



REPUBLIC OF
GAMERS

F15251

MANUEL UTILISATEUR

ROG Rapture GT-AC5300

ASUS

F15251

Deuxième Édition

Juillet 2019

Copyright © 2019 ASUSTeK Computer Inc. Tous droits réservés.

Aucun extrait de ce manuel, incluant les produits et logiciels qui y sont décrits, ne peut être reproduit, transmis, transcrit, stocké dans un système de restitution, ou traduit dans quelque langue que ce soit sous quelque forme ou quelque moyen que ce soit, à l'exception de la documentation conservée par l'acheteur dans un but de sauvegarde, sans la permission écrite expresse de ASUSTeK Computer Inc. ("ASUS").

La garantie sur le produit ou le service ne sera pas prolongée si (1) le produit est réparé, modifié ou altéré, à moins que cette réparation, modification ou altération ne soit autorisée par écrit par ASUS ; ou (2) si le numéro de série du produit est dégradé ou manquant.

ASUS FOURNIT CE MANUEL "EN L'ÉTAT" SANS GARANTIE D'AUCUNE SORTE, EXPLICITE OU IMPLICITE, Y COMPRIS, MAIS NON LIMITÉ AUX GARANTIES IMPLICITES OU AUX CONDITIONS DE COMMERCIALISABILITÉ OU D'ADÉQUATION À UN BUT PARTICULIER. En aucun cas ASUS, ses directeurs, ses cadres, ses employés ou ses agents ne peuvent être tenus responsables des dégâts indirects, spéciaux, accidentels ou consécutifs (y compris les dégâts pour manque à gagner, pertes de profits, perte de jouissance ou de données, interruption professionnelle ou assimilé), même si ASUS a été prévenu de la possibilité de tels dégâts découlant de tout défaut ou erreur dans le présent manuel ou produit.

LES SPÉCIFICATIONS ET LES INFORMATIONS CONTENUES DANS CE MANUEL SONT FOURNIES À TITRE INDICATIF SEULEMENT ET SONT SUJETTES À DES MODIFICATIONS SANS PRÉAVIS, ET NE DOIVENT PAS ÊTRE INTERPRÉTÉES COMME UN ENGAGEMENT DE LA PART D'ASUS. ASUS N'EST EN AUCUN CAS RESPONSABLE D'ÉVENTUELLES ERREURS OU INEXACTITUDES PRÉSENTES DANS CE MANUEL, Y COMPRIS LES PRODUITS ET LES LOGICIELS QUI Y SONT DÉCRITS.

Les noms des produits et des sociétés qui apparaissent dans le présent manuel peuvent être, ou non, des marques commerciales déposées, ou sujets à copyrights pour leurs sociétés respectives, et ne sont utilisés qu'à des fins d'identification ou d'explication, et au seul bénéfice des propriétaires, sans volonté d'infraction.

Table des matières

| | | |
|----------|--|----|
| 1 | Présentation de votre routeur Wi-Fi | |
| 1.1 | Bienvenue !..... | 7 |
| 1.2 | Contenu de la boîte..... | 7 |
| 1.3 | Votre routeur Wi-Fi..... | 8 |
| 1.4 | Placer le routeur..... | 10 |
| 1.5 | Pré-requis..... | 11 |
| 2 | Prise en main | |
| 2.1 | Configurer le routeur..... | 12 |
| | A. Connexion filaire..... | 12 |
| | B. Connexion Wi-Fi..... | 13 |
| 2.2 | Configuration internet rapide avec auto-détection..... | 15 |
| 2.3 | Connexion à un réseau Wi-Fi..... | 18 |
| 3 | Configurer les paramètres généraux de ROG Gaming Center | |
| 3.1 | Se connecter à l'interface de gestion..... | 19 |
| 3.2 | Tableau de bord..... | 21 |
| 3.3 | Game IPS (Système de Prévention d'Intrusion)..... | 22 |
| | 3.3.1 Configurer Game IPS..... | 23 |
| | 3.3.2 Blocage de sites malveillants..... | 25 |
| | 3.3.3 Two-Way IPS..... | 26 |
| | 3.3.4 Protection et blocage des périphériques infectés..... | 27 |
| | 3.3.5 Configurer le contrôle parental..... | 28 |
| 3.4 | Game Boost..... | 31 |
| | 3.4.1 QoS..... | 32 |
| | 3.4.2 Historique internet..... | 33 |
| 3.5 | Game Private Network (Réseau privé de jeu WTFast)..... | 34 |
| 3.6 | Game Profile (Profil de jeu)..... | 36 |
| 3.7 | Game Radar..... | 38 |
| 3.8 | WiFi Radar..... | 40 |
| | 3.8.1 Enquête site Wi-Fi..... | 41 |
| | 3.8.2 Statistiques canal sans fil..... | 42 |

Table des matières

| | | |
|----------|--|----|
| 3.8.3 | Dépannage avancé..... | 42 |
| 3.9 | VPN..... | 43 |
| 3.10 | Dispositif d'analyse du trafic..... | 44 |
| 4 | Configurer les paramètres avancés | |
| 4.1 | Utiliser la carte du réseau | 45 |
| 4.1.1 | Configurer les paramètres de sécurité Wi-Fi..... | 46 |
| 4.1.2 | Gérer les clients du réseau | 47 |
| 4.1.3 | Surveiller un périphérique USB | 49 |
| 4.2 | Wi-Fi | 51 |
| 4.2.1 | General (Général)..... | 51 |
| 4.2.2 | WPS | 53 |
| 4.2.3 | Pontage WDS..... | 55 |
| 4.2.4 | Filtrage d'adresses MAC | 57 |
| 4.2.5 | Service RADIUS..... | 58 |
| 4.2.6 | Professional (Professionnel) | 59 |
| 4.3 | Créer un réseau invité..... | 63 |
| 4.4 | Réseau local (LAN)..... | 65 |
| 4.4.1 | Adresse IP du routeur..... | 65 |
| 4.4.2 | Serveur DHCP | 66 |
| 4.4.3 | Routage | 68 |
| 4.4.4 | Télévision sur IP | 69 |
| 4.5 | Réseau étendu (WAN) | 70 |
| 4.5.1 | Connexion internet..... | 70 |
| 4.5.2 | Dual WAN (Double WAN)..... | 73 |
| 4.5.3 | Déclenchement de port | 74 |
| 4.5.4 | Serveur virtuel et redirection de port | 76 |
| 4.5.5 | Zone démilitarisée | 79 |
| 4.5.6 | Service DDNS | 80 |
| 4.5.7 | NAT Passthrough | 81 |
| 4.6 | Utiliser les applications USB..... | 82 |
| 4.6.1 | Utiliser AiDisk | 83 |

Table des matières

| | | |
|----------|---|------------|
| 4.6.2 | Utiliser les centres de serveurs | 85 |
| 4.6.3 | 3G/4G | 90 |
| 4.7 | Utiliser iCloud 2.0..... | 91 |
| 4.7.1 | Cloud Disk..... | 92 |
| 4.7.2 | Smart Access..... | 94 |
| 4.7.3 | iCloud Sync | 95 |
| 4.8 | IPv6 (Protocole IPv6) | 96 |
| 4.9 | Pare-feu | 97 |
| 4.9.1 | General (Général)..... | 97 |
| 4.9.2 | Filtrage d'URL | 97 |
| 4.9.3 | Filtrage de mots-clés | 98 |
| 4.9.4 | Filtrage de services réseau..... | 99 |
| 4.9.5 | Pare-feu IPv6..... | 100 |
| 4.10 | Administration..... | 101 |
| 4.10.1 | Mode de fonctionnement..... | 101 |
| 4.10.2 | Système | 102 |
| 4.10.3 | Mise à niveau du firmware..... | 103 |
| 4.10.4 | Restaurer/Sauvegarder/Transférer les paramètres de configuration | 103 |
| 4.11 | Journal système | 104 |
| 4.12 | Smart Connect..... | 105 |
| 4.12.1 | Configurer Smart Connect..... | 105 |
| 4.12.2 | Règles de Smart Connect..... | 106 |
| 5 | Utilitaires | |
| 5.1 | Device Discovery (Détection d'appareils) | 109 |
| 5.2 | Firmware Restoration (Restauration du firmware)..... | 110 |
| 5.3 | Configurer un serveur d'impression | 111 |
| 5.3.1 | Utilitaire ASUS EZ Printer Sharing | 111 |
| 5.3.2 | Utiliser le protocole LPR pour partager une imprimante | 115 |
| 5.4 | Download Master | 120 |
| 5.4.1 | Configurer les paramètres BitTorrent | 121 |
| 5.4.2 | Paramètres NZB..... | 122 |

6 Dépannage

| | | |
|-----|---------------------------------|-----|
| 6.1 | Dépannage de base | 123 |
| 6.2 | Foire aux questions (FAQ) | 125 |

Annexes

| | |
|-----------------------------------|-----|
| Notices | 134 |
| Informations de contact ASUS..... | 149 |
| Centres d'appel mondiaux | 150 |

1 Présentation de votre routeur Wi-Fi

1.1 Bienvenue !

Merci d'avoir acheté un routeur Wi-Fi ROG Rapture GT-AC5300 ! Éléгант, le routeur GT-AC5300 est compatible avec les réseaux Wi-Fi à double bande 2,4 GHz, 5 GHz-1 et 5 GHz-2, offrant un streaming HD Wi-Fi et simultané inégalable. Il intègre également les serveurs SMB, UPnP AV et FTP pour un partage de fichiers 24h/24, 7j/7 et possède la capacité de prendre en charge 300 000 sessions. Enfin la technologie ASUS Green Network permet de faire jusqu'à 70 % d'économie d'énergie.

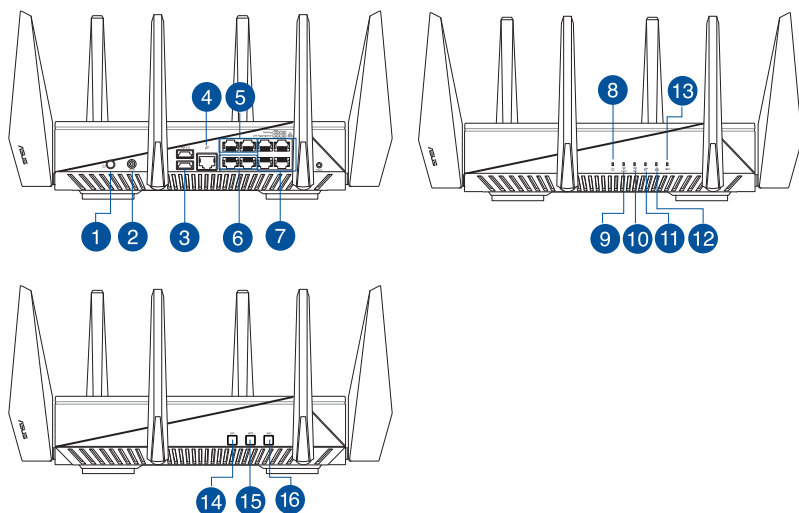
1.2 Contenu de la boîte

- | | |
|---|---|
| <input checked="" type="checkbox"/> Routeur Wi-Fi GT-AC5300 | <input checked="" type="checkbox"/> Adaptateur secteur |
| <input checked="" type="checkbox"/> Câble réseau (RJ-45) | <input checked="" type="checkbox"/> Guide de démarrage rapide |

REMARQUES :

- Contactez votre service après-vente ASUS si l'un des éléments est manquant ou endommagé. Consultez la liste des centres d'appel ASUS en fin de manuel.
 - Conservez l'emballage d'origine pour toutes futures demandes de prises sous garantie.
-

1.3 Votre routeur Wi-Fi



-
- 1 Bouton d'alimentation**
Ce bouton permet d'allumer ou d'éteindre le routeur.
-
- 2 Port d'alimentation (CC)**
Insérez l'adaptateur secteur dans ce port puis reliez votre routeur à une source d'alimentation.
-
- 3 Port USB 3.0**
Insérez un dispositif USB 3.0 tel qu'un périphérique de stockage USB dans ce port.
-
- 4 Port réseau étendu (WAN) (Internet)**
Connectez un câble réseau sur ce port pour établir une connexion à un réseau étendu (WAN).
-
- 5 Ports de jeu (1-2)**
Connectez des câbles réseau sur ces ports pour prioriser les paquets.
-
- 6 Ports d'agrégation de lien (5-6)**
Connectez des câbles réseau sur ces ports pour utiliser l'agrégation de lien (802.11ad).
-
- 7 Ports réseau local (LAN) (3-4,7-8)**
Connectez des câbles réseau sur ces ports pour établir une connexion à un réseau local (LAN).
-
- 8 Voyant d'alimentation**
Éteint : Aucune alimentation.
Allumé : Le routeur est prêt.
Clignote lentement : Mode de secours.
-
- 9 Voyant de bande 2,4 GHz**
Éteint : Aucun signal 2,4 GHz.
Allumé : Routeur prêt à établir une connexion Wi-Fi.
Clignotant : Transmission ou réception de données Wi-Fi.
-

