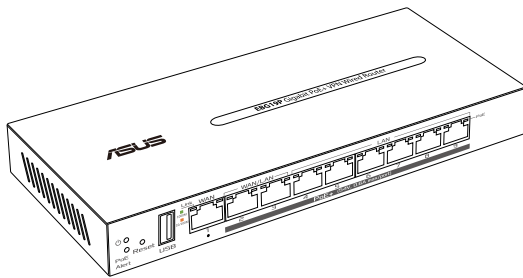


Panduan Pengguna

ASUS EBG19P

Penghala Berwayar VPN PoE+ Gigabit

Model: EBG19P



MY27419

Edisi Semakan v2

Mac 2026

Hak cipta © 2026 ASUSTeK COMPUTER INC. Hak Cipta Terpelihara.

Tiada bahagian daripada manual ini, termasuk produk dan perisian yang diterangkan di dalamnya boleh dikeluarkan semula, dipindahkan, ditranskrip, disimpan dalam sistem pengambilan, atau diterjemah ke dalam sebarang bahasa dalam sebarang bentuk atau apa-apa kaedah, kecuali dokumentasi yang disimpan oleh pembeli untuk tujuan sandaran, tanpa kebenaran tersurat bertulis ASUSTeK COMPUTER INC. ("ASUS").

Waranti atau perkhidmatan produk tidak akan dilanjutkan jika: (1) produk dibaiki, diubah suai atau diubah, melainkan pembaikan, pengubahsuaian atau perubahan itu dibenarkan secara bertulis oleh ASUS; atau (2) nombor siri produk itu rosak atau hilang.

ASUS menyediakan manual ini "seperti sebagaimana ada" tanpa sebarang jaminan dalam sebarang bentuk, sama ada tersurat atau tersirat, termasuk tetapi tidak terhad kepada waranti yang dikenakan atau syarat kebolehdagangan atau kesesuaian untuk tujuan tertentu. ASUS, para pengarah, pegawai, pekerja atau agennya tidak akan bertanggungjawab dalam apa-apa keadaan sekalipun di atas sebarang kerosakan tidak langsung, khusus, iringan atau lanjutan (termasuk kerosakan di atas kerugian hasil, kerugian perniagaan, kerugian penggunaan atau data, gangguan perniagaan dan yang sama dengannya), walaupun jika ASUS telah dinasihatkan tentang kemungkinan kerosakan tersebut yang timbul daripada sebarang kerosakan atau ralat di dalam manual atau produk ini.

Spesifikasi dan maklumat yang terkandung di dalam manual ini disediakan untuk pemberitahuan sahaja dan tertakluk pada perubahan pada bila-bila masa tanpa notis dan tidak boleh ditafsirkan sebagai komitmen oleh ASUS. ASUS tidak akan menanggung tanggungjawab atau liabiliti untuk sebarang ralat atau ketidaktepatan yang mungkin muncul dalam manual ini, termasuk produk dan perisian yang dijelaskan di dalamnya.

Nama produk dan korporat yang muncul di dalam manual ini mungkin atau mungkin bukan tanda dagangan atau hak cipta berdaftar bagi syarikatnya masing-masing, dan hanya digunakan untuk pengenalan atau penerangan dan untuk faedah pemilik, tanpa niat untuk melanggar.

PENYATA KEBOLEHCAPAIAN

ASUS komited untuk menjadikan dokumentasi kami mudah diakses, selaras dengan Arahan (EU) 2019/882 Parlimen Eropah dan Majlis. Dokumen ini direka untuk memenuhi keperluan WCAG 2.1 (tahap AA)/EN 301 549 dan boleh diakses oleh pembaca skrin seperti NVDA Screen Reader atau Microsoft Narrator.

Untuk maklumat produk lanjut, sila rujuk laman web produk:

<https://qr.asus.com/networking/asus-expertwifi-ebg19p>



Perkhidmatan dan Sokongan

Lawati laman web kami yang pelbagai bahasa di <https://www.asus.com/support>.



Kandungan

1 Mengenali EBG19P anda

1.1 Selamat datang!	8
1.2 Kandungan pakej	8
1.3 Penghala berwayar anda	9
1.4 Menetapkan kedudukan penghala anda	11
1.5 Keperluan Penyediaan	12

2 Bermula

2.1 Penyediaan Penghala	13
Soalan Lazim	13
Sambungan berwayar	14
2.2 Melog masuk ke GUI web	15
2.3 Pengesanan automatik WAN	16
Soalan Lazim	16

3 Tutorial

ExpertWiFi	18
------------	----

4 Mengkonfigurasi EBG19P

4.1 Mudah Suai QoS	19
4.1.1 Monitor Lebar Jalur	19
4.1.2 QoS	20
4.1.3 Web History (Sejarah Web)	20
4.1.4 Kelajuan Internet	21
4.2 Pentadbiran	22
4.2.1 Mod Operasi	22
4.2.2 Sistem	23
4.2.3 Menatarkan perisian tegar	24
4.2.4 Tetapan Pemulihan/Penyimpanan/Memuat Naik	25

4.2.5 Feedback (Maklum Balas)	26
4.2.6 Privasi	27
4.3 AiMesh.....	28
4.3.1 Menyediakan sistem AiMesh ExpertWiFi	28
4.3.2 Menguruskan klien rangkaian anda.....	29
4.4 AiProtection	30
4.4.1 Perlindungan Rangkaian.....	30
4.5 Dashboard (Papan Pemuka)	33
4.6 Kawalan akses peranti	34
4.6.1 Penapis Web & Aplikasi	34
4.6.2 Penjadualan Waktu	35
4.7 Tembok Api.....	36
4.7.1 Umum	36
4.7.2 Penapis URL	37
4.7.3 Penapis kata kunci.....	38
4.7.4 Penapis Perkhidmatan Rangkaian.....	39
4.8 IPv6	40
4.9 LAN	41
4.9.1 LAN IP	41
4.9.2 Pelayan DHCP	42
4.9.3 Hala.....	44
4.9.4 IPTV.....	45
4.9.5 Kawalan Suis.....	45
4.9.6 VLAN	46
4.10 Alatan Rangkaian.....	48
4.10.1 Analisis Rangkaian	48
4.10.2 Netstat.....	48
4.10.3 Hidupkan LAN	48
4.10.4 Peraturan Sambung Pintar.....	48

4.11 Rangkaian Ditetapkan Sendiri.....	49
4.11.1 Pekerja.....	50
4.11.2 Portal Tetamu.....	50
4.11.3 Rangkaian Tetamu.....	51
4.11.4 Rangkaian Berjadual.....	51
4.11.5 Rangkaian IoT.....	52
4.11.6 Rangkaian VPN.....	52
4.11.7 Penjelajah Senario.....	53
4.11.8 Rangkaian Tersuai.....	54
4.12 Log Sistem.....	55
4.13 Penganalisis Trafik.....	56
4.13.1 Penganalisis Trafik.....	56
4.14 Aplikasi USB.....	57
4.14.1 Pelayan Media.....	57
4.14.2 Perkongsian (Samba) Tempat Rangkaian.....	58
4.14.3 Kongsi FTP.....	58
4.14.4 Pelayan Pencetak Rangkaian.....	59
4.14.5 Modem USB.....	67
4.15 VPN Fusion (Gabungan VPN).....	68
4.15.1 Mencipta gabungan VPN.....	68
4.15.2 Sambungan Internet.....	69
4.16 VPN Server (Pelayan VPN).....	70
4.16.1 PPTP.....	70
4.16.2 OpenVPN.....	71
4.16.3 IPSec VPN.....	72
4.16.4 WireGuard® VPN.....	73
4.17 WAN.....	74
4.17.1 Sambungan Internet.....	74
4.17.2 Berbilang WAN.....	76
4.17.3 Picu Port.....	78
4.17.4 Pelayan Maya/Pemajuan Port.....	80
4.17.5 DMZ.....	83

4.17.6 DDNS	84
4.17.7 Masuk Lalu NAT.....	85
4.18 Wayarles.....	86
4.18.1 Umum	86
4.18.2 Penapis MAC Wayarles.....	87
4.18.3 Senarai Sekatan Perayauan	88

5 Menyelesai Masalah

5.1 Penyelesaian Masalah Asas	89
5.2 Soalan Lazim (FAQs)	91

Lampiran

Appendices

Maklumat keselamatan	118
Notis WEEE	120

1 Mengenal EBG19P anda

1.1 Selamat datang!

Terima kasih kerana membeli ASUS EBG19P!

EBG19P menyediakan rangkaian yang pantas, selamat dan boleh skala, kestabilan rangkaian dipertingkatkan melalui ketersambungan Ethernet dan menyediakan sandaran Internet dengan dua port WAN/LAN dan satu port USB untuk menyokong operasi.

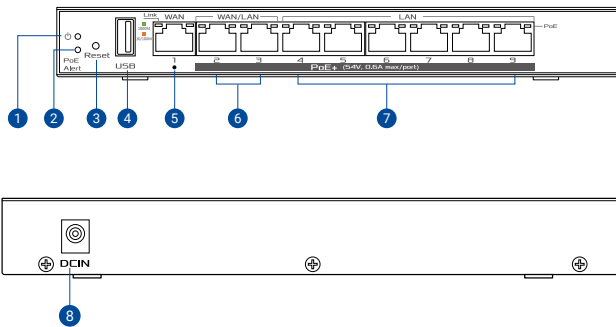
1.2 Kandungan pakej

- EBG19P
- Kabel rangkaian (RJ-45)
- Penyesuai kuasa
- Panduan Mula Pantas
- Pelekat maklumat log masuk setempat
- Kad waranti

NOTA:

- Jika mana-mana daripada item ini rosak atau tiada, hubungi ASUS untuk membuat pertanyaan teknikal dan sokongan. Rujuk kepada **Perkhidmatan dan Sokongan** dalam manual pengguna ini.
 - Simpan bahan pembungkusan yang asal sekiranya anda inginkan perkhidmatan waranti pada masa hadapan seperti pembaikan atau penggantian.
-

1.3 Penghala berwayar anda



1. LED Kuasa

Mati: Tiada kuasa.

Hidup: Peranti sudah sedia.

Berkelip perlahan: Mod Penyelamat.

2. LED PoE Isyarat

Mati: Tiada kuasa atau sambungan fizikal.

Hidup: Kuasa sedang dibekalkan kepada peranti yang disambungkan ke port PoE+.

NOTA: Anda boleh menyemak status operasi penghala dalam aplikasi ExpertWiFi.

3. Butang tetap semula

Butang ini menetapkan semula atau menyimpan sistem ke tetapan lalai kilang.

4. Port USB 3.2 Gen 1

Masukkan peranti yang serasi dengan USB 3.2 Gen 1 seperti cakera keras USB atau pemacu kilat USB ke dalam port ini.

5. Port WAN (Internet)

Sambung kabel rangkaian ke dalam port ini untuk membentuk sambungan WAN. Port ini dikenalpasti dengan titik taktil.

6. Port WAN/LAN (dengan PoE+)

Sambung kabel rangkaian ke dalam port ini untuk membentuk sambungan WAN/LAN.

7. Port LAN (dengan PoE+)

Sambung kabel rangkaian ke dalam port ini untuk membentuk sambungan LAN.

8. Port Kuasa (DCIN)

Masukkan adapter AC yang diletakkan bersama ke dalam port ini dan sambung penghala anda ke sumber kuasa.

Penunjuk LED port Ethernet

Penunjuk LED			
LED kelajuan (Hijau)		LED Paut/Act (Ambar)	
1Gbps	HIDUP	1Gbps/100Mbps/10Mbps	Berkelip
100Mbps/10Mbps	MATI	Tiada Trafik	HIDUP

NOTA:

- Hanya guna adapter yang disertakan bersama pakej anda. Menggunakan adapter lain boleh merosakkan peranti.

- **Spesifikasi:**

Adapter Kuasa DC (Output DC): +54V dengan arus maks. 2.778A

Suhu Pengendalian: 0 hingga 40 °C

Suhu Penyimpanan: 0 hingga 70 °C

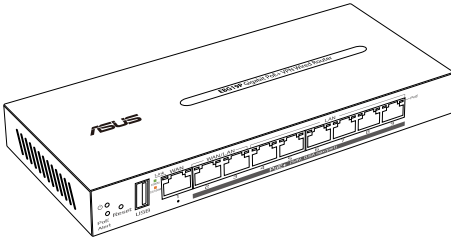
Kelembapan Operasi: 50 hingga 90%

Kelembapan Penyimpanan: 20 hingga 90%

1.4 Menetapkan kedudukan penghala anda

Untuk pengalaman perangkaian yang terbaik, pastikan bahawa anda:

- Sentiasa kemas kini ke perisian tegar yang terkini. Lawati laman web ASUS di <https://www.asus.com> untuk mendapatkan kemas kini perisian tegar yang terkini.



1.5 Keperluan Penyediaan

Untuk menyediakan rangkaian anda, anda perlukan satu atau dua komputer yang memenuhi keperluan sistem yang berikut:

- Port Ethernet RJ-45 (LAN) (10Base-T/100Base-TX/1000Base-TX)
- Perkhidmatan TCP/IP yang terpasang
- Penyemak imbas Web seperti Microsoft Internet Explorer, Firefox, Safari, atau Google Chrome

NOTA: Kabel Ethernet RJ-45 yang digunakan untuk menyambungkan peranti rangkaian tidak boleh melebihi 100 meter.

2 Bermula

2.1 Penyediaan Penghala

PENTING!

Sebelum menyediakan penghala berwayar ASUS anda, lakukan yang berikut:

- Jika anda sedang menggantikan penghala yang sedia ada, tanggalkannya daripada rangkaian anda.
 - Putuskan sambungan kabel/wayar dari modem anda yang sedia ada. Jika modem anda mempunyai bateri sandaran, tanggalkannya juga.
 - But semua komputer anda (disarankan).
-



AMARAN!

- Kord bekalan kuasa mesti dipalam masuk ke salur keluar soket yang disediakan dengan pbumian yang sesuai. Sambungkan peralatan hanya ke salur keluar soket berdekatan yang mudah diakses.
 - Jika Penyesuai, jangan cuba untuk membetulkannya sendiri. Hubungi juruteknik servis bertauliah atau peruncit anda.
 - JANGAN guna kord kuasa, aksesori atau persisian lain yang rosak.
 - JANGAN pasang peralatan ini lebih tinggi daripada 2 meter.
 - Gunakan produk ini dalam persekitaran dengan suhu ambien antara 0°C (32°F) dan 40°C (104°F).
-

Soalan Lazim

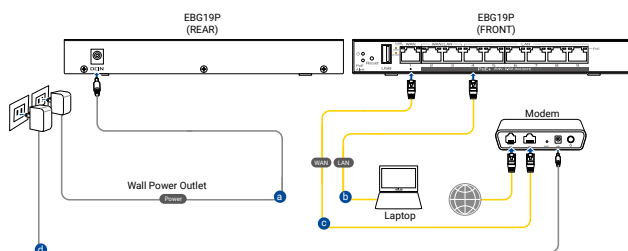
- Menyiapkan melalui aplikasi ExpertWiFi
- Penyediaan melalui GUI Web (ASUSWRT)
- Penyediaan melalui QIS (Penyediaan Internet Pantas)

Sambungan berwayar

NOTA: Penghala wayarles anda menyokong kedua-dua kabel tembus lalu atau silang atas semasa menyediakan sambungan berwayar.

Untuk menyediakan rangkaian menggunakan sambungan berwayar:

1. Pasang masuk penghala anda ke sumber kuasa dan hidupkan kuasanya. Sambungkan kabel rangkaian dari komputer anda ke port LAN pada penghala anda.



2. Buka pelayar web dan navigasi ke <http://expertwifi.net> untuk penyediaan.

GUI web dilancarkan secara automatik apabila anda membuka pelayar web. Jika ia tidak melakukan pelancaran auto, masuki <http://expertwifi.net>.

3. Ikut arahan-arahan untuk penyediaan.

2.2 Melog masuk ke GUI web

Penghala Berwayar ASUS anda menggunakan antara muka pengguna berasaskan web yang membolehkan anda untuk mengkonfigurasi penghala menggunakan sebarang penyemak imbas web seperti Microsoft Edge, Safari, atau Google Chrome.

NOTA: Ciri mungkin berbeza dengan versi perisian tegar berbeza.

Menyambung ke rangkaian anda secara berwayar

Untuk log masuk ke GUI web:

1. Di penyemak imbas web anda, masukkan <http://expertwifi.net>.
2. Ikut arahan-arahan untuk penyediaan.

2.3 Pengesanan automatik WAN

Soalan Lazim

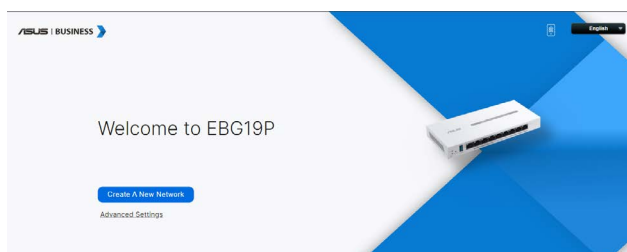
- Menyiapkan melalui aplikasi ExpertWiFi
- Penyediaan melalui GUI Web (ASUSWRT)
- Penyediaan melalui QIS (Penyediaan Internet Pantas)

Ciri Persediaan Internet Cepat (QIS) membimbing anda untuk menyediakan sambungan Internet anda dengan cepat.

NOTA: Semasa menetapkan sambungan Internet buat pertama kali, tekan butang Tetap semula pada penghalang berwayar anda untuk menetakannya ke tetapan lalai kilang.

Untuk menggunakan QIS dengan pengesanan cepat:

1. Log masuk ke GUI Web, dan klik **Create A New Network (Cipta Rangkaian Baharu)**.



2. klik **Next (Seterusnya)** untuk mengelog masuk dengan nama pengguna dan kata laluan lalai.

Local Login Set up Local Login username and password to prevent unauthorized access to your ASUS networking device.

Username / Password

Settings

Username

admin

New password

☒ Use default Local Login Password
The default encrypted Local Login Password provides a secure login process when you connect to this ASUS networking device locally.

[How to find Local Login Password](#)

Previous Next

Nyahtandakan **Use default Local Login Password** (**Gunakan Kata Laluan Log Masuk Setempat lalai**), dan masukkan nama pengguna dan kata laluan baharu, kemudian klik **Next (Seterusnya)**.

Local Login
Username / Password
Settings

Set up Local Login username and password to prevent unauthorized access to your ASUS networking device.

Username
admin

New password 

Danger

Retype Password

☐ Use default Local Login Password
The default encrypted Local Login Password provides a secure login process when you connect to this ASUS networking device locally.

[How to find Local Login Password](#)

[Previous](#) [Next](#)

3. Klik Firmware Upgrade (Kemas Kini Perisian Tegar) untuk menaik taraf perisian tegar menjadi terkini atau klik Cancel (Batal) untuk mengekalkan versi semasa.

Firmware Upgrade
The latest firmware is available now. To improve the system efficiency, ASUS highly recommend upgrading your firmware version.

The latest version
3006_102_44136-g94573dc_349-g59e89

[Cancel](#) [Firmware Upgrade](#)

NOTA: Skrin hanya muncul apabila versi perisian tegar baharu tersedia.

3 Tutorial

ExpertWiFi

Persediaan imbasan kod QR yang mudah (penghala siri ASUS ExpertWiFi)

Bagaimanakah cara untuk saya mengakses halaman penyediaan penghala ExpertWiFi saya melalui GUI Web?

Apakah itu Rangkaian Ditentukan Sendiri (SDN) dan bagaimana cara untuk menetapkan SDN?

Bagaimana untuk menyediakan suis ExpertWiFi dalam Mod ExpertWiFi AiMesh dan Mod Berdiri Sendiri?

Bagaimana menangani masalah bekalan kuasa yang tidak stabil dengan penghala berwayar gigabit PoE+ VPN seperti ExpertWiFi EBG19P?

