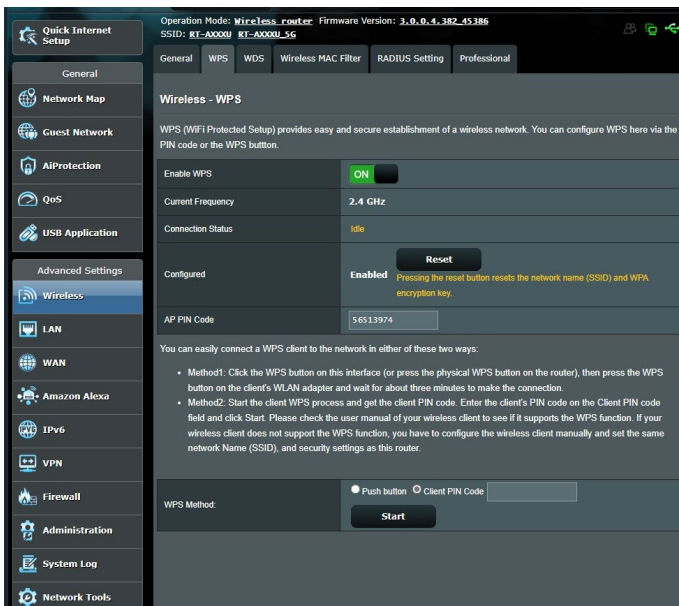
9. Pilih salah satu pilihan Enkripsi WEP (Wired Equivalent Privacy) untuk data yang dikirim melalui jaringan nirkabel Anda:
  - **Nonaktif:** Menonaktifkan enkripsi WEP
  - **64-bit:** Mengaktifkan enkripsi WEP yang lemah
  - **128-bit:** Mengaktifkan enkripsi WEP yang lebih baik.
10. Setelah selesai, klik **Apply (Terapkan)**.



## 4.1.2 WPS

WPS (Wi-Fi Protected Setup) adalah standar keamanan nirkabel yang memungkinkan Anda menyambungkan perangkat ke jaringan nirkabel dengan mudah. Anda dapat mengkonfigurasi fungsi WPS melalui kode PIN atau tombol WPS.

**CATATAN:** Pastikan perangkat mendukung WPS.



### Untuk mengaktifkan WPS di perangkat nirkabel:

1. Dari panel navigasi, buka tab **Advanced Settings (Pengaturan Lanjutan) > Wireless (Nirkabel) > WPS**.
2. Pada kolom **Enable WPS (Aktifkan WPS)**, geser panel ke **ON (Aktif)**.
3. WPS menggunakan 2.4GHz secara default. Jika ingin mengubah frekuensi menjadi 5GHz, alihkan fungsi WPS ke **OFF (NONAKTIF)**, klik **Switch Frequency (Ganti Frekuensi)** dalam bidang **Current Frequency (Frekuensi Saat Ini)**, lalu alihkan kembali WPS ke **ON (AKTIF)**.

---

**CATATAN:** WPS mendukung otentikasi menggunakan Sistem Terbuka, WPA-Pribadi, WPA2-Pribadi dan WPA3-Pribadi. WPS tidak mendukung jaringan nirkabel yang menggunakan Kode Bersama, WPA-Pribadi, WPA2-Perusahaan, WPA3-Perusahaan, dan metode enkripsi RADIUS.

---

4. Dalam bidang WPS Method (Metode WPS), pilih **Push Button (Tekan Tombol)** atau kode **Client PIN (PIN Klien)**. Jika memilih **Push Button (Tekan Tombol)**, lanjutkan ke langkah 5. Jika memilih kode **Client PIN (PIN Klien)**, lanjutkan ke langkah 6.
5. Untuk mengkonfigurasi WPS menggunakan tombol WPS router, lakukan langkah-langkah berikut:
  - a. Klik **Start (Mulai)** atau tekan tombol WPS yang terdapat di bagian belakang router nirkabel.
  - b. Tekan tombol WPS di perangkat nirkabel. Ini biasanya diidentifikasi oleh logo WPS.

---

**CATATAN:** Untuk mengetahui lokasi tombol WPS, periksa perangkat nirkabel atau baca panduan pengguna.

---

- c. Router nirkabel akan memindai perangkat WPS yang tersedia. Jika tidak menemukan perangkat WPS apa pun, maka router nirkabel akan beralih ke mode siaga.
6. Untuk mengkonfigurasi WPS menggunakan kode PIN Klien, lakukan langkah-langkah berikut:
  - a. Cari kode PIN WPS pada panduan pengguna perangkat nirkabel atau pada perangkat itu sendiri.
  - b. Masukkan kode PIN Klien dalam kotak teks.
  - c. Klik **Start (Mulai)** untuk memasukkan router nirkabel dalam mode survei WPS. Indikator LED router akan berkedip cepat tiga kali hingga konfigurasi WPS selesai.

## 4.1.3 WDS

Perantara atau WDS (Wireless Distribution System) memungkinkan router nirkabel ASUS menyambung ke jalur akses nirkabel lain secara eksklusif, sehingga perangkat atau stasiun nirkabel lainnya tidak dapat mengakses router ASUS Anda. WDS juga dapat dianggap sebagai repeater nirkabel, yakni router nirkabel ASUS dapat berkomunikasi dengan jalur akses dan perangkat nirkabel lainnya.

Quick Internet Setup

Operation Mode: **wireless\_router** Firmware Version: **3.0.0.4.382\_45386**  
SSID: RT-AXXXX RT-AXXXX\_5g

General WPS WDS Wireless MAC Filter RADIUS Setting Professional

### Wireless - Bridge

Bridge (or named WDS - Wireless Distribution System) function allows your RT-AX30U 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 APs WDS management interface, key in the this router's MAC address.
4. To get the best performance, please go to Advanced Settings > Wireless > General and assign the same channel bandwidth, control channel, and extension channel to every router in the network.

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

#### Basic Config

2.4 GHz: MAC	FC: 34: 97: 09: 0F: 80
5 GHz: MAC	FC: 34: 97: 09: 0F: 84
Band	5 GHz
AP Mode	AP Only
Connect to APs in list	<input type="radio"/> Yes <input checked="" type="radio"/> No

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

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

[Help & Support](#) [Manual](#) | [Product Registration](#) | [Feedback](#) [FAQ](#)

## Untuk mengkonfigurasi perantara nirkabel:

1. Dari panel navigasi, buka tab **Advanced Settings (Pengaturan Lanjutan) > Wireless (Nirkabel) > WDS**.
2. Pilih band untuk perantara nirkabel.
3. Pada kolom **AP Mode (Mode AP)**, gunakan pilihan berikut:
  - **AP Only (Hanya AP)**: Menonaktifkan fungsi WDS.
  - **WDS Only (Hanya WDS)**: Mengaktifkan fitur WDS, namun mencegah perangkat nirkabel/stasiun lainnya menyambung ke router.
  - **HYBRID (Hibrid)**: Mengaktifkan fitur Wireless Bridge (Perantara Nirkabel) dan mengizinkan perangkat nirkabel/stasiun lainnya menyambung ke router.

---

**CATATAN:** Dalam mode Hybrid (Hibrid), perangkat nirkabel yang tersambung ke router nirkabel ASUS hanya akan menerima separuh dari kecepatan sambungan Jalur Akses.


---

4. Pada kolom **Connect to APs (Sambungkan ke AP)**, klik **Yes (Ya)** jika Anda ingin menyambung ke Jalur Akses yang tercantum dalam Daftar AP Jauh.
5. Pada bidang **Control Channel (Saluran Kontrol)**, pilih saluran pengoperasian untuk perantara nirkabel. Pilih **Auto (Otomatis)** agar router dapat memilih saluran dengan sedikit gangguan secara otomatis.

---

**CATATAN:** Ketersediaan saluran di setiap negara atau kawasan dapat berbeda.

---

6. Pada Remote AP List (Daftar AP Jauh), ketik alamat MAC, lalu klik tombol **Add (Tambah)**  untuk memasukkan alamat MAC Jalur Akses lain yang tersedia

---

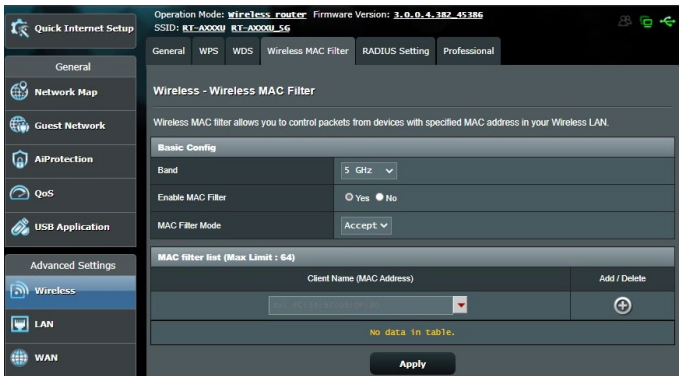
**CATATAN:** Jalur Akses yang ditambahkan ke daftar harus berada di Saluran Kontrol dan bandwidth Saluran tetap yang sama seperti router nirkabel ASUS lokal.

---


7. Klik **Apply (Terapkan)**.

## 4.1.4 Filter MAC Nirkabel

Filter MAC Nirkabel dilengkapi kontrol atas paket yang dikirim ke alamat MAC (Media Access Control) tertentu di jaringan nirkabel.

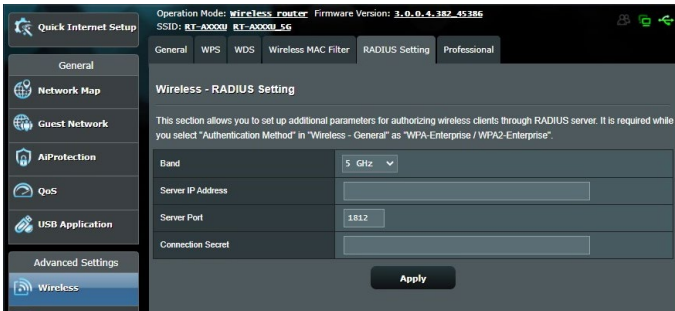


### Untuk mengkonfigurasi filter MAC Nirkabel:

1. Dari panel navigasi, buka tab **Advanced Settings (Pengaturan Lanjutan) > Wireless (Nirkabel) > Wireless MAC Filter (Filter MAC Nirkabel)**.
2. Klik **Yes (Ya)** pada kolom **Enable Mac Filter (Aktifkan Filter Mac)**.
3. Dalam daftar dropdown **MAC Filter Mode (Mode Filter MAC)**, pilih **Accept (Terima)** atau **Reject (Tolak)**.
  - Pilih **Accept (Terima)** agar perangkat dalam daftar filter MAC dapat mengakses jaringan nirkabel.
  - Pilih **Reject (Tolak)** agar perangkat dalam daftar filter MAC tidak dapat mengakses jaringan nirkabel.
4. Pada MAC filter list (Daftar filter MAC), klik tombol **Add (Tambah)** , lalu masukkan alamat MAC jaringan nirkabel.
5. Klik **Apply (Terapkan)**.

## 4.1.5 Pengaturan RADIUS

Pengaturan RADIUS (Remote Authentication Dial In User Service) dilengkapi keamanan tambahan bila Anda memilih WPA-Perusahaan, WPA2-Perusahaan, WPA3-Perusahaan, atau Radius dengan 802.1x sebagai Mode Otentikasi.