-
- 10** **Voyant de bande 5 GHz**
Éteint : Aucun signal 5 GHz.
Allumé : Routeur prêt à établir une connexion Wi-Fi.
Clignotant : Transmission ou réception de données Wi-Fi.
-
- 11** **Voyant réseau étendu (WAN) (Internet)**
Rouge : Aucune adresse IP ou aucune connexion physique.
Allumé : Connexion établie à un réseau étendu (WAN).
-
- 12** **Voyant réseau local (LAN)**
Éteint : Routeur éteint ou aucune connexion physique.
Allumé : Connexion établie à un réseau local (LAN).
-
- 13** **Voyant WPS**
Éteint : Le processus de vérification WPS est désactivé ou terminé.
Clignotant : Le processus de vérification WPS est activé.
-
- 14** **Bouton LED**
Appuyez sur ce bouton pour allumer ou éteindre les voyants du panneau.
-
- 15** **Bouton WPS**
Ce bouton permet de lancer l'assistant WPS.
-
- 16** **Bouton Wi-Fi**
Appuyez sur ce bouton pour activer/désactiver la connexion Wi-Fi.
-

REMARQUES :

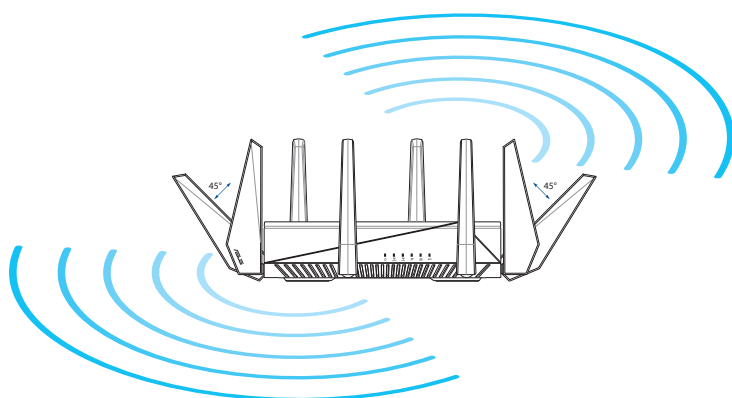
- Utilisez uniquement l'adaptateur secteur fourni avec votre appareil. L'utilisation d'autres adaptateurs peut endommager l'appareil.
- **Caractéristiques :**

| | | | |
|--------------------------------------|------------------------------|----------|---------|
| Adaptateur secteur CC | Sortie CC : +19V (max 3,42A) | | |
| Température de fonctionnement | 0-40°C | Stockage | 0-70°C |
| Humidité de fonctionnement | 50-90 % | Stockage | 20-90 % |

1.4 Placer le routeur

Pour optimiser la transmission du signal Wi-Fi entre votre routeur et les périphériques réseau y étant connectés, veuillez vous assurer des points suivants :

- Placez le routeur Wi-Fi dans un emplacement central pour obtenir une couverture Wi-Fi optimale.
- Maintenez le routeur à distance des obstructions métalliques et des rayons du soleil.
- Maintenez le routeur à distance d'appareils ne fonctionnant qu'avec les normes/fréquences Wi-Fi 802.11g ou 20MHz, les périphériques 2,4 GHz et Bluetooth, les téléphones sans fil, les transformateurs électriques, les moteurs à service intense, les lumières fluorescentes, les micro-ondes, les réfrigérateurs et autres équipements industriels pour éviter les interférences ou les pertes de signal Wi-Fi.
- Mettez toujours le routeur à jour dans la version de firmware la plus récente. Visitez le site Web d'ASUS sur <http://www.asus.com> pour consulter la liste des mises à jour.
- Orientez les quatre antennes amovibles comme illustré ci-dessous pour améliorer la qualité de couverture du signal Wi-Fi.



1.5 Pré-requis

Pour établir votre réseau Wi-Fi, vous aurez besoin d'un ou deux ordinateurs répondant aux critères suivants :

- Port Ethernet RJ-45 (LAN) (10Base-T/100Base-TX/1000Base-TX)
- Compatible avec la norme Wi-Fi IEEE 802.11a/b/g/n/ac
- Un service TCP/IP installé
- Navigateur internet tel qu'Internet Explorer, Firefox, Safari ou Google Chrome

REMARQUES :

- Si votre ordinateur ne possède pas de module Wi-Fi, installez une carte Wi-Fi compatible avec la norme IEEE 802.11a/b/g/n/ac sur votre ordinateur.
 - Avec sa technologie tri-bande, votre routeur Wi-Fi prend en charge les signaux Wi-Fi des bandes 2,4 GHz et 5 GHz-1 et 5 GHz-2 simultanément. Ceci vous permet de naviguer sur Internet ou de lire/écrire des e-mails sur la bande 2,4 GHz tout en profitant de streaming audio/vidéo en haute définition sur la bande 5 GHz.
 - Certains appareils dotés de capacités Wi-Fi IEEE 802.11n ne sont pas compatibles avec la bande à 5 GHz. Consultez le mode d'emploi de vos dispositifs Wi-Fi pour plus d'informations.
 - Les câbles réseau Ethernet RJ-45 utilisés pour établir une connexion réseau ne doivent pas excéder une longueur de 100 mètres.
-

2 Prise en main

2.1 Configurer le routeur

IMPORTANT !

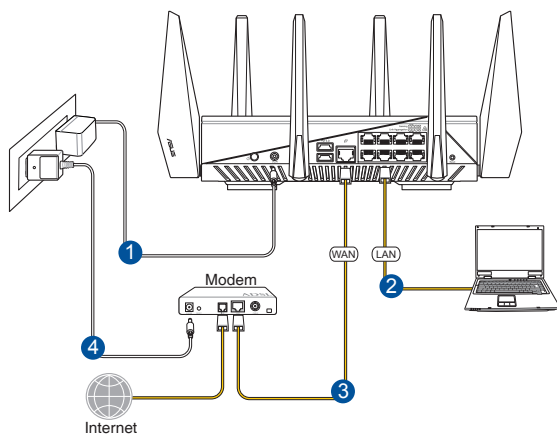
- Il est recommandé d'utiliser une connexion filaire pour la configuration initiale afin d'éviter des problèmes d'installation causés par l'instabilité du réseau Wi-Fi.
- Avant toute chose, veuillez vous assurer des points suivants :
- Si vous remplacez un routeur existant, déconnectez-le de votre réseau.
- Déconnectez tous les câbles de votre configuration modem actuelle. Si votre modem possède une batterie de secours, retirez-la.
- Redémarrez votre ordinateur (recommandé).

A. Connexion filaire

REMARQUE : Une fonction de détection de croisement automatique est intégrée au routeur Wi-Fi pour que vous puissiez aussi bien utiliser un câble Ethernet droit que croisé.

Pour configurer votre routeur via une connexion filaire :

1. Branchez le routeur sur une prise électrique, puis allumez-le. Utilisez le câble réseau pour relier votre ordinateur au port de réseau local (LAN) du routeur.



2. L'interface de gestion du routeur s'affiche automatiquement lors de l'ouverture de votre navigateur internet. Si ce n'est pas le cas, entrez <http://router.asus.com> dans la barre d'adresse.
3. Définissez un mot de passe afin d'éviter les accès non autorisés au routeur.

Login Information Setup

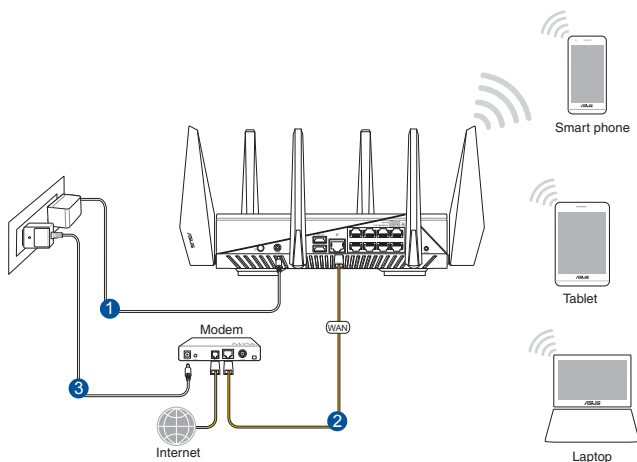
Change the router password to prevent unauthorized access to your ASUS wireless router.

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

B. Connexion Wi-Fi

Pour configurer votre routeur via une connexion Wi-Fi :

1. Branchez le routeur sur une prise électrique, puis allumez-le.



2. Connectez-vous au réseau dont le nom (SSID) est affiché sur l'étiquette du produit située à l'arrière du routeur. Pour garantir une plus grande sécurité, modifiez le nom du réseau et le mot de passe.



| | |
|---------------------|-------------------|
| Nom du réseau Wi-Fi | ASUS_XX_2G |
| 2,4 G (SSID) : | |
| Nom du réseau Wi-Fi | ASUS_XX_5G |
| 5 G-1 (SSID) : | |
| Nom du réseau Wi-Fi | ASUS_XX_5G_Gaming |
| 5 G-2 (SSID) : | |

* **XX** correspond aux deux derniers chiffres de l'adresse MAC 2,4 GHz. Vous pouvez les trouver sur l'étiquette située à l'arrière de votre routeur ROG.

- Une fois connecté, l'interface de gestion du routeur s'affiche automatiquement lors de l'ouverture de votre navigateur internet. Si ce n'est pas le cas, entrez <http://router.asus.com> dans la barre d'adresse..
- Définissez un mot de passe afin d'éviter les accès non autorisés au routeur.

REMARQUES :

- Référez-vous au manuel de la carte Wi-Fi pour la procédure de configuration de la connexion Wi-Fi.
- Pour configurer les paramètres de sécurité de votre réseau, consultez la section **Définir les paramètres de sécurité** du chapitre 3 de ce manuel.

Login Information Setup

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

Router Login Name:

New Password:

Retype Password: Show password

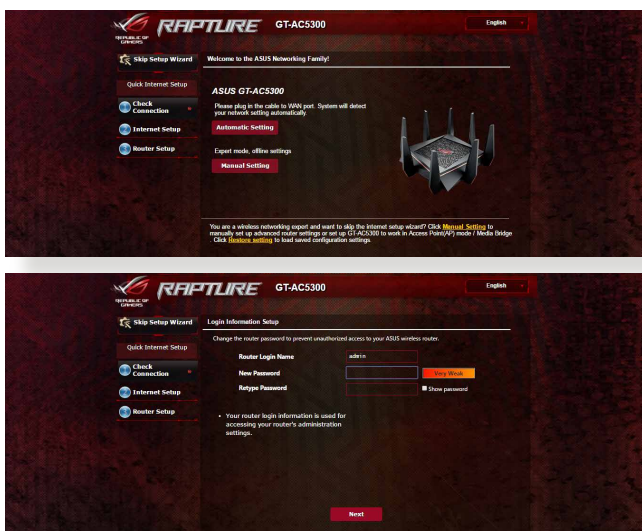
2.2 Configuration internet rapide avec auto-détection

L'assistant de configuration vous aide à configurer rapidement votre connexion internet.

REMARQUE : Lors de la toute première configuration de connexion internet, appuyez sur le bouton de réinitialisation de votre routeur Wi-Fi pour restaurer ses paramètres par défaut.

Utilisation de l'assistant de configuration internet avec auto-détection :

1. Ouvrez un navigateur internet. Vous serez automatiquement redirigé vers l'assistant de configuration ASUS (Configuration internet rapide). Si ce n'est pas le cas, tapez manuellement <http://router.asus.com>.
2. Dans la page de **Configuration des informations de connexion**, modifiez le mot de passe de connexion du routeur afin d'éviter les accès non autorisés au routeur Wi-Fi.

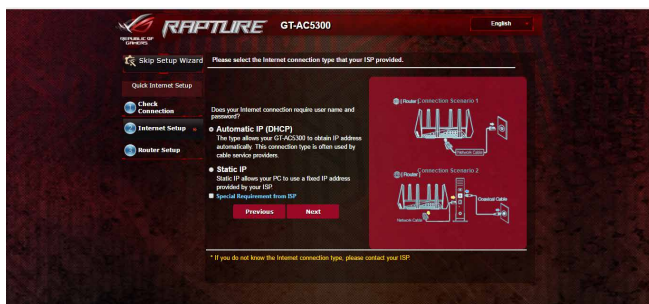


REMARQUE : Le nom d'utilisateur et le mot de passe de connexion sont différents des identifiants dédiés au SSID (2,4/5 GHz) et à la clé de sécurité. Le nom d'utilisateur et le mot de passe de connexion permettent d'accéder à l'interface de gestion des paramètres du routeur Wi-Fi. Le SSID (nom du réseau Wi-Fi) et la clé de sécurité permettent aux dispositifs Wi-Fi de se connecter au réseau 2,4 GHz/5 GHz de votre routeur.

3. Le routeur Wi-Fi détecte automatiquement si la connexion internet fournie par votre FAI utilise une **IP dynamique** ou le protocole **PPPoE**, **PPTP** ou **L2TP**. Entrez les informations nécessaires en fonction de votre type de connexion.

IMPORTANT ! Vous pouvez obtenir vos informations de connexion auprès de votre FAI (Fournisseur d'accès à Internet).