Bagaimana cara menyambungkan titik akses PoE kepada penghala, suis, atau pintu gerbang?

Bagaimana untuk melaraskan saluran WiFi dan lebar jalur pada nod ExpertWiFi AiMesh yang berbeza?

Bagaimana untuk menambah suis PoE dan titik akses PoE sebagai nod AiMesh kepada penghala berwayar VPN saya?

Bagaimana untuk menguruskan titik akses PoE melalui GUI Web ExpertWiFi?

Bagaimana untuk menyediakan kumpulan multi-WAN pada penghala VPN ExpertWiFi?

Bagaimanakah cara untuk menyediakan peranti ExpertWiFi sebagai nod AiMesh?

Bagaimana untuk menambah tapak ke ASUS Multi-Site Manager?

Bagaimana untuk mencipta kumpulan dalam ASUS Multi-Site Manager?

Bagaimanakah cara untuk menyediakan Portal Tetamu dalam Rangkaian yang Ditentukan Sendiri (SDN) untuk menyediakan akses internet kepada peranti WiFi?

Bagaimanakah cara untuk menyediakan VLAN pada penghala ASUS ExpertWiFi?

Bagaimana untuk mengeluarkan peranti luar talian?

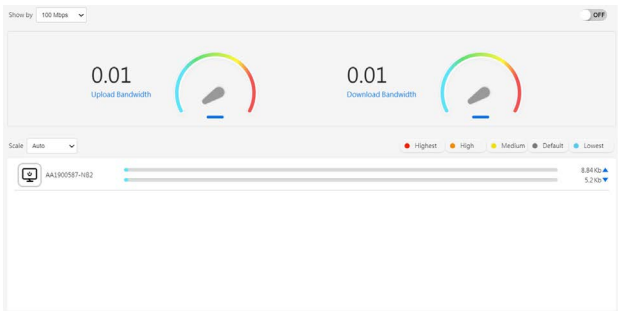
4 Mengkonfigurasi EBG19P

4.1 Mudah Suai QoS

4.1.1 Monitor Lebar Jalur

Monitor Lebar Jalur membolehkan anda memantau jumlah dan penggunaan lebar jalur muat turun dan muat naik bagi setiap klien.

Untuk menggunakan **Bandwidth Monitor (Monitor Lebar Jalur)**, pergi ke **Settings (Tetapan) > Adaptive QoS (QoS Mudah Suai) > Bandwidth Monitor (Monitor Lebar Jalur)**.

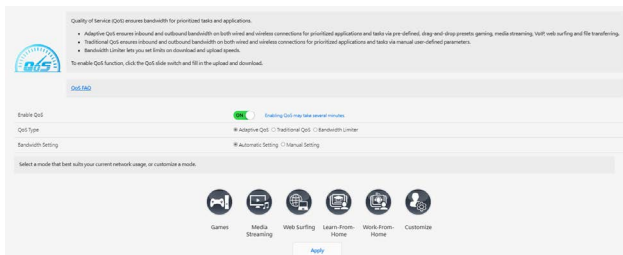


NOTA: Untuk maklumat lanjut, sila lawati <https://www.asus.com/support/faq/1008717>.

4.1.2 QoS

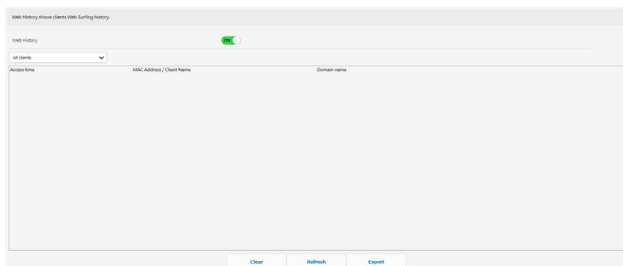
Kualiti Perkhidmatan (QoS) memastikan lebar jalur untuk tugas dan aplikasi yang diutamakan.

1. **Adaptive QoS (QoS Mudah Suai)** memastikan lebar jalur yang masuk dan keluar pada kedua-dua sambungan berwayar dan wayarles untuk aplikasi dan tugas yang diutamakan melalui praset seret dan lepas yang ditentukan lebih awal: permainan, penstriman media, VoIP, pelayaran web dan pemindahan fail.
2. **Traditional QoS (QoS Tradisional)** memastikan lebar jalur masuk dan keluar pada kedua-dua sambungan berwayar dan wayarles untuk aplikasi dan tugas yang diutamakan melalui parameter yang ditentukan oleh pengguna manual.
3. **Bandwidth Limiter (Pengehad Lebar Jalur)** membolehkan anda menetapkan had kelajuan muat turun dan muat naik.



4.1.3 Web History (Sejarah Web)

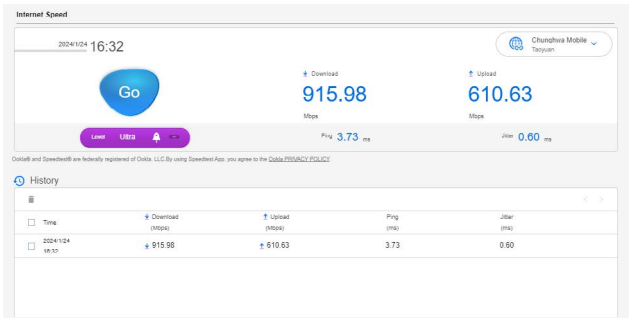
Halaman **Web History (Sejarah Web)** memaparkan sejarah pelayaran web klien.



4.1.4 Kelajuan Internet

Perkhidmatan ini disediakan oleh Ookla®. Ia mengesan kelajuan muat turun dan muat naik daripada penghala anda ke Internet.

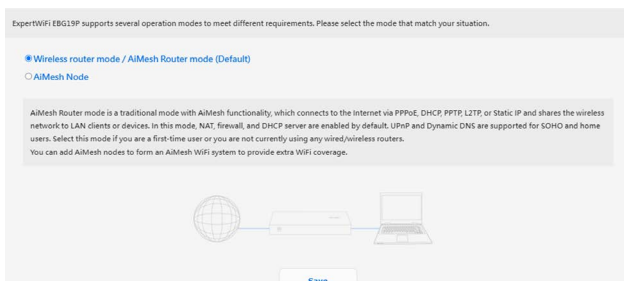
Klik **GO** untuk memulakan ujian kelajuan Internet, yang mengambil masa lebih kurang satu minit untuk selesai.



4.2 Pentadbiran

4.2.1 Mod Operasi

Halaman Mod Operasi membolehkan anda memilih mod bersesuaian untuk rangkaian anda.



Untuk menyediakan mod operasi:

1. Daripada panel navigasi, pergi ke **Settings (Tetapan) > Administration (Pentadbiran) > Operation Mode (Mod Operasi)**.
2. Pilih mana-mana mod operasi ini:
 - **Wireless router mode / AiMesh Router mode (Mod penghala wayarles / Mod Penghala AiMesh) (lalai):** Mod Penghala AiMesh ialah mod tradisional dengan fungsi AiMesh, yang bersambung ke Internet melalui PPPoE, DHCP, PPTP, L2TP, atau IP Statik dan berkongsi rangkaian wayarles ke klien atau peranti LAN. Dalam mod ini, NAT, firewall (tembok api), dan pelayan DHCP didayakan secara lalai. UPnP dan DNS Dinamik disokong untuk pengguna SOHO dan rumah.
 - **AiMesh Node (Nod AiMesh):** Anda boleh menambah nod AiMesh untuk membentuk sistem Wi-Fi AiMesh bagi menyediakan liputan Wi-Fi tambahan.
3. Klik **Save (Simpan)**.

NOTA: Penghalaan ini akan but semula bila anda menukar mod.

4.2.2 Sistem

Halaman System (Sistem) membolehkan anda mengkonfigurasi tetapan penghala anda.

Untuk menyediakan tetapan Sistem:

1. Daripada panel navigasi, pergi ke **Settings (Tetapan) > Administration (Pentadbiran) > System (Sistem)**.
2. Anda boleh mengkonfigurasi tetapan berikut:
 - **Change router login password (Ubah kata laluan log masuk penghala):** Anda boleh menukar kata laluan dan nama log masuk penghala berwayar dengan memasukkan nama dan kata laluan baru.
 - **USB setting (Tetapan USB):** Anda boleh Dayakan Hibernasi HDD dan ubah mod USB.
 - **Time Zone (Zon Masa):** Pilih zon masa rangkaian anda.
 - **NTP Server (Pelayan NTP):** Penghala berwayar boleh mengakses pelayan NTP (Protokol Masa Rangkaian) untuk menyegerakkan masa.
 - **Network Monitoring (Pemantauan Rangkaian):** Anda boleh mendayakan Pertanyaan DNS untuk menyemak Nama Hos dan Alamat IP Yang Ditetapkan, atau mendayakan Ping, kemudian, semak Sasaran Ping anda.
 - **Auto Logout (Log Keluar Auto):** Anda boleh menetapkan masa log keluar auto.
 - **Enable WAN down browser redirect notice (Dayakan notis menghala semula pelayar ketika WAN tiada):** Ciri ini membolehkan pelayar memaparkan halaman amaran apabila penghala terputus sambungan daripada Internet. Apabila didayakan, halaman amaran tidak akan muncul.
 - **Enable Telnet (Dayakan Telnet):** Klik **Yes (Ya)** untuk mendayakan perkhidmatan Telnet pada rangkaian. Klik **No (Tidak)** untuk menyahdayakan Telnet.
 - **Authentication Method (Kaedah Pengesahan):** Anda boleh memilih HTTP, HTTPS, atau kedua-dua protokol untuk menjamin akses penghala.
 - **Enable Reboot Scheduler (Dayakan Penjadual But Semula):** Apabila didayakan, anda boleh menetapkan Tarikh untuk But Semula dan Masa untuk But Semula.
 - **Enable Web Access from WAN (Dayakan Akses Web daripada WAN):** Pilih **Yes (Ya)** untuk membolehkan peranti di luar rangkaian untuk mengakses tetapan GUI penghala berwayar. Pilih **No (Tidak)** untuk menghalang akses.
 - **Enable Access Restrictions (Dayakan Sekatan Akses):**

Klik **Yes (Ya)** jika anda ingin menentukan alamat IP peranti yang dibenarkan mengakses tetapan GUI penghala berwayar daripada WAN/LAN.

- **Service (Perkhidmatan):** Ciri ini membolehkan anda mengkonfigurasi Dayakan Telnet/Dayakan SSH/Port SSH/Benarkan Log Masuk Kata Laluan/Kunci Dibenarkan/Masa Tamat Melahu.

3. Klik **Apply (Guna)**.

4.2.3 Menatarkan perisian tegar

NOTA: Muat turun perisian tegar terkini dari laman web ASUS di <https://www.asus.com>.

Untuk menatarkan perisian tegar:

1. Daripada panel navigasi, pergi ke **Settings (Tetapan) > Administration (Pentadbiran) > Firmware Upgrade (Naik Taraf Perisian Tegar)**.
2. Dalam item **New Firmware File (Fail Perisian Tegar baru)**, klik **Browse (Semak Imbas)**. Navigasi ke fail perisian tegar yang dimuat turun.
3. Klik **Upload (Muat naik)**.

NOTA:

- Apabila proses naik taraf selesai, tunggu seketika untuk sistem but semula.
- Jika proses penataran gagal, penghala berwayar secara automatik memasuki mod penyelamat dan penunjuk kuasa LED di panel depan mula berkelip-kelip secara perlahan.

The screenshot shows the 'Auto Firmware Upgrade' and 'Security Upgrade' settings on an ASUS router. The 'Auto Firmware Upgrade' section has a toggle switch set to 'ON' and a 'Preferable Upgrade Time' set to 04:47 on Monday, Jan 01 00:11:28 2024. Below this, a note states that some upgrades will still be downloaded and installed automatically even if the feature is turned off. The 'Security Upgrade' section also has a toggle switch set to 'ON'. Below this, a note states that some upgrades will still be downloaded and installed automatically even if the feature is turned off. The 'Firmware Version' section has a 'Check' button and a checkbox labeled 'I would like to retrieve beta firmware.' which is currently unchecked. Below this, the 'AiMesh router' section shows the 'Current Version' as 3.0.0.6.382.45841-43051067.346-616540 and the 'Manual firmware update' as U60080. At the bottom, a note states: 'Note: A manual firmware update will only update selected AiMesh routers / nodes, when using the AiMesh system. Please make sure you are updating the correct AiMesh firmware version to each applicable router / node.'

4.2.4 Tetapan Pemulihan/Penyimpanan/Memuat Naik

Untuk memulihkan/menyimpan/memuat naik tetapan penghala berwayar:

1. Daripada panel navigasi, pergi ke **Settings (Tetapan) > Administration (Pentadbiran) > Restore/Save/Upload Setting (Tetapan Pemulihan/Simpan/Muat Naik)**.
2. Pilih tugas yang anda ingin lakukan:
 - **Factory default (Lalai kilang)**: Asalkan semua tetapan, dan kosongkan semua log data untuk AiProtection, Penganalisis Trafik dan Sejarah Web.
 - **Save setting (Simpan tetapan)**: Klik pada kotak semak ini jika anda mahu berkongsi fail konfigurasi untuk penyahpepajian. Memandangkan kata laluan asal dalam fail konfigurasi akan dialih keluar, jangan import fail itu ke penghala anda..
 - **Restore setting (Pulihkan tetapan)**: Muat naik tetapan pemulihan yang ingin anda guna.

PENTING! Jika isu berlaku, muat naik versi perisian tegar terkini dan konfigurasi tetapan baru. Jangan pulihkan penghalan ke tetapan lalai.

This function allows you to save current settings of ExpertWiFi (EMSB) to a file, or load settings from a file.

Factory default	Restore	☒ Initialize all the settings, and clear all the data log for AiProtection, Traffic Analyzer and Web History.
Save setting	Save setting	☐ Click on this checkbox if you want to share the config file for debugging. Since the original password in the config file will be removed, please do not import the file into your router.
Restore setting	Upload	

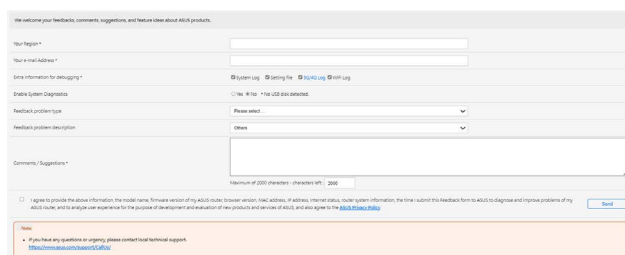
4.2.5 Feedback (Maklum Balas)

Untuk menggunakan Maklum Balas:

1. Dari panel navigasi, pergi ke **Settings (Tetapan) > Administration (Pentadbiran) > Feedback (Maklum Balas)**.
2. Masukkan wilayah, alamat e-mel, maklumat tambahan anda untuk penyahpejatan, komen dan cadangan, serta hantarkan kembali log penghala anda untuk penyelesaian masalah.

PENTING!

- Huraikan komen anda berkenaan situasi itu secara terperinci untuk mendapatkan jawapan pantas.
- Sila bersetuju dengan Dasar Privasi ASUS.



The screenshot shows the ASUS Feedback form. At the top, it says "We welcome your feedback, comments, suggestions, and feature ideas about ASUS products." Below this are several input fields: "Your Region" (a dropdown menu), "Your e-mail Address" (a text input field), and "Email information for debugging" (a section with checkboxes for "System Log", "Setting file", "Firmware Log", and "Web Log"). Below these are "Enable System Diagnostics" (a checkbox), "Feedback problem type" (a dropdown menu with "Phone error" selected), and "Feedback problem description" (a dropdown menu with "Others" selected). At the bottom is a large text area for "Comments / Suggestions" with a character count "Maximum of 2000 characters - characters left: 2000". Below the form is a checkbox for "I agree to provide the above information (the model name, firmware version of my ASUS router, browser version, IP address, internet status, router system information, the time I submit this feedback form to ASUS to diagnose and improve problems of my ASUS router, and to arrange user experience for the purpose of development and evaluation of new products and services of ASUS, and also agree to the [ASUS Privacy Policy](#))" and a "Send" button. At the very bottom, there is a note: "Note: If you have any questions or urgent issues, please contact technical support. [https://www.asus.com/support/Contact](#)".

4.2.6 Privasi

1. Untuk pengikatan akaun, sambungan DDNS dan Jauh (Aplikasi Penghala ASUS/Aplikasi Lyra/AiCloud/AiDisk):

Sila ambil perhatian bahawa maklumat anda, termasuk nama model produk anda, versi perisian tegar, status Internet, Alamat IP, alamat MAC dan nama DDNS, akan dikumpulkan oleh ASUS menerusi fungsi di atas.

Jika anda mahu menyahdayakan perkongsian maklumat anda dengan ASUS menerusi fungsi di atas, sila klik **Withdraw (Tarik Balik)** di bawah. Walau bagaimanapun, sila ambil perhatian bahawa ciri/fungsi ini mungkin tidak berfungsi jika anda berhenti berkongsi maklumat anda dengan ASUS.

PENTING!

- Selepas anda mengklik Tarik Balik, beberapa perubahan akan berlaku seperti yang disenaraikan di bawah:
 - Nama DDNS yang sedang anda guna tidak akan disimpan dalam penghala anda.
 - Aplikasi Penghala ASUS, aplikasi Lyra, AiCloud, AiDisk hanya boleh digunakan apabila peranti anda berada dalam LAN yang sama dengan penghala.

2. Notis PRIVASI ASUS (untuk naik taraf perisian tegar/keselamatan):

Sila ambil perhatian bahawa maklumat anda akan dikumpulkan oleh penghala ASUS bagi tujuan naik taraf perisian tegar/keselamatan. Jika anda mahu menyahdayakan perkongsian maklumat anda dengan penghala ASUS, sila klik **Withdraw (Tarik Balik)** di bawah.

PENTING! Mengklik **Withdraw (Tarik Balik)** di sini boleh menyebabkan kegagalan menaik taraf perisian tegar terkini dan mendapatkan perlindungan terkini pada penghala ASUS anda. Walau bagaimanapun, untuk melindungi keselamatan penghala anda dan memastikan pematuhan terhadap undang-undang, naik taraf bagi menangani masalah keselamatan penting atau memenuhi keperluan undang-undang/kawal selia masih akan dimuat turun dan dipasang secara automatik.

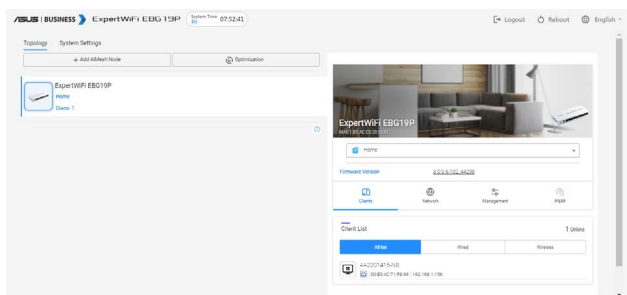
4.3 AiMesh

4.3.1 Menyediakan sistem AiMesh ExpertWiFi

Untuk membina sistem AiMesh ExpertWiFi anda, anda perlu mengkonfigurasi tetapannya.

Untuk menyediakan tetapan sistem AiMesh ExpertWiFi:

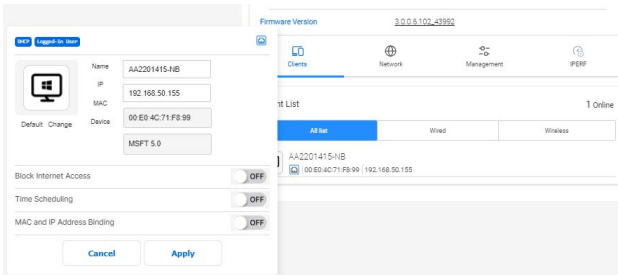
1. Dari panel navigasi, pergi ke **AiMesh > Topology (Topologi)**.
2. Anda boleh mengklik bahagian bawah **Set up as AiMesh Node (Sediakan sebagai Nod AiMesh)** untuk menambah peranti ExpertWiFi di bawah kawalan EBG19P.