### Untuk mengkonfigurasi pengaturan RADIUS nirkabel:

1. Pastikan mode otentikasi router nirkabel diatur ke WPA-Perusahaan, WPA2-Perusahaan dan WPA3-Perusahaan.

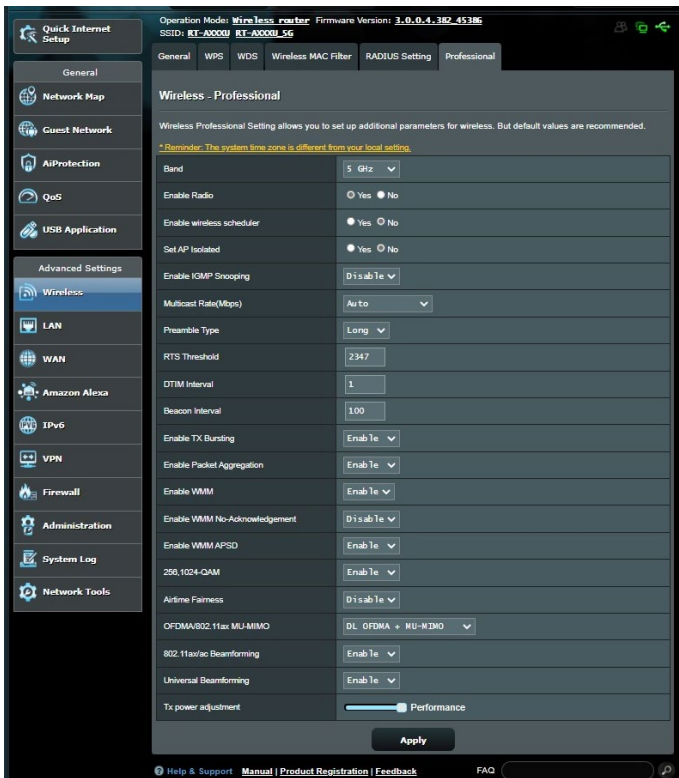
**CATATAN:** Lihat bagian **4.1.1 Umum** untuk mengkonfigurasi Mode Otentikasi router nirkabel.

2. Dari panel navigasi, buka **Advanced Settings (Pengaturan Lanjutan) > Wireless (Nirkabel) > RADIUS Setting (Pengaturan RADIUS)**.
3. Pilih band frekuensi.
4. Pada kolom **Server IP Address (Alamat IP Server)**, masukkan Alamat IP server RADIUS.
5. Pada kolom **Connection Secret (Sambungan Rahasia)**, buat sandi untuk mengakses server RADIUS.
6. Klik **Apply (Terapkan)**.

## 4.1.6 Professional

Layar Professional (Professional) akan menampilkan pilihan konfigurasi lanjutan.

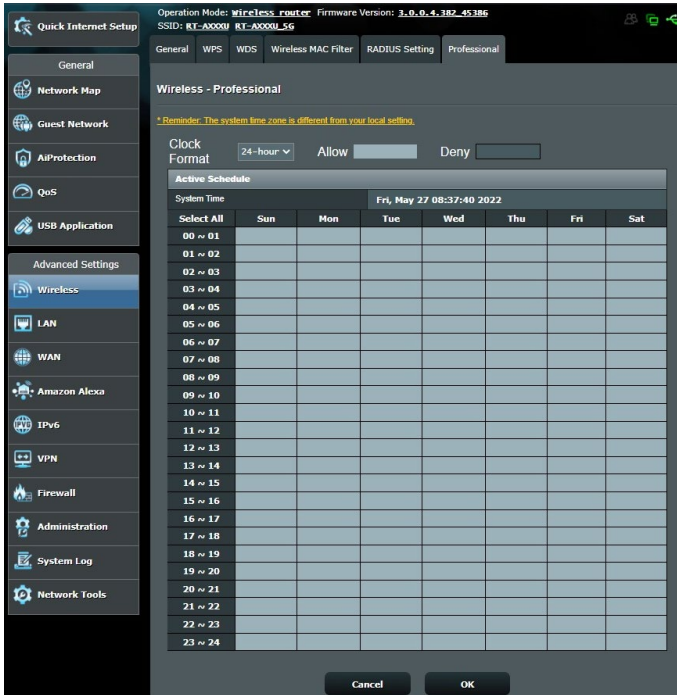
**CATATAN:** Sebaiknya gunakan nilai default pada halaman ini.



Di layar **Professional Settings (Pengaturan Profesional)**, Anda dapat mengkonfigurasi hal berikut:

- **Band:** Pilih band frekuensi untuk menerapkan pengaturan profesional.
- **Enable Radio (Aktifkan Radio):** Pilih **Yes (Ya)** untuk mengaktifkan jaringan nirkabel. Pilih **No (Tidak)** untuk menonaktifkan jaringan nirkabel.

- **Mengaktifkan penjadwal nirkabel:** Anda dapat memilih format 24 jam atau 12 jam. Warna pada tabel menunjukkan **Allow (Diizinkan)** atau **Deny (Tidak Diizinkan)**. Klik masing-masing bingkai untuk mengubah pengaturan masing-masing jam di setiap harinya, lalu klik **OK (Oke)** jika sudah selesai.



- **Set AP isolated (AP yang diatur terisolasi):** Pilihan Set AP isolated (AP yang diatur terisolasi) akan mencegah perangkat nirkabel di jaringan berkomunikasi dengan satu sama lain. Fitur ini berguna jika Anda ingin membuat jaringan nirkabel publik yang hanya membolehkan tamu untuk mengakses Internet. Pilih **Yes (Ya)** untuk mengaktifkan fitur ini atau pilih **No (Tidak)** untuk menonaktifkannya.
- **Multicast rate (Mbps) (Kecepatan multicast (Mbps)):** Pilih kecepatan transmisi multicast atau klik **Disable (Nonaktifkan)** untuk menonaktifkan satu transmisi secara bersamaan.



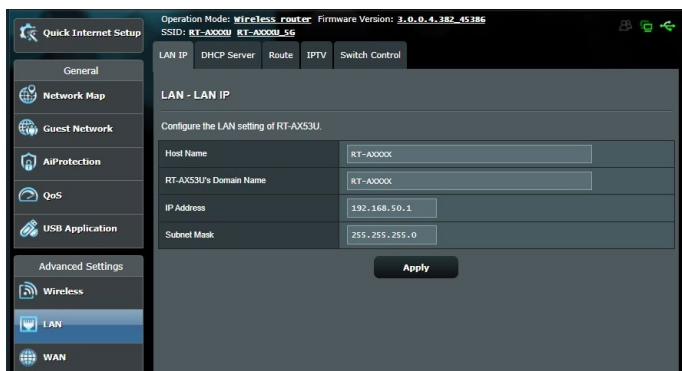
- **Preamble Type (Jenis Preamble):** Jenis Preamble akan menentukan durasi yang digunakan router untuk CRC (Cyclic Redundancy Check). CRC adalah metode deteksi kesalahan selama transmisi data berlangsung. Pilih **Short (Pendek)** untuk jaringan nirkabel sibuk dengan lalu lintas jaringan tinggi. Pilih **Long (Panjang)** jika jaringan nirkabel terdiri atas perangkat nirkabel lama atau versi sebelumnya.
- **RTS Threshold (Ambang Batas RTS):** Pilih nilai lebih rendah untuk Ambang Batas RTS (Request to Send) agar dapat meningkatkan komunikasi nirkabel di jaringan nirkabel yang sibuk atau bising dengan lalu lintas jaringan tinggi dan berbagai perangkat nirkabel.
- **DTIM Interval (Interval DTIM):** Interval DTIM (Delivery Traffic Indication Message) atau Kecepatan Beacon Data adalah interval waktu sebelum sinyal dikirim ke perangkat nirkabel dalam mode tidur yang menunjukkan bahwa paket data menunggu untuk dikirim. Nilai default-nya adalah 3 milidetik.
- **Beacon Interval (Interval Beacon):** Interval Beacon adalah waktu antara satu DTIM dan DTIM berikutnya. Nilai default-nya adalah 100 milidetik. Kurangi nilai Interval Beacon untuk sambungan nirkabel yang tidak stabil atau perangkat roaming.
- **Enable TX Bursting (Aktifkan TX Berurutan):** Fitur Aktifkan TX Berurutan akan meningkatkan kecepatan transmisi antara router nirkabel dan perangkat 802.11g.
- **Mengaktifkan WMM APSD (APSD WMM):** Aktifkan WMM APSD (Wi-Fi Multimedia Automatic Power Save Delivery) (APSD WMM) untuk meningkatkan manajemen daya di antara perangkat nirkabel. Pilih **Disable (Nonaktifkan)** untuk menonaktifkan WMM APSD (APSD WMM).

## 4.2 LAN

### 4.2.1 IP LAN

Layar IP LAN memungkinkan Anda mengubah pengaturan IP LAN pada router nirkabel.

**CATATAN:** Perubahan apa pun pada alamat IP LAN akan ditampilkan pada pengaturan DHCP.

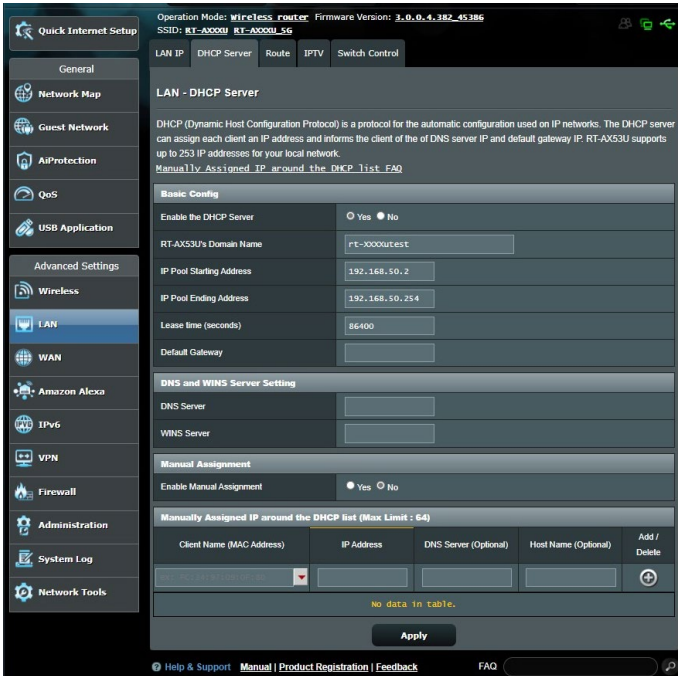


#### Untuk mengubah pengaturan IP LAN:

1. Dari panel navigasi, buka tab **Advanced Settings (Pengaturan Lanjutan) > LAN > LAN IP (IP LAN)**.
2. Ubah **IP address (Alamat IP)** dan **Subnet Mask**.
3. Setelah selesai, klik **Apply (Terapkan)**.

## 4.2.2 Server DHCP

Router nirkabel ini menggunakan DHCP untuk menetapkan alamat IP secara otomatis di jaringan. Anda dapat menentukan rentang alamat IP dan waktu aktif bagi klien di jaringan.



Untuk mengkonfigurasi server DHCP:

1. Dari panel navigasi, buka tab **Advanced Settings (Pengaturan Lanjutan) > LAN > DHCP Server (Server DHCP)**.
2. Pada kolom **Enable the DHCP Server (Aktifkan Server DHCP)**, pilih **Yes (Ya)**.

3. Dalam kotak teks **Domain Name (Nama Domain)**, masukkan nama domain untuk router nirkabel.
4. Pada kolom **IP Pool Starting Address (Alamat Awal Kumpulan IP)**, masukkan alamat awal IP.
5. Pada kolom **IP Pool Ending Address (Alamat Akhir Kumpulan IP)**, masukkan alamat akhir IP.
6. Pada kolom **Lease Time (Waktu Aktif)**, tentukan waktu berakhirnya alamat IP yang ditetapkan dalam hitungan detik. Setelah batas ini tercapai, selanjutnya server DHCP akan menetapkan alamat IP baru.