Connexion à adresse IP automatique (DHCP)



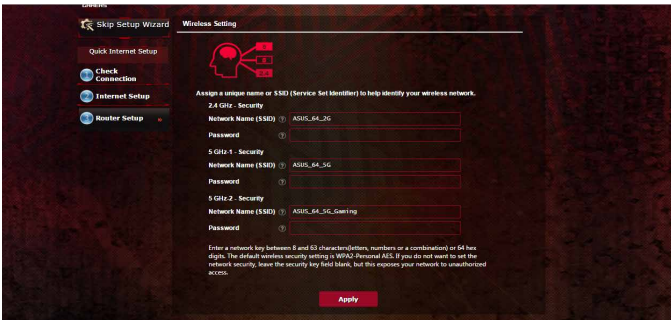
Connexion utilisant le protocole PPPoE, PPTP ou L2TP



REMARQUES:

- L'auto-détection de votre type de connexion a lieu lorsque vous configurez le routeur Wi-Fi pour la première fois ou lorsque vous restaurez les paramètres par défaut du routeur.
 - Si votre type de connexion internet n'a pas pu être détecté, cliquez sur **Skip to manual setting** (Configuration manuelle) pour configurer manuellement vos paramètres de connexion.
-

- Attribuez un nom au réseau (SSID) ainsi qu'une clé de sécurité pour votre connexion Wi-Fi 2,4 GHz et/ou 5 GHz. Cliquez sur **Apply** (Appliquer) une fois terminé.



- Lisez l'introduction des fonctionnalités du GT-AC5300, en particulier la fonctionnalité Game IPS pour plus d'informations. Il est fortement recommandé d'activer Game IPS lors de la première utilisation pour plus de sécurité.





- Vos paramètres Wi-Fi apparaissent à l'écran. Cliquez sur **Next** (Suivant) pour accéder à ROG Gaming Center.



2.3 Connexion à un réseau Wi-Fi

Après avoir configuré la connexion internet sur votre routeur, vous pouvez connecter votre ordinateur, ou tout autre appareil disposant d'une connectivité Wi-Fi, à votre réseau Wi-Fi.

Pour vous connecter à un réseau Wi-Fi sous Windows :

1. Sur votre ordinateur, cliquez sur l'icône réseau  de la zone de notification pour afficher la liste des réseaux Wi-Fi disponibles.
2. Sélectionnez le réseau Wi-Fi avec lequel vous souhaitez établir une connexion, puis cliquez sur **Connect** (Connecter).
3. Si nécessaire, entrez la clé de sécurité du réseau Wi-Fi, puis cliquez sur **OK**.
4. Patientez le temps que votre ordinateur puisse établir une connexion au réseau Wi-Fi. L'état de la connexion apparaît et l'icône réseau  affiche le statut Connecté.

REMARQUES :

- Consultez les chapitres suivants pour plus de détails sur les divers paramètres de configuration Wi-Fi disponibles.
 - Référez-vous au mode d'emploi de votre appareil pour plus de détails sur la connexion à un réseau Wi-Fi.
-

3 Configurer les paramètres généraux de ROG Gaming Center

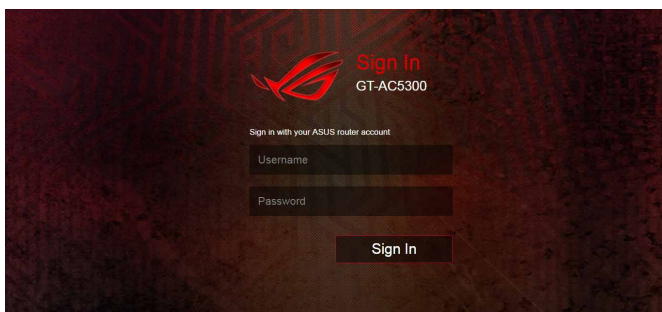
3.1 Se connecter à l'interface de gestion

Votre routeur Wi-Fi ROG intègre une interface utilisateur en ligne - ROG Gaming Center, qui vous donne un contrôle total sur votre réseau et vous fournit les informations à savoir telles que l'état des périphériques connectés et les valeurs pings des serveurs internet de jeu ainsi qu'un accès immédiat à toutes les fonctionnalités de jeu.

REMARQUE : Les fonctionnalités présentées peuvent varier en fonction du modèle.

Pour vous connecter à l'interface de gestion :

1. Dans la barre d'adresse de votre navigateur internet, entrez l'adresse IP par défaut de votre routeur Wi-Fi : <http://router.asus.com>.
2. Dans la page de connexion, entrez le nom d'utilisateur par défaut (**admin**) et le mot de passe que vous avez configuré dans **2.2 Configuration internet rapide**.



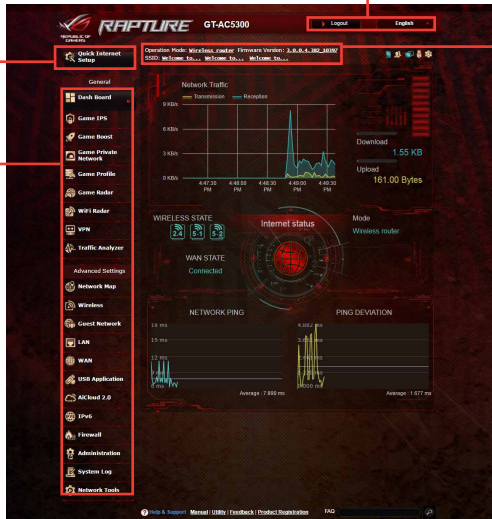
3. Vous pouvez dès lors configurer une grande variété de paramètres dédiés à votre routeur Wi-Fi ASUS.

Boutons de commande

Assistant de configuration internet

Voilet de navigation

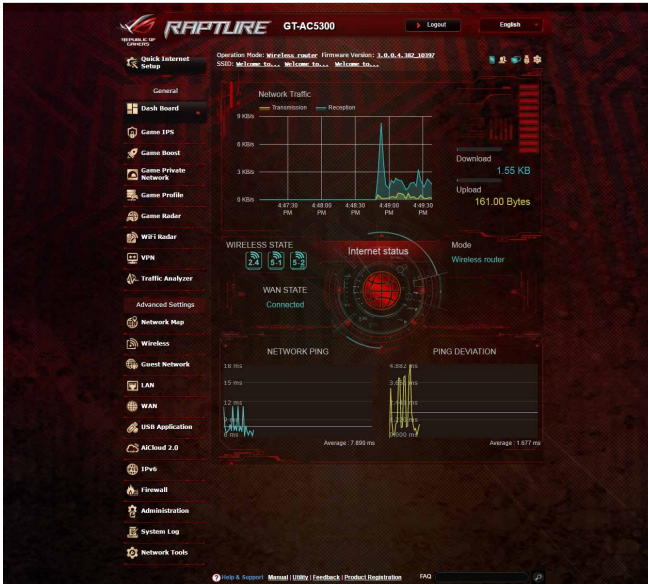
Zone d'infos



REMARQUE : Lors du tout premier accès à l'interface de gestion du routeur, vous serez automatiquement redirigé vers la page de configuration de connexion internet.

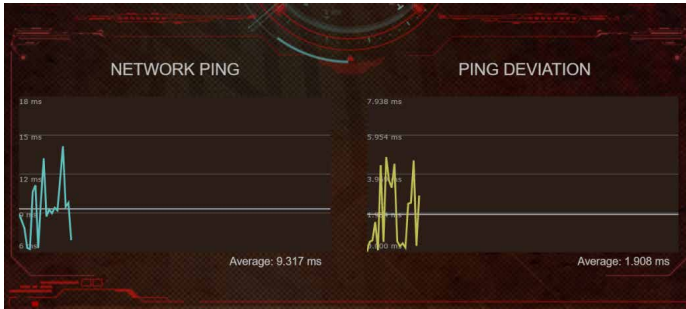
3.2 Tableau de bord

Le tableau de bord vous permet de surveiller le trafic en temps réel de votre environnement réseau et d'analyser le ping de réseau en temps réel ainsi que la déviation de ping.



Le ping de réseau fait référence aux expériences de jeu en ligne. Plus le ping est élevé plus la latence est élevée pour les jeux en temps réel. Un ping de réseau inférieur à 99 ms est considéré comme de bonne qualité pour la plupart des jeux en ligne. Si le ping de réseau est inférieur à 150 ms, la qualité est considérée comme acceptable. En général, si le ping de réseau est supérieur à 150 ms, il est difficile de pouvoir jouer de manière fluide.

La déviation de ping influence aussi fortement l'expérience de jeu en ligne. Avec une déviation de ping élevée, il est plus facile de créer un toggle lors d'un jeu en ligne. Il n'existe pas de référence pour la déviation de ping. Toutefois, une faible déviation de ping est préférable.



3.3 Game IPS (Système de Prévention d'Intrusion)

Game IPS fournit une surveillance en temps réel qui permet de détecter les logiciels malveillants, les logiciels espions et les accès non autorisés. Game IPS filtre également les sites internet et les applications indésirables et vous permet de planifier le temps d'accès à Internet d'un périphérique connecté.

Game IPS

Game IPS with Trend Micro uses real-time network monitoring to detect malware, viruses and other intrusions before it reaches your PC or connected devices. Parental Controls let you schedule times that a connected device is able to access the Internet. You can also restrict unwanted websites and apps.

Network Protection

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

Parental Controls

- Time Scheduling
- Web & Apps Filters

3.3.1 Configurer Game IPS

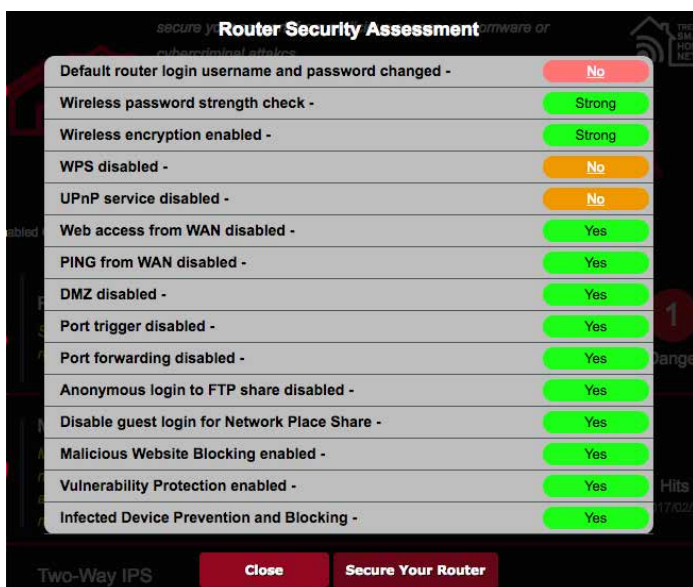
Game IPS évite les risques d'exploitation du réseau et protège le réseau contre les accès non autorisés.



Pour configurer Game IPS :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **Game IPS**.
2. À partir de la page principale de Game IPS, cliquez sur **Network Protection** (Protection du réseau).
3. À partir de l'onglet Network Protection (Protection du réseau), cliquez sur **Scan** (Analyser).

Les résultats de l'analyse s'affichent sur la page **Router Security Assessment** (Évaluation de la sécurité du routeur).



IMPORTANT ! Les éléments suivis de la marque **Yes** (Oui) sur la page **Router Security Assessment** (Évaluation de la sécurité du routeur) sont considérés comme sûrs.

4. (Optionnel) Dans la page **Router Security Assessment** (Évaluation de la sécurité du routeur), configurez manuellement les éléments suivis de la marque **No** (Non), **Weak** (Faible) ou **Very Weak** (Très faible). Pour ce faire :
 - a. Cliquez sur un élément pour aller à la page de configuration de l'élément.
 - b. À partir de la page des paramètres de sécurité de l'élément, modifiez les paramètres nécessaires puis cliquez sur **Apply** (Appliquer) une fois terminé.
 - c. Revenez à la page **Router Security Assessment** (Évaluation de la sécurité du routeur), puis cliquez sur **Close** (Fermer) pour quitter la page.
5. Pour configurer automatiquement les paramètres de sécurité, cliquez sur **Secure Your Router** (Sécuriser votre routeur).
6. Cliquez sur **OK** à l'apparition du message de confirmation.

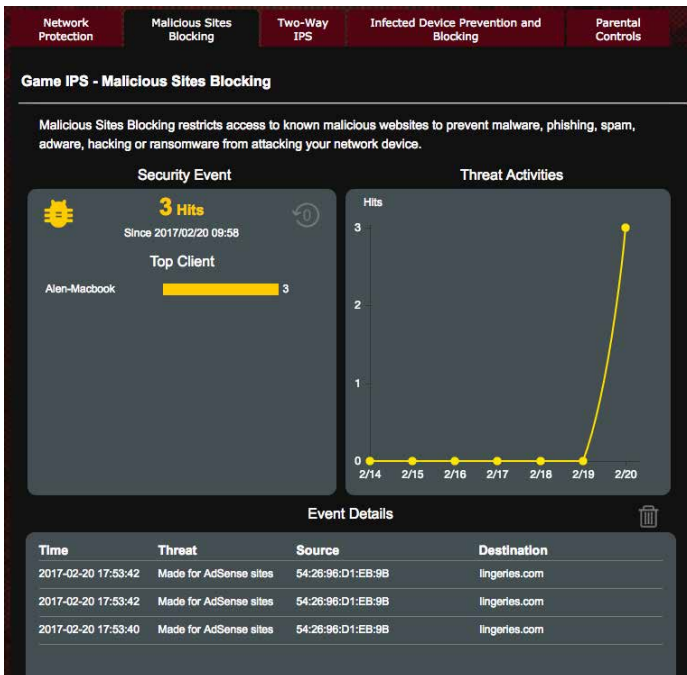
3.3.2 Blocage de sites malveillants

Cette fonctionnalité restreint l'accès aux sites internet malveillants connus figurant sur une base de données dans le Cloud pour une protection toujours à jour.