3. Pergi ke **AiMesh > System Settings (Tetapan Sistem)** untuk mendayakan atau menyahdayakan **AiMesh node Ethernet auto setup (Penyediaan auto Ethernet nod AiMesh)**, **Ethernet Backhaul Mode (Mod Angkut Balik Ethernet)**, konfigurasi **Roaming Block List (Senarai Sekatan Perayauan)**, **System Reset to Factory Default (Penetapan Semula Sistem kepada Lalai Kilang)** atau **System Reset (Penetapan Semula Sistem)**.



4.3.2 Menguruskan klien rangkaian anda

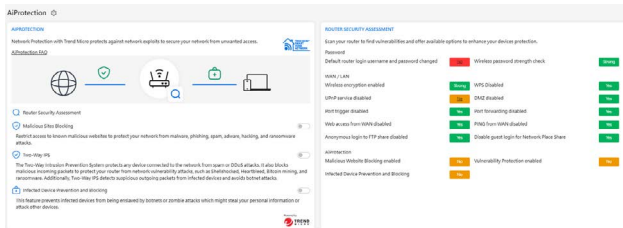


Untuk mengurus klien rangkaian anda:

1. Dari panel navigasi, pergi ke **AiMesh > Topology (Topologi)**.
2. Pilih ikon **Clients (Klien)** untuk memaparkan maklumat klien rangkaian anda seperti nama, alamat MAC dan IP klien.
3. Anda boleh menyekat akses klien kepada rangkaian anda, menyahdayakan penjadualan waktunya atau menyahdayakan pengikatan MAC dan IP dengan mengalihkan penggelongsor kepada **OFF (MATI)**.
4. Klik **Apply (Guna)** setelah selesai.

4.4 AiProtection

AiProtection menyediakan pemantauan masa nyata yang mengesan perisian hasad, perisian pengintip dan akses tidak dikehendaki. Ia juga menapis laman web dan aplikasi yang tidak dikehendaki serta membolehkan anda menjadualkan masa supaya peranti yang bersambung dapat mengakses Internet.

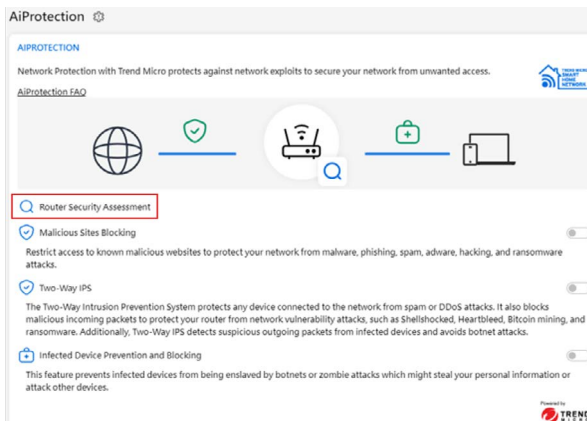


4.4.1 Perlindungan Rangkaian

Perlindungan Rangkaian menghalang rangkaian daripada mengeksploitasi dan menjamin keselamatan rangkaian anda daripada akses yang tidak dikehendaki.

Untuk menilai keselamatan penghala anda:

1. Dari panel navigasi, pergi ke **AiProtection**.
2. Klik **Router Security Assessment (Penilaian Keselamatan Penghala)** untuk memaparkan keputusan penilaian keselamatan.



ROUTER SECURITY ASSESSMENT		
Scan your router to find vulnerabilities and offer available options to enhance your devices protection.		
Password		
Default router login username and password changed	No	Wireless password strength check
		Strong
WAN / LAN		
Wireless encryption enabled	Strong	WPS Disabled
		Yes
UPnP service disabled	No	DMZ disabled
		Yes
Port trigger disabled	Yes	Port forwarding disabled
		Yes
Web access from WAN disabled	Yes	PING from WAN disabled
		Yes
Anonymous login to FTP share disabled	Yes	Disable guest login for Network Place Share
		Yes
AiProtection		
Malicious Website Blocking enabled	No	Vulnerability Protection enabled
		No
Infected Device Prevention and Blocking	No	

PENTING! Item yang ditandai sebagai **Yes (Ya)** pada halaman **ROUTER SECURITY ASSESSMENT (PENILAIAN KESELAMATAN PENGHALA)** dianggap berada pada status safe (selamat). Item ditandai sebagai **No (Tidak)** amat disyorkan untuk dikonfigurasi sewajarnya.

- (Pilihan) Dari halaman **ROUTER SECURITY ASSESSMENT (PENILAIAN KESELAMATAN PENGHALA)**, secara manual konfigurasi item ditandai sebagai **No (Tidak)**. Untuk melakukan ini:

- Klik item.

NOTA: Apabila anda mengklik item, utiliti memajukan anda ke halaman tetapan item.

- Dari halaman tetapan keselamatan item, konfigurasi dan buat perubahan yang perlu kemudian klik **Apply (Guna)** apabila selesai.
 - Kembali ke halaman **ROUTER SECURITY ASSESSMENT (PENILAIAN KESELAMATAN PENGHALA)** dan klik **Close (Tutup)** untuk keluar halaman.
- Untuk mengkonfigurasi tetapan keselamatan secara automatik, klik **Secure Your Router (Jamin Keselamatan Penghala Anda)**.
 - Apabila gesaan mesej muncul, klik OK.

Untuk mendayakan perlindungan rangkaian:

- Dari panel navigasi, pergi ke **AiProtection**.

2. Pilih jenis perlindungan yang mahu anda laksanakan dan luncurkan ia kepada hidup. Anda boleh memilih antara **Malicious Sites Blocking (Sekatan Laman Berniat Jahat)**, **Two-Way IPS (IPS Dua Hala)** dan **Infected Device Prevention and Blocking (Pencegahan dan Sekatan Peranti Dijangkiti)**.

Pemblokian Tapak Hasad

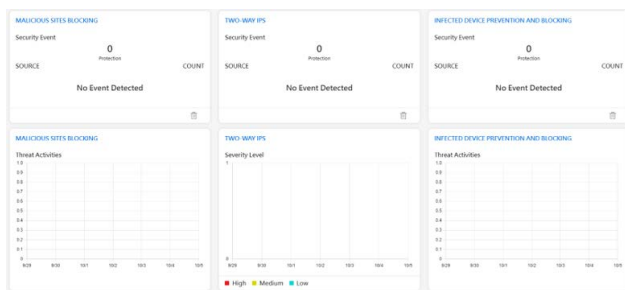
Ciri ini menyekat akses kepada laman web berniat jahat yang dikenali untuk melindungi rangkaian anda daripada perisian hasad, pemancingan data, spam, perisian iklan, penggodaman dan serangan ransomware.

IPS Dua Hala

IPS Dua Hala (Sistem Pencegahan Pencerobohan) melindungi peranti yang bersambung daripada spam atau serangan DDoS. Ia juga menyekat paket masuk berniat jahat untuk melindungi penghala anda daripada serangan kerentanan rangkaian, seperti Shellshocked, Heartbleed, pelombongan Bitcoin, dan ransomware. Selain itu, IPS Dua Hala mengesan paket keluar yang mencurigakan daripada peranti yang dijangkiti dan mengelakkan serangan botnet.

Pencegahan Peranti Terjangkit dan Halangan

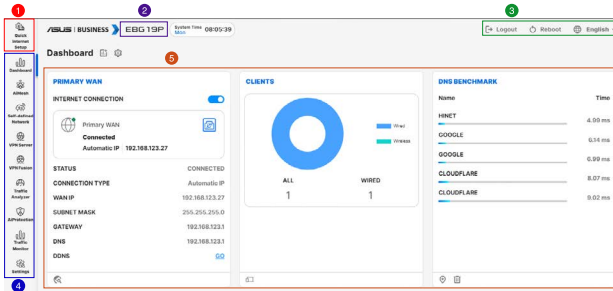
Ciri ini menghalang peranti yang dijangkiti daripada dijadikan hamba oleh botnet atau serangan zombi yang mungkin mencuri maklumat peribadi anda atau menyerang peranti lain.



3. Setuju dengan **Trend Micro End User License Agreement (Perjanjian Lesen Pengguna Akhir Mikro Trend)**.

4.5 Dashboard (Papan Pemuka)

Papan pemuka membolehkan anda mengurus rangkaian anda seperti sambungan Internet, sambungan klien, penanda aras DNS, status sistem, port Ethernet, dan monitor trafik.



1. QIS (Penyediaan Internet Pantas)
2. Nama model
3. Butang arahan
4. Navigasi panel
5. Maklumat papan pemuka

4.6 Kawalan akses peranti

4.6.1 Penapis Web & Aplikasi

Penapis Web & Aplikasi membenarkan anda untuk menghalang akses kepada laman web dan aplikasi tidak diingini.

Untuk menggunakan Penapis Web & Aplikasi:

1. Dari panel navigasi, pergi ke **Settings (Tetapan) > Device access control (Kawalan akses peranti) > Web & Apps Filters (Penapis Web & Aplikasi)**.
2. Luncurkan bar kepada **ON (HIDUP)** untuk mendayakan **Web & Apps Filters (Penapis Web & Aplikasi)**.
3. Dalam lajur **Client Name (Nama Klien)**, pilih klien yang penggunaan rangkaiannya anda mahu kawal. Nama klien boleh diubah suai dalam senarai klien peta rangkaian.
4. Tandakan kategori kandungan tidak diingini.
5. Klik **+** untuk menambah peraturan dan klik **Apply (Guna)**.

Jika anda mahu menyahdayakan peraturan secara sementara, nyah tandakan peraturan itu.

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

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

If you want to disable the rule temporarily, uncheck the check box in front of rule.

Web & Apps Filters ☒

Client Name (Max Limit: 64)	Client Address	Content Category	Add / Delete
☐		☐ Adult Block undesirable content to prevent children from viewing sites that contain material of a sexual, violent, and vulgar nature.	
☒	ex: 08-BF-0B-28-1C-C0	☐ Instant Message and Communication Block instant communication software and messaging apps to prevent children from becoming addicted to social networking sites.	+
		☐ P2P and File Transfer By blocking P2P and File Transferring you can make sure your network has a better quality of data transmission.	
		☐ Streaming and Entertainment By blocking streaming and entertainment services you can limit the time your children spend online.	

No data in table

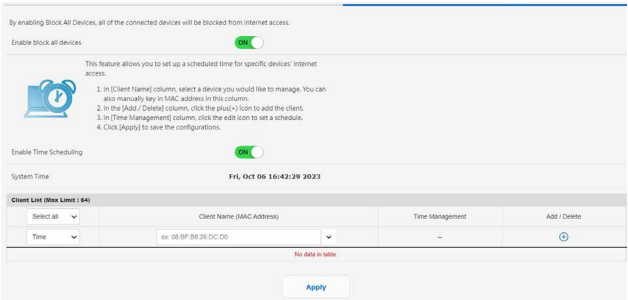
Powered by

4.6.2 Penjadualan Waktu

Penjadualan Waktu membolehkan anda menyediakan waktu berjadual untuk akses Internet peranti khusus.

Untuk menggunakan Penjadualan Waktu:

- 1. Dari panel navigasi, pergi ke **Settings (Tetapan) > Device access control (Kawalan akses peranti) > Time Scheduling (Penjadualan Waktu)**.
- 2. Luncurkan bar kepada **ON (HIDUP)** untuk mendayakan **Enable Time Scheduling (Dayakan Penjadualan Waktu)**.
- 3. Dari lajur **Clients Name (Nama Klien)**, pilih atau masukkan nama klien daripada kotak senarai jantai bawah.
- 4. Klik **+** untuk menambah profil klien.
- 5. Klik **Apply (Guna)** untuk menyimpan tetapan



4.7 Tembok Api

4.7.1 Umum

Penghala berwayar boleh menjadi tembok api perkakas untuk rangkaian anda

NOTA: Ciri Tembok Api didayakan secara lalai.

Untuk menyediakan tetapan Tembok Api asas:

1. Daripada panel navigasi, pergi ke **Settings (Tetapan) > Firewall (Tembok Api) > General (Am)**.
2. Pada medan **Enable Firewall (Dayakan Tembok Api)**, pilih **Yes (Ya)**.
3. Pada perlindungan **Enable DoS (Dayakan DoS)**, pilih **Yes (Ya)** untuk melindungi rangkaian anda daripada serangan DoS (Nafi Khidmat) walaupun ini mungkin menjejaskan prestasi penghala anda.
4. Anda juga boleh memantau pertukaran paket antara sambungan LAN dan WAN. Pada Jenis paket yang dilog, pilih **Dropped (Digugurkan)**, **Accepted (Diterima)**, atau **Both (Kedua-duanya)**.
5. Klik **Apply (Guna)**.

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

Enable Firewall Yes No

Enable DoS protection No Yes

Outgoing packets type None

Request OS fingerprint (Request from WAN) No Yes

Basic Config

Enable WAN inbound Firewall rules No Yes

Inbound Firewall Rules (After Local LAN)

Source IP	Port Range	Protocol	Action
		TCP	No data in table

Outbound Firewall

All outbound traffic coming from WAN needs on your LAN is allowed, as well as related inbound traffic. Any other inbound traffic must be specifically allowed here. You can have the remote IP block to allow traffic from any remote host. A subnet can also be specified. (2000:1111:2222:3333:: for example)

Basic Config

Enable WAN Outbound No Yes

Outbound Server List

Outbound Firewall Rules (After Local LAN)

Service Name	Remote IP/CIDR	Local IP	Port Range	Protocol	Action
				TCP	

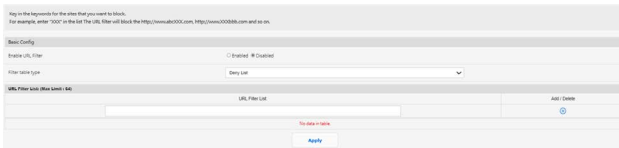
4.7.2 Penapis URL

Anda boleh menentukan kata kerja atau alamat web untuk mengelakkan akses ke URL tertentu.

NOTA: Penapis URL adalah berdasarkan pertanyaan DNS. Jika klien rangkaian telah mengakses tapak web seperti `http://www.abcxxx.com`, maka tapak web tidak akan disekat (cache DNS dakan sistem menyimpan tapak web yang dilawati sebelum ini). Untuk menyelesaikan isu ini, kosongkan cache DNS sebelum menyediakan Penapis URL.

Untuk menyediakan penapis URL:

1. Daripada panel navigasi, pergi ke **Settings (Tetapan) > Firewall (Tembok Api) > URL Filter (Penapis URL)**.
2. Pada medan **Enable URL Filter (Dayakan Penapis URL)**, pilih **Enabled (Didayakan)**.
3. Masukkan URL dan klik butang .
4. Klik **Apply (Guna)**.



Apply to the keywords for the sites that you want to block.
For example, enter "192.1" in the list URL Filter will block the `http://www.192.168.0.0/` and so on.

Basic Config

Enable URL Filter ☒ Enabled ☐ Disabled

Filter action type Drop

URL Filter List (Show Lines) 0/4

URL Filter List

No data to display

[Apply](#)

4.7.3 Penapis kata kunci

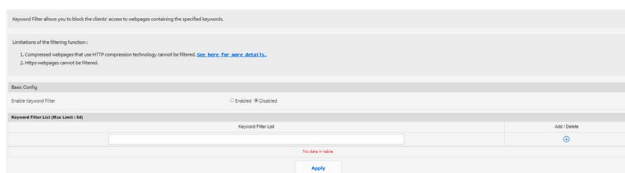
Penapis kata kunci menyekat akses ke laman web mengandungi kata kunci yang dinyatakan.

Untuk menyediakan penapis kata kunci:

1. Daripada panel navigasi, pergi ke **Settings (Tetapan) > Firewall (Tembok Api) > Keyword Filter (Penapis Kata Kunci)**.
2. Pada medan **Enable Keyword Filter (Dayakan Penapis Kata Kunci)**, pilih **Enabled (Didayakan)**.
3. Masukkan perkataan atau frasa dan klik butang .
4. Klik **Apply (Guna)**.

NOTA:

- Penapis Kata Kunci adalah berdasarkan pertanyaan DNS. Jika klien rangkaian telah mengakses tapak web seperti `http://www.abcxxx.com`, maka tapak web tidak akan disekat (cache DNS dakan sistem menyimpan tapak web yang dilawati sebelum ini). Untuk menyelesaikan isu ini, kosongkan cache DNS sebelum menyediakan Penapis Kata Kunci.
 - Laman web termampat menggunakan pemampatan HTTP tidak boleh ditapis. Halaman HTTPS juga tidak boleh disekat menggunakan penapis kata kunci.
-



4.7.4 Penapis Perkhidmatan Rangkaian

Penapis Perkhidmatan Rangkaian menyekat pertukaran paket LAN ke WAN dan mengehadkan klien rangkaian daripada mengakses perkhidmatan web khusus seperti Telnet atau FTP.

Untuk menyediakan penapis Perkhidmatan Rangkaian:

1. Klik **Daftar** pada panel navigasi, pergi ke **Settings (Tetapan) > Firewall (Tembok Api) > Network Service Filter (Penapis Perkhidmatan Rangkaian)**.
2. Pada medan **Enable Network Services Filter (Dayakan Penapis Perkhidmatan Rangkaian)**, pilih **Yes (Ya)**.
3. Pilih jenis jadual Penapis. **Deny List (Senarai Nafikan)** menyekat perkhidmatan rangkaian yang ditentukan. **Allow List (Senarai Benarkan)** menghadkan akses hanya ke perkhidmatan rangkaian yang ditentukan.
4. Nyatakan hari dan masa apabila penapis akan diaktifkan.
5. Untuk menentukan Perkhidmatan Rangkaian untuk menapis, masukkan IP Sumber, IP Destinasi, Liputan Port, dan Protokol. Klik .
6. Klik **Apply (Guna)**.

Network Services Use the blocks the client is allowed to exchange and enable them from setting specific network services.

For example, if you do not want the client to use the Internet service, you go to the destination port, the traffic that can use port 80 will be blocked (but https can still be blocked).

When you click the block icon to enable the client to use the client-side applications.

Days List Duration: (during the scheduled duration, clients in the Days List cannot use the specified network service, the specified durations, all the clients in the List can access the specified network services.

After List Duration: (during the scheduled duration, clients in the After List can use (SMTP) can use the specified network service.

NOTE: If you set the value for the After List, IP addresses outside the network will not be able to access the Internet at any Internet service.

Network Services Filter

Enable Network Services Filter ☐ / Yes: No / Yes

Filter Mode Type

User/Group Applications

Date to Enable LANs to WANs Filter

Time of Day to Enable LANs to WANs Filter

Date to Enable LANs to WANs Filter

Time of Day to Enable LANs to WANs Filter

Filtered DHCP packet types

Network Services Filter (New Lan: 10)

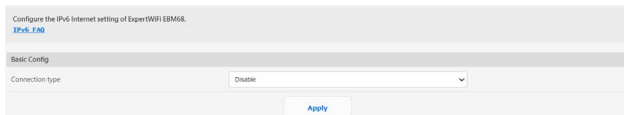
Source IP	Port Range	Destination IP	Port Range	Protocol	Action
				TCP	v

[No data to view](#)

[Add](#)

4.8 IPv6

Penghala berwayar ini menyokong pengalamatan IPv6, sistem yang menyokong lebih alamat IP. Hubungi ISP anda jika perkhidmatan Internet anda menyokong IPv6.



Untuk menyediakan IPv6:

1. Daripada panel navigasi, pergi ke **Settings (Tetapan) > IPv6**.
2. Pilih **Connection type (Jenis sambungan)** anda. Pilih konfigurasi berbeza bergantung pada jenis sambungan terpilih anda.
3. Masukkan tetapan IPv6 LAN dan DNS anda.
4. Klik **Apply (Guna)**.