---

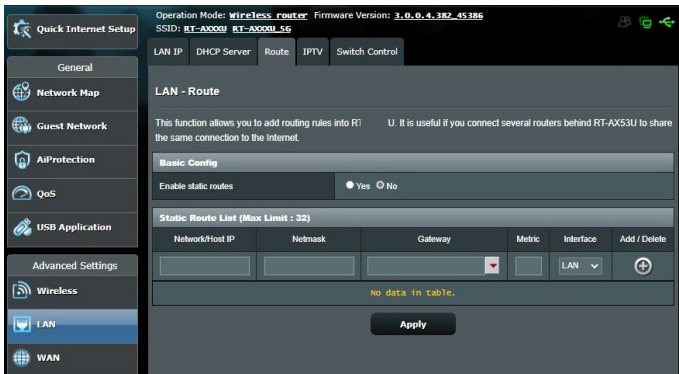
**CATATAN:**

- Sebaiknya gunakan format alamat IP 192.168.50.xxx (xxx adalah angka antara 2 hingga 254) saat menentukan rentang alamat IP.
  - Alamat Awal Kumpulan IP tidak boleh lebih besar daripada Alamat Akhir Kumpulan IP.
- 
7. Di bagian **DNS and Server Settings (Pengaturan DNS dan Server)**, masukkan alamat IP Server DNS dan Server WINS jika perlu.
  8. Router nirkabel ini juga dapat secara manual menetapkan alamat IP ke perangkat di jaringan. Pada kolom **Enable Manual Assignment (Aktifkan Penetapan Manual)**, pilih **Yes (Ya)** untuk menetapkan alamat IP ke alamat MAC spesifik di jaringan. Maksimal 32 alamat MAC dapat ditambahkan ke daftar DHCP untuk penetapan manual.



## 4.2.3 Rute

Jika jaringan menggunakan beberapa router nirkabel, Anda dapat mengkonfigurasi tabel routing untuk berbagi layanan Internet yang sama.

**CATATAN:** Sebaiknya jangan ubah pengaturan default rute, kecuali jika Anda sangat memahami tentang tabel routing.

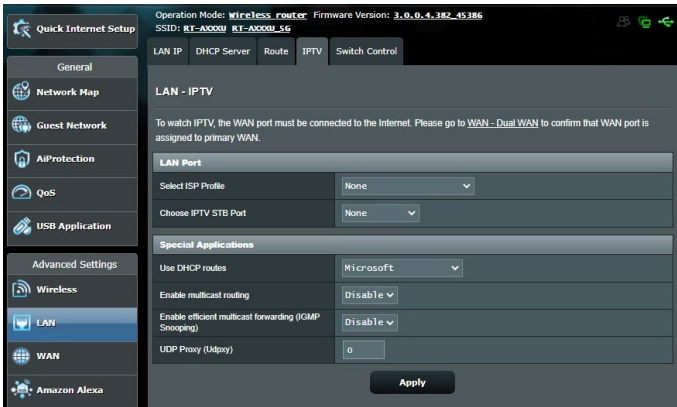


### Untuk mengkonfigurasi tabel Routing LAN:

1. Dari panel navigasi, buka tab **Advanced Settings (Pengaturan Lanjutan) > LAN > Route (Rute)**.
2. Pada kolom **Enable static routes (Aktifkan rute statis)**, pilih **Yes (Ya)**.
3. Dalam **Static Route List (Daftar Rute Statis)**, masukkan informasi jaringan jalur akses atau node lain. Untuk menambahkan atau menghapus perangkat dalam daftar, klik tombol **Add (Tambah)**  atau **Delete (Hapus)** .
4. Klik **Apply (Terapkan)**.

## 4.2.4 IPTV

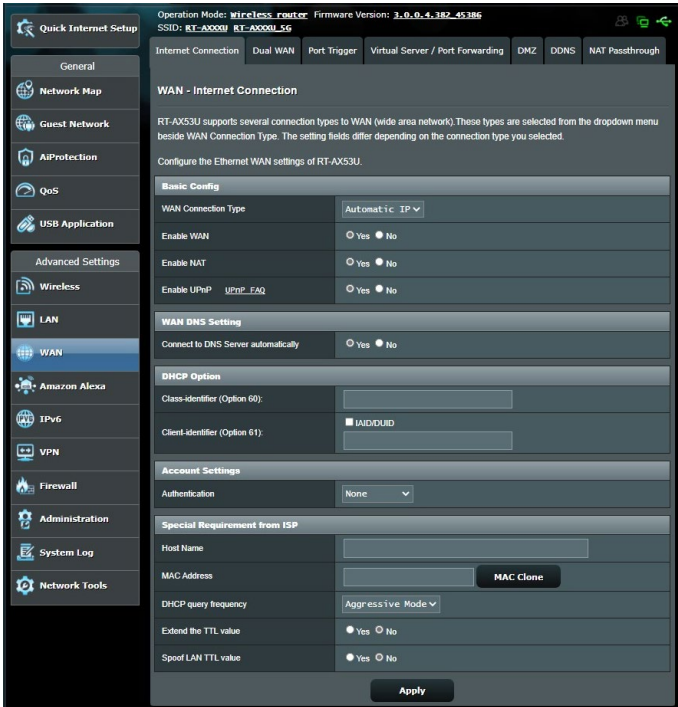
Router nirkabel mendukung sambungan ke layanan IPTV melalui ISP atau LAN. Tab IPTV menyediakan pengaturan konfigurasi yang diperlukan untuk mengkonfigurasi IPTV, VoIP, multicast, dan UDP bagi layanan. Untuk informasi spesifik tentang layanan, hubungi ISP Anda.



## 4.3 WAN

### 4.3.1 Sambungan Internet

Layar Internet Connection (Sambungan Internet) memungkinkan Anda mengkonfigurasi pengaturan berbagai jenis sambungan WAN.



Untuk mengkonfigurasi pengaturan sambungan WAN:

1. Dari panel navigasi, buka tab **Advanced Settings (Pengaturan Lanjutan) > WAN > Internet Connection (Sambungan Internet)**.
2. Konfigurasi pengaturan berikut. Setelah selesai, klik **Apply (Terapkan)**.
  - **WAN Connection Type (Jenis Sambungan WAN):** Pilih jenis Penyedia Layanan Internet. Pilihan yang tersedia adalah **Automatic IP (IP Otomatis)**, **PPPoE**, **PPTP**, **L2TP**, atau **Static IP (IP Statis)**. Hubungi ISP jika router tidak dapat memperoleh alamat IP yang valid atau jika Anda tidak yakin tentang jenis sambungan WAN.

- **Enable WAN (Aktifkan WAN):** Pilih **Yes (Ya)** untuk mengizinkan akses Internet router. Pilih **No (Tidak)** untuk menonaktifkan akses Internet.
- **Enable NAT (Aktifkan NAT):** NAT (Network Address Translation) adalah sistem yang memungkinkan penggunaan satu IP publik (WAN IP) untuk menyediakan akses Internet bagi klien jaringan dengan alamat IP pribadi di LAN. Alamat IP pribadi dari setiap klien jaringan akan disimpan dalam tabel NAT dan digunakan untuk merutekan paket data yang masuk.
- **Enable UPnP (Aktifkan UPnP):** UPnP (Universal Plug and Play) memungkinkan beberapa perangkat (seperti router, televisi, sistem stereo, konsol game, dan ponsel) dikontrol via jaringan berbasis IP dengan atau tanpa kontrol pusat melalui gateway. UPnP akan menyambungkan PC dari semua bentuk dan ukuran, yang menyediakan jaringan lancar untuk konfigurasi dan transfer data jarak jauh. Dengan menggunakan UPnP, perangkat jaringan baru akan ditemukan secara otomatis. Setelah tersambung ke jaringan, perangkat dapat dikonfigurasi dari jauh untuk mendukung aplikasi P2P, game interaktif, konferensi video, dan server web atau proxy. Tidak seperti Penerusan port, yang terkait dengan konfigurasi pengaturan port secara manual, UPnP akan secara otomatis mengkonfigurasi router untuk menerima sambungan masuk dan mengarahkan permintaan ke PC tertentu di jaringan lokal.
- **Connect to DNS Server (Sambungkan ke Server DNS):** Memungkinkan router ini secara otomatis mendapatkan alamat IP DNS dari ISP. DNS adalah host di Internet yang menerjemahkan nama Internet menjadi alamat IP numerik.
- **Authentication (Otentikasi):** Pilihan ini dapat ditentukan oleh beberapa ISP. Hubungi ISP dan isi jika diminta.

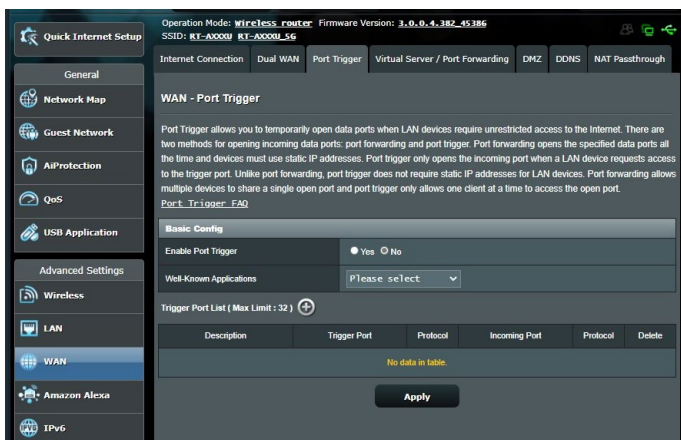


- **Host Name (Nama Host):** Kolom ini memungkinkan Anda memberikan nama host untuk router. Nama host biasanya merupakan persyaratan khusus dari ISP. Jika ISP menetapkan nama host untuk komputer Anda, masukkan nama host tersebut di sini.
- **MAC Address (Alamat MAC):** Alamat MAC (Media Access Control) adalah pengidentifikasi unik untuk perangkat jaringan. Beberapa ISP akan memantau alamat MAC perangkat jaringan yang tersambung ke layanan dan menolak perangkat tidak dikenal yang berupaya menyambung. Untuk menghindari masalah sambungan karena alamat MAC tidak terdaftar, Anda dapat:
  - Menghubungi ISP dan memperbarui alamat MAC yang terhubung dengan layanan ISP.
  - Menyalin atau mengubah alamat MAC router nirkabel ASUS untuk menyesuaikan dengan alamat MAC perangkat jaringan terdahulu yang dikenali oleh ISP.

## 4.3.2 Pemicu Port

Pemicuan rentang port akan membuka port masuk yang telah ditentukan selama periode waktu terbatas setiap kali klien di jaringan area lokal membuat sambungan keluar ke port tertentu. Pemicuan port digunakan dalam skenario berikut:

- Beberapa klien lokal memerlukan penerusan port untuk aplikasi yang sama pada waktu berbeda.
- Aplikasi memerlukan port masuk khusus yang berbeda dari port keluar.



### Untuk mengkonfigurasi Pemicu Port:

1. Dari panel navigasi, buka tab **Advanced Settings (Pengaturan Lanjutan) > WAN > Port Trigger (Pemicu Port)**.
2. Konfigurasi pengaturan berikut di bawah ini. Setelah selesai, klik **Apply (Terapkan)**.
  - **Mengaktifkan Port Trigger (Pemicu Port):** Pilih **Yes (Ya)** untuk mengaktifkan Port Trigger (Pemicu Port).
  - Pada kolom **Well-Known Applications (Aplikasi Terkenal)**, pilih game dan layanan web populer untuk ditambahkan ke Daftar Pemicu Port.