REMARQUE : Cette fonction est automatiquement activée lors de l'exécution de l'évaluation du niveau de sécurité du routeur.

Pour activer le blocage des sites malveillants :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **Game IPS**.
2. À partir de la page principale de Game IPS, cliquez sur **Network Protection** (Protection du réseau).
3. À partir du panneau de blocage des sites malveillants, cliquez sur **ON** (OUI).



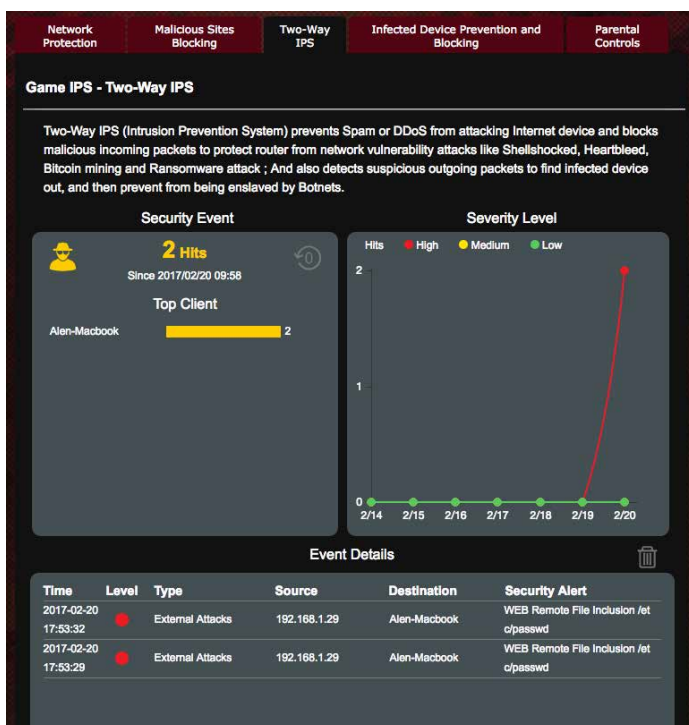
3.3.3 Two-Way IPS

Cette fonctionnalité résout les exploitations courantes pouvant subsister dans la configuration du routeur.

REMARQUE : Cette fonction est automatiquement activée lors de l'exécution de l'évaluation du niveau de sécurité du routeur.

Pour activer Two-Way IPS :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **Game IPS**.
2. À partir de la page principale de Game IPS, cliquez sur **Network Protection** (Protection du réseau).
3. À partir du panneau Two-Way IPS, cliquez sur **ON** (OUI).



3.3.4 Protection et blocage des périphériques infectés

Cette fonctionnalité permet d'empêcher les périphériques infectés de communiquer des informations personnelles ou un état infecté à des entités tierces.

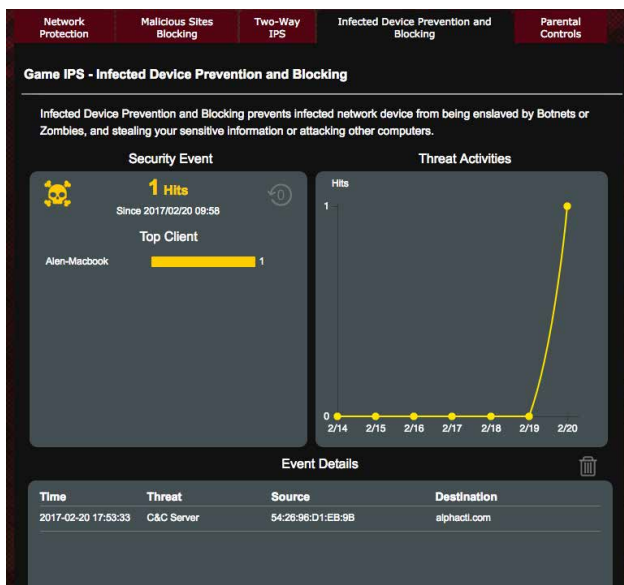
REMARQUE : Cette fonction est automatiquement activée lors de l'exécution de l'évaluation du niveau de sécurité du routeur.

Pour activer la protection et le blocage des périphériques infectés :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **Game IPS**.
2. À partir de la page principale de Game IPS, cliquez sur Network Protection (Protection du réseau).
3. À partir du panneau de protection et de blocage des périphériques infectés, cliquez sur **ON** (OUI).

Pour configurer les préférences d'envoi d'alertes :

1. À partir du panneau de protection et de blocage des périphériques infectés, cliquez sur **Alert Preference** (Préférence d'envoi d'alertes).
2. Sélectionnez ou entrez le nom du service de messagerie électronique, l'adresse email et le mot de passe, puis cliquez sur **Apply** (Appliquer).



3.3.5 Configurer le contrôle parental

Le contrôle parental permet de contrôler le temps d'accès à Internet ou de limiter le temps d'accès au réseau d'un client.

Pour activer Two-Way IPS :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **Game IPS**.
2. À partir de la page principale de Game IPS, cliquez sur l'onglet **Parental Controls** (Contrôle parental).

Game IPS - Web & Apps Filters

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

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

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

Web & Apps Filters ON

Client List (Max Limit : 16)

| Client Name (MAC Address) | Content Category | Add / Delete |
|--|---|--------------|
| <input type="text" value="ex: 2C:4D:54:E8:64:00"/> | <input checked="" type="checkbox"/> Adult <i>Block adult content can prevent child from visiting sexy, violence and illegal related content.</i> | |
| | <input checked="" type="checkbox"/> Instant Message and Communication <i>Block IM and communication content can prevent child from addicted to social networking usage.</i> | |
| | <input checked="" type="checkbox"/> P2P and File Transfer <i>Block P2P and File Transfer content can keep your network in a better transmission quality.</i> | |
| | <input checked="" type="checkbox"/> Streaming and Entertainment <i>Block Streaming and Entertainment content can prevent child from spending long time on Internet entertainment.</i> | |


No data in table.

Apply

Filtrage de sites et d'applications

Le filtrage de sites et d'applications est une fonctionnalité du contrôle parental qui permet de bloquer l'accès à certains sites internet ou applications indésirables.

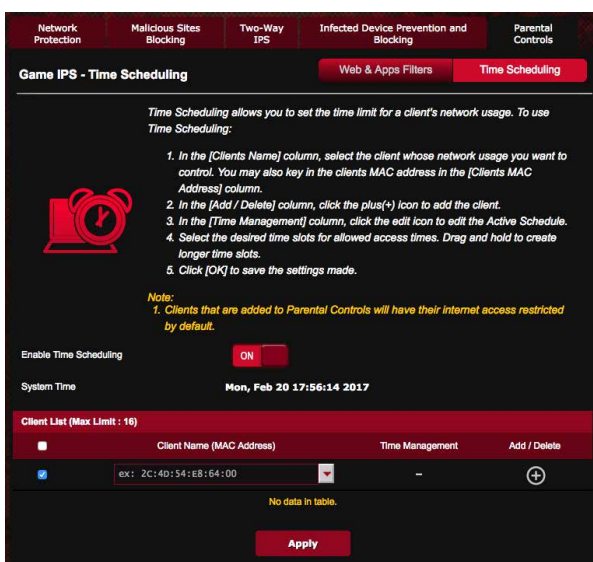
Pour configurer le filtrage de sites et d'applications :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **Game IPS**.
2. À partir de la page principale de Game IPS, cliquez sur l'icône **Parental Controls** (Contrôle parental) pour accéder à l'onglet de contrôle parental.
3. À partir du panneau **Enable Web & Apps Filters** (Activer le filtrage de sites et d'applications), cliquez sur **ON** (OUI).
4. Cliquez sur **I agree** (J'accepte) pour accepter le contrat de licence pour utilisateur final.
5. Dans la colonne **Client List** (Liste des clients), sélectionnez un client ou tapez son nom dans la liste déroulante.
6. Dans la colonne **Content Category** (Catégorie de contenu), sélectionnez le contenu à filtrer : **Adult** (Adulte), **Instant Message and Communication** (Messagerie instantanée et communications), **P2P and File Transfer** (P2P et transfert de fichiers) et **Streaming and Entertainment** (Streaming et divertissement).
7. Cliquez sur  pour ajouter le profil du client.
8. Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications.

Planification horaire

La planification horaire vous permet de limiter le temps d'accès d'un client au réseau.

REMARQUE : Vérifiez que la date et l'heure du système sont bien synchronisés avec le serveur NTP.



Pour configurer la planification horaire :

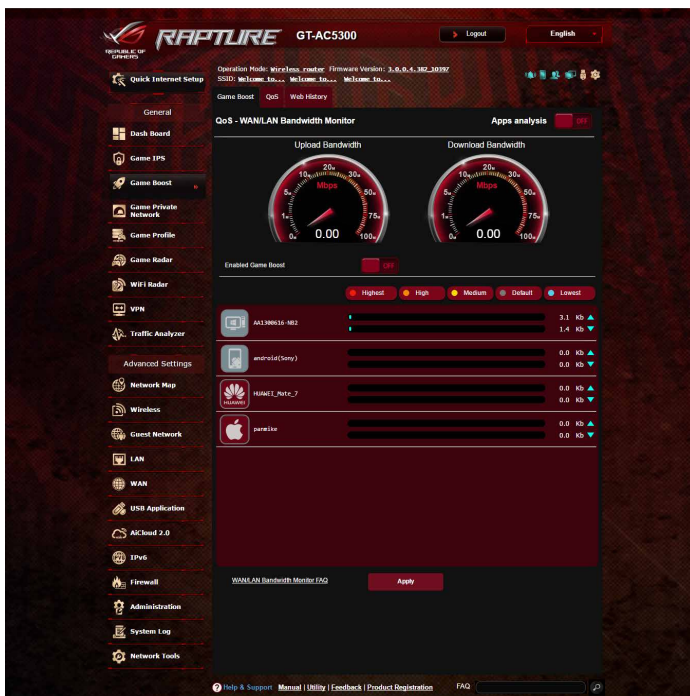
1. À partir du volet de navigation, cliquez sur **General** (Général) > **Game IPS** > **Parental Controls** (Contrôle parental) > **Time Scheduling** (Planification horaire).
2. À partir du panneau **Enable Time Scheduling** (Activer la planification horaire), cliquez sur **ON** (OUI).
3. Dans la colonne **Clients Name** (Nom des clients), sélectionnez un client ou tapez son nom dans la liste déroulante.

REMARQUE : Vous pouvez aussi entrer l'adresse MAC du client dans la colonne Client MAC Address (Adresse MAC du client). Assurez-vous que le nom du client ne possède pas de caractères spéciaux ou d'espaces car cela peut causer un dysfonctionnement du routeur.

4. Cliquez sur **+** pour ajouter le profil du client.
5. Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications.

3.4 Game Boost

Cette fonctionnalité vous permet d'activer Game Boost en un clic. Lorsque la fonctionnalité Game Boost est activée, le routeur donne la priorité aux paquets de jeu pour vous offrir une expérience de jeu optimale.



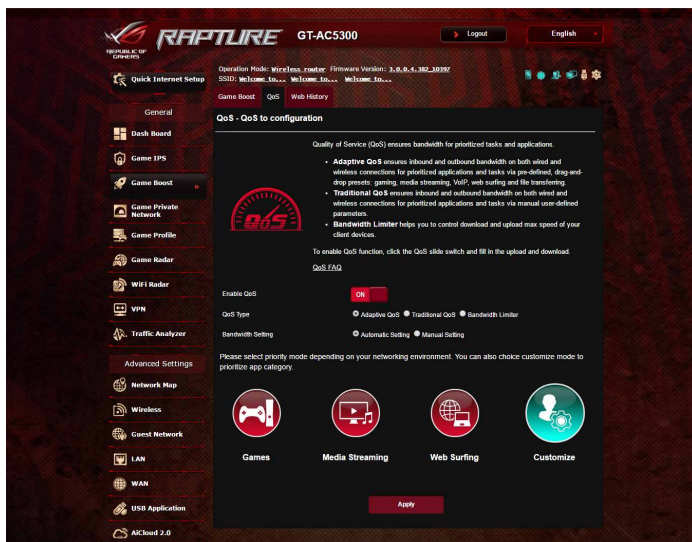
Analyse des applications

Pour activer l'analyse des applications :

À partir de l'onglet **Game Boost**, allez dans le panneau **Apps Analysis** (Analyse des applications) et cliquez sur **ON** (OUI).

3.4.1 QoS

Cette fonctionnalité permet d'assurer une bande passante suffisante pour les tâches et les applications prioritaires.



Pour activer la fonction QoS :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **Game Boost** > onglet **QoS**.
2. À partir du panneau **Enable QoS** (Activer QoS), cliquez sur **ON** (OUI).
3. Remplissez les champs réservés à la bande passante montante et descendante.