NOTA:

- Sila rujuk ISP anda berkenaan maklumat khusus IPv6 untuk perkhidmatan Internet anda.
 - Untuk maklumat lanjut, sila lawati <https://www.asus.com/support/FAQ/113990>.
-

4.9 LAN

4.9.1 LAN IP

Skrin IP LAN membolehkan anda mengubah suai tetapan IP LAN penghala berwayar anda.

NOTA: Apa-apa perubahan kepada alamat IP LAN akan ditunjukkan pada tetapan DHCP anda.

Configure the LAN setting of EBG19P.

Host Name	EBG19P-1064
EBG19P's Domain Name	
IP Address	192.168.50.1
Subnet Mask	255.255.255.0

Apply

Untuk mengubah suai tetapan IP LAN:

1. Daripada panel navigasi, pergi ke **Settings (Tetapan) > LAN > IP LAN**.
2. Mengubah suai **IP address (alamat IP)** dan **Subnet Mask**.
3. Apabila selesai, klik **Apply (Guna)**.

4.9.2 Pelayan DHCP

DHCP (Protokol Konfigurasi Hos Dinamik) adalah protokol untuk konfigurasi automatik yang digunakan pada rangkaian IP. Pelayan DHCP boleh menetapkan alamat IP kepada setiap klien dan memaklumkan klien tentang IP pelayan DNS dan IP get laluan lalai.

DHCP (Dynamic Host Configuration Protocol) is a protocol for the automatic configuration used on IP networks. The DHCP server can assign each client an IP address and delivers the client of the DNS server IP and default gateway. WinBox DHCP supports up to 255 IP addresses for your local network.

[Manually assigned IP address: DHCP, 192.168.80.2-192.168.80.254](#)

Basic Config

Enable the DHCP Server ☒ Yes ☐ No

Export/Import DHCP's Domain Name

IP Pool Starting Address

IP Pool Ending Address

Lease Time (seconds)

Default Gateway

DHCP and DNS Server Setting

DHCP Server 1

DHCP Server 2

Advertisement router's IP in addition to user specified DNS

DNS Server

Manual Assignment

Enable Manual Assignment ☐ Yes ☐ No

Manually Assigned IP address (DHCP Pool Range: 192.168.80.2-192.168.80.254)	Client Name (Optional)	IP Address	DNS Server (Optional)	Host Name (Optional)	Add/Remove
192.168.80.2-192.168.80.254					

Untuk mengkonfigurasi pelayan DHCP:

1. Daripada panel navigasi, pergi ke **Settings (Tetapan) > LAN > DHCP Server (Pelayan DHCP)**.
2. Dalam medan **Enable the DHCP Server (Dayakan Pelayan DHCP)**, tandakan **Yes (Ya)**.
3. Dalam kotak teks **Domain Name (Nama Domain)**, masukkan nama domain untuk penghala berwayar.
4. Dalam medan **IP Pool Starting Address (Alamat Permulaan Kumpulan IP)**, masukkan alamat IP permulaan.
5. Dalam medan **IP Pool Ending Address (Alamat Akhir Kumpulan IP)**, masukkan alamat IP akhir.

6. Dalam medan **Lease Time (Masa Pajakan)**, nyatakan dalam saat bila alamat IP yang diuntukkan akan tamat tempoh. Sebaik sahaja ia mencapai had masa ini, pelayan DHCP kemudiannya akan menguntukkan alamat IP yang baru.

NOTA:

- ASUS menyarankan agar anda menggunakan format alamat IP 192.168.1.xxx (di mana xxx boleh jadi sebarang nombor antara 2 dan 254) apabila menyatakan julat alamat IP.
 - IP Pool Starting Address (Alamat Permulaan Kumpulan IP) tidak boleh melebihi Alamat Akhir Kumpulan IP).
-
7. Dalam bahagian **DNS and WINS Server Settings (Tetapan DNS dan WINS Pelayan)**, masukkan alamat IP Pelayan DNS dan Pelayan WINS jika diperlukan.
 8. Penghala berwayar ada juga boleh menugaskan alamat IP kepada peranti pada rangkaian secara manual. Pada medan **Enable Manual Assignment (Dayakan Tugas Manual)**, pilih **Yes (Ya)** untuk menugaskan alamat IP ke alamat MAC khusus pada rangkaian. Sehingga 32 alamat MAC boleh ditambah pada senarai DHCP untuk penugasan manual.

4.9.3 Hala

Fungsi ini membolehkan anda menambah peraturan penghalaan pada penghala. Ia berguna jika anda menyambungkan beberapa penghala di belakang EBG19P untuk berkongsi sambungan yang sama kepada Internet.

This function allows you to add routing rules into ExpertWiFi EBM68. It is useful if you connect several routers behind ExpertWiFi EBM68 to share the same connection to the Internet.

Basic Config

Enable static routes ☒ Yes ☐ No

Static Route List (Max Limit : 32)

Network/Host IP	Network	Gateway	Metric	Interface	Add / Delete
					⊕

No data in table.

Untuk mengkonfigurasi jadual Penghalaan LAN:

1. Daripada panel navigasi, pergi ke **Settings (Tetapan) > LAN > Route (Hala)**.
2. Pada medan **Enable static route (Dayakan hala statik)**, pilih **Yes (Ya)**.
3. Pada **Static Route List (Senarai Hala Statik)**, masukkan maklumat rangkaian titik akses atau nod lain. Klik butang **⊕** atau **⊖** untuk menambah atau membuang peranti pada senarai.
4. Klik **Apply (Guna)**.

4.9.4 IPTV

Penghala berwayar menyokong sambungan ke perkhidmatan IPTV melalui ISP atau LAN. Tab IPTV memberikan tetapan konfigurasi yang diperlukan untuk menyediakan IPTV, VoIP, multisiar, dan UDP untuk perkhidmatan anda. Hubungi ISP anda untuk maklumat khusus mengenai perkhidmatan anda.

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

LAN Port

Select IP Profile

None

Choose IPTV STB Port

None

Special Applications

Use DHCP routes

Microsoft

Enable multicast routing

Disable

UDP Proxy (udpnp)

0

Apply

4.9.5 Kawalan Suis

Membolehkan anda menyediakan penghala untuk fungsi kawalan suis. Anda boleh menggabungkan dua port LAN 1Gbps untuk menghantar sehingga kelajuan berwayar 2Gbps melalui ikatan dengan NAS anda yang serasi atau peranti rangkaian lebar jalur tinggi yang lain.

NOTA:

- Untuk menggunakan fungsi Protokol Kawalan Pengagregatan Pautan (LACP), peranti mesti menyokong protokol IEEE 802.3ad.
- Fungsi pengagregatan LAN boleh dikendalikan dengan menjadikan port LAN3 berpasangan dengan port LAN2.

Setting ExpertWiFi (802.3ad) switch control.

Jumbo Frame

Enable

Bonding/ Link aggregation

Enable

Enable Bonding (802.3ad) support for your wired client and then connect it to your Router's LAN3 and LAN2 port.

Apply

45

4.9.6 VLAN

VLAN (Rangkaian Kawasan Setempat Maya) merupakan rangkaian logik yang dicipta dalam rangkaian fizikal yang lebih besar. VLAN membolehkan anda membahagikan rangkaian kepada subrangkaian yang lebih kecil dan maya, yang boleh digunakan untuk mengasingkan trafik dan meningkatkan prestasi rangkaian.

Untuk menyediakan VLAN:

1. Daripada panel navigasi, pergi ke **Settings (Tetapan) > LAN > VLAN**.
2. Klik tab **Profile (Profil)** dan kemudian **+** untuk mencipta profil VLAN. Anda boleh menetapkan ID VLAN anda sendiri.
3. **Port isolation (Pengasingan port)** menyekat hak akses peranti yang berbeza dalam VLAN yang sama. Anda kini mencipta “Rangkaian VLAN Sahaja”, yang bermaksud rangkaian dengan VID tetapi tanpa DHCP.

VLAN Profile

VLAN Profile here refers to create a VLAN only network. If you want to create VLAN with DHCP, please go to Self-defined Network

Profile List			
Network Name (SSID)	VLAN ID	Port Isolation	Add / Delete
...		☐	+

AllMesh router

• EBG19P • 00:90:4C:19:10:64 • 00:90:4C:19:10:64	2 1 Gbps	3 1 Gbps	4 1 Gbps	5 1 Gbps
Mode	All(Default)	All(Default)	All(Default)	All(Default)
SDN (VLAN) Profile	Default	Default	Default	Default
• 00:90:4C:19:10:64	6 1 Gbps	7 1 Gbps	8 1 Gbps	9 1 Gbps
Mode	All(Default)	All(Default)	All(Default)	All(Default)
SDN (VLAN) Profile	Default	Default	Default	Default

4. Klik tab **VLAN** untuk memilih port dengan profil khusus dan mod (**Trunk / Access (Trunk/ Akses)**).

NOTA: Anda boleh memilih satu daripada mod lalai berikut:

Semua (Lalai) membolehkan semua paket bertag dan tidak bertag untuk mengakses.

Mod **Access (Akses)** membolehkan SDN(VLAN) yang dipilih mengakses. Anda boleh memilih profil yang dicipta oleh Rangkaian Tetamu pro atau VLAN.

Mod Trunk:

- - Benarkan semua bertag: Hanya paket bertag dibenarkan untuk mengakses.
- - Dengan SDN(VLAN) yang dipilih: Hanya SDN atau VLAN yang dipilih dibenarkan untuk mengakses.

5. Apabila selesai, klik **Apply (Guna)**.

NOTA: Untuk maklumat lanjut, sila lawati <https://www.asus.com/support/FAQ/1049415/>.

4.10 Alatan Rangkaian

Untuk menggunakan alatan rangkaian, dari panel navigasi, pergi ke **Settings (Tetapan) > Network Tools (Alatan Rangkaian)**.

4.10.1 Analisis Rangkaian

Hantar paket ICMP ECHO_REQUEST ke hos rangkaian.

4.10.2 Netstat

Paparkan butiran rangkaian.

4.10.3 Hidupkan LAN

Ciri WOL (Bangkit Pada LAN) membolehkan anda membangkitkan komputer daripada mana-mana peranti dalam rangkaian.

4.10.4 Peraturan Sambung Pintar

Sediakan maklumat berkaitan Smart Connect.

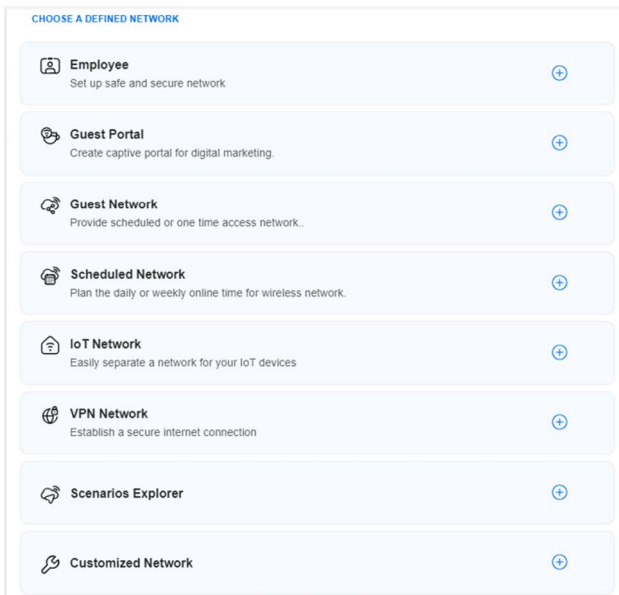
4.11 Rangkaian Ditetapkan Sendiri

Rangkaian Ditetapkan Sendiri (SDN) menyediakan sehingga lima SSID untuk memisahkan dan mengutamakan peranti bagi penggunaan perniagaan yang berbeza dan alternatif rangkaian, mewujudkan segmen rangkaian untuk pekerja, portal tetamu, rangkaian tetamu, rangkaian berjadual, rangkaian IoT dan rangkaian VPN.

PENTING! Untuk menjadikan fungsi Wi-Fi tersedia, pastikan Titik Akses (AP) wayarles seperti ExpertWiFi EBA63 atau penghala seperti ExpertWiFi EBR63 atau ExpertWiFi EBM68 disepadukan dalam rangkaian AiMesh EBG19P.

Untuk mencipta Rangkaian Ditetapkan Sendiri:

1. Dari panel navigasi, pergi ke **Self-defined Network (Rangkaian Ditetapkan Sendiri)**.
2. Pilih rangkaian ditetapkan yang sesuai dengan senario khusus anda.



4.11.1 Pekerja

Membolehkan anda menyediakan tahap akses untuk penggunaan berbeza bagi meningkatkan keselamatan rangkaian. Disyorkan untuk pejabat yang menetapkan kebenaran ke jabatan yang berbeza.

Employee

Network Name (SSID)

Security

Password

RADIUS Setting

Authentication Method

WPA2-Personal

Wireless Security

More Config

Apply

4.11.2 Portal Tetamu

Membolehkan anda mencipta portal tetamu untuk pemasaran digital. Disyorkan untuk penggunaan di restoran, hotel atau trak makanan.

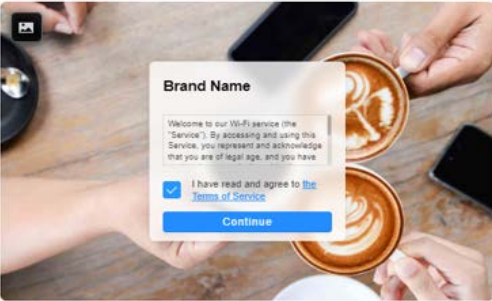
Guest Portal

Network Name (SSID)

Portal Type

Free WiFi

Brand Name

A preview of the guest portal interface. It shows a background image of hands holding coffee cups. Overlaid on this is a white box with the title 'Brand Name'. Inside the box, there is a welcome message: 'Welcome to our Wi-Fi service (the "Service"). By accessing and using this Service, you represent and acknowledge that you are of legal age, and you have'. Below this is a checked checkbox next to the text 'I have read and agree to the Terms of Service'. At the bottom of the box is a blue 'Continue' button.

More Config

Apply

4.11.3 Rangkaian Tetamu

Menyediakan pelawat sementara dengan akses berjadual atau satu kali kepada rangkaian. Disyorkan untuk penggunaan di pusat membeli-belah, gimnasium atau untuk pelawat.

The screenshot shows the 'Guest Network' configuration page. It includes fields for 'Network Name (SSID)', 'Security' (with an 'Open System' button and a 'Password' field), and 'WiFi Scheduling' (which is turned on). Under 'WiFi Scheduling', there are radio buttons for 'Scheduled' and 'One Time Access' (selected). Below these are buttons for access duration: '30 mins', '1 hr(s)', '2 hr(s)' (highlighted in blue), '4 hr(s)', '6 hr(s)', and 'Custom'. At the bottom, there is a 'More Config' section with a dropdown arrow and an 'Apply' button.

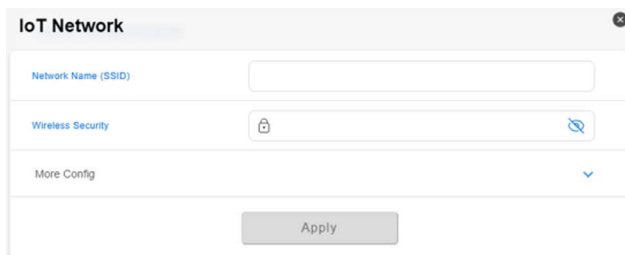
4.11.4 Rangkaian Berjadual

Merancang waktu dalam talian harian atau mingguan untuk rangkaian wayarles. Disyorkan untuk pembelajaran jauh, bilik darjah atau kegunaan kanak-kanak.

The screenshot shows the 'Scheduled Network' configuration page. It includes fields for 'Network Name (SSID)', 'Wireless Security' (with a lock icon and a key icon), and 'WiFi Scheduling' (which is turned on). Under 'WiFi Scheduling', there is an 'Online schedule' section with two rows: 'WEEKDAY(S)' with a time range of '17:00 - 21:00' and 'WEEKEND' with a time range of '16:00 - 22:00'. Each row has a toggle switch (both are turned on) and a trash icon. At the bottom, there is a 'More Config' section with a dropdown arrow and an 'Apply' button.

4.11.5 Rangkaian IoT

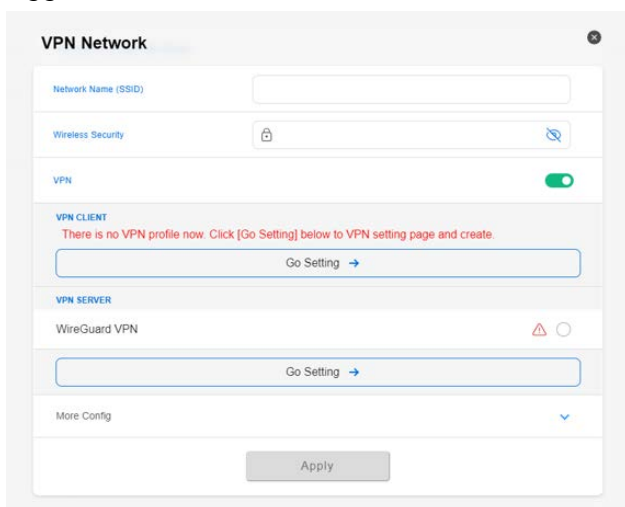
Membolehkan anda menyediakan rangkaian berasingan untuk peranti IoT dengan mudah. Disyorkan untuk penggunaan dengan peranti pengawasan, pembantu suara, lampu, kamera loceng pintu, kunci pintar dan sensor.



The IoT Network configuration interface is a light gray box with a title bar 'IoT Network' and a close button. It contains three main sections: 'Network Name (SSID)' with a text input field, 'Wireless Security' with a dropdown menu showing a lock icon and a blue link icon, and 'More Config' with a blue downward arrow. At the bottom is a gray 'Apply' button.

4.11.6 Rangkaian VPN

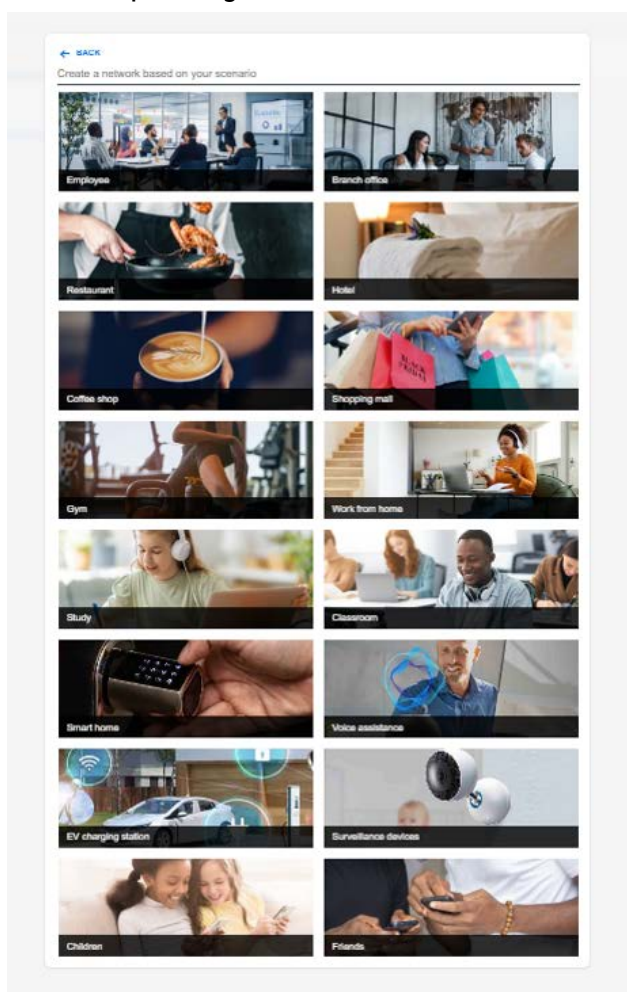
Membantu mewujudkan sambungan Internet selamat menggunakan VPN.