- **Description (Keterangan):** Masukkan nama atau keterangan singkat untuk layanan.
  - **Trigger Port (Port Pemicu):** Tentukan port pemicu untuk membuka port masuk.
  - **Protocol (Protokol):** Pilih protokol, TCP, atau UDP.
  - **Incoming Port (Port Masuk):** Tentukan port masuk untuk menerima data masuk dari Internet.
- 

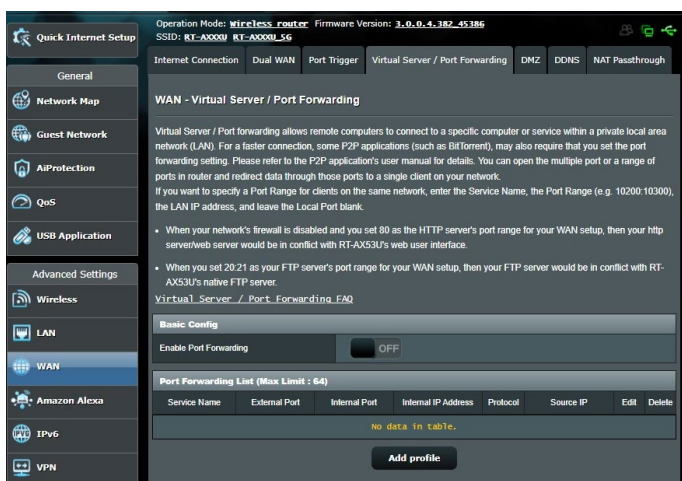
#### **CATATAN:**

- Saat menyambung ke server IRC, PC klien akan membuat sambungan keluar menggunakan rentang port pemicu 66660-7000. Server IRC akan merespons dengan memverifikasi nama pengguna dan membuat sambungan baru ke PC klien menggunakan port masuk.
  - Jika Pemicu Port dinonaktifkan, maka router akan menghentikan sambungan karena tidak mampu menentukan PC yang meminta akses IRC. Bila Pemicu Port diaktifkan, maka router akan menetapkan port masuk untuk menerima data masuk. Port masuk ini akan tertutup setelah periode waktu tertentu karena router tidak yakin kapan aplikasi dihentikan.
  - Pemicuan port hanya mengizinkan satu klien di jaringan untuk menggunakan layanan dan port masuk tertentu secara bersamaan.
  - Anda tidak dapat menggunakan aplikasi yang sama untuk memicu port di beberapa PC secara bersamaan. Router hanya akan meneruskan port kembali ke komputer terakhir untuk mengirim permintaan/pemicu ke router.
-

### 4.3.3 Server Virtual/Penerusan Port

Penerusan port adalah metode pengarahannya lalu lintas jaringan dari Internet ke port tertentu maupun rentang port tertentu ke satu atau beberapa perangkat di jaringan lokal. Dengan mengkonfigurasi Penerusan Port di router, PC di luar jaringan dapat mengakses layanan tertentu yang disediakan oleh PC di jaringan Anda.

**CATATAN:** Bila penerusan port diaktifkan, router ASUS akan memblokir lalu lintas masuk yang tidak diinginkan dari Internet dan hanya membolehkan jawaban atas permintaan luar dari LAN. Klien jaringan tidak memiliki akses langsung ke Internet, begitu juga sebaliknya.



#### Untuk mengkonfigurasi Penerusan Port:

1. Dari panel navigasi, buka tab **Advanced Settings (Pengaturan Lanjutan) > WAN > Virtual Server/Port Forwarding (Server Virtual/Penerusan Port)**.
2. Konfigurasi pengaturan berikut di bawah ini. Setelah selesai, klik **Apply (Terapkan)**.
  - **Penerusan Port:** Pilih **Yes (Ya)** untuk mengaktifkan Port Forwarding (Penerusan Port).

- Pada kolom **Famous Server List (Daftar Server Terkenal)**, pilih jenis layanan yang akan diakses.
- Pada kolom **Famous Game List (Daftar Game Terkenal)**, pilih game populer yang akan diakses. Pilihan ini berisi port yang diperlukan agar game online populer pilihan dapat berjalan dengan benar.
- **Port Server FTP:** Hindari penetapan rentang port 20:21 untuk FTP karena akan bertentangan dengan tugas server FTP awal router.
- **Service Name (Nama Layanan):** Masukkan nama layanan.
- **Port Range (Rentang Port):** Jika ingin menentukan Rentang Port untuk klien di jaringan yang sama, masukkan Nama Layanan, Rentang Port (misalnya, 10200:10300), alamat IP LAN, dan kosongkan Port Lokal. Rentang port menerima berbagai format seperti Rentang Port (300:350), masing-masing port (566,789), atau Campuran (1015:1024,3021).

---

#### **CATATAN:**

- Bila firewall jaringan dinonaktifkan dan Anda menetapkan 80 sebagai rentang port server HTTP untuk konfigurasi WAN, maka server http/server web akan konflik dengan antarmuka pengguna web router.
  - Jaringan menggunakan port agar dapat bertukar data, dengan penetapan nomor dan tugas khusus untuk setiap port. Misalnya, port 80 digunakan untuk HTTP. Port khusus hanya dapat digunakan oleh satu aplikasi atau layanan pada satu waktu. Oleh karena itu, upaya dua PC untuk mengakses data melalui port yang sama secara bersamaan akan gagal. Misalnya, Anda tidak dapat mengkonfigurasi Penerusan Port untuk port 100 di dua PC secara bersamaan.
-

- **Local IP (IP Lokal):** Masukkan alamat IP LAN klien.
- 

**CATATAN:** Gunakan alamat IP statis untuk klien lokal agar penerusan port berfungsi dengan benar. Untuk informasi, lihat bagian "**4.2 LAN**".

---

- **Local Port (Port Lokal):** Masukkan port khusus untuk menerima paket yang diteruskan. Kosongkan kolom ini jika ingin agar paket masuk diarahkan kembali ke rentang port yang ditentukan.
- **Protocol (Protokol):** Pilih protokol. Jika tidak yakin, pilih **BOTH** (Keduanya).

### **Untuk memeriksa apakah Penerusan Port berhasil dikonfigurasi:**

- Pastikan server atau aplikasi siap digunakan.
- Anda akan memerlukan klien di luar LAN, namun memiliki akses Internet (disebut "klien Internet"). Klien ini tidak boleh disambungkan ke router ASUS.
- Di klien Internet, gunakan IP WAN router untuk mengakses server. Jika penerusan port berhasil, Anda dapat mengakses file atau aplikasi.

### **Perbedaan antara pemicu port dan penerusan port:**

- Pemicuan port akan berfungsi meskipun tanpa mengkonfigurasi alamat IP LAN khusus. Tidak seperti penerusan port, yang memerlukan alamat IP LAN statis, pemicuan port memungkinkan penerusan port dinamis menggunakan router. Rentang port yang telah ditentukan akan dikonfigurasi untuk menerima sambungan masuk selama periode waktu tertentu. Pemicuan port memungkinkan beberapa komputer menjalankan aplikasi yang biasanya memerlukan penerusan port yang sama secara manual ke setiap PC di jaringan.
- Pemicuan port lebih aman dibandingkan penerusan port karena port masuk tidak terbuka sepanjang waktu. Port masuk hanya akan terbuka bila aplikasi membuat sambungan keluar melalui port pemicu.

### 4.3.4 DMZ

DMZ virtual akan menampilkan satu klien di Internet sehingga dapat menerima semua paket masuk yang diarahkan ke Jaringan Area Lokal.

Lalu lintas masuk dari Internet biasanya akan diabaikan dan dirutekan ke klien khusus hanya setelah penerusan port atau pemicu port dikonfigurasi di jaringan. Pada konfigurasi DMZ, satu klien jaringan akan menerima semua paket masuk.

Mengkonfigurasi DMZ di jaringan akan berguna bila port masuk perlu dibuka atau Anda ingin meng-host server domain, web, maupun email.

---

**PERHATIAN!** Membuka akses semua port di klien ke Internet akan membuat jaringan rentan terhadap serangan dari luar. Waspadai risiko keamanan terkait penggunaan DMZ.

---

#### Untuk mengkonfigurasi DMZ:

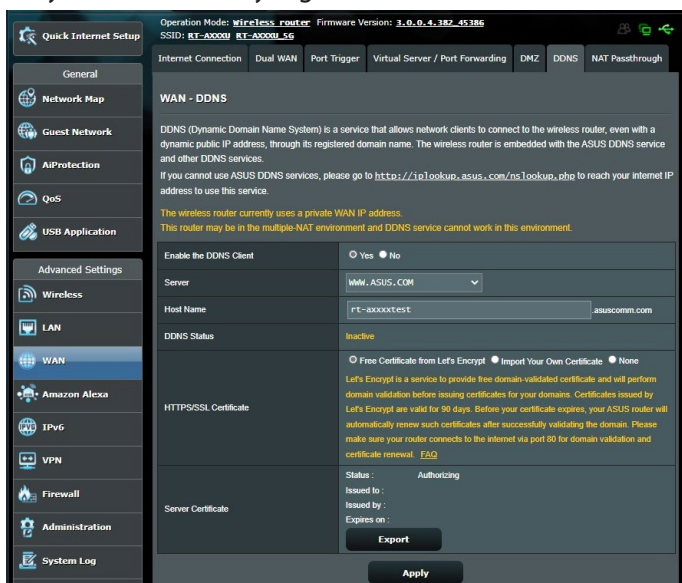
1. Dari panel navigasi, buka tab **Advanced Settings (Pengaturan Lanjutan) > WAN > DMZ**.
2. Konfigurasi pengaturan di bawah ini. Setelah selesai, klik **Apply (Terapkan)**.
  - **IP address of Exposed Station (Alamat IP Stasiun yang Ditampilkan):** Masukkan alamat IP LAN klien yang akan menyediakan layanan DMZ dan ditampilkan di Internet. Pastikan klien server memiliki alamat IP statis.

#### Untuk menghapus DMZ:

1. Hapus alamat IP LAN klien dari kotak teks **IP Address of Exposed Station (Alamat IP Stasiun yang Ditampilkan)**.
2. Setelah selesai, klik **Apply (Terapkan)**.

## 4.3.5 DDNS

Mengkonfigurasi DDNS (DNS Dinamis) memungkinkan Anda mengakses router dari luar jaringan melalui Layanan DDNS ASUS atau layanan DDNS lain yang tersedia.



### Untuk mengkonfigurasi DDNS:

1. Dari panel navigasi, buka tab **Advanced Settings (Pengaturan Lanjutan) > WAN > DDNS**.
2. Konfigurasi pengaturan berikut. Setelah selesai, klik **Apply (Terapkan)**.
  - **Enable the DDNS Client (Aktifkan Klien DDNS):** Aktifkan DDNS untuk mengakses router ASUS melalui nama DNS, bukan alamat IP WAN.
  - **Server and Host Name (Server dan Nama Host):** Pilih DDNS ASUS atau DDNS lain. Jika ingin menggunakan DDNS ASUS, masukkan Nama Host dalam format xxx.asuscomm.com (xxx adalah nama host Anda).
  - Jika ingin menggunakan layanan DDNS lain, klik **FREE TRIAL (Uji Coba Gratis)** dan daftar secara online terlebih dulu. Isi kolom Nama Pengguna atau Alamat Email dan Sandi, maupun Kode DDNS.



- **Enable wildcard (Aktifkan wildcard):** Aktifkan wildcard jika layanan DDNS memerlukannya.

---

## CATATAN:

Layanan DDNS tidak akan berfungsi dalam kondisi berikut:

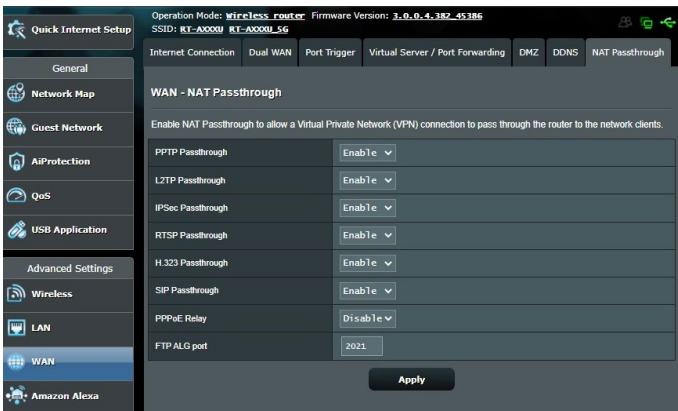
- Bila router nirkabel menggunakan alamat IP WAN pribadi (192.168.x.x, 10.x.x.x, atau 172.16.x.x), sebagaimana ditunjukkan pada teks berwarna kuning.
- Router mungkin berada di jaringan yang menggunakan beberapa tabel NAT.