REMARQUE : Obtenez vos informations de bande passante auprès de votre FAI (Fournisseur d'accès à Internet). Vous pouvez aussi vous rendre sur le site <http://speedtest.net> pour vérifier et obtenir vos informations de bande passante.

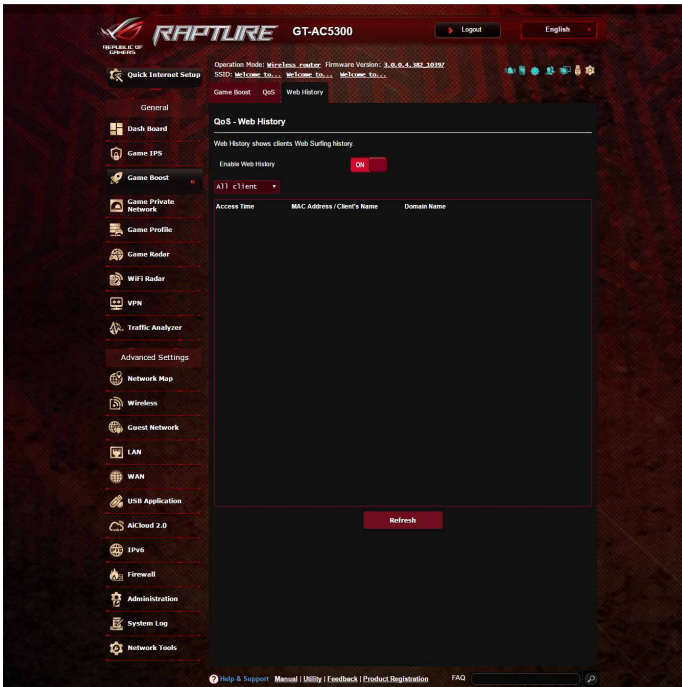
4. Sélectionnez le type de service QoS (adaptatif, standard ou limiteur de bande passante) de votre configuration.

REMARQUE : La définition de chacun des types de service QoS est expliquée dans l'onglet QoS.

5. Cliquez sur **Apply** (Appliquer).

3.4.2 Historique internet

Cette fonctionnalité affiche l'historique et les détails des sites ou des URL visités par le client.

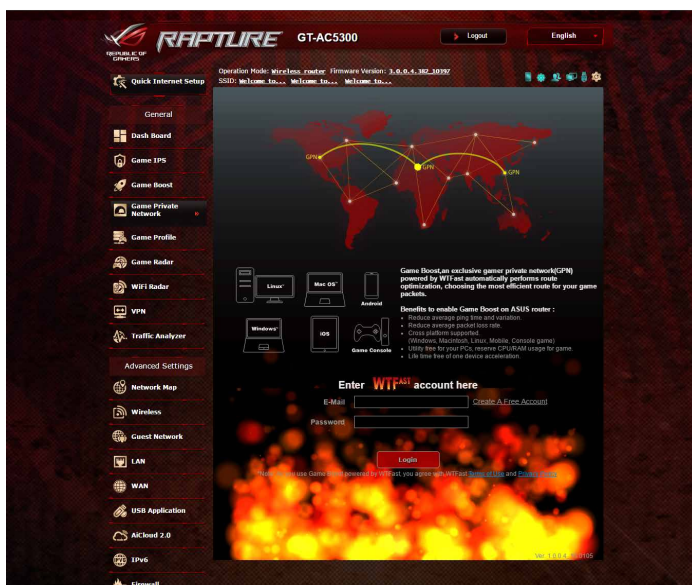


Pour visualiser l'historique internet :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **Game Boost** > onglet **Web History** (Historique internet).
2. (Optionnel) Cliquez sur **Refresh** (Actualiser) pour rafraîchir la liste.

3.5 Game Private Network (Réseau privé de jeu WTFast)

Le réseau de gaming privé optimisé par WTFast réduit votre latence de jeu moyenne, les pics de flux et les pertes de paquet de votre connexion. Vous pouvez ainsi profiter d'une connexion plus réactive, plus fluide et plus rapide avec pratiquement tous les MMO.



Pour mettre à jour le firmware :

1. Ouvrez votre navigateur internet et saisissez l'adresse <http://router.asus.com>, entrez le nom de connexion et le mot de passe par défaut (admin/admin) pour accéder à l'interface de gestion ASUSWRT.
2. Allez dans **Administration > Firmware Upgrade** (Mise à niveau du firmware), cliquez sur **Check** (Vérifier) et suivez les instructions apparaissant à l'écran pour mettre à niveau le firmware.

Vous pouvez également télécharger la dernière version de firmware depuis l'adresse <http://support.asus.com/ServiceHome.aspx> pour mettre à niveau manuellement le firmware.

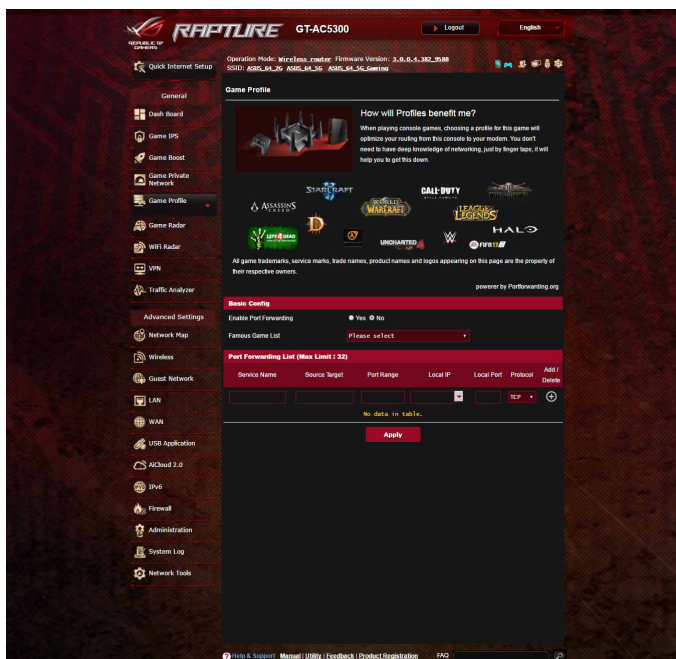
Pour utiliser WFast :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **Game Boost**.
2. Créez un compte WFast gratuit via l'adresse <https://www.wtfast.com/>.
3. Connectez-vous à votre compte WFast.
4. Dans la liste **WTFast Rules** (Règles WFast), créez un profil pour le périphérique sur lequel vous souhaitez utiliser le réseau de gaming privé WFast.
5. Sélectionnez un serveur de réseau de gaming privé en fonction de votre emplacement ou sélectionnez "Auto" et "Apply" (Appliquer) les paramètres.
6. Activez le profil de réseau de gaming privé AVANT de commencer à jouer.

REMARQUE : Les comptes gratuits ne prennent en charge qu'un seul périphérique, si vous souhaitez mettre à niveau votre version pour qu'elle prenne en charge plusieurs périphériques, cliquez sur **Upgrade** (Mettre à niveau) et achetez un abonnement.

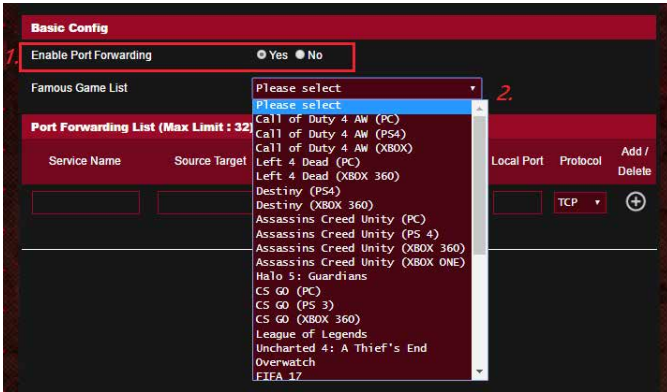
3.6 Game Profile (Profil de jeu)


En jouant sur ordinateur ou sur console de jeu, certains problèmes de connexion peuvent apparaître en raison du FAI ou des paramètres du routeur de votre environnement tels que le NAT et les blocs port. La fonctionnalité Profil de jeu empêche le routeur de bloquer la connexion de jeu.

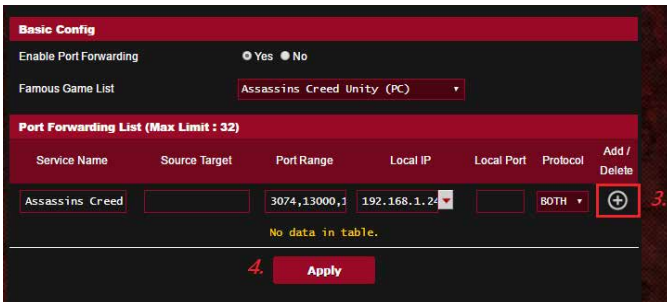


Pour utiliser Profil de jeu :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **Game Profile** (Profil de jeu) puis cochez **Yes** (Oui) pour activer la redirection de port.
2. Choisissez un jeu dans **Famous Game List** (Liste des jeux populaires), qui sera mise à jour périodiquement.

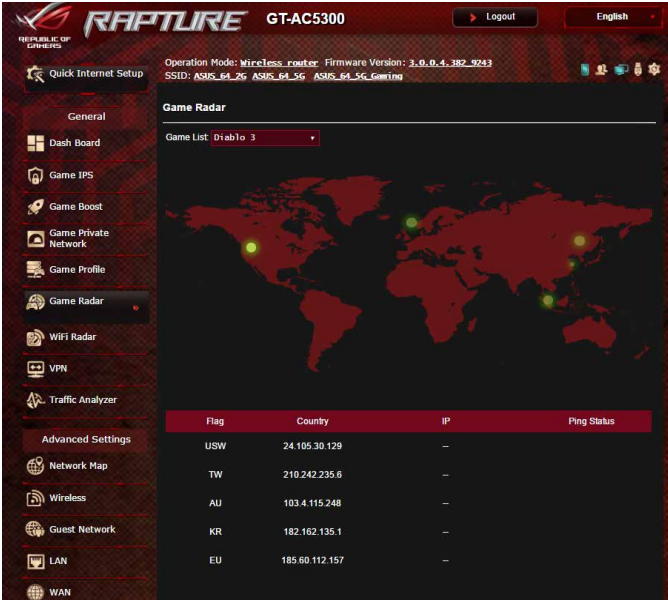


3. Cliquez sur  pour ajouter le jeu.
4. Cliquez sur **Apply** (Appliquer) pour appliquer tous les profils.



3.7 Game Radar

Game Radar est un outil de diagnostic qui vous aide à identifier la qualité de la connexion des serveurs pour des jeux spécifiques.

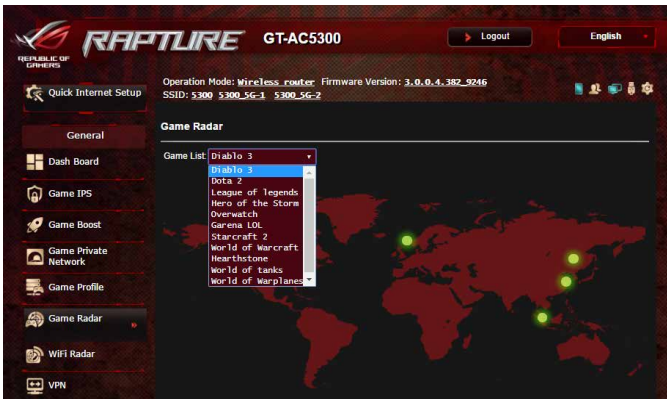


The screenshot shows the RAFTURE GT-AC5300 web interface. The header includes the RAFTURE logo, the model number GT-AC5300, and a Logout button. The main content area is titled "Game Radar" and features a "Game List" dropdown menu set to "Diablo 3". Below this is a world map with several green dots indicating server locations. A table below the map displays the following data:

| Flag | Country | IP | Ping Status |
|------|----------------|----|-------------|
| USW | 24.105.30.129 | - | |
| TW | 210.242.235.6 | - | |
| AU | 103.4.115.248 | - | |
| KR | 182.162.135.1 | - | |
| EU | 185.60.112.157 | - | |

Pour utiliser Game Radar :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **Game Radar** et sélectionnez un jeu de la liste.

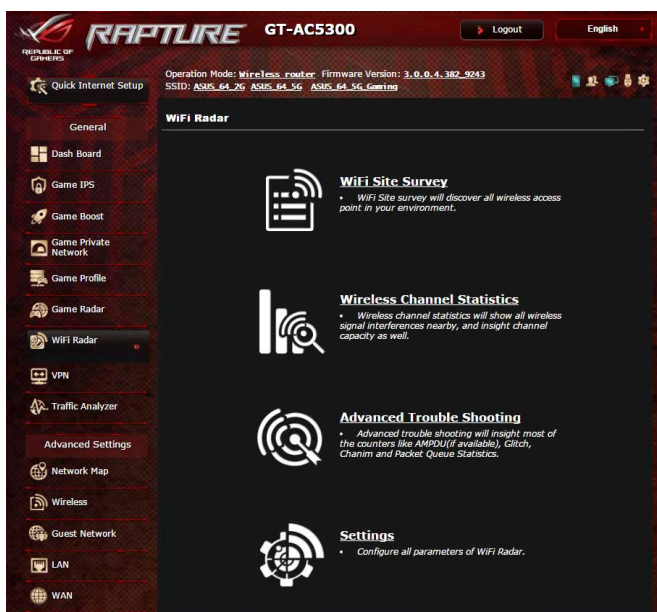


2. Vérifiez le **Ping Status** (l'état de ping) de chaque serveur.
3. Pour une expérience de jeu en ligne fluide, sélectionnez un serveur de jeu disposant d'un état de ping faible.