The VPN Network configuration interface is a light gray box with a title bar 'VPN Network' and a close button. It contains several sections: 'Network Name (SSID)' with a text input field, 'Wireless Security' with a dropdown menu showing a lock icon and a blue link icon, and a 'VPN' toggle switch that is turned on. Below the toggle is a 'VPN CLIENT' section with a red warning message: 'There is no VPN profile now. Click [Go Setting] below to VPN setting page and create.' followed by a 'Go Setting' button with a right arrow. Below that is a 'VPN SERVER' section with a 'WireGuard VPN' entry, a warning icon, and a 'Go Setting' button with a right arrow. At the bottom is a 'More Config' section with a blue downward arrow and a gray 'Apply' button.

4.11.7 Penjelajah Senario

Jika anda tidak tahu rangkaian yang mahu dicipta, anda boleh memilih sektor yang sepadan dengan gabungan anda untuk mencipta rangkaian.



4.11.8 Rangkaian Tersuai

Membolehkan anda memilih pilihan rangkaian diperibadikan.

Customized Network

Network Name (SSID)

Wireless Security

More Config

Apply

4.12 Log Sistem

Log Sistem mengandungi aktiviti rangkaian terakam anda.

NOTA: Log sistem menetapkan semula apabila penghala dibuat semula atau dimatikan.

Untuk melihat log sistem anda:

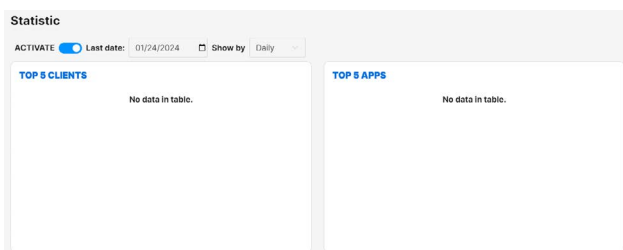
1. Daripada panel navigasi, pergi ke **Settings (Tetapan) > System Log (Log Sistem)**.
2. Anda boleh melihat aktiviti rangkaian anda dalam mana-mana tab ini:
 - General Log (Log Am)
 - DHCP Leases (Pajakan DHCP)
 - Port Forwarding (Pemajuan Port)
 - Routing Table (Jadual Penghalaan)
 - IPv6
 - Connections (Sambungan)

4.13 Penganalisis Trafik

4.13.1 Penganalisis Trafik

Untuk menggunakan penganalisis trafik:

1. Hidupkan **ACTIVATE (AKTIFKAN)**.
2. Tentukan tarikh terakhir untuk dipaparkan, dan pilih untuk memantau trafik rangkaian berasaskan harian, mingguan atau bulanan daripada senarai jantai bawah **Show by (Tunjukkan mengikut)**.
3. Lima klien teratas, lima aplikasi teratas, peranti, status klien dan analisis aplikasi akan dipaparkan.



4.14 Aplikasi USB

4.14.1 Pelayan Media

Pelayan media membolehkan anda menyediakan pelayan iTunes dan UPnP.

Setup the iTunes and UPnP media server.

iTunes Server

Enable iTunes Server ☐ OFF

Media Server

Enable UPnP Media Server ☒ ON

Media Server Name

Media Server Status Idle

Media Server Path Setting ☒ All Disks Shared ☐ Manual Media Server Path

[Apply](#)

Untuk melancarkan halaman tetapan Pelayan Media, pergi ke **Settings (Tetapan) > USB Application (Aplikasi USB) > Media Server (Pelayan Media)**.

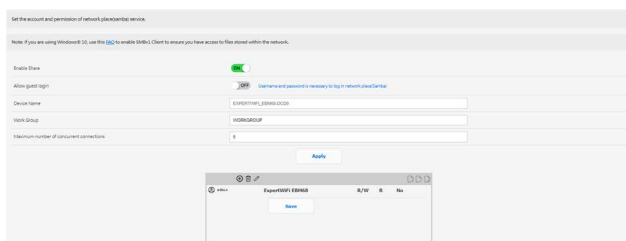
Rujuk ekpada yang berikut untuk huraian medan:

- **Enable iTunes Server (Dayakan Pelayan iTunes):** Pilih HIDUP/MATI untuk mendayakan / nyahdaya Pelayan iTunes.
- **Enable UPnP Media Server (Dayakan Pelayan Media UPnP):** Pilih HIDUP/MATI untuk mendayakan / nyahdaya Pelayan Media UPnP.
- **Media Server Name (Nama Pelayan Media):** Memasukkan nama pelayan media.
- **Media Server Path Setting (Tetapan Laluan Pelayan Media):** Pilih All Disks Shared (Semua Cakera Dikongsikan) atau Manual Media Server Path (Laluan Pelayan Media Manual).

Apabila selesai, klik **Apply (Guna)**.

4.14.2 Perkongsian (Samba) Tempat Rangkaian

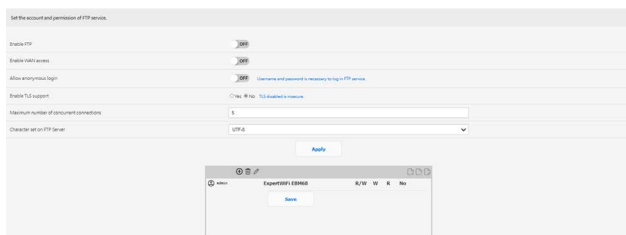
Kongsi Tempat Rangkaian (Samba) membolehkan anda menyediakan akaun dan kebenaran untuk perkhidmatan Samba.



Untuk menggunakan kongsi Samba, pergi ke **Settings (Tetapan) > USB Application (Aplikasi USB) > Network Place (Samba) Share (Perkongsian (Samba) Tempat Rangkaian)**.

4.14.3 Kongsi FTP

FTP Share membolehkan anda menyediakan akaun dan kebenaran untuk perkhidmatan FTP.



Untuk menggunakan Kongsi FTP, pergi ke **Settings (Tetapan) > USB Application (Aplikasi USB) > FTP Share (Kongsi FTP)**.

4.14.4 Pelayan Pencetak Rangkaian

4.14.4.1 ASUS EZ Printer Sharing

Utiliti ASUS EZ Printing Sharing membolehkan anda menyambung pencetak USB ke port USB penghala berwayar anda dan menyediakan pelayan pencetak. Ini membolehkan klien rangkaian anda mencetak dan mengimbas fail secara tanpa wayar.

NOTA: Fungsi pelayan pencetak disokong pada Windows® 10 dan Windows® 11.

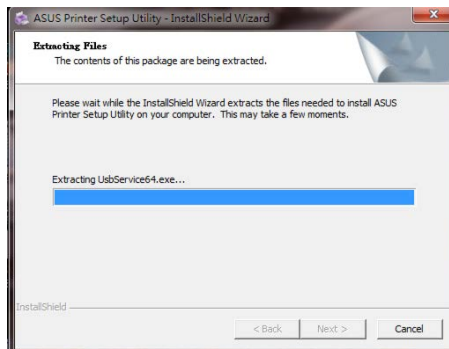
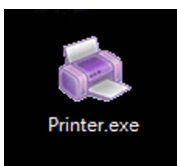
Untuk menyediakan mod perkongsian EZ Printer:

1. Daripada panel navigasi, pergi ke **Settings (Tetapan) > USB Application (Aplikasi USB) > Network Printer Server (Rangkaian Pelayan Pencetak)**.
2. Klik **Download Now! (Muat Turun Sekarang!)** untuk memuat turun utiliti rangkaian pencetak.

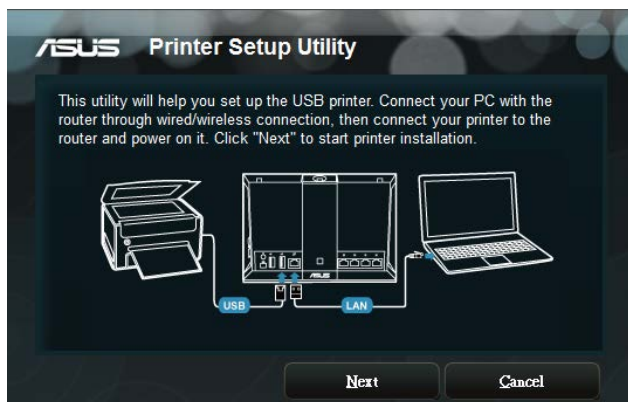


NOTA: Utiliti rangkaian pencetak disokong pada Windows® 10 dan Windows® 11 sahaja. Untuk memasang utiliti pada Mac OS, pilih **Use LPR protocol for sharing printer (Guna protokol LPR untuk perkongsian pencetak)**.

3. Nyahzip fail yang dimuat turun dan klik ikon Pencetak untuk menjalankan program penyediaan rangkaian pencetak.



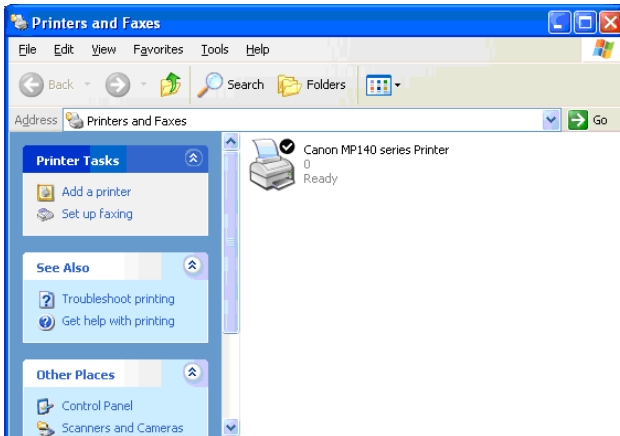
- Ikuti arahan pada skrin untuk menyediakan perkakas anda, kemudian klik **Next (Seterusnya)**.



- Tunggu beberapa minit untuk penyediaan pemulaan selesai. Klik **Next (Seterusnya)**.
- Klik **Finish (Selesai)** untuk melengkapkan pemasangan.
- Ikuti arahan OS Windows® untuk memasang pemacu pencetak.



8. Selepas pemasangan pemacu pencetak selesai, klien rangkaian boleh menggunakan pencetak.

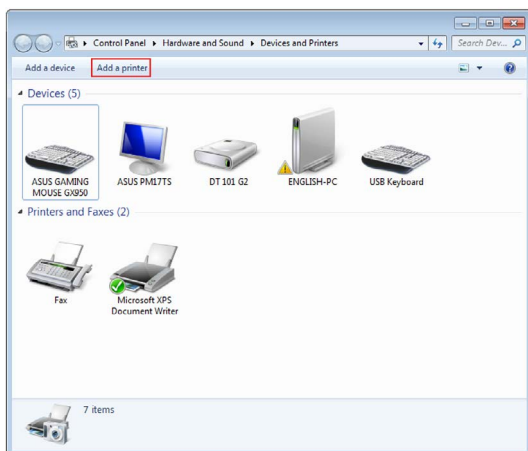


4.14.4.2 Menggunaka LPR untuk Berkongsi Pencetak

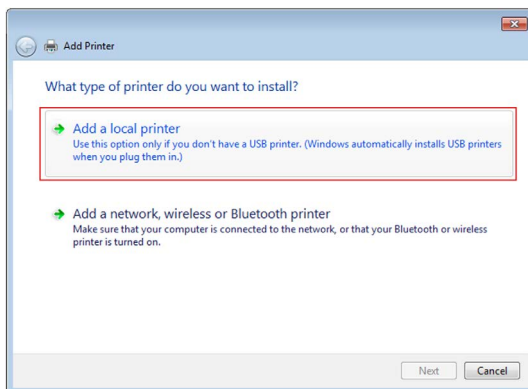
Anda boleh berkongsi pencetak anda dengan komputer yang berjalan pada sistem operasi Windows® dan MAC menggunakan LPR/LPD (Kawalan Jauh Talian Pencetak/ Daemon Talian Pencetak).

Untuk berkongsi pencetak LPR anda:

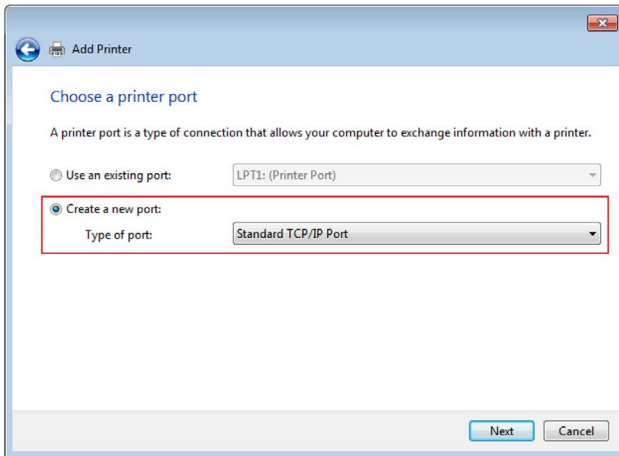
1. Dari desktop Windows®, klik **Start (Mula) > Devices and Printers (Peranti dan Pencetak) > Add a printer (Tambah Pecetak)** untuk menjalankan **Add Printer Wizard (Wizard Tambah Pencetak)**.



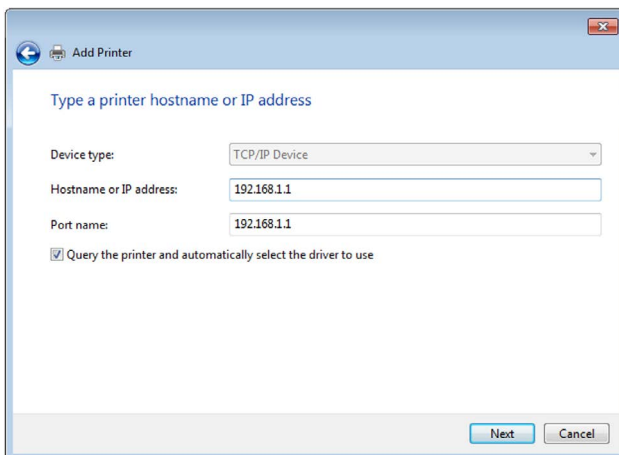
2. Pilih **Add a local printer (Tambah pencetak setempat)** dan kemudian klik **Next (Seterusnya)**.



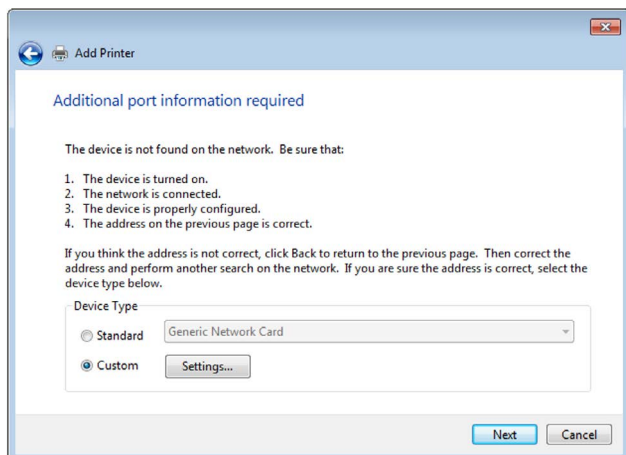
3. Pilih **Create a new port (Cipta port baru)** kemudian tetapkan **Type of Port (Jenis Port)** untuk **Standard TCP/IP Port (TCP/Port IP Standard)**. Klik **Next (Seterusnya)**.



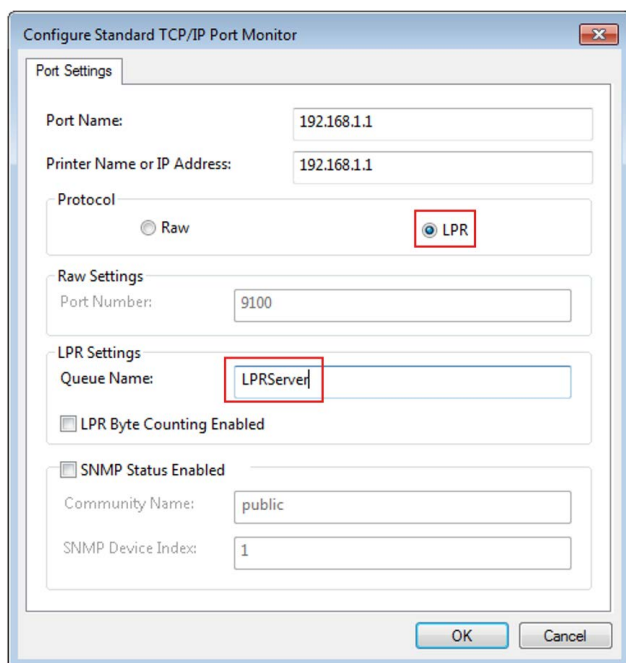
4. Dalam medan **Hostname or IP address (Nama hos atau alamat IP)**, masukkan alamat IP penghala berwayar kemudian klik **Next (Seterusnya)**.



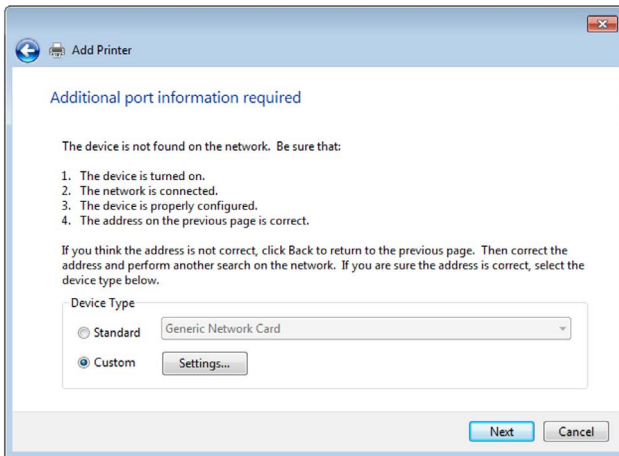
5. Pilih **Custom (Tersuai)** kemudian klik **Settings (Tetapan)**.



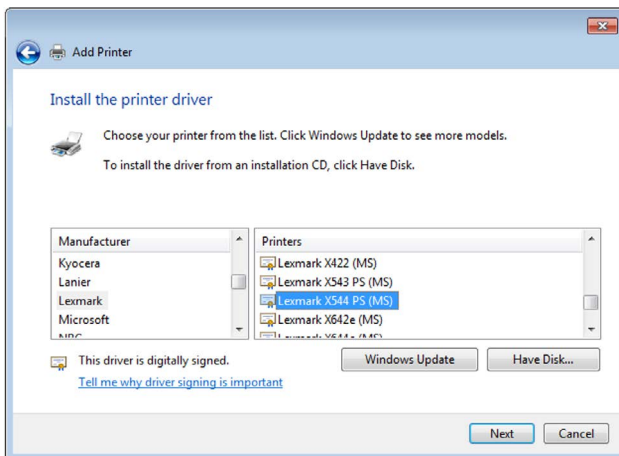
6. Tetapkan **Protocol (Protokol)** ke **LPR**. Dalam medan **Queue Name (Nama Baris)**, masukkan **LPRServer** kemudian klik **OK** untuk meneruskan.



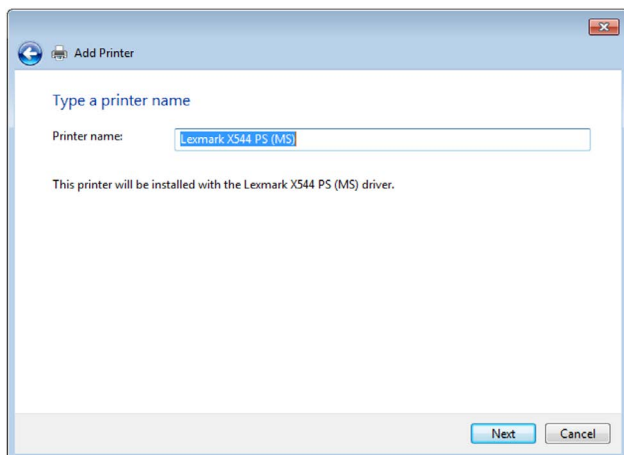
7. Klik **Next (Seterusnya)** untuk menyelesaikan menyediakan port TCP/IP standard.