---

### 4.3.6 Passthrough NAT

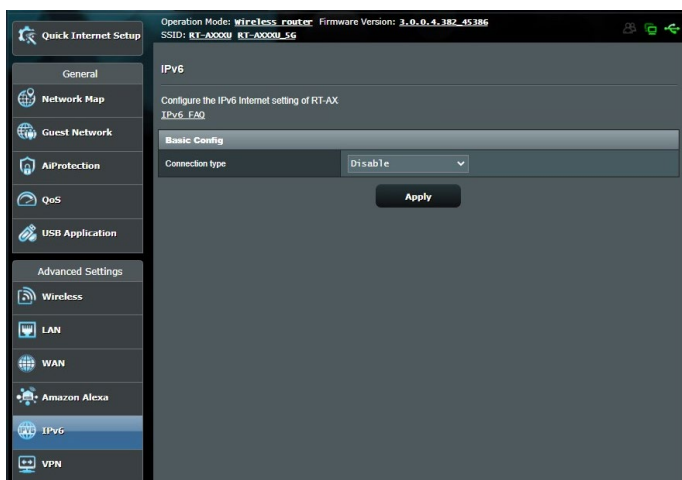
Passthrough NAT memungkinkan sambungan VPN (Virtual Private Network) melewati router ke klien jaringan. Passthrough PPTP, Passthrough L2TP, Passthrough IPsec, dan Passthrough RTSP akan diaktifkan secara default.

Untuk mengaktifkan/menonaktifkan pengaturan Passthrough NAT, buka tab **Advanced Settings (Pengaturan Lanjutan) > WAN > NAT Passthrough (Passthrough NAT)**. Setelah selesai, klik **Apply (Terapkan)**.



## 4.4 IPv6

Router nirkabel ini mendukung alamat IPv6, yaitu sistem yang mendukung alamat IP. Standar ini belum tersedia secara luas. Hubungi ISP (Penyedia Layanan Internet) jika layanan Internet Anda mendukung IPv6.



### Untuk mengkonfigurasi IPv6:

1. Dari panel navigasi, buka **Advanced Settings (Pengaturan Lanjutan) > IPv6**.
2. Pilih **Connection Type (Jenis Sambungan)**. Pilihan konfigurasi berbeda, tergantung pada jenis sambungan yang dipilih.
3. Masukkan pengaturan IPv6 LAN dan DNS.
4. Klik **Apply (Terapkan)**.

---

**CATATAN:** Lihat ISP (Penyedia Layanan Internet) tentang informasi IPv6 tertentu untuk layanan Internet.

---

## 4.5 Firewall

Router nirkabel dapat berfungsi sebagai firewall perangkat keras untuk jaringan.

---

**CATATAN:** Fitur Firewall akan diaktifkan secara default.

---

### 4.5.1 Umum

**Untuk mengkonfigurasi pengaturan dasar Firewall:**

1. Dari panel navigasi, buka tab **Advanced Settings (Pengaturan Lanjutan) > Firewall > General (Umum)**.
2. Pada kolom **Enable Firewall (Aktifkan Firewall)**, pilih **Yes (Ya)**.
3. Di **Enable DoS protection (Aktifkan perlindungan DoS)**, pilih **Yes (Ya)** untuk melindungi jaringan dari serangan DoS (Denial of Service). Namun, cara ini dapat mempengaruhi performa router.
4. Anda juga dapat memantau pertukaran paket antara sambungan LAN dan WAN. Pada Logged packets type (Jenis paket yang tercatat), pilih **Dropped (Dihentikan), Accepted (Diterima)**, atau **Both (Keduanya)**.
5. Klik **Apply (Terapkan)**.

### 4.5.2 Filter URL


Anda dapat menentukan kata kunci atau alamat web untuk mencegah akses ke URL tertentu.

---

**CATATAN:** Filter URL didasarkan pada permintaan DNS. Jika klien jaringan telah mengakses situs web seperti `http://www.abcxxx.com`, maka situs web tersebut tidak akan diblokir (cache DNS dalam sistem akan menyimpan situs web yang sebelumnya dikunjungi). Untuk mengatasi masalah ini, kosongkan cache DNS sebelum mengkonfigurasi Filter URL.

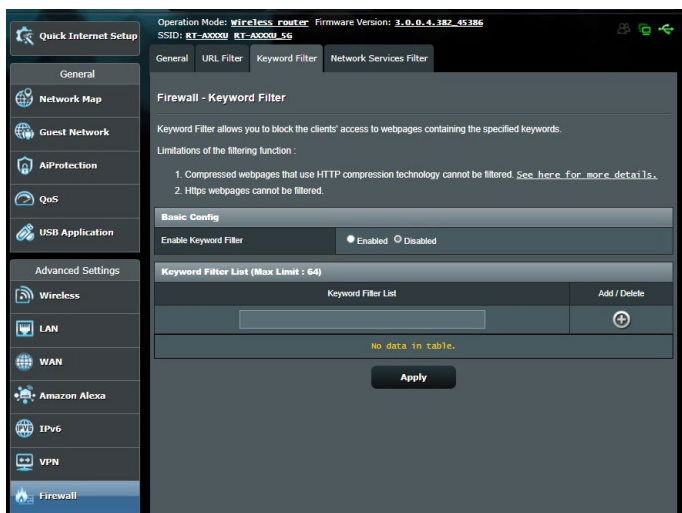
---

## Untuk mengkonfigurasi filter URL:

1. Dari panel navigasi, buka tab **Advanced Settings (Pengaturan Lanjutan) > Firewall > URL Filter (Filter URL)**.
2. Pada kolom **Enable URL Filter (Aktifkan Filter URL)**, pilih **Enabled (Diaktifkan)**.
3. Masukkan URL, lalu klik tombol .
4. Klik **Apply (Terapkan)**.

### 4.5.3 Filter kata kunci

Filter kata kunci akan memblokir akses ke halaman web berisi kata kunci tertentu.



## Untuk mengkonfigurasi filter kata kunci:

1. Dari panel navigasi, buka tab **Advanced Settings (Pengaturan Lanjutan) > Firewall > Keyword Filter (Filter Kata Kunci)**.
2. Pada kolom **Enable Keyword Filter (Aktifkan Filter Kata Kunci)**, pilih **Enabled (Diaktifkan)**.
3. Masukkan kata atau frasa, lalu klik tombol **Add (Tambah)**.

#### 4. Klik **Apply (Terapkan)**.

#### CATATAN:

- Filter Kata Kunci didasarkan pada permintaan DNS. Jika klien jaringan telah mengakses situs web seperti <http://www.abcxxx.com>, maka situs web tersebut tidak akan diblokir (cache DNS dalam sistem akan menyimpan situs web yang sebelumnya dikunjungi). Untuk mengatasi masalah ini, kosongkan cache DNS sebelum mengkonfigurasi Filter Kata Kunci.
- Halaman web yang dikompresi menggunakan kompresi HTTP tidak dapat difilter. Halaman HTTPS juga tidak dapat diblokir menggunakan filter kata kunci.

### 4.5.4 Filter Layanan Jaringan

Filter Layanan Jaringan akan memblokir pertukaran paket LAN ke WAN dan membatasi klien jaringan dari akses ke layanan web tertentu seperti Telnet atau FTP.

The screenshot shows the configuration page for the Firewall - Network Services Filter. The interface includes a sidebar with navigation options like General, Network Map, Guest Network, AllProtection, QoS, USB Application, and Advanced Settings (Wireless, LAN, WAN, Amazon Alexa, IPv6, VPN, Firewall, Administration, System Log, Network Tools). The main content area is titled "Firewall - Network Services Filter" and contains the following information:


- Operation Mode:** wireless\_router, **Firmware Version:** 3.0.0.4.382\_45386
- SSID:** RT-XXXXX, **RT-XXXXX\_56**
- General** | URL Filter | Keyword Filter | **Network Services Filter**
- Firewall - Network Services Filter**
- The Network Services filter blocks the LAN to WAN packet exchanges and restricts devices from using specific network services. For example, if you do not want the device to use the Internet service, key in 00 in the destination port. The traffic that uses port 80 will be blocked (but https can not be blocked). Leave the source IP field blank to apply this rule to all LAN devices.
- Deny List Duration:** During the scheduled duration, clients in the Deny List cannot use the specified network services. After the specified duration, all the clients in LAN can access the specified network services.
- Allow List Duration:** During the scheduled duration, clients in the Allow List can ONLY use the specified network.
- NOTE:** If you set the subnet for the Allow List, IP addresses outside the subnet will not be able to access the Internet or any Internet service.
- \*Reminder:** The system time zone is different from your local setting.
- Network Services Filter**
- Enable Network Services Filter:**  Yes  No
- Filter table type:** Deny List
- Well-Known Applications:** User Defined
- Date to Enable LAN to WAN Filter:**  Mon  Tue  Wed  Thu  Fri
- Time of Day to Enable LAN to WAN Filter:** 00 : 00 - 23 : 59
- Date to Enable LAN to WAN Filter:**  Sat  Sun
- Time of Day to Enable LAN to WAN Filter:** 00 : 00 - 23 : 59
- Filtered ICMP packet types:**
- Network Services Filter Table (Max Limit : 32)**

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

No data in table.

**Apply**

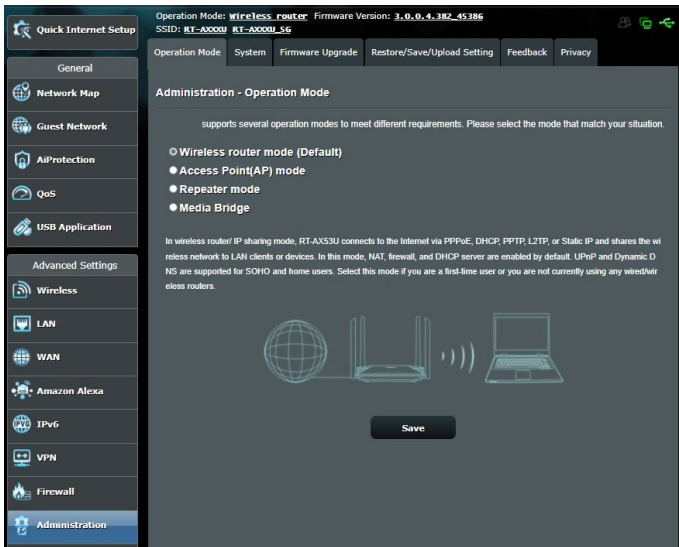
## Untuk mengkonfigurasi Filter Layanan Jaringan:

1. Dari panel navigasi, buka tab **Advanced Settings (Pengaturan Lanjutan) > Firewall > Network Service Filter (Filter Layanan Jaringan)**.
2. Pada kolom Enable Network Services Filter Aktifkan Filter Layanan Jaringan, pilih **Yes (Ya)**.
3. Pilih jenis tabel Filter. **Black List (Daftar Hitam)** akan memblokir layanan jaringan yang ditentukan. **White List (Daftar Putih)** akan membatasi akses hanya ke layanan jaringan yang ditentukan.
4. Tentukan hari dan waktu saat filter aktif.
5. Untuk menentukan Layanan Jaringan yang akan difilter, masukkan IP Sumber, IP Tujuan, Rentang Port, dan Protokol. Klik tombol .
6. Klik **Apply (Terapkan)**.

## 4.6 Administrasi

### 4.6.1 Mode Pengoperasian

Halaman Operation Mode (Mode Pengoperasian) memungkinkan Anda memilih mode yang sesuai untuk jaringan.



**Untuk mengkonfigurasi mode pengoperasian:**

1. Dari panel navigasi, buka tab **Advanced Settings (Pengaturan Lanjutan)** > **Administration (Administrasi)** > **Operation Mode (Mode Pengoperasian)**.
2. Pilih salah satu mode pengoperasian berikut:
  - **Mode route nirkabel (default):** Dalam mode ini, router nirkabel akan menyambung ke Internet dan menyediakan akses Internet untuk perangkat yang tersedia di jaringan lokal.
  - **Mode AP (Jalur Akses):** Dalam mode ini, router akan membuat jaringan nirkabel baru di jaringan yang ada.
  - **Mode repeater:** Mode ini mengubah router menjadi repeater nirkabel untuk memperluas jangkauan sinyal Anda.
3. Klik **Apply (Terapkan)**.