3.8 WiFi Radar

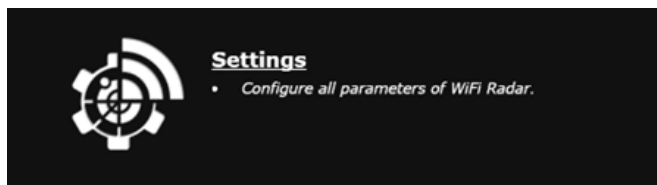
Wi-Fi Radar est un outil d'analyse avancé pour votre réseau Wi-Fi qui traite en détail les canaux et les données de paquets pour dépanner les problèmes.

REMARQUE : L'activation de WiFi Radar peut entraîner une chute des performances Wi-Fi. Activez Wi-Fi Radar uniquement lorsque nécessaire.



Pour utiliser WiFi Radar :

1. Rendez-vous dans Paramètres et configurez tous les paramètres Wi-Fi.
1. À partir du volet de navigation, cliquez sur **General** (Général) > **WiFi Radar** et planifiez l'enregistrement des données.



2. Cliquez sur **Start Data Collection** (Démarrer la collecte de données).
3. Cliquez sur **Submit** (Soumettre) après avoir configuré tous les paramètres.

Home Site Survey Channel Statistics Advanced Troubleshooting Configure

Settings
Configure all parameters of WiFi Radar.

Sample Interval:
 5 Second 10 Second 15 Second 20 Second

Start/Stop Data Collection:

Start collecting data every
 Sunday Monday Tuesday Wednesday Thursday Friday Saturday
 From To

Database Size: MB
 (Please note that, for example, 2 STA's connected using a 5 seconds sample interval run for 1 hour will occupy approximately 1.30 MB of database)
 Once Database size reaches maximum limit: Overwrite Older Data Stop Datacollection

Counters:

| | |
|--|---|
| <input checked="" type="checkbox"/> Channel Statistics | <input checked="" type="checkbox"/> Packet Retired |
| <input checked="" type="checkbox"/> Chanm Statistics | <input checked="" type="checkbox"/> Queue Utilization |
| <input checked="" type="checkbox"/> Rx CRC8 glitches | <input checked="" type="checkbox"/> Queue Length Per Precedence |
| <input checked="" type="checkbox"/> Bad FCS | <input checked="" type="checkbox"/> Data Throughput |
| <input checked="" type="checkbox"/> Bad FCS | <input checked="" type="checkbox"/> Physical Rate |
| <input checked="" type="checkbox"/> Packet Requested | <input checked="" type="checkbox"/> RTT's Fail |
| <input checked="" type="checkbox"/> Packet Stored | <input checked="" type="checkbox"/> Retry Drop |
| <input checked="" type="checkbox"/> Packet Dropped | <input checked="" type="checkbox"/> PS Betsy |
| | <input checked="" type="checkbox"/> Acked |

Export Database:

3.8.1 Enquête site Wi-Fi

Enquête site Wi-Fi permet de rechercher des réseaux sans fil dans votre environnement.



3.8.2 Statistiques canal sans fil

Cette fonctionnalité affiche l'utilisation des canaux de toutes les bandes et les statistiques de distribution de canal dans votre environnement.



3.8.3 Dépannage avancé

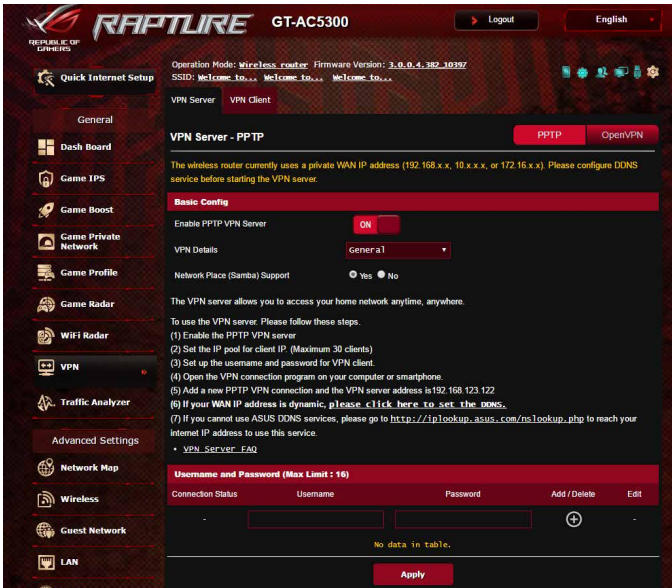
Cette fonctionnalité affiche les statistiques de dysfonctionnement Wi-Fi dans votre environnement.




3.9 VPN

Un VPN (Virtual Private Network) offre un moyen de communication sécurisé sur un ordinateur ou réseau distant par le biais d'un réseau public tel qu'Internet.

REMARQUE : Avant de configurer une connexion VPN, l'adresse IP ou le nom de domaine d'un serveur VPN sont nécessaires.

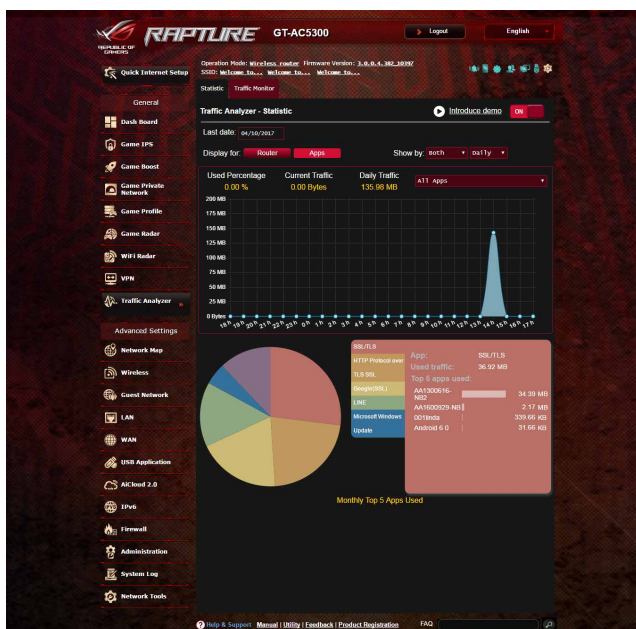


Pour configurer l'accès à un serveur VPN :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **VPN**.
2. Dans le champ **Enable PPTP VPN Server** (Activer le serveur VPN PPTP), sélectionnez **ON** (OUI).
3. Dans la liste déroulante **VPN Details** (Détails VPN), sélectionnez **Advanced Settings** (Paramètres avancés) pour configurer d'autres paramètres avancés comme la diffusion de contenu, l'authentification, le chiffrement MPPE et la plage d'adresses IP.
4. Dans le champ **Network Place (Samba) Support** (Prise en charge de serveur Samba), cochez **Yes** (Oui).
5. Entrez le nom d'utilisateur et le mot de passe d'accès au serveur VPN. Cliquez sur .
6. Cliquez sur **Apply** (Appliquer).

3.10 Dispositif d'analyse du trafic

Le dispositif d'analyse du trafic vous donne un aperçu rapide des événements de votre réseau de manière quotidienne, hebdomadaire ou mensuelle. Il vous permet de visualiser rapidement l'utilisation de la bande passante de chaque utilisateur, les appareils et applications utilisés, pour vous aider à réduire les congestions de votre connexion internet. C'est aussi un moyen de surveiller l'utilisation et les activités internet des utilisateurs.



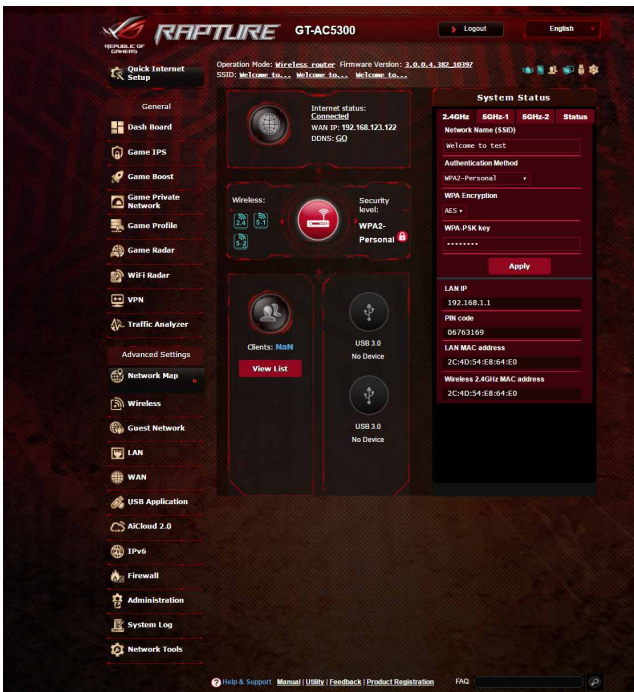
Pour configurer le dispositif d'analyse du trafic :

1. À partir du volet de navigation, cliquez sur **General** (Général) > **Traffic Analyzer** (Dispositif d'analyse du trafic).
2. À partir de la page principale de **Traffic Analyzer** (Dispositif d'analyse du trafic), activez les statistiques du dispositif d'analyse du trafic.
3. Sélectionnez la date du graphique à afficher.
4. Dans le champ **Display for** (Afficher pour), sélectionnez Router (Routeur) ou Apps (Applications) pour afficher les informations de trafic.
5. Dans le champ **Show by** (Afficher par), sélectionnez comment afficher les informations de trafic.

4 Configurer les paramètres avancés

4.1 Utiliser la carte du réseau

La carte du réseau vous permet d'avoir une vue d'ensemble du réseau, mais aussi de configurer certains paramètres de sécurité, de gérer les clients du réseau et de surveiller les dispositifs USB connectés au routeur.



4.1.1 Configurer les paramètres de sécurité Wi-Fi

Pour protéger votre réseau Wi-Fi contre les accès non autorisés, vous devez configurer les paramètres de sécurité du routeur.

Pour configurer les paramètres de sécurité Wi-Fi :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Network Map** (Carte du réseau).
2. La colonne **System status** (État du système) affiche les options de sécurité telles que le SSID, le niveau de sécurité et la méthode de chiffrement.

REMARQUE : Vous pouvez définir des paramètres de sécurité différents pour les bandes 2,4 GHz et 5 GHz.

Paramètres de sécurité 2,4 GHz Paramètres de sécurité 5 GHz-1

The screenshot shows the 'System Status' configuration page for the 2.4GHz band. At the top, there are four tabs: '2.4GHz', '5GHz-1', '5GHz-2', and 'Status', with '2.4GHz' selected. The page contains the following fields: 'Network Name (SSID)' with the value 'Welcome to test', 'Authentication Method' set to 'WPA2-Personal', 'WPA Encryption' set to 'AES', and 'WPA-PSK key' with a masked password. An 'Apply' button is at the bottom.

The screenshot shows the 'System Status' configuration page for the 5GHz-1 band. At the top, there are four tabs: '2.4GHz', '5GHz-1', '5GHz-2', and 'Status', with '5GHz-1' selected. The page contains the following fields: 'Network Name (SSID)' with the value 'Welcome to test_5G', 'Authentication Method' set to 'WPA2-Personal', 'WPA Encryption' set to 'AES', and 'WPA-PSK key' with a masked password. An 'Apply' button is at the bottom.

Paramètres de sécurité 5 GHz-2

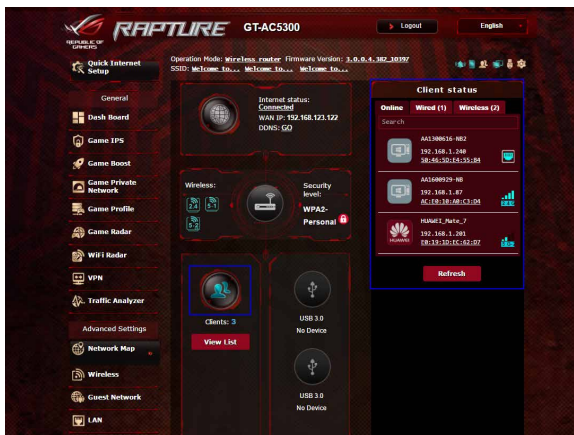
The screenshot shows the 'System Status' configuration page for the 5GHz-2 band. At the top, there are four tabs: '2.4GHz', '5GHz-1', '5GHz-2', and 'Status', with '5GHz-2' selected. The page contains the following fields: 'Network Name (SSID)' with the value 'Welcome to test_5G-2', 'Authentication Method' set to 'WPA2-Personal', 'WPA Encryption' set to 'AES', and 'WPA-PSK key' with a masked password. An 'Apply' button is at the bottom.