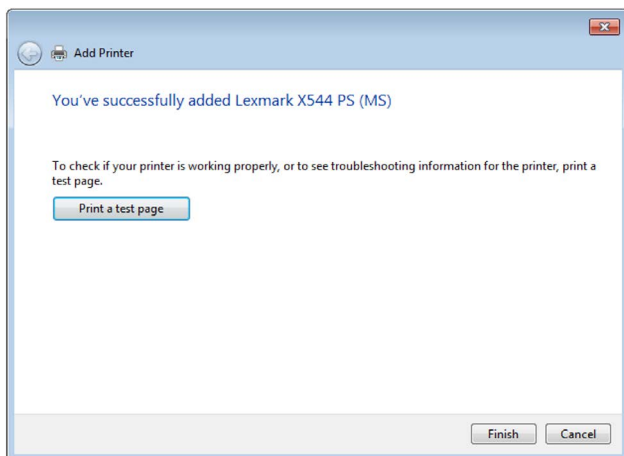
8. Pasang pemacu pencetak dari senarai model vendor. Jika pencetak anda tiada dalam senarai, klik **Have Disk (Ada Cakera)** untuk memasang pemacu pencetak secara manual daripada CD-ROM atau fail.



9. Klik **Next (Seterusnya)** untuk menerima nama lalai pencetak.



10. Klik **Finish (Selesai)** untuk melengkapkan pemasangan.



4.14.5 Modem USB

Tukar kepada mod USB untuk menggunakan dongel wayarles USB 3G/4G atau telefon Android sebagai modem USB.

Untuk menggunakan modem USB, pergi ke **Settings (Tetapan) > USB Application (Aplikasi USB) > USB Modem (Modem USB)**.

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

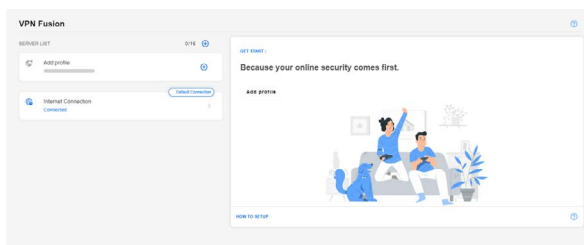
Basic Config	
Enable USB Mode	☒
Select USB Device	Auto
APN Configuration	Auto
Telecommunications Standards	3GPP GSM (GPRS) / LTE
APN (non-optional)	Internet
Dial Number	1921
Username	
Password	
Authentication	None
PPS Code	
USB Adapter	Auto
USB LPU	0
Special Requirements from ISP	
Extend the TTL value	☐ Yes ☒ No
Extend the TTL value	☐ Yes ☒ No

Apply

4.15 VPN Fusion (Gabungan VPN)

4.15.1 Mencipta gabungan VPN

Gabungan VPN membolehkan anda menyambung ke berbilang pelayan VPN secara serentak dan menugaskan peranti klien anda untuk menyambung ke terowong VPN yang berbeza.

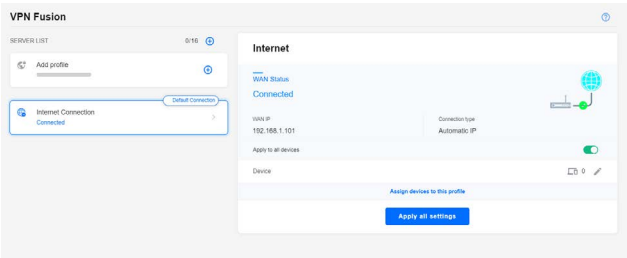


1. Dari panel navigasi, pergi ke **VPN Fusion (Gabungan VPN)**.
2. Klik **+** pada medan **Add profile (Tambah profil)** untuk menyediakan terowong VPN baharu.
3. Lengkapkan konfigurasi VPN termasuk nama sambungan, jenis VPN, wilayah, kunci persendirian dan peranti.
4. Klik **Apply and Enable (Guna dan Dayakan)**.

The screenshot shows the 'Add profile' form. It includes a 'Connection Name' text field. Below it is a 'VPN authentication' section featuring a 'Surfshark' banner for a '2-Year VPN Plan 82% off'. The 'VPN type' dropdown is set to 'Surfshark'. There is a 'Create an account' button with a checkmark. Below that are 'Region' and 'Private Key' dropdowns. At the bottom, there's a 'Device' field with a list icon and an 'Assign devices to this profile' link. The 'Apply and Enable' button is at the very bottom.

4.15.2 Sambungan Internet

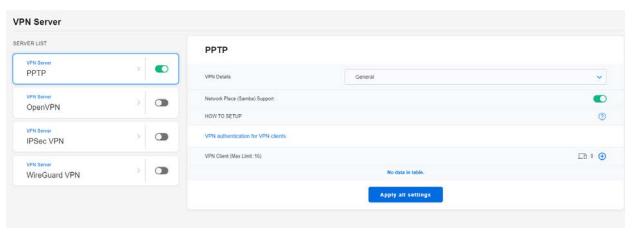
Membolehkan anda mengurus status WAN peranti yang bersambung.



4.16 VPN Server (Pelayan VPN)

4.16.1 PPTP

1. Dari panel navigasi, pergi ke **VPN Server (Pelayan VPN)** > **PPTP** dan alihkan penggelongsor ke kanan (ia ditetapkan kepada mati di bahagian kiri secara lalai).
2. Pada medan **VPN Client (Max Limit: 16)** [**Klien VPN (Had Maks: 16)**], klik  untuk menambah akaun.

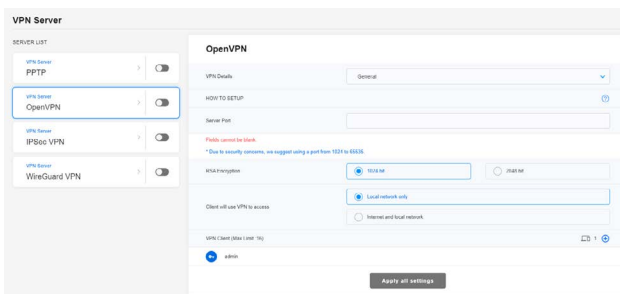


3. Masukkan [*Nama Pengguna*] dan [*Kata Laluan*] tersuai, dan klik **OK**.

NOTA: Sebaik sahaja [*Nama Pengguna*] dan [*Kata Laluan*] ditetapkan, ia tidak boleh diubah. Untuk maklumat lanjut, sila lawati <https://www.asus.com/support/FAQ/114892/>.

4.16.2 OpenVPN

1. Dari panel navigasi, pergi ke **VPN Server (Pelayan VPN)** > **OpenVPN (Buka VPN)** dan alihkan penggelongsor ke kanan (ia ditetapkan kepada mati di bahagian kiri secara lalai).
2. Konfigurasikan tetapan umum dalam medan **VPN Details (Butiran VPN)**.
3. Masukkan nama pengguna dan kata laluan anda dalam lajur kosong.
4. Pada medan **VPN Client (Max Limit: 16) [Klien VPN (Had Maks: 16)]**, klik  untuk menambah akaun.
5. Kata laluan disembunyikan secara automatik. Klik **Apply all settings (Gunakan semua tetapan)**.

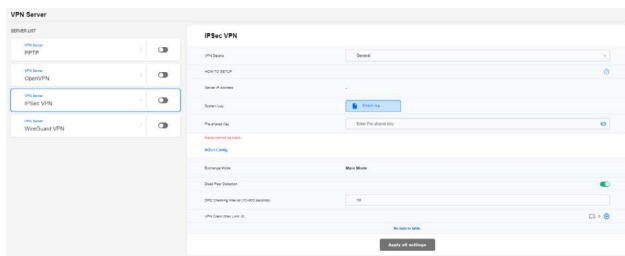


The screenshot shows the 'VPN Server' configuration page. On the left, under 'SERVER LIST', the 'OpenVPN' service is selected and its toggle is turned on. The main area is titled 'OpenVPN' and contains several sections: 'VPN Details' with a dropdown set to 'General'; 'HOW TO SETUP' with a 'Server Port' field; a note 'Public cannot be blank' and a suggestion '*Due to security concerns, we suggest using a port from 1024 to 65535.'; 'VPN Preselection' with radio buttons for '1024 bit' (selected) and '2048 bit'; 'Client will use VPN to access' with radio buttons for 'Local network only' (selected) and 'Internet and local network'; and a 'VPN Client (Max Limit: 16)' section with a plus icon and a minus icon. At the bottom right is an 'Apply all settings' button.

NOTA: Untuk maklumat lanjut, sila lawati <https://www.asus.com/support/FAQ/1008713/>.

4.16.3 IPSec VPN

1. Dari panel navigasi, pergi ke **VPN Server (Pelayan VPN)** > **IPSec VPN** dan alihkan penggelongsor ke kanan (ia ditetapkan kepada mati di bahagian kiri secara lalai).
2. Masukkan kunci dalam medan **Pre-shared Key (Kunci Dikongsi Awal)**.
3. Pada medan **VPN Client (Max Limit: 8) [Klien VPN (Had Maks: 8)]**, klik **+** untuk menambah akaun.
4. Masukkan **[Nama Pengguna]** dan **[Kata Laluan]** tersuai, dan klik **Apply all settings (Gunakan semua tetapan)**.

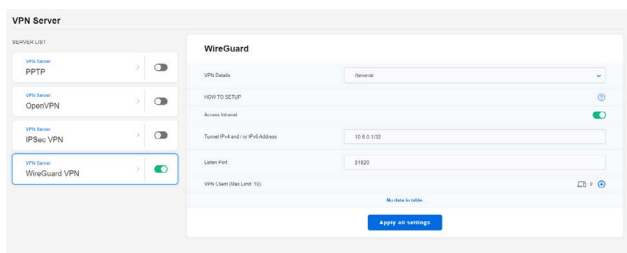


NOTA: Sebaik sahaja **[Nama Pengguna]** dan **[Kata Laluan]** ditetapkan, ia tidak boleh diubah. Untuk maklumat lanjut, sila lawati <https://www.asus.com/support/FAQ/1044190/>.

4.16.4 WireGuard® VPN

1. Dari panel navigasi, pergi ke **VPN Server (Pelayan VPN) > WireGuard VPN**.
2. Pada medan **VPN Client (Max Limit: 10) [Klien VPN (Had Maks: 10)]**, klik  untuk menambah akaun. Untuk peranti umum seperti komputer riba atau telefon pintar, klik **Apply (Guna)**.
3. Klik **Apply all settings (Gunakan semua tetapan)** untuk mendayakan WireGuard® VPN.
4. Klik “...” untuk butiran lanjut.

NOTA: Jika anda menggunakan telefon pintar untuk menyambung ke WireGuard® VPN, sila muat turun aplikasi WireGuard® daripada Google Play atau App Store, dan imbas kod dalam aplikasi untuk memuat turun fail konfigurasi.



NOTA: Untuk maklumat lanjut, sila lawati <https://www.asus.com/support/FAQ/1048280/>.

4.17 WAN

4.17.1 Sambungan Internet

Skrin Sambungan Internet membolehkan anda mengkonfigurasi tetap pelbagai jenis sambungan WAN.

ExpertWiFi ERM68 supports several connection types to WAN (wide area network). These types are selected from the dropdown menu beside WAN Connection Type. The setting fields differ depending on the connection type you selected.

Add Profile

WAN Index	
WAN Type	WAN

Internet Settings

Profile	Internet
WAN Connection Type	Automatic IP
Enable WAN	☒ Yes ☐ No
Enable NAT	☒ Yes ☐ No
Enable UPnP	☒ Yes ☐ No

802.1Q

Enable	☐ Yes ☒ No
--------	---

VLAN ID

0	(2 - 4094)
---	------------

Untuk mengkonfigurasi tetap sambungan WAN:

1. Daripada panel navigasi, pergi ke **Settings (Tetapan) > WAN > Internet Connection (Sambungan Internet)**.
2. Konfigurasi tetap di bawah yang berikut. Apabila selesai, klik **Apply (Guna)**.
 - **WAN Connection Type (Jenis Sambungan WAN):** Pilih jenis Pembekal Perkhidmatan Internet anda. Pilihan adalah **Automatic IP (IP Automatik)**, **PPPoE**, **PPTP**, **L2TP** atau **static IP (IP statik)**. Rujuk ISP anda jika penghala tidak boleh mendapatkan alamat IP sah atau jika anda tidak pasti jenis sambungan WAN.
 - **Enable WAN (Dayakan WAN):** Pilih **Yes (Ya)** untuk membolehkan akses penghala Internet. Pilih **No (Tidak)** untuk mendayakan akses Internet.
 - **Dayakan NAT:** NAT (Terjemahan Alamat Rangkaian) adalah sistem di mana satu IP awam (IP WAN) digunakan untuk memberikan akses Internet ke klien rangkaian dengan alamat IP peribadi dalam LAN. Alamat IP peribadi setiap klien rangkaian disimpan dalam jadual NAT dan ia digunakan pada paket data masuk penghala.
 - **Enable UPnP (Mendayakan UPnP):** UPnP (Universal Plug and Play) (Palam dan Main Universal) membenarkan beberapa peranti (seperti penghala, televisyen, sistem stereo, konsol permainan, dan

telefon selular) untuk dikawal melalui rangkaian berasaskan IP dengan atau tanpa kawalan pusat melalui get laluan. UPnP menyambungkan PC semua betuk faktor, memberikan rangkaian tak berkelim untuk konfigurasi jauh dan pemindahan data. Menggunakan UPnP, peranti rangkaian baru ditemui secara automatik. Apabila bersambung ke rangkaian, peranti boleh dikonfigurasi untuk menyokong aplikasi P2P, permainan interaktif, persidangan video, dan web atau pelayan proksi. Tidak seperti Pemajuan Port, yang melibatkan konfigurasi tetapan port secara manual, UPnP secara mengkonfigurasi penghala secara automatik untuk menerima sambungan masuk dan mengarahkan permintaan ke PC khusus pada rangkaian setempat.

- **Connect to DNS Server (Menyambung kepada Pelayan DNS):** Benarkan penghala ini untuk mendapatkan alamat IP DNS daripada ISP secara automatik. DNS adalah hos pada Internet yang menterjemahkan nama Internet ke alamat IP angka.
- **Authentication (Pengesahan):** Item ini mungkin ditentukan oleh beberapa ISP. Semak dengan ISP anda dan isikannya jika diperlukan.
- **Host Name (Nama Hos):** Medan ini membenarkan anda untuk memberikan nama hos untuk penghala anda. Biasanya ia adalah keperluan istimewa daripada ISP anda. Jika ISP anda diberikan nama hos kepada komputer anda, masukkan nama hos di sini.
- **MAC Address (Alamat MAC):** Alamat MAC (Kawalan Capaian Media) adalah pengecam unik untuk peranti perangkaian anda. Beberapa ISP memantau alamat MAC peranti perangkaian yang bersambung ke perkhidmatan mereka dan menolak mana-mana peranti yang tidak dikenali yang mencuba untuk bersambung. Untuk mengelakkan isu sambungan disebabkan alamat MAC yang tidak didaftar, anda boleh:
 - Hubungi ISP anda dan kemas kini alamat MAC berkaitan dengan perkhidmatan ISP anda.
 - Klon atau menukar alamat MAC penghala berwayar ASUS untuk sepadan dengan alamat MAC peranti perangkaian sebelumnya dikenali oleh ISP.

4.17.2 Berbilang WAN

Berbilang WAN membolehkan anda memilih sambungan berbilang ISP ke penghala anda dan kumpulan WAN untuk kedua-dua WAN primer dan sekunder.

Untuk mengkonfigurasi Multi-WAN (Berbilang WAN):

1. Dari panel navigasi, pergi ke **Settings (Tetapan) > WAN > Multi-WAN (Berbilang WAN)**.
2. Hidupkan **Enable Multi-WAN (Dayakan Berbilang WAN)**.
3. Pilih **Primary WAN (WAN Primer)** dan **Secondary WAN (WAN Sekunder)** anda. Terdapat WAN, USB, LAN Ethernet untuk pilihan anda.
4. Pilih **Fail Over (Gagal Seluruh)** atau **Time (Masa)**.
 - **Fail Over (Gagal Seluruh)**: Gunakan WAN sekunder untuk akses rangkaian sandaran.
 - **Time (Masa)**: Tetapkan masa untuk menjadualkan dasar Berbilang WAN anda.
5. Pilih **Active Backup WAN when any primary WAN port failed (WAN Sandaran Aktif apabila mana-mana port WAN primer gagal)** atau **Active Backup WAN when all primary WAN port failed (WAN Sandaran Aktif apabila semua port WAN primer gagal)**.

Enable Multi-WAN ☒

Group Settings

WAN Group
Primary WAN

WAN 1

[Add Port](#)

WAN Group
Secondary WAN

[Add Port](#)

Set policy with Multi-WAN

Mode ☒ Fail Over ☐ Time

Policy ☒ Active Backup WAN when any primary WAN port failed ☐ Active Backup WAN when all primary WAN port failed

6. Hidupkan atau matikan **Allow failback (Benarkan gagal undur)**.

7. Tentukan selang pengesanan.
8. Tentukan bilangan kekerapan kegagalan berterusan sebelum WAN semasa dianggap terputus sambungan.
9. Tentukan bilangan kekerapan WAN Primer dikesan secara berterusan mempunyai sambungan Internet aktif melalui kabel fizikal, yang mencetuskan gagal undur ke WAN Primer.
10. Pilih **DNS Query (Pertanyaan DNS)** atau **Ping**.
11. Klik **Apply all settings (Gunakan semua tetapan)**.

Allow failback ☒

Per-Port Settings

WAN 1

Detect Interval	Every 3 seconds
Internet Connection Diagnosis	When the current WAN fails 2 continuous times, it is deemed a disconnection.
Failback Trigger Condition	When the Primary WAN is detected to have an active internet connection using a physical cable for 4 continuous times, failback to the Primary WAN.
Network Monitoring	☐ DNS Query ☐ Ping

Apply all settings

NOTA: Penerangan terperinci boleh didapati pada Soalan Lazim Laman Sokongan <https://www.asus.com/support/FAQ/1011719>.

4.17.3 Picu Port

Picu Port membolehkan anda mendayakan port data buat sementara waktu apabila peranti LAN memerlukan akses tanpa had kepada Internet. Terdapat dua kaedah untuk membuka port data masuk: pemajuan port dan picu port.

- Pemajuan port mendayakan port data tertentu sepanjang masa dan peranti mesti menggunakan alamat IP statik.
- Picu port hanya mendayakan port masuk apabila peranti LAN meminta akses kepada port picu.

Tidak seperti pemajuan port, picu port tidak memerlukan alamat IP statik untuk peranti LAN. Pemajuan port membolehkan peranti berbilang untuk berkongsi satu port buka dan port picu hanya membenarkan satu klien pada satu-satu masa untuk mengakses port buka.

Port Trigger allows you to temporarily open data ports when LAN devices require unrestricted access to the Internet. There are two methods for opening incoming data ports: port forwarding and port trigger. Port forwarding opens the specified data ports all the time and devices must use static IP addresses. Port trigger only opens the incoming port when a LAN device requests access to the trigger port. Unlike port forwarding, port trigger does not require static IP addresses for LAN devices. Port forwarding allows multiple devices to share a single open port and port trigger only allows one client at a time to access the open port.