**CATATAN:** Router akan menjalankan boot ulang bila Anda mengubah mode.

## 4.6.2 Sistem

Halaman **System (Sistem)** memungkinkan Anda mengkonfigurasi pengaturan router nirkabel.

**Untuk mengkonfigurasi pengaturan sistem:**

1. Dari panel navigasi, buka tab **Advanced Settings (Pengaturan Lanjutan) > Administration (Administrasi) > System (Sistem)**.
2. Anda dapat mengkonfigurasi pengaturan berikut:
  - **Change router login password (Ubah sandi login router):** Anda dapat mengubah sandi dan nama login router nirkabel dengan memasukkan nama dan sandi baru.
  - **Aktivitas tombol WPS:** Tombol WPS pada router nirkabel dapat digunakan untuk mengaktifkan WPS atau menonaktifkan jaringan nirkabel.
  - **Time Zone (Zona Waktu):** Pilih zona waktu untuk jaringan.
  - **NTP Server (Server NTP):** Router nirkabel dapat mengakses server NTP (Network Time Protocol) untuk mensinkronisasikan waktu.
  - **Enable Telnet (Aktifkan Telnet):** Klik **Yes (Ya)** untuk mengaktifkan layanan Telnet di jaringan. Klik **No (Tidak)** untuk menonaktifkan Telnet.
  - **Authentication Method (Metode Otentikasi):** Anda dapat memilih HTTP, HTTPS, atau kedua protokol untuk mengamankan akses router.
  - **Enable Web Access from WAN (Aktifkan Akses Web dari WAN):** Pilih **Yes (Ya)** agar perangkat di luar jaringan dapat mengakses pengaturan GUI router nirkabel. Pilih **No (Tidak)** untuk mencegah akses tersebut.
  - **Allow only specified IP address (Bolehkan hanya alamat IP yang ditetapkan):** Klik **Yes (Ya)** jika ingin menetapkan alamat IP perangkat yang diperbolehkan mengakses pengaturan GUI router nirkabel dari WAN.
  - **Daftar Klien:** Masukkan alamat WAN IP (IP WAN) perangkat jaringan yang diizinkan untuk mengakses pengaturan router nirkabel. Daftar ini akan digunakan jika Anda mengklik **Yes (Ya)** pada item **Only allow specific IP (Bolehkan hanya IP tertentu)**.
3. Klik **Apply (Terapkan)**.



### 4.6.3 Upgrade Firmware

---

**CATATAN:** Download firmware terbaru dari situs web ASUS di <http://www.asus.com>.

---

**Untuk meng-upgrade firmware:**

1. Dari panel navigasi, buka tab **Advanced Settings (Pengaturan Lanjutan) > Administration (Administrasi) > Firmware Upgrade (Upgrade Firmware)**.
  2. Pada kolom **New Firmware File (File Firmware Baru)**, klik **Browse (Telusuri)** untuk mencari file yang telah di-download.
  3. Klik **Upload**.
- 

**CATATAN:**

- Setelah proses upgrade selesai, tunggu beberapa saat sementara sistem menjalankan boot ulang.
  - Jika proses upgrade gagal, router nirkabel akan secara otomatis beralih ke mode penyelamatan dan indikator LED daya di panel depan akan mulai berkedip perlahan. Untuk memulihkan atau mengembalikan sistem, lihat bagian **5.2 Pengembalian Firmware**.
- 

### 4.6.4 Mengembalikan/Menyimpan/Meng-upload Pengaturan

**Untuk mengembalikan/menyimpan/meng-upload pengaturan router nirkabel:**

1. Dari panel navigasi, buka tab **Advanced Settings (Pengaturan Lanjutan) > Administration (Administrasi) > Restore/Save/Upload Setting (Kembalikan/Simpan/Upload Pengaturan)**.
  2. Pilih tugas yang akan dijalankan:
    - Untuk mengembalikan pengaturan default pabrik, klik **Restore (Kembalikan)**, lalu klik **OK** pada pesan konfirmasi.
    - Untuk menyimpan pengaturan sistem aktif, klik **Save (Simpan)**, arahkan ke folder tempat penyimpanan file, lalu klik **Save (Simpan)**.
    - Untuk mengembalikan dari file pengaturan sistem yang tersimpan, klik **Browse (Telusuri)** agar dapat mencari file, lalu klik **Upload**.
- 

**PENTING!** Jika terjadi masalah, upload firmware versi terbaru, lalu konfigurasi pengaturan baru. Jangan kembalikan router ke pengaturan default.

---

## 4.7 Log Sistem

System Log (Log Sistem) berisi aktivitas jaringan yang tercatat.

**CATATAN:** Log sistem akan diatur ulang bila router menjalankan boot ulang atau dimatikan.

### Untuk melihat log sistem:

1. Dari panel navigasi, buka **Advanced Settings (Pengaturan Lanjutan) > System Log (Log Sistem)**.
2. Anda dapat melihat aktivitas jaringan di salah satu tab berikut:
  - General Log (Log Umum)
  - Wireless Log (Log Nirkabel)
  - DHCP Leases (Waktu Aktif DHCP)
  - IPv6
  - Routing Table (Tabel Routing)
  - Port Forwarding (Penerusan Port)
  - Connections (Sambungan)

The screenshot displays the 'System Log - General Log' page in a web browser. The interface includes a left-hand navigation menu with options like 'General', 'Network Map', 'Guest Network', 'AIProtection', 'QoS', 'USB Application', 'Advanced Settings', 'Wireless', 'LAN', 'WAN', 'Amazon Alexa', 'IPv6', 'VPN', 'Firewall', 'Administration', 'System Log', and 'Network Tools'. The main content area shows the 'System Log - General Log' section with a sub-header 'This page shows the detailed system's activities.' Below this, the 'System Time' is 'Fri, May 27 08:54:48 2022'. The 'Update' section shows '11 days 2 hour(s) 37 minute(s) 56 seconds'. There is a 'Remote Log Server' field with the value '514' and a note: '\* The default port is 514. If you reconfigured the port number, please make sure that the remote log server or IoT devices settings match your current configuration.' An 'Apply' button is visible. The log entries themselves are a list of kernel messages, such as 'May 27 08:33:02 kernel: [568570.636880] McCmdChannelSwitch: ctrl\_ch1=157, ctrl\_ch2=0, cent\_ch=157, Rsp:'. At the bottom, there are 'Clear' and 'Save' buttons, and a footer with 'Help & Support', 'Manual', 'Product Registration', 'Feedback', and 'FAQ'.

## 5 Utilitas

### CATATAN:

- Download dan instal utilitas router nirkabel dari situs web ASUS:
  - Device Discovery v1.4.7.1 di <http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Discovery.zip>
  - Firmware Restoration v1.9.0.4 di <http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Rescue.zip>
- Utilitas ini tidak didukung di OS MAC.

### 5.1 Pencarian Perangkat

Device Discovery (Pencarian Perangkat) adalah utilitas WLAN ASUS yang mendeteksi router nirkabel ASUS yang ada di jaringan nirkabel dan dapat digunakan untuk mengkonfigurasi perangkat.

#### Untuk mengaktifkan utilitas Pencarian Perangkat:

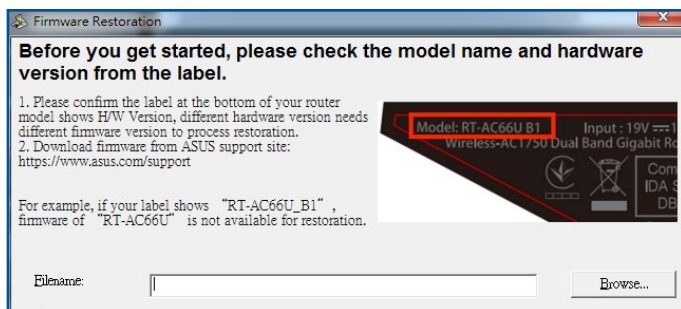
- Klik **Start (Mulai) > All Programs (Semua Program) > ASUS Utility (Utilitas ASUS) > Wireless Router (Router Nirkabel RT-AX53U) > Device Discovery (Pencarian Perangkat)**



**CATATAN:** Bila menetapkan router ke Access Point mode (Mode Jalur Akses), Anda harus menggunakan Device Discovery (Pencarian Perangkat) untuk mendapatkan alamat IP router.

## 5.2 Pengembalian Firmware

Firmware Restoration (Pengembalian Firmware) digunakan pada Router Nirkabel ASUS setelah upgrade firmware gagal. Utilitas ini akan meng-upload file firmware ke router nirkabel. Proses ini memerlukan waktu sekitar 3 hingga 4 menit.



---

**PENTING!** Aktifkan mode perbaikan sebelum menggunakan utilitas Firmware Restoration (Pengembalian Firmware).

---

**CATATAN:** Fitur ini tidak didukung di MAC OS.

---

## **Untuk mengaktifkan mode perbaikan dan menggunakan utilitas Firmware Restoration (Pengembalian Firmware):**

1. Lepas router nirkabel dari catu dayanya.
2. Sambil menekan terus tombol Atur Ulang di bagian belakang router nirkabel, sambungkan router nirkabel ke catu daya. Lepas tombol Atur Ulang saat LED Daya di panel depan mulai berkedip perlahan, yang menunjukkan bahwa router nirkabel sedang menjalankan mode perbaikan.
3. Gunakan yang berikut untuk mengkonfigurasi pengaturan TCP/IP:  
**Alamat IP:** 192.168.1.x  
**Subnet mask:** 255.255.255.0
4. Dari desktop komputer, klik **Start (Mulai) > All Programs (Semua Program) > ASUS Utility (Utilitas ASUS) > Wireless Router (Router Nirkabel) > Firmware Restoration (Pengembalian Firmware)**.
5. Klik **Browse (Cari)** untuk menavigasi ke file firmware, lalu klik **Upload**.

---

**CATATAN:** Utilitas Firmware Restoration (Pengembalian Firmware) tidak digunakan untuk meng-upgrade firmware Router Nirkabel ASUS yang sedang digunakan. Upgrade firmware biasa harus dilakukan melalui GUI Web. Untuk informasi rinci, lihat **Bab 4: Mengkonfigurasi Pengaturan Lanjutan**.

---

## 6 Mengatasi Masalah

Bab ini berisi solusi masalah yang mungkin Anda temui pada router. Jika Anda menemukan masalah yang tidak disebutkan dalam bab ini, kunjungi situs dukungan ASUS di:

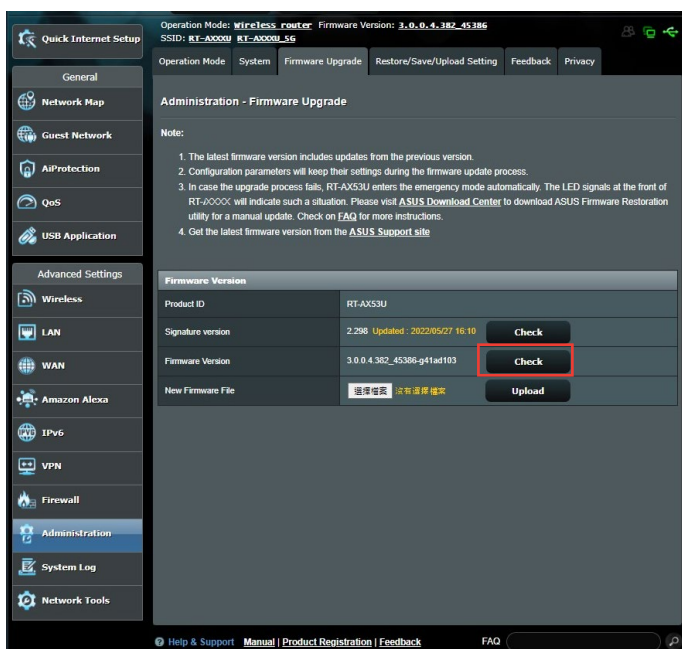
<https://www.asus.com/support/> untuk informasi lebih lanjut tentang produk dan informasi kontak Dukungan Teknis ASUS.