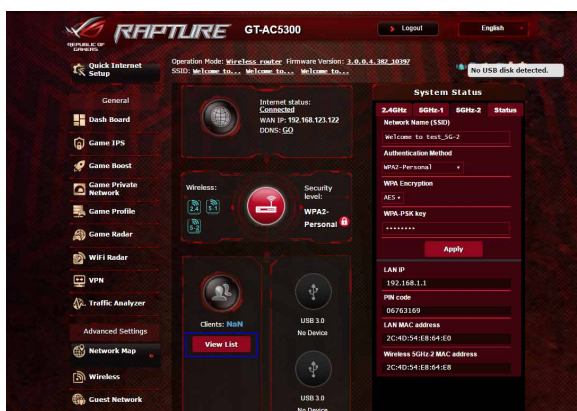
3. Dans le champ **Wireless name (SSID)** (Nom Wi-Fi (SSID)), spécifiez un nom unique pour votre réseau Wi-Fi.
4. Dans le menu déroulant **Authentication Method** (Méthode d'authentification), sélectionnez la méthode de chiffrement. Si vous sélectionnez WPA-Personal ou WPA-2 Personal comme méthode de chiffrement, entrez une clé de sécurité appropriée.

IMPORTANT ! La norme IEEE 802.11n/ac n'autorise pas l'utilisation du haut débit avec les méthodes de chiffrement WEP ou WPA-TKIP. Si vous utilisez ces méthodes de chiffrement, votre débit ne pourra pas excéder les limites de vitesse établies par la norme IEEE 802.11g 54 Mb/s.

- 5 Cliquez sur **Apply** (Appliquer) une fois terminé.

4.1.2 Gérer les clients du réseau





All By interface

All list [Hide]

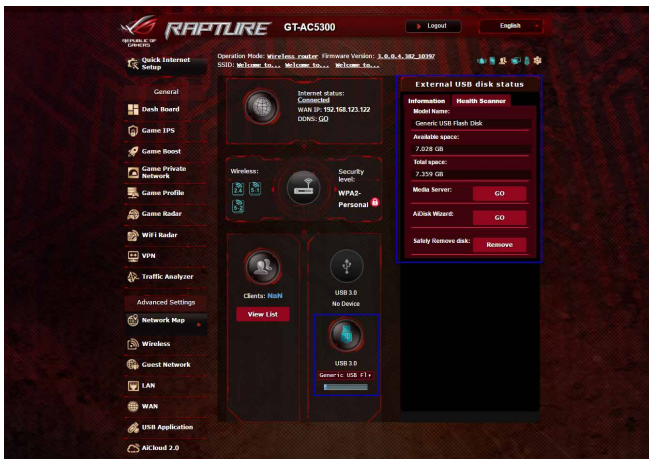
| Internet | Icon | Clients Name | Clients IP Address | Clients MAC Address | Interface | Tx Rate (Mbps) | Rx Rate (Mbps) | Access time |
|----------|------|---------------|--------------------|---------------------|-------------------|----------------|----------------|-------------|
| | | android(Sony) | 192.168.1.116 | DHCP | A0:E4:53:FC:42:CA | 433.3 | 40.5 | 02:50:55 |
| | | HUAWEl_Mate_7 | 192.168.1.201 | DHCP | E0:19:1D:EC:62:07 | 150 | 13.5 | 02:31:02 |

Pour gérer les clients de votre réseau :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Network Map** (Carte du réseau).
2. Dans l'écran **Network Map** (Carte du réseau), cliquez sur l'icône **Clients** (Clients) pour afficher les informations relatives aux clients de votre réseau.
3. Cliquez sur View List (Afficher la liste) sous l'icône **Clients** pour afficher tous les clients.
4. Pour bloquer l'accès d'un client à votre réseau, sélectionnez le client, puis cliquez sur l'icône représentant un cadenas ouvert.

4.1.3 Surveiller un périphérique USB

Le routeur Wi-Fi ASUS intègre deux ports USB pour la connexion de périphériques USB, tels qu'un périphérique de stockage ou une imprimante USB. Ces ports vous permettent de surveiller votre environnement de travail, partager des fichiers ou une imprimante avec les clients de votre réseau.



REMARQUES :

- Pour utiliser cette fonctionnalité, vous devez connecter un périphérique de stockage USB (ex : disque dur ou clé USB) à l'un des ports USB 2.0 / 3.0 situés à l'arrière de votre routeur Wi-Fi. Assurez-vous que le périphérique de stockage USB est formaté et correctement partitionné. Visitez le site internet d'ASUS sur <http://event.asus.com/networks/disksupport> pour consulter la liste des formats de fichiers pris en charge.
- Les ports USB prennent en charge deux lecteurs USB ou un lecteur USB plus une imprimante USB.

IMPORTANT ! Vous devrez d'abord créer un compte de partage (doté des permissions d'accès nécessaires) avant de pouvoir autoriser d'autres clients du réseau à accéder au périphérique USB par le biais d'un site FTP, des centres de serveurs, Samba ou AiCloud. Pour plus de détails, consultez les sections **4.6 Utiliser les applications USB** et **4.7 Utiliser AiCloud 2.0** de ce manuel.

Pour surveiller votre périphérique USB :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Network Map** (Carte du réseau).
2. Dans l'écran Network Map (Carte du réseau), cliquez sur l'icône **USB Disk Status** (État de disque USB) pour afficher les informations du disque USB connecté au routeur Wi-Fi.
3. Dans le champ AiDisk Wizard (Assistant AiDisk), cliquez sur **GO** pour configurer un serveur FTP permettant le partage de fichiers sur Internet.


REMARQUES:

- Pour plus de détails, consultez la section **4.6.2 Utiliser les centres de serveurs** de ce manuel.
- Le routeur Wi-Fi fonctionne avec la plupart des périphériques de stockage USB d'une capacité maximale de 4 To et prend en charge la lecture/écriture pour les formats de fichiers FAT16, FAT32, NTFS et HFS+.

Éjecter un disque USB

IMPORTANT : Une mauvaise éjection du périphérique de stockage USB peut endommager les données contenues sur le disque.

Pour éjecter un disque USB en toute sécurité :

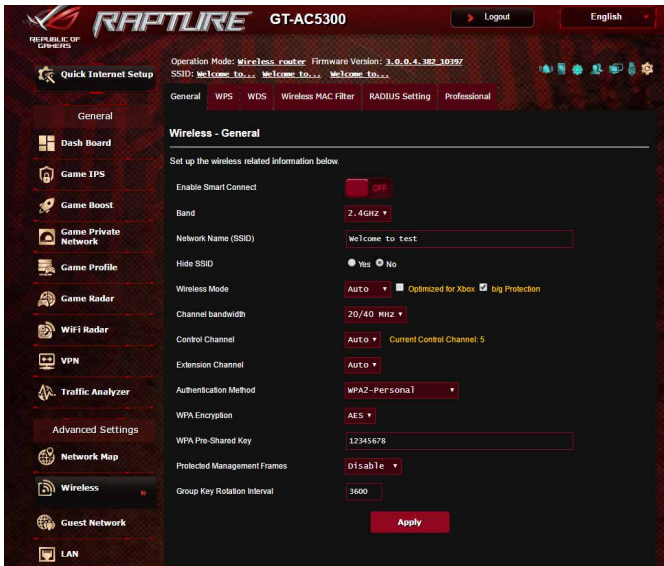
1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Network Map** (Carte du réseau).
2. Cliquez d'abord sur l'icône  située dans le coin supérieur droit de l'écran, puis sur l'option **Eject USB disk** (Éjecter le disque USB). Lorsque le disque a été éjecté, l'état du disque apparaît comme étant **Unmounted** (Non monté).



4.2 Wi-Fi

4.2.1 General (Général)

L'onglet General (Général) vous permet de configurer les paramètres Wi-Fi de base.



Pour configurer les paramètres Wi-Fi de base :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Wireless** (Wi-Fi) > onglet **General** (Général).
2. Sélectionnez la bande de fréquence 2,4 GHz ou 5 GHz destinée au réseau Wi-Fi.
3. Déplacez l'interrupteur de l'élément **Enable Smart Connect** (Activer Smart Connect) sur **ON** (Activé) pour activer la fonction Smart Connect. Cette fonction permet de connecter automatiquement les clients Wi-Fi à la bande de fréquence 2,4 GHz ou 5 GHz appropriée pour une vitesse optimale.

4. Attribuez un nom unique composé d'un maximum de 32 caractères faisant office de SSID (Service Set Identifier) et permettant d'identifier votre réseau Wi-Fi. Les appareils disposant de capacités Wi-Fi peuvent identifier et se connecter à votre réseau Wi-Fi par le biais du SSID. Les SSID de la barre d'informations sont mis à jour une fois les nouveaux SSID sauvegardés dans les paramètres.

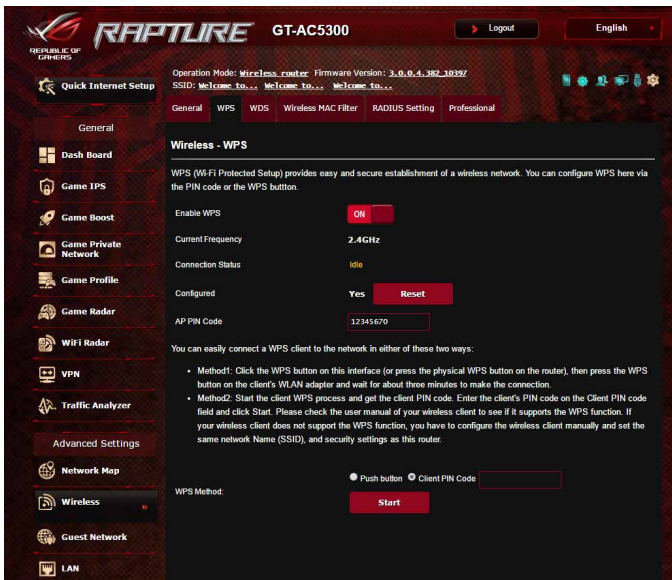
REMARQUE : Vous pouvez affecter différents SSID pour les bandes de fréquence 2,4 GHz et 5 GHz.

5. Dans le champ **Hide SSID** (Masquer le SSID), sélectionnez **Yes** (Oui) si vous ne souhaitez pas que les périphériques Wi-Fi puissent détecter votre SSID. Lorsque cette option est activée, vous devez saisir manuellement le SSID sur l'appareil souhaitant se connecter à votre réseau Wi-Fi.
6. Sélectionnez ensuite l'un des modes Wi-Fi disponibles pour déterminer quels types d'appareils Wi-Fi peuvent se connecter à votre routeur :
 - **Auto** : Les appareils utilisant les normes 802.11ac, 802.11n, 802.11g et 802.11b peuvent se connecter au routeur Wi-Fi.
 - **N only (N uniquement)**: Permet de maximiser les performances de la norme 802.11n. Toutefois, le matériel prenant en charge les normes 802.11g et 802.11b ne pourra pas établir de connexion au routeur Wi-Fi.
 - **Legacy (Hérité)**: Les appareils utilisant les normes 802.11b/g/n peuvent se connecter au routeur Wi-Fi. Toutefois le matériel prenant en charge la norme 802.11n de manière native, ne fonctionnera qu'à une vitesse maximum de 54 Mb/s.
7. Sélectionnez le canal d'opération du routeur. Choisissez **Auto** pour autoriser le routeur à sélectionner automatiquement le canal générant le moins d'interférences.
8. Sélectionnez l'un des canaux de bande passante disponibles.
9. Choisissez l'une des méthodes d'authentification disponibles.
10. Une fois terminé, cliquez sur **Apply** (Appliquer).

4.2.2 WPS

WPS (Wi-Fi Protected Setup) est une norme de sécurité simplifiant la connexion d'un appareil à un réseau Wi-Fi. Vous pouvez utiliser la fonctionnalité WPS par le biais d'un code de sécurité ou du bouton WPS dédié.

REMARQUE : Vérifiez que votre périphérique Wi-Fi soit compatible avec la norme WPS avant de tenter d'utiliser cette fonctionnalité.



Pour activer et utiliser la fonctionnalité WPS sur votre réseau Wi-Fi :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Wireless** (Wi-Fi) > onglet **WPS**.
2. Déplacez l'interrupteur sur **ON** (OUI) pour activer la fonctionnalité WPS.
3. Par défaut, la norme WPS utilise la bande de fréquence 2,4 GHz. Si vous souhaitez plutôt utiliser la bande à 5 GHz, déplacez l'interrupteur sur **OFF** (Désactiver), cliquez sur le bouton **Switch Frequency** (Changer de fréquence) dans le champ **Current Frequency** (Fréquence actuelle), puis déplacez de nouveau l'interrupteur sur **ON** (OUI).

REMARQUE : La norme WPS est compatible avec les méthodes d'authentification à système ouvert, WPA-Personal et WPA2-Personal. Les chiffrements à clés partagées, WPA-Enterprise, WPA2-Enterprise et RADIUS ne sont pas pris en charge.

3. Dans le champ WPS Method (Méthode de connexion WPS), sélectionnez **Push Button** (Pression de bouton) ou **Client PIN code** (Code PIN). Si vous souhaitez utiliser le bouton WPS, continuez à l'étape 4. Si vous optez plutôt pour le code PIN, passez directement à l'étape 5.
4. Pour utiliser le bouton WPS :
 - a. Cliquez sur **Start** (Démarrer) ou sur le bouton WPS placé à l'arrière du routeur.
 - b. Appuyez ensuite sur le bouton WPS de votre périphérique Wi-Fi. Un logo WPS figure normalement sur ce bouton.