Port Trigger [FAQ](#)

Basic Config

Enable Port Trigger ☒ Yes ☐ No

Well-Known Applications

Trigger Port List (Max Limit : 32) [+](#)

Description	Trigger Port	Protocol	Incoming Port	Protocol	Device
No data in table					

[Apply](#)

Untuk menyediakan Picu Port:

1. Daripada panel navigasi, pergi ke **Settings (Tetapan) > WAN > Port Trigger (Picu Port)**.
2. Konfigurasi tetapan di bawah yang berikut. Apabila selesai, klik **Apply (Guna)**.
 - **Enable Port Trigger (Mendayakan Pencetus Port):** Pilih Yes (Ya) untuk mendayakan Picu Port.
 - **Well-Known Applications (Aplikasi Yang Diketahui):** Pilih permainan dan perkhidmatan web popular untuk menambah ke Senarai Picu Port.
 - **Description (Penerangan):** Masukkan nama pendek atau huraian untuk perkhidmatan ini.

- **Trigger Port (Port Picu):** Tentukan port picu untuk membukan port masuk.
 - **Protocol (Protokol):** Pilih protokol, TCP, atau UDP.
 - **Incoming Port (Port Masuk):** Nyatakan port masuk untuk menerima data masuk daripada Internet.
-

NOTA:

- Apabila menyambung ke pelayan IRC, PC klien membuat sambungan keluar menggunakan julat port picu 66660-7000. Pelayan IRC respons dengan mengesahkan nama pengguna dan mencipta sambungan baru kepada PC klien menggunakan port masuk.
 - Jika Picu Port dinyahdayakan, penghalang menjatuhkan sambungan kerana ia tidak boleh menentukan PC yang mana yang meminta akses IRC. Apabila Picu Port didayakan, penghalang menugaskan port masuk untuk menetapkan data masuk. Port masuk ini ditutup apabila tempoh masa khusus telah berlalu kerana penghalang tidak pasti apabila aplikasi telah ditamatkan.
 - Picu port hanya membenarkan satu klien dalam rangkaian menggunakan perkhidmatan tertentu dan port masuk khusus pada masa yang sama.
 - Anda tidak boleh menggunakan aplikasi yang sama untuk memicu port dalam lebih daripada satu PC pada masa yang sama. Penghalang hanya memajukan port semula ke komputer terakhir yang menghantar permintaan/picu penghalang.
 - Untuk maklumat lanjut, sila lawati <https://www.asus.com/support/FAQ/114110>.
-

4.17.4 Pelayan Maya/Pemajuan Port

Pelayan Maya / Pemajuan port membolehkan komputer jauh untuk disambungkan ke komputer atau perkhidmatan tertentu dalam rangkaian kawasan setempat (LAN) persendirian. Untuk sambungan lebih laju, beberapa aplikasi P2P (seperti BitTorrent) mungkin juga memerlukan anda untuk menetapkan tetapan pemajuan port. Sila rujuk manual pengguna aplikasi P2P untuk mendapatkan butiran. Anda boleh mendayakan berbilang port atau liputan port dalam penghala dan menghalakan semula data melalui port tersebut ke klien tunggal pada rangkaian anda.

Jika anda mahu menentukan Julat Port untuk klien pada rangkaian yang sama, masukkan Nama Perkhidmatan, Julat Port (cth. 10200:10300), alamat IP LAN dan biarkan Port Setempat kosong.

NOTA: Apabila pemajuan port dinyahdayakan, penghala ASUS menyekat trafik masuk tanpa diminta dari Internet dan hanya membenarkan balasan daripada permintaan luar daripada LAN. Klien rangkaian tidak mempunyai akses kepada Internet secara langsung, dan sebaliknya.

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

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

When your network's firewall is disabled and you set 80 as the HTTP server's port range for your WAN setup, then your http server/web server would be in conflict with ExpertWiFi (EWM's web user interface).

[Virtual Server - / Port Forwarding, E80](#)

Basic Config

Enable Port Forwarding ☐ OFF

Port Forwarding List (Max Limit : 64)

Service Name	External Port	Internal Port	Internal IP Address	Protocol	Source IP	Edit	Delete
No data in table.							
Add profile							

Untuk menyediakan Pemajuan Port:

1. Daripada panel navigasi, pergi ke **Settings (Tetapan) > WAN > Virtual Server / Port Forwarding (Pelayan Maya / Pemajuan Port)**.
2. Luncurkan bar kepada **ON (HIDUP)** untuk mendayakan **Port Forwarding (Pemajuan Port)**, kemudian klik **Add Profile (Tambah Profil)**. Selepas mengkonfigurasi tetapan berikut, klik **OK**.

Quick Select	
Famous Server List	Please select ▼
Famous Game List	Please select ▼

Custom Configuration	
Service Name	* Optional
Protocol	TCP ▼
External Port	
Internal Port	* Optional
Internal IP Address	▼
Source IP	* Optional

* External Port
The External Port accepts the following formats:
 1. Port ranges using a colon ":" between the starting and ending port, such as 300:350.
 2. Single ports using a comma "," between individual ports, such as 566,789.
 3. A Mix of port ranges and single ports, using colons ":" and commas ","; such as 1015:1024,3021.

* Source IP
If you want to open your port to a specific IP address from the internet, input the IP address you want to specify in the Source IP field.

Cancel

OK

- **Famous Server List (Senarai Pelayan Terkenal):** Tentukan jenis perkhidmatan yang manakah yang anda ingin akses.
- **Famous Game List (Senarai Permainan Terkenal):** Item ini menyenaraikan port yang diperlukan untuk permainan dalam talian popular untuk berfungsi dengan betul.
- **Service Name (Nama Perkhidmatan):** Masukkan nama perkhidmatan.
- **Protocol (Protokol):** Pilih protokol. Jika anda tidak pasti, pilih **BOTH (KEDUA-DUANYA)**.
- **External Port (Port Luaran):** Terima format berikut:
 - 1) Julat port menggunakan tanda titik bertindih ":" di tengah untuk menentukan had atas dan bawah julat, seperti 300:350;
 - 2) Nombor port berasingan menggunakan koma "," untuk memisahnya, seperti 566, 789;
 - 3) Campuran julat port dan port berasingan, menggunakan tanda titik bertindih ":" dan koma ",", seperti 1015:1024, 3021.

- **Internal Port (Port Dalaman):** Masukkan port khusus untuk menerima paket yang dimajukan. Biarkan medan ini kosong jika anda mahu paket masuk dihalakan semula ke julat port yang dinyatakan.
- **Internal IP Address (Alamat IP Dalaman):** Masukkan alamat IP LAN klien.
- **Source IP (IP Sumber):** Jika anda mahu membuka port anda ke alamat IP khusus daripada Internet, masukkan alamat IP yang anda berikan akses dalam medan ini.

NOTA: Gunakan alamat IP statik untuk klien setempat untuk menjadikan pemajuan port berfungsi dengan baik. Rujuk bahagian **4.9 LAN** untuk maklumat.

Untuk memeriksa jika Pemajuan Port telah berjaya dikonfigurasi:

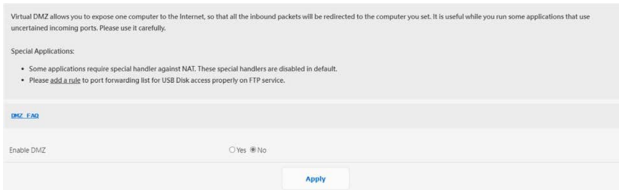
- Pastikan pelayan atau aplikasi anda disediakan dan berjalan.
- Anda memerlukan klien di luar LAN anda tetapi mempunyai akses Internet (dirujuk sebagai "Klien Internet"). Klien ini tidak boleh disambungkan ke penghala ASUS.
- Pada klien Internet, gunakan IP WAN penghala untuk mengakses pelayan. Jika pemajuan port telah berjaya, anda boleh mengakses fail atau aplikasi.

Perbezaan antara picu port dan pemajuan port:

- Picu port akan berfungsi walaupun tanpa menyediakan alamat IP LAN khusus. Tidak seperti pemajuan port, yang memerlukan alamat IP LAN statik, picu port membolehkan pemajuan port dinamik menggunakan penghala. Julat port yang telah ditetapkan dikonfigurasi untuk menerima sambungan masuk untuk tempoh masa terhad. Picu port membolehkan berbilang komputer untuk menjalankan aplikasi yang biasanya memerlukan pemajuan secara manual port yang sama ke setiap PC pada rangkaian.
- Picu port adalah lebih selamat daripada pemajuan port memandangkan port masuk tidak dibuka pada setiap masa. Ia dibuka hanya apabila aplikasi membuat sambungan keluar melalui port picu.

4.17.5 DMZ

DMZ Maya membolehkan anda mendedahkan satu komputer kepada Internet supaya semua paket masuk akan dihalakan semula ke komputer yang anda tetapkan. Ia berguna semasa anda menjalankan beberapa aplikasi yang menggunakan port masuk yang tidak pasti. Sila gunakannya dengan berhati-hati.



Untuk menyediakan DMZ:

1. Daripada panel navigasi, pergi ke **Settings (Tetapan) > WAN > DMZ**.
2. Konfigurasi tetapan di bawah. Apabila selesai, klik **Apply (Guna)**.
 - **Alamat IP bagi Stesen Terdedah:** Masukkan alamat IP LAN klien yang akan menyediakan perkhidmatan DMZ dan terdedah pada Internet. Pastikan klienn pelayan mempunyai alamat IP statik.

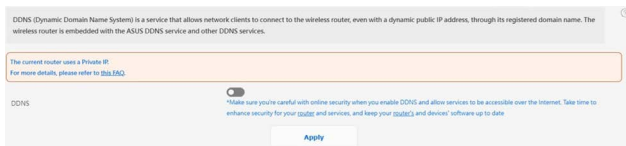
Untuk membuang DMZ:

1. Padam alamat IP LAN klien dari kotak teks **IP Address of Exposed Station (Alamat IP Stesen Terdedah)**.
2. Apabila selesai, klik **Apply (Guna)**.

NOTA: Untuk maklumat lanjut, sila lawati <https://www.asus.com/support/FAQ/1011723>.

4.17.6 DDNS

DDNS (Sistem Nama Domain Dinamik) merupakan perkhidmatan yang membolehkan klien rangkaian menyambung ke penghala berwayar, walaupun dengan alamat IP awam yang dinamik, melalui nama domainnya yang berdaftar. Penghala berwayar dibenamkan dengan perkhidmatan DDNS ASUS dan perkhidmatan DDNS lain.



Untuk menyediakan DDNS:

1. Daripada panel navigasi, pergi ke **Settings (Tetapan) > WAN > DDNS**.
2. Konfigurasi tetapan di bawah yang berikut. Apabila selesai, klik **Apply (Guna)**.
 - **Enable the DDNS Client (Mendayakan Klien DDNS):** Dayakan DDNS untuk mengakses penghala ASUS melalui nama DNS dan bukannya alamat IP WAN.
 - **Server and Host Name (Pelayan dan Nama Hos):** Pilih DDNS ASUS atau DDNS lain. Jika anda ingin menggunakan DDNS ASUS, isi Nam Hos dalam format xxx.asuscomm.com (xxx adalah nama hos anda).
 - Jika anda ingin menggunakan perkhidmatan DDNS berbeza, klik **FREE TRIAL (BAAN PERCUMA)** an mendaftar dalam talian dahulu. Isi **User Name (Nama Pengguna)** atau **E-mail Address and Password (Alamat E-mel dan Kata Laluan)** atau medan **DDNS Key (Kunci DDNS)**.
 - **Enable wildcard (Mendayakan kad bebas):** Dayakan kad bebas jika perkhidmatan DDNS anda memerlukan satu.

NOTA:

Perkhidmatan DDNS tidak akan berfungsi di bawah keadaan ini:

- Apabila penghala berwayar menggunakan alamat peribadi IP WAN (192.168.x.x, 10.x.x.x, atau 172.16.x.x), seperti yang ditunjukkan oleh teks berwarna kuning.
- Penghala mungkin berada pada rangkaian yang menggunakan jadual NAT berbilang.

4.17.7 Masuk Lalu NAT

Dayakan Masuk Lalu NAT untuk membolehkan sambungan Rangkaian Peribadi Maya (VPN) melalui penghala ke klien rangkaian.

Untuk menyediakan Masuk Lalu NAT, pergi ke **Settings (Tetapan) > WAN > NAT Passthrough (Masuk Lalu NAT)**. Apabila selesai, klik **Apply (Guna)**.

Enable NAT Passthrough to allow a Virtual Private Network (VPN) connection to pass through the router to the network clients.

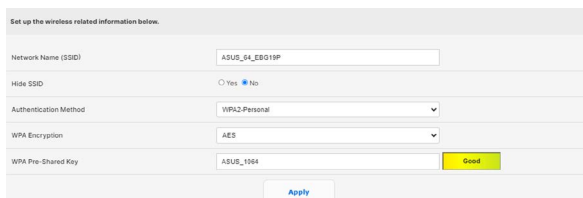
PPTP Passthrough	Enable
L2TP Passthrough	Enable
IPSec Passthrough	Enable
RTSP Passthrough	Enable
H.323 Passthrough	Enable
SIP Passthrough	Enable
PPPoE Relay	Disable
FTP ALG port	2021

Apply

4.18 Wayarles

4.18.1 Umum

Tab General (Am) membolehkan anda mengkonfigurasi tetapan wayarles asas.



Untuk mengkonfigurasi tetapan wayarles asas:

1. Daripada panel navigasi, pergi ke **Settings (Tetapan) > Wireless (Wayarles) > General (Am)**.
2. Berikan nama unik untuk SSID (Pengecam Set Perkhidmatan) atau nama rangkaian anda untuk mengenal pasti rangkaian wayarles anda. Peranti Wi-Fi boleh mengenal pasti dan menyambung ke rangkaian wayarles melalui SSID ditentukan anda. SSID pada panji maklumat dikemas kini apabila SSID baru disimpan pada tetapan.

PENTING! Untuk menjadikan fungsi Wi-Fi tersedia, pastikan Titik Akses (AP) wayarles seperti ExpertWiFi EBA63 atau penghala seperti ExpertWiFi EBR63 atau ExpertWiFi EBM68 disepadukan dalam rangkaian AiMesh EBG19P.

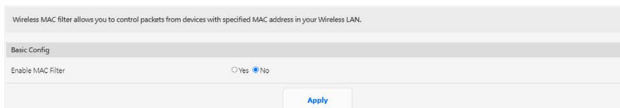
3. Dalam medan **Hide SSID (Sembunyi SSID)**, pilih **Yes (Ya)** untuk mengelakkan peranti wayarles daripada mengesan SSID anda. Apabila fungsi ini didayakan, anda perlu memasukkan SSID secara manual pada peranti wayarles untuk mengakses rangkaian wayarles.
4. Pilih mana-mana kaedah pengesahan ini:
 - **Open System (Sistem Terbuka):** Pilihan ini tidak menyediakan keselamatan.
 - **WPA/WPA2/WPA3-Personal (WPA/WPA2/WPA3 Peribadi):** Pilihan ini menyediakan keselamatan yang kukuh. Anda boleh menggunakan sama ada WPA (dengan TKIP) atau WPA2 (dengan AES). Jika anda

memilih pilihan ini, anda perlu menggunakan penyulitan TKIP + AES dan masukkan ungkapan laluan WPA (kunci ragkaian).

- **WPA/WPA2/WPA3-Enterprise (WPA/WPA2/WPA3 Peribadi):** Pilihan ini menyediakan keselamatan yang sangat kukuh. Ia adalah dengan pelayan EAP bersepadu atau pelayan pengesahan bahagian belakang luaran RADIUS.
5. Tetapkan kata laluan unik untuk kunci dikongsi awal WPA anda.

4.18.2 Penapis MAC Wayarles

Penapis MAC Wayarles memberikan kawalan ke atas paket yang dihantar ke alamat MAC (Kawalan Akses Media) yang dinyatakan pada rangkaian wayarles anda.



Untuk menyediakan penapis Wayarles MAC:

1. Daripada panel navigasi, pergi ke **Settings (Tetapan) > Wireless (Wayarles) > Wireless MAC Filter (Penapis MAC Wayarles)**.
2. Raitkan **Yes (Ya)** dalam medan **Enable Mac Filter (Dayakan Penapis Mac)**.
3. Dalam senarai jatuh bawah **MAC Filter Mode (Mod Penapis MAC)**, pilih sama ada **Accept (Terima)** atau **Reject (Tolak)**.
 - Pilih **Accept (Terima)** untuk membenarkan peranti dalam senarai penapis MAC untuk mengakses rangkaian wayarles.
 - Pilih **Reject (Tolak)** untuk menghalang peranti dalam senarai penapis MAC untuk mengakses rangkaian wayarles.
4. Pada senarai penapis MAC, klik butang **+** dan masukkan alamat MAC peranti wayarles.
5. Klik **Apply (Guna)**.

4.18.3 Senarai Sekatan Perayauan

Ciri ini membolehkan anda menambah peranti ke senarai sekat perayauan dan menghalangnya daripada melakukan perayauan antara nod AiMesh.

You can add devices into roaming deny list, and the devices will not be roamed between AiMesh nodes.

Basic Config

Enable roaming deny list ☒ Yes ☐ No

Roaming Block List (Max Limit : 64)

Client Name (MAC Address)	Add / Delete
ex: 08:BF:88:36:DC:D8	
No data in table.	

[Apply](#)

5 Menyelesai Masalah

Bab ini memberikan penyelesaian untuk isu yang anda mungkin hadapi dengan penghala anda. Jika anda menghadapi masalah yang tidak disebut dalam bab ini, lawati tapak sokongan ASUS di: <https://www.asus.com/support/> untuk maklumat produk lanjut dan butiran untuk dihubungi Sokongan Teknikal ASUS.

5.1 Penyelesaian Masalah Asas

Jika anda mengalami masalah dengan penghala anda, cuba langkah asas dalam bahagian ini sebelum mencari penyelesaian lanjut.

Naik taraf Perisian Tegar ke versi terkini.

1. Daripada panel navigasi, pergi ke **Settings (Tetapan) > Administration (Pentadbiran) > Firmware Upgrade (Naik Taraf Perisian Tegar)**. Klik **Check (Periksa)** untuk mengesahkan jika perisian tegar terkini tersedia.
2. Jika perisian tegar tersedia, lawati tapak web global ASUS di untuk memuat turun perisian tegar terkini.
3. Daripada halaman **Firmware Upgrade (Naik Taraf Perisian Tegar)**, klik **Browse (Imbas)** untuk mencari fail perisian tegar.
4. Klik **Upload (Muat Naik)** untuk menaik taraf perisian tegar.

Mula semula rangkaian anda dalam urutan berikut:

1. Matikan modem.
2. Cabut keluar palam.
3. Matikan penghala dan komputer.
4. Palamkan modem.

5. Hidupkan modem dan tunggu selama 2 minit.
6. Hidupkan penghala dan tunggu selama 2 minit.
7. Hidupkan komputer.

Periksa jika kabel Ethernet dipalam dengan betul.

- Apabila kabel Ethernet menyambungkan penghala dengan modem dipalam dengan betul, LED WAN akan dihidupkan.
- Apabila kabel Ethernet menyambungkan komputer yang dihidupkan anda dengan penghala dipalam dengan betul, LED LAN berkenaan akan dihidupkan.

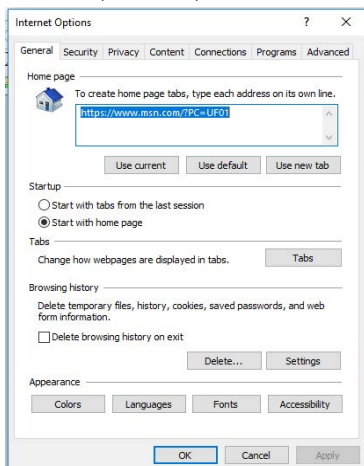
Periksa jika tetapan rangkaian anda betul.