### 6.1 Mengatasi Masalah Mendasar

Jika Anda mengalami masalah pada router, coba langkah-langkah dasar di bagian ini sebelum mencari solusi lebih lanjut.

#### Upgrade Firmware ke versi terbaru.

1. Aktifkan GUI web. Buka tab **Advanced Settings (Pengaturan Lanjutan)** > **Administration (Administrasi)** > **Firmware Upgrade (Upgrade Firmware)**. Klik **Check (Periksa)** untuk memastikan ketersediaan firmware terbaru.



2. Jika firmware terbaru tersedia, kunjungi situs web global ASUS di <https://www.asus.com/Networking/RT-AX53U/HelpDesk/Download/> untuk men-download firmware terbaru.
3. Dari halaman **Firmware Upgrade (Upgrade Firmware)**, klik **Browse (Telusuri)** untuk mencari file firmware.
4. Untuk meng-upgrade firmware, klik **Upload**.

### **Hidupkan ulang jaringan dengan urutan berikut:**

1. Matikan modem.
2. Lepas sambungan modem.
3. Matikan router dan komputer.
4. Sambungkan modem.
5. Hidupkan modem, lalu tunggu selama 2 menit.
6. Hidupkan router, lalu tunggu selama 2 menit.
7. Hidupkan komputer.

### **Pastikan kabel Ethernet telah terpasang dengan benar.**

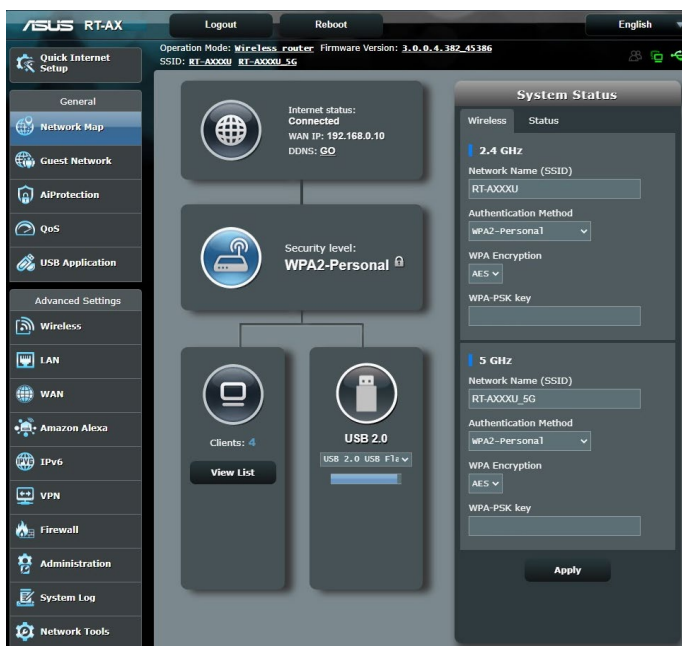
- Bila kabel Ethernet penyambung router dan modem terpasang dengan benar, maka LED WAN akan aktif.
- Bila kabel Ethernet penyambung komputer yang menyala dengan router terpasang dengan benar, maka LED LAN akan aktif.

### **Pastikan pengaturan nirkabel di komputer sudah sesuai.**

- Bila Anda menyambungkan komputer ke router secara nirkabel, pastikan SSID (nama jaringan nirkabel), metode enkripsi, dan sandi sudah benar.

## Pastikan pengaturan jaringan sudah benar.

- Setiap klien di jaringan harus memiliki alamat IP yang valid. ASUS menyarankan agar Anda menggunakan server DHCP router nirkabel untuk menetapkan alamat IP ke komputer di jaringan.
- Sejumlah penyedia layanan modem berkabel mengharuskan Anda menggunakan alamat MAC komputer yang awalnya didaftarkan di akun. Anda dapat melihat alamat MAC di GUI web, halaman **Network Map (Peta Jaringan) > Clients (Klien)**, lalu mengarahkan kursor perangkat ke **Client Status (Status Klien)**.





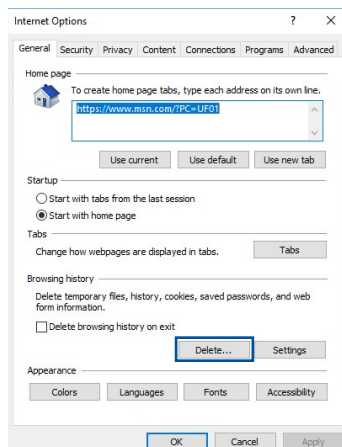
## 6.2 Tanya Jawab

### Saya tidak dapat mengakses GUI router menggunakan browser web

- Jika komputer tersambung, periksa sambungan kabel Ethernet dan status LED sebagaimana dijelaskan di bagian sebelumnya.
- Pastikan Anda menggunakan informasi login yang benar. Nama dan sandi login pabrik default adalah "admin/admin". Pastikan tombol Caps Lock nonaktif saat Anda memasukkan informasi login.

- Hapus cookie dan file di browser web Anda. Untuk Internet Explorer, ikuti langkah-langkah ini:

1. Buka Internet Explorer, lalu klik **Tools (Alat Bantu) > Internet Options (Pilihan Internet)**.
2. Di tab **General (Umum)**, dalam **Browsing History (Riwayat Penelusuran)**, klik **Delete... (Hapus...)**, pilih **Temporary Internet file and website files (File Internet sementara dan file situs web)** serta **Cookies and website data (Cookie dan data situs web)**, lalu klik **Delete (Hapus)**.



#### CATATAN:

- Perintah untuk menghapus cookie dan file berbeda, tergantung pada browser web.
- Nonaktifkan pengaturan server proxy, batalkan sambungan dial-up, lalu tetapkan pengaturan TCP/IP untuk memperoleh alamat IP secara otomatis. Untuk informasi lebih rinci, lihat Bab 1 dalam panduan pengguna ini.
- Pastikan Anda menggunakan kabel Ethernet CAT5e atau CAT6.

## Sambungan nirkabel antara klien dan router tidak dapat dibuat.

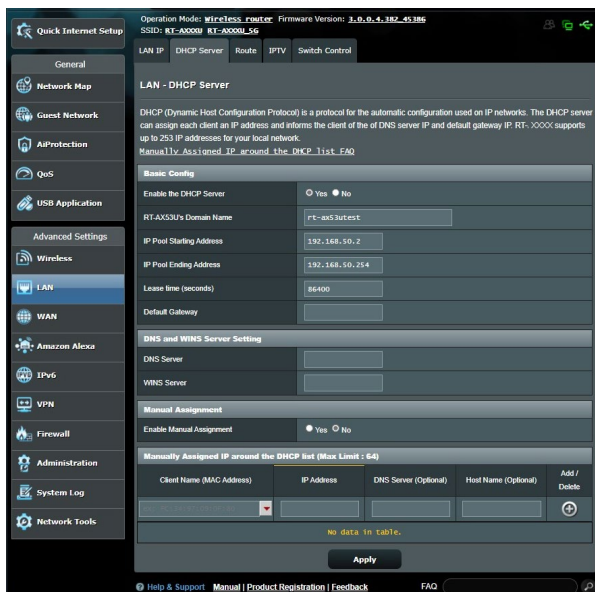
**CATATAN:** Jika Anda mengalami masalah sambungan ke jaringan 5 GHz, pastikan perangkat nirkabel mendukung 5 GHz atau dilengkapi kemampuan dual band.

### • Di Luar Jangkauan:

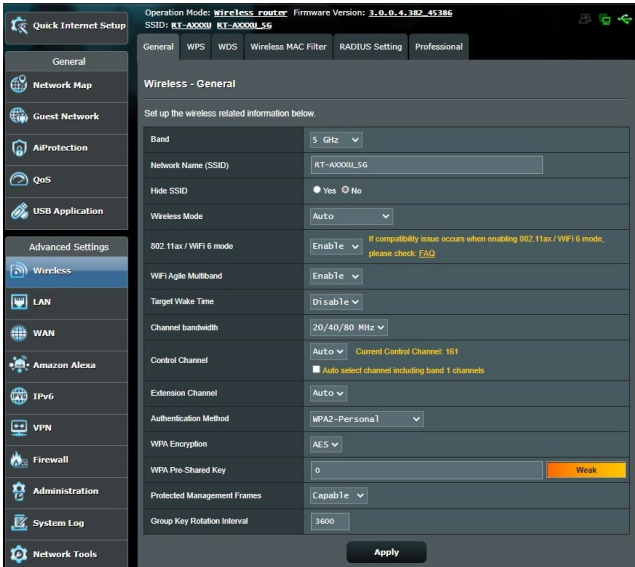
- Dekatkan posisi router dengan klien nirkabel.
- Coba sesuaikan arah terbaik antena router sebagaimana dijelaskan di bagian **1.4 Mengatur posisi router**.

### • Server DHCP telah dinonaktifkan:

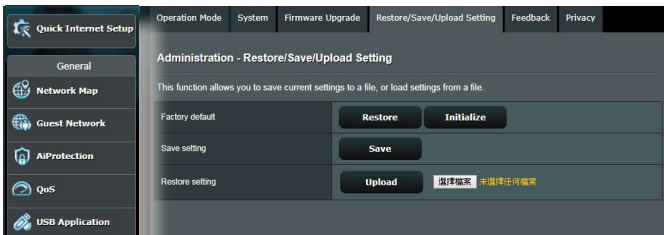
1. Aktifkan GUI web. Buka **General (Umum) > Network Map (Peta Jaringan) > Clients (Klien)**, lalu cari perangkat yang akan disambungkan ke router.
2. Jika Anda tidak dapat menemukan perangkat di **Network Map (Peta Jaringan)**, buka **Advanced Settings (Pengaturan Lanjutan) > LAN > DHCP Server (Server DHCP)**, daftar **Basic Config (Konfigurasi Dasar)**, pilih **Yes (Ya)** di **Enable the DHCP Server (Aktifkan Server DHCP)**.



- SSID disembunyikan. Jika perangkat dapat menemukan SSID dari router lain, namun tidak dapat menemukan SSID router Anda, buka **Advanced Settings (Pengaturan Lanjutan) > Wireless (Nirkabel) > General (Umum)**, pilih **No (Tidak)** di **Hide SSID (Sembunyikan SSID)**, lalu pilih **Auto (Otomatis)** di **Control Channel (Saluran Kontrol)**.



- Jika Anda menggunakan adaptor LAN nirkabel, periksa apakah saluran nirkabel yang digunakan sudah sesuai dengan saluran yang tersedia di negara/wilayah Anda. Jika tidak, sesuaikan saluran, bandwidth saluran, dan mode nirkabel.
- Jika router tetap tidak dapat tersambung secara nirkabel, Anda dapat mengulang router ke pengaturan default pabrik. Di GUI router, klik **Administration (Administrasi) > Restore/Save/Upload Setting (Kembalikan/Simpan/Upload Pengaturan)**, lalu klik **Restore (Kembalikan)**.