- Setiap klien pada rangkaian perlu mempunyai alamat IP yang sah. ASUS mengesyorkan anda menggunakan pelayan DHCP penghala berwayar untuk menugaskan alamat IP ke komputer pada rangkaian anda.
- Beberapa modem kabel pembekal perkhidmatan memerlukan anda menggunakan alamat MAC komputer yang pada mulanya didaftarkan pada akaun. Anda boleh melihat alamat MAC dalam GUI web, halaman **Dashboard (Papan Pemuka) > Clients (Klien)**.

5.2 Soalan Lazim (FAQs)

Saya tidak dapat mengakses GUI penghala menggunakan penyemak imbas web.

- Jika komputer anda diwayarkan, periksa sambungan kabel Ethernet dan status LED seperti yang diterangkan dalam bahagian sebelum ini.
- Pastikan anda menggunakan maklumat log masuk yang betul. Pastikan kunci Huruf Besar dinyahdaya semasa anda memasukkan maklumat log masuk.
- Padam kuki dan fail dalam penyemak imbas anda. Untuk Internet Explorer, ikuti langkah ini:
 1. Lancarkan Internet Explorer anda, kemudian klik **Tools (Alatan) > Internet Options (Pilihan Internet)**.
 2. Dalam tab **General (Umum)**, di bawah **Browsing history (Sejarah pelayaran)**, klik **Delete... (Padam...)**, pilih **Temporary Internet files and website files (Fail Internet sementara dan fail laman web)** dan **Cookies and website data (Kuki dan data laman web)** kemudian klik **Delete (Padam)**.



NOTA:

- Arahan untuk memadam kuki dan fail berbeza mengikut penyemak imbas web.
- Nyahdayakan tetapan pelayan proksi, keluarkan sebarang sambungan dail naik, dan tetapkan tetapan TCP/IP untuk menetapkan alamat IP secara automatik. Untuk butiran lanjut, rujuk Bab 1 manual pengguna ini.
- Pastikan anda menggunakan kabel ethernet CAT5e atau CAT6.

Klien tidak dapat mewujudkan sambungan wayarles dengan penghala.

PENTING! Untuk menjadikan fungsi Wi-Fi tersedia, pastikan Titik Akses (AP) wayarles seperti ExpertWiFi EBA63 atau penghala seperti ExpertWiFi EBR63 atau ExpertWiFi EBM68 disepadukan dalam rangkaian AiMesh EBG19P.

- Pelayan DHCP telah dinyahdayakan:
 1. Lancarkan Web GUI. Pergi ke **Dashboard (Papan Pemuka) > Clients (Klien)** dan cari peranti yang anda ingin sambung ke penghala.
 2. Jika anda tidak boleh mencari peranti dalam **Dashboard (Papan Pemuka)**, pergi ke **Settings (Tetapan) > LAN > DHCP Server (Pelayan DHCP)**.

DHCP (Dynamic Host Configuration Protocol) is a protocol for the automatic configuration used on IP networks. The DHCP server can assign each client an IP address and inform the client of the IP of DNS server IP and default gateway IP. ExpertWiFi EBR63 supports up to 255 IP addresses for your local network.

[Tutorial for Assigning IP Address via DHCP Server](#)

Basic Config				
Enable the DHCP Server	☒ Yes ☐ No			
ExpertWiFi EBR63's Domain Name				
IP Pool Starting Address	192.168.80.2			
IP Pool Ending Address	192.168.80.254			
Lease Time (seconds)	60480			
Default Gateway				
DNS and DNSSEC Server Setting				
DNS Server 1				
DNS Server 2				
Activate router's IP in addition to user specified DNS	☒ Yes ☐ No			
UnDNS Server				
Internet Assignment				
Enable Internet Assignment	☒ Yes ☐ No			
Priority Assign IP Address via DHCP for Other Users (LAN)				
Client Name (DNS Address)	IP Address	DNS Server (Optional)	Host Name (Optional)	Add Device
en-01-01-01-01-01-01				

- SSID telah disembunyikan. Jika peranti anda boleh mencari SSID dari penghala lain tetapi tidak boleh mencari SSID penghala anda, pergi ke **Settings (Tetapan) > Wireless (Wayarles) > General (Am)**, pilih **NO (TIDAK)** pada **Hide SSID (Sembunyi SSID)**, dan pilih Auto pada Control Channel (Saluran Kawalan).

- Jika anda menggunakan adapter LAN wayarles, periksa jika saluran wayarles yang digunakan mengikut saluran tersedia di negara/kawasan anda. Jika tidak, laraskan saluran, lebar jalur saluran, dan mod wayarles.
- Jika anda masih tidak boleh bersambung ke penghala secara berwayar, anda boleh menetapkan semula tetapan lalai kilang. Dalam GUI penghala, klik **Settings (Tetapan) > Administration (Pentadbiran) > Restore/Save/Upload Setting (Tetapan Pemulihan/Simpan/Muat Naik)**, dan klik **Restore (Pemulihan)**.

Internet tidak dapat diakses.

- Periksa jika penghala anda boleh bersambung ke alamat IP WAN ISP anda. Untuk melakukannya, lancarkan GUI web dan pergi ke **Dashboard (Papan Pemuka)**, dan periksa Status Internet.
- Jika penghala anda tidak boleh bersambung ke alamat IP WAN ISP anda, cuba mula semula rangkaian anda seperti yang diterangkan dalam bahagian **Restart your network in following sequence (Mula semula rangkaian anda dalam urutan berikut)** di bawah **Basic Troubleshooting (Penyelesai Masalah Asas)**.

- Jika masih tiada akses Internet, cuba but semula komputer anda dan sahkan alamat IP rangkaian dan alamat get laluan.
- Periksa penunjuk status pada modem ADSL dan penghala berwayar. Jika LED WAN pada penghala berwayar tidak HIDUP, periksa jika semua kabel dipalam dengan betul.

Anda terlupa SSID (nama rangkaian) atau kata laluan rangkaian

- Sediakan SSID dan kunci penyulitan baru melalui sambungan berwayar (kabel Ethernet). Lancarkan GUI web, pergi ke **Dashboard (Papan Pemuka)**, klik ikon penghala, masukkan SSID dan kunci penyulitan baru, dan kemudian klik **Apply (Guna)**.
- Tetap semula penghala anda ke tetapan lalai. Lancarkan GUI web, pergi ke **Settings (Tetapan) > Administration (Pentadbiran) > Restore/Save/Upload Setting (Tetapan Pemulihan/Simpan/Muat Naik)**, dan klik **Restore (Pemulihan)**.

Bagaimanakah anda memulihkan sistem kepada tetapan lalainya?

- Pergi ke **Settings (Tetapan) > Administration (Pentadbiran) > Restore/Save/Upload Setting (Tetapan Pemulihan/Simpan/Muat Naik)**, dan klik **Restore (Pemulihan)**.

Naik taraf perisian tegar gagal.

Lancarkan mod penyelamat dan jalankan utiliti **Firmware Restoration (Pemulihan Perisian Tegar)**.

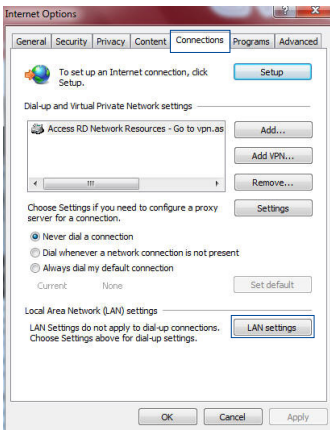
Tidak dapat mengakses GUI Web

Sebelum anda mengkonfigurasi penghalang berwayar anda, lakukan langkah yang diterangkan dalam bahagian ini untuk komputer hos dan klien rangkaian anda.

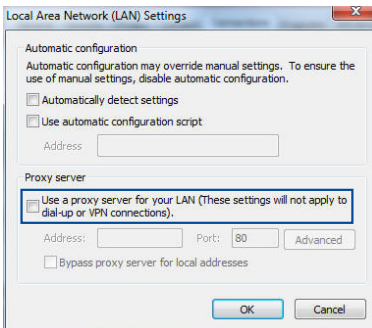
A. Nyahdayakan sebarang pelayan proksi yang dikonfigurasi.

Windows®

1. Klik **Start (Mula)** > **Internet Explorer** untuk melancarkan penyemak imbas.
2. Klik **Tools (Alatan)** > **Internet options (Pilihan Internet)** > **Connections (Sambungan)** > **LAN settings (Tetapan LAN)**.

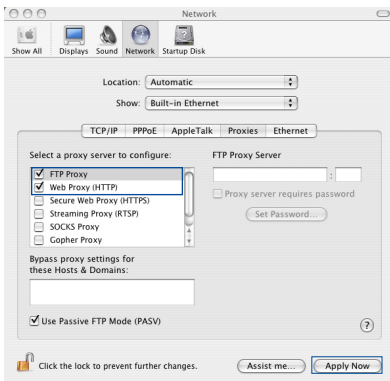


3. Dari tettingkap Local Area Network (LAN) Settings, buang tanda **Use a proxy server for your LAN (Gunakan pelayan proksi untuk LAN anda)**.
4. Klik **OK** setelah selesai.



MAC OS

1. Dari penyemak imbas Safari anda, klik **Safari (Safari) > Preferences (Keutamaan) > Advanced (Lanjutan) > Change Settings...(Tukar Tetapan...)**.
2. Dari skrin Network (Rangkaian), buang tanda **FTP Proxy (FTP Proksi)** dan **Web Proxy (HTTP) (Proksi Web)**.
3. Klik **Apply Now (Guna Sekarang)** setelah selesai.

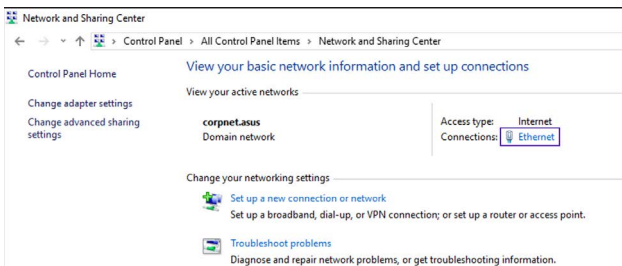


NOTA: Rujuk ciri bantuan penyemak imbas anda untuk butiran mengenai menyahdaya pelayan proksi.

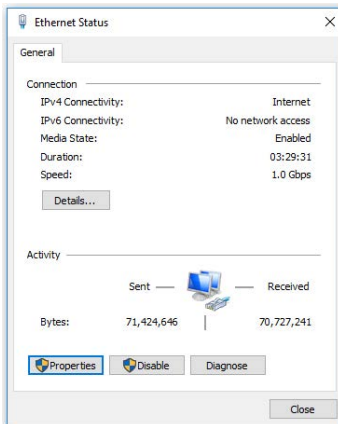
B. Menetapkan tetapan TCP/IP untuk dapatkan alamat IP secara automatik.

Windows®

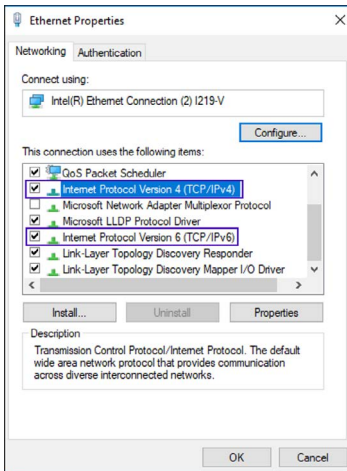
1. Klik **Start (Mula) > Control Panel (Panel Kawalan) > Network and Sharing Center (Rangkaian dan Pusat Perkongsian)**, kemudian klik sambungan rangkaian untuk memaparkan tetapan statusnya.



2. Klik **Properties (Sifat)** untuk memaparkan tettingkap **Ethernet Properties (Sifat Ethernet)**.



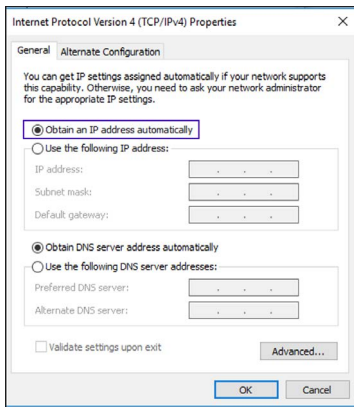
3. Pilih **Internet Protocol Version 4 (TCP/IPv4) (Protokol Internet Versi 4 (TCP/IPv4))** atau **Internet Protocol Version 6 (TCP/IPv6) (Protokol Internet Versi 6 (TCP/IPv6))**, kemudian klik **Properties (Sifati)**.



4. Untuk mendapatkan tetapan IP IPv4 secara automatik, tandakan **Obtain an IP address automatically (Dapatkan alamat IP secara automatik)**.

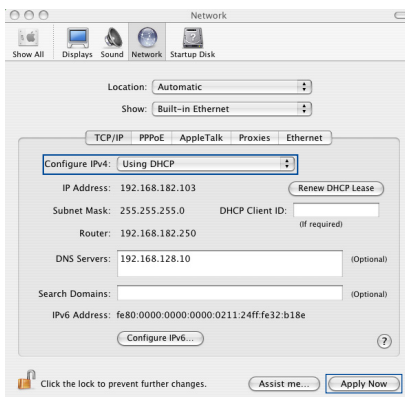
Untuk mendapatkan tetapan IP IPv6 secara automatik, tandakan **Obtain an IP address automatically (Dapatkan alamat IP secara automatik)**.

5. Klik **OK** setelah selesai.



MAC OS

1. Klik ikon Apple  terletak di bahagian atas sebelah kiri skrin anda.
2. Klik **System Preferences (Keutamaan Sistem) > Network (Rangkaian) > Configure (Konfigurasi)...**
3. Dari tab **TCP/IP**, pilih **Using DHCP (Menggunakan DHCP)** dalam senarai jatuh bawah **Configure IPv4 (Konfigurasi IPv4)**.
4. Klik **Apply Now (Guna Sekarang)** setelah selesai.

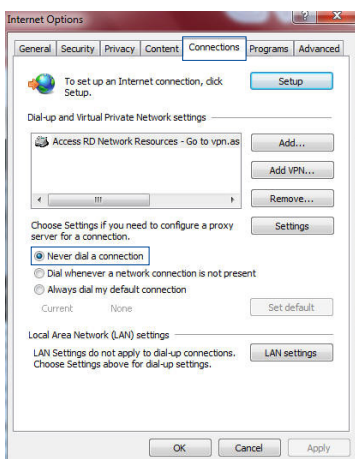


NOTA: Rujuk bantuan dan ciri sokongan sistem operasi anda untuk butiran mengenai mengkonfigurasi tetapan TCP/IP komputer anda.

C. Nyahdayakan sambungan dailan, jika didayakan.

Windows®

1. Klik **Start (Mula) > Internet Explorer** untuk melancarkan penyemak imbas.
2. Klik **Tools (Alatan) > Internet options (Pilihan Internet) > Connections (Sambungan)**.
3. Tandakan **Never dial a connection (Jangan sekali-kali mendail sambungan)**.
4. Klik **OK** setelah selesai.



NOTA: Rujuk ciri bantuan penyemak imbas anda untuk butiran mengenai menyahdaya sambungan dailan.

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

Maklumat keselamatan

Apabila menggunakan produk ini, sentiasa patuhi langkah berjaga-jaga asas, termasuk tetapi tidak terhad pada berikut:



AMARAN!

- Kord bekalan kuasa mesti dipalam masuk ke salur keluar soket yang disediakan dengan pbumian yang sesuai. Sambungkan peralatan hanya ke salur keluar soket berdekatan yang mudah diakses.
 - Jika Penyesuai, jangan cuba untuk membetulkannya sendiri. Hubungi juruteknik servis bertauliah atau peruncit anda.
 - JANGAN guna kord kuasa, aksesori atau persisian lain yang rosak.
 - JANGAN pasang peralatan ini lebih tinggi daripada 2 meter.
 - Gunakan produk ini dalam persekitaran dengan suhu ambien antara 0°C (32°F) dan 40°C (104°F).
 - Baca garis panduan operasi dan julat suhu yang diberikan sebelum menggunakan produk.
 - Berikan perhatian khusus kepada keselamatan diri semasa menggunakan peranti ini di lapangan terbang, hospital, stesen minyak dan garaj profesional.
 - Gangguan peranti perubatan: Kekalkan jarak minimum sekurang-kurangnya 15 cm (6 inci) di antara peranti perubatan yang diimplan dan produk ASUS untuk mengurangkan risiko gangguan.
 - Gunakan produk ASUS di kawasan dengan penerimaan isyarat yang baik untuk meminimumkan tahap radiasi.
 - Jauhkan peranti daripada wanita hamil dan bahagian abdomen remaja.
 - JANGAN gunakan produk ini jika kerosakan jelas boleh diperhatikan atau ia telah basah atau rosak atau diubah suai. Cari perkhidmatan servis untuk mendapatkan bantuan.
-



AMARAN!

- JANGAN letakkan pada permukaan kerja yang tidak rata atau tidak stabil.
 - JANGAN letakkan atau jatuhkan objek di bahagian atas produk. Elakkan produk terdedah kepada kejutan mekanikal seperti penghancuran, pembengkokan, pembocoran atau pencincangan.
 - JANGAN tanggalkan, buka, gelombang mikro, bakar, cat, atau sumbat sebarang objek asing ke dalam produk ini.
 - Rujuk label perkadaran di bahagian bawah produk anda dan pastikan penyesuaian kuasa anda mematuhi perkadaran ini.
 - Jauhkan produk daripada api dan sumber haba.
 - JANGAN dedahkan kepada atau gunakan berdekatan cecair, hujan atau kelembapan. JANGAN gunakan produk semasa ribut elektrik.
 - Sambungkan litar output PoE produk ini secara eksklusif ke rangkaian PoE, tanpa penghalaan ke kemudahan luaran.
 - Untuk mengelak bahaya kejutan elektrik, putus sambungan kabel kuasa daripada salur keluar elektrik sebelum menempatkan semula sistem.
 - Hanya gunakan aksesori yang telah diluluskan oleh pengeluar peranti untuk berfungsi dengan model ini. Penggunaan jenis aksesori lain boleh membatalkan waranti atau melanggar peraturan dan undang-undang tempatan, dan boleh menimbulkan risiko keselamatan. Hubungi penjual tempatan anda untuk ketersediaan aksesori yang dibenarkan.
 - Menggunakan produk ini dengan cara yang tidak disyorkan dalam arahan yang diberikan boleh menyebabkan risiko kebakaran atau kecederaan diri.
 - Produk ini hanya untuk kegunaan dalam rumah.
-

Notis WEEE



Arahan Peralatan Elektrik dan Elektronik Terbuang (WEEE) (Arahan 2012/19/EU) ialah undang-undang Kesatuan Eropah yang bertujuan mengurangkan impak alam sekitar daripada peralatan elektrik dan elektronik. Ia mewajibkan pengeluar untuk mengambil tanggungjawab terhadap pengurusan akhir hayat produk mereka, mempromosikan pengumpulan, rawatan, dan kitar semula untuk meminimumkan sisa dan menggalakkan pemulihan sumber.

Jangan buang peralatan elektrik dan elektronik ke dalam sampah domestik.

Simbol tong sampah beroda yang dipalang pada produk atau pembungkusan menunjukkan bahawa produk ini (termasuk sebarang bateri yang terdapat di dalamnya), tidak boleh dibuang bersama sampah rumah anda.

Untuk mengelakkan potensi bahaya kepada alam sekitar dan kesihatan manusia, rangka kerja pengumpulan harus digunakan untuk memulangkan, mengitar semula, dan memulihkan sisa peralatan elektrik dan elektronik (WEEE), dan produk ini telah direka bentuk untuk membolehkan penggunaan semula bahagian-bahagian serta memudahkan kitar semula bahan-bahan tertentu.

Pembuangan yang tidak betul mungkin melibatkan risiko akibat kehadiran bahan berbahaya dalam peralatan elektrik dan elektronik, seperti plumbum, BFR, dan komponen berbahaya lain.

Semak perkhidmatan kitar semula tempatan anda untuk produk elektronik (<https://esg.asus.com/en/circular-economy/resource-regeneration/global-take-back-service>).