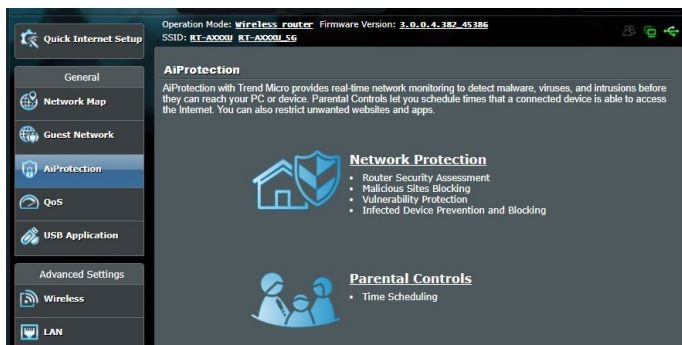


## Internet berkabel tidak dapat diakses.

- Periksa apakah router dapat menyambung ke alamat IP WAN ISP. Untuk melakukannya, aktifkan GUI web dan buka **General (Umum) > Network Map (Peta Jaringan)**, lalu periksa **Internet Status (Status Internet)**.
- Jika router tidak dapat menyambung ke alamat IP WAN ISP, coba hidupkan ulang jaringan sebagaimana dijelaskan di bagian **Hidupkan ulang jaringan dengan urutan berikut** dalam **Basic Troubleshooting (Mengatasi Masalah Mendasar)**.



- Perangkat telah diblokir melalui fungsi Kontrol Orang Tua. Buka **General (Umum) > AiProtection > Parental Control (Kontrol Orang Tua)**, lalu lihat apakah perangkat ini termasuk dalam daftar. Jika perangkat tercantum dalam **Client Name (Nama Klien)**, hapus perangkat menggunakan tombol **Delete (Hapus)** atau sesuaikan Pengaturan Manajemen Waktu.



- Jika akses Internet masih belum tersedia, coba jalankan boot ulang komputer, lalu verifikasi alamat IP dan alamat gateway jaringan.
- Periksa indikator status pada modem ADSL dan router nirkabel. Jika LED WAN pada router nirkabel mati, pastikan semua kabel telah terpasang dengan benar.

## Anda lupa SSID (nama jaringan) atau sandi jaringan

- Konfigurasi SSID dan kode enkripsi baru melalui sambungan berkabel (kabel Ethernet). Aktifkan GUI web, buka **Network Map (Peta Jaringan)**, klik ikon router, masukkan SSID dan kode enkripsi baru, lalu klik **Apply (Terapkan)**.
- Atur ulang router ke pengaturan default. Aktifkan GUI web, buka **Administration (Administrasi) > Restore/Save/Upload Setting (Kembalikan/Simpan/Upload Pengaturan)**, lalu klik **Restore (Kembalikan)**. Akun dan sandi login default adalah "admin".

## Bagaimana cara mengembalikan sistem ke pengaturan default?

- Buka **Administration (Administrasi) > Restore/Save/Upload Setting (Pengaturan Pengembalian/Penyimpanan/Upload)**, lalu klik **Restore (Kembalikan)**.

Berikut adalah pengaturan default pabrik:

<b>Nama pengguna:</b>	admin
<b>Sandi:</b>	admin
<b>Aktifkan DHCP:</b>	Yes (jika kabel WAN tersambung)
<b>Alamat IP:</b>	router.asus.com
<b>Nama domain:</b>	(Kosong)
<b>Subnet Mask</b>	255.255.255.0
<b>Server DNS 1:</b>	192.168.1.1
<b>Server DNS 2:</b>	(Blank)
<b>SSID (2.4GHz):</b>	ASUS
<b>SSID (5GHz):</b>	ASUS_5G

## Upgrade firmware gagal.

Aktifkan mode penyelamatan dan jalankan utilitas Firmware Restoration. Lihat bagian **5.2 Pengembalian Firmware** tentang cara menggunakan utilitas Firmware Restoration.

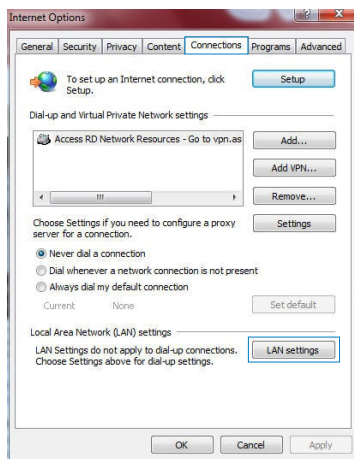
## Tidak dapat mengakses GUI Web

Sebelum mengkonfigurasi router nirkabel, lakukan langkah-langkah yang dijelaskan di bagian ini untuk komputer host dan klien jaringan.

### A. Nonaktifkan server proxy jika diaktifkan.

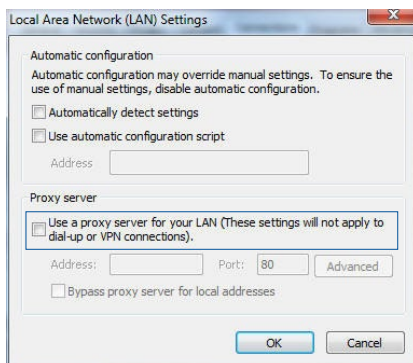
#### Windows®

1. Untuk membuka browser, klik **Start (Mulai) > Internet Explorer**.
2. Klik tab **Tools (Alat Bantu) > Internet Options (Pilihan Internet) > Connections (Sambungan) > LAN settings (Pengaturan LAN)**.



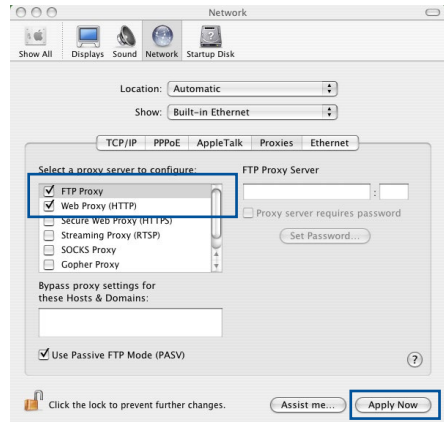
3. Dari layar Local Area Network (LAN) Settings (Pengaturan LAN (Local Area Network)), hapus centang **Use a proxy server for your LAN (Gunakan server proxy untuk LAN)**.

4. Setelah selesai, klik **OK**.



## OS MAC

1. Dari browser Safari, klik **Safari > Preferences (Preferensi) > Advanced (Lanjutan) > Change Settings... (Ubah Pengaturan...)**
2. Dari layar Network (Jaringan), hapus centang **FTP Proxy (Proxy FTP)** dan **Web Proxy (HTTP) (Proxy Web (HTTP))**.
3. Setelah selesai, klik **Apply Now (Terapkan Sekarang)**.

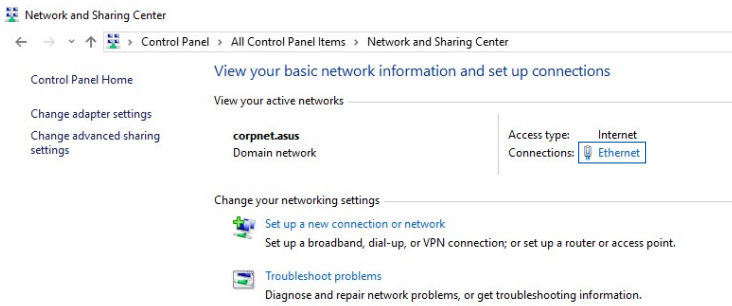


**CATATAN:** Untuk informasi rinci tentang cara menonaktifkan server proxy, lihat fitur bantuan browser Anda.

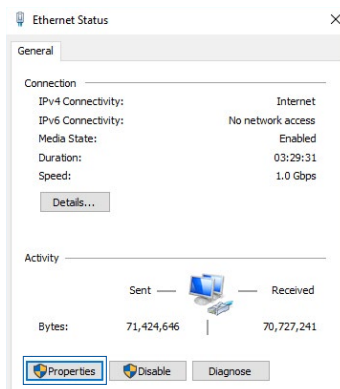
## B. Tetapkan pengaturan TCP/IP untuk mendapatkan alamat IP secara otomatis.

### Windows®

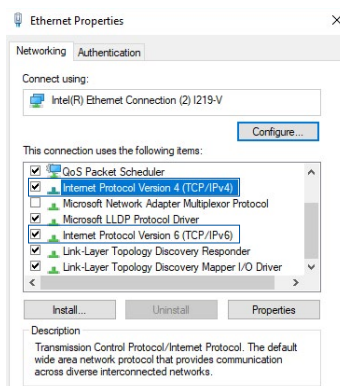
1. Klik **Start (Mulai) > Control Panel (Panel Kontrol) > Network and Internet (Jaringan dan Internet) > Network and Sharing Center (Jaringan dan Pusat Berbagi)**, lalu klik sambungan jaringan untuk menampilkan jendela statusnya.



2. Klik **Properties (Properti)** untuk menampilkan jendela Properti Ethernet.



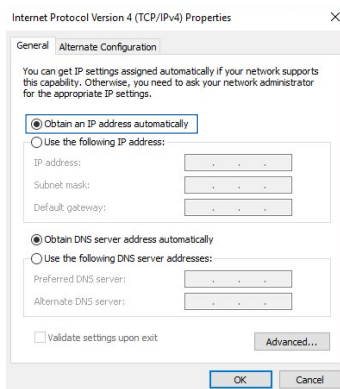
3. Pilih **Internet Protocol Version 4 (TCP/IPv4)** (Protokol Internet Versi 4 (TCP/IPv4)) atau **Internet Protocol Version 6 (TCP/IPv6)** (Protokol Internet Versi 6 (TCP/IPv6)), lalu klik **Properties (Properti)**.



4. Untuk mendapatkan pengaturan IP IPv4 secara otomatis, centang **Obtain an IP address automatically** (Dapatkan alamat IP secara otomatis).


Untuk mendapatkan pengaturan IP IPv6 secara otomatis, centang **Obtain an IPv6 address automatically** (Dapatkan alamat IPv6 secara otomatis).

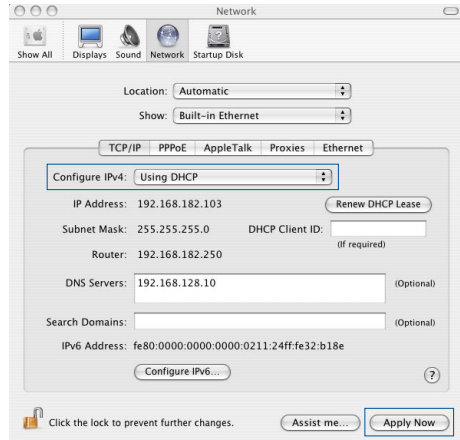
5. Setelah selesai, klik **OK**.





## OS MAC

1. Klik ikon Apple  yang berada di kiri atas layar.
2. Klik **System Preferences (Preferensi Sistem) > Network (Jaringan) > Configure... (Konfigurasikan...)**
3. Dari tab **TCP/IP**, pilih **Using DHCP (Menggunakan DHCP)** dalam daftar dropdown **Configure IPv4 (Konfigurasikan IPv4)**.
4. Setelah selesai, klik **Apply Now (Terapkan Sekarang)**.

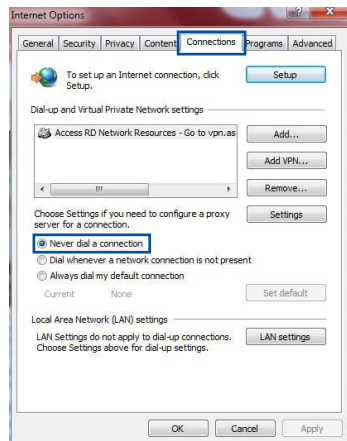


**CATATAN:** Untuk informasi rinci tentang cara mengkonfigurasi pengaturan TCP/IP komputer, lihat fitur bantuan dan dukungan sistem operasi Anda.

## C. Nonaktifkan sambungan dial-up jika diaktifkan.

### Windows®

1. Untuk membuka browser, klik **Start (Mulai) > Internet Explorer**.
2. Klik tab **Tools (Alat Bantu) > Internet Options (Pilihan Internet) > Connections (Sambungan)**.
3. Centang **Never dial a connection (Jangan pernah buat sambungan)**.
4. Setelah selesai, klik **OK**.



**CATATAN:** Untuk informasi rinci tentang cara menonaktifkan sambungan dial-up, lihat fitur bantuan browser Anda.

# Lampiran

## 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

## Layanan dan Dukungan

Kunjungi, situs multibahasa kami di <https://www.asus.com/support>.