REMARQUE : Inspectez votre périphérique Wi-Fi ou consultez son mode d'emploi pour localiser l'emplacement du bouton WPS.

- c. Le routeur Wi-Fi recherchera automatiquement la présence de dispositifs WPS à proximité. Si aucun appareil WPS n'est détecté, le routeur basculera en mode veille.
5. Pour utiliser un code PIN :
 - a. Munissez-vous du code PIN de votre périphérique Wi-Fi. Celui-ci est généralement situé sur l'appareil lui-même ou dans son mode d'emploi.
 - b. Entrez le code PIN dans le champ réservé à cet effet.
 - c. Cliquez sur **Start** (Démarrer) pour basculer le routeur Wi-Fi en mode d'attente WPS. Le voyant lumineux WPS clignote rapidement trois fois de manière consécutive jusqu'à ce que la connexion WPS soit établie.

4.2.3 Pontage WDS

Le pontage WDS (Wireless Distribution System) permet à votre routeur ASUS de se connecter de manière exclusive à un autre point d'accès Wi-Fi, empêchant d'autres périphériques Wi-Fi ou stations d'établir une connexion au routeur Wi-Fi ASUS. Dans ce scénario d'utilisation, le routeur ASUS peut faire office de répéteur Wi-Fi communiquant avec un autre point d'accès et d'autres clients.



Pour configurer un pont Wi-Fi :


1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Wireless** (Wi-Fi) > onglet **WDS** (Pontage).
2. Sélectionnez une bande de fréquence Wi-Fi.

3. Dans le champ **AP Mode** (Mode point d'accès), sélectionnez l'une des options suivantes :
 - **AP Only (Point d'accès uniquement)**: Désactive le pontage Wi-Fi.
 - **WDS Only (WDS uniquement)**: Active le pontage Wi-Fi mais bloque la connexion d'autres périphériques Wi-Fi/clients au routeur.
 - **HYBRID (Hybride)**: Active le pontage Wi-Fi et autorise la connexion d'autres périphériques Wi-Fi/clients au routeur.

REMARQUE : En mode hybride, les périphériques Wi-Fi connectés au routeur Wi-Fi ASUS ne bénéficieront que de la moitié du débit Wi-Fi du point d'accès.

4. Dans le champ **Connect to APs in list** (Se connecter aux points d'accès de la liste), cliquez sur **Yes** (Oui) si vous souhaitez établir une connexion à un point d'accès distant.
5. Par défaut, le canal d'opération / de contrôle du pont Wi-Fi est réglé sur **Auto** pour autoriser le routeur à choisir automatiquement le canal générant le moins d'interférences.
Vous pouvez modifier le **Control Channel** (Canal de contrôle) dans **Advanced Settings** (Paramètres avancés) > **Wireless** (Wi-Fi) > **General** (Général).

REMARQUE : Les canaux disponibles varient en fonction du pays ou de la région.

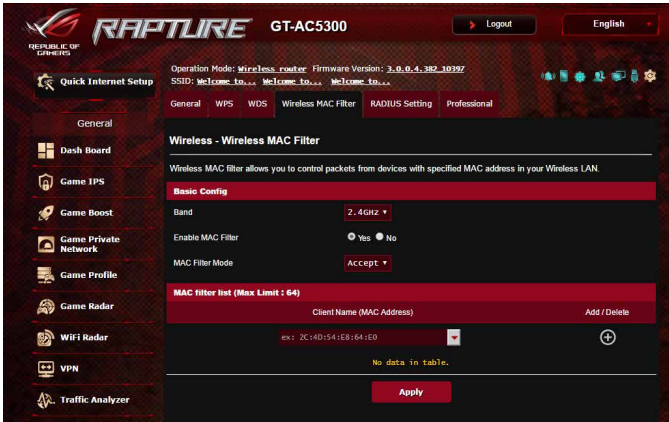
6. Dans Remote AP List (Liste des points d'accès distants), entrez une adresse MAC, puis cliquez sur le bouton **Ajouter**  pour ajouter l'adresse à la liste des points d'accès disponibles.

REMARQUE : Tous les points d'accès ajoutés à la liste doivent posséder le même canal d'opération que celui utilisé par le routeur Wi-Fi ASUS.


7. Cliquez sur **Apply** (Appliquer).

4.2.4 Filtrage d'adresses MAC

Le filtrage d'adresses MAC offre un certain contrôle sur les paquets transmis vers une adresse MAC spécifique de votre réseau Wi-Fi.

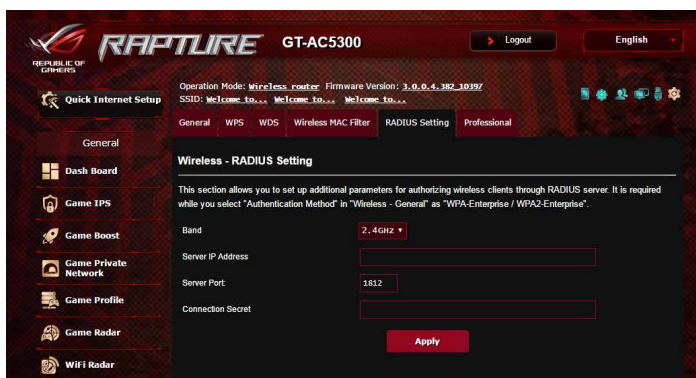


Pour configurer le filtrage d'adresses MAC :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Wireless** (Wi-Fi) > onglet **Wireless MAC Filter** (Filtrage d'adresses MAC).
2. Cochez **Yes** (Oui) dans le champ **Enable Mac Filter** (Activer le filtrage d'adresses MAC).
3. Dans le menu déroulant **MAC Filter Mode** (Mode de filtrage d'adresses MAC), sélectionnez **Accept** (Accepter) ou **Reject** (Rejeter).
 - Sélectionnez **Accept** (Accepter) pour autoriser les appareils faisant partie de la liste de filtrage d'adresses MAC à accéder au réseau Wi-Fi.
 - Sélectionnez **Reject** (Rejeter) pour ne pas autoriser les appareils faisant partie de la liste de filtrage d'adresses MAC à accéder au réseau Wi-Fi.
4. Entrez une adresse MAC, puis cliquez sur le bouton **Add** (Ajouter)  pour l'ajouter à la liste.
5. Cliquez sur **Apply** (Appliquer).

4.2.5 Service RADIUS

Le service RADIUS (Remote Authentication Dial In User Service) offre un niveau de sécurité additionnel lorsque vous sélectionnez la méthode de chiffrement WPA-Enterprise, WPA2-Enterprise ou Radius with 802.1x.



Pour configurer le service RADIUS :

1. Assurez-vous que le mode d'authentification du routeur est bien de type WPA-Enterprise ou WPA2-Enterprise.

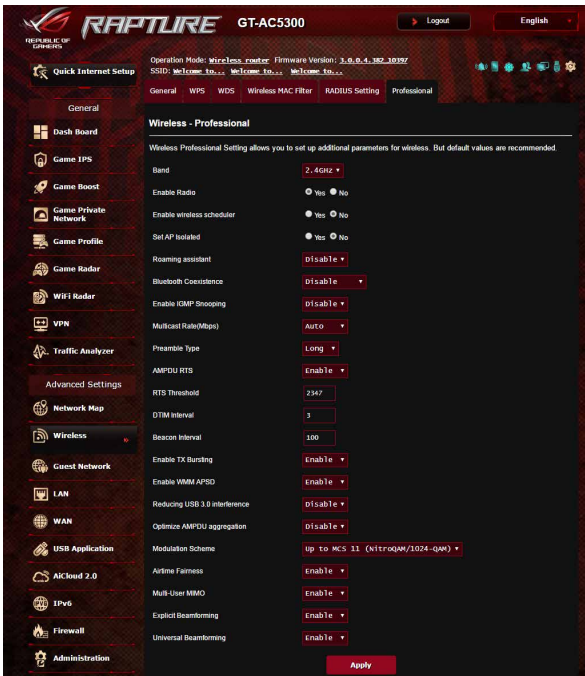
REMARQUE : Consultez la section **4.2.1 Général** pour en savoir plus sur les différents modes d'authentification de votre routeur Wi-Fi.

2. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Wireless** (Wi-Fi) > onglet **RADIUS Setting** (RADIUS).
3. Sélectionnez une bande de fréquence.
4. Dans le champ **Server IP Address** (Adresse IP du serveur), entrez l'adresse IP du serveur RADIUS.
5. Dans le champ **Server Port** (Port du serveur), entrez l'adresse du port du serveur RADIUS.
6. Dans le champ **Connection Secret** (Phrase secrète), affectez le mot de passe d'accès au serveur RADIUS.
7. Cliquez sur **Apply** (Appliquer).

4.2.6 Professional (Professionnel)

L'onglet Professionnel offre diverses options de configuration avancées.

REMARQUE : Il est recommandé de conserver les valeurs par défaut de cet onglet.



Sur l'écran **Professional Settings** (Paramètres professionnels), les options de configuration suivantes sont disponibles :

- **Frequency (Fréquence):** Sélectionnez une bande de fréquence.
- **Enable Radio (Activer la radio):** Sélectionnez **Yes** (Oui) pour activer le module radio Wi-Fi, ou **No** (Non) pour le désactiver. Cochez **No** (Non) pour désactiver le réseau sans fil.
- **Date to Enable Radio (weekdays) (Jours d'activation de la radio (semaine)):** Permet de spécifier les jours de semaine pour lesquels vous souhaitez activer le module radio Wi-Fi.
- **Time of Day to Enable Radio (Horaires d'activation de la radio):** Permet de spécifier une plage horaire (en semaine) spécifique pour laquelle vous souhaitez activer le module radio Wi-Fi.

- **Date to Enable Radio (weekend) (Jours d'activation de la radio (week-end))**: Permet de spécifier les jours pour lesquels vous souhaitez activer le module radio Wi-Fi le week-end.
- **Time of Day to Enable Radio (Horaires d'activation de la radio)**: Permet de spécifier une plage horaire (le week-end) spécifique pour laquelle vous souhaitez activer le module radio Wi-Fi.
- **Set AP isolated (Isoler le point d'accès)**: Permet de ne pas autoriser la communication entre les clients du réseau. Ceci est utile si votre réseau héberge fréquemment des utilisateurs invités. Sélectionnez **Yes** (Oui) ou **No** (Non) pour activer ou désactiver cette fonctionnalité.
- **Roaming Assistant (Assistant itinérance)** : Dans les configurations réseau impliquant plusieurs points d'accès, ou un répéteur, les clients Wi-Fi se retrouvent parfois dans l'incapacité de se connecter automatiquement aux points d'accès disponibles car ils sont toujours connectés au routeur principal. En activant ce paramètre, le client se déconnectera du routeur principal si la force du signal est inférieure à un certain seuil pour se connecter à un signal plus puissant.
- **Enable IGMP Snooping (Activer le filtrage IGMP)** : Activer cette fonction permet de surveiller et d'optimiser le trafic IGMP (Internet Group Management Protocol) entre plusieurs périphériques.
- **Multicast rate (Mb/s) (Débit multi-diffusion)**: Entrez une valeur ou cliquez sur **Disable** (Désactiver) pour désactiver cette fonctionnalité.
- **Preamble Type (Type de préambule)** : Détermine le temps alloué au routeur pour vérifier les redondances cycliques permettant de détecter les erreurs lors du transfert de paquets CRC (Cyclic Redundancy Check). Le CRC est une méthode de détection d'erreurs pendant la transmission de données. Sélectionnez **Short** (Court) pour un réseau disposant d'un trafic élevé, **Long** si votre réseau Wi-Fi est composé de périphériques Wi-Fi plus anciens ou hérités. Sélectionnez **Long** si votre réseau sans fil est composé de périphériques Wi-Fi plus anciens ou hérités.
- **AMPDU RTS** : Activer cette fonction permet de créer un

groupe de trames avant leur transmission ainsi que d'activer le RTS pour chaque AMPDU lors des communications entre les appareils 802.11g et 802.11b.

- **RTS Threshold (Palier RTS):** Spécifiez une valeur de palier RTS basse pour améliorer les communications Wi-Fi dans un réseau au trafic chargé et disposant d'un grand nombre d'appareils.
- **DTIM Interval (Intervalle DTIM):** L'intervalle DTIM (Delivery Traffic Indication Message) est l'intervalle de temps avant lequel un signal est envoyé sur un périphérique Wi-Fi en veille pour indiquer qu'un paquet attend d'être transmis. La valeur par défaut est de 3 millisecondes.
- **Beacon Interval (Intervalle de balise):** L'intervalle de balise (Beacon Interval) correspond au temps en un DTIM et le suivant. La valeur par défaut est de 100 ms. Baissez la durée de l'intervalle si la connexion est instable ou pour les appareils itinérants.
- **Enable TX Bursting (État TX Burst):** Cette fonctionnalité permet d'améliorer la vitesse de transfert entre le routeur Wi-Fi et les appareils 802.11g.
- **Enable WMM APSD (WMM APSD):** Activez l'option WMM APSD (Wi-Fi Multimedia Automatic Power Save Delivery) pour améliorer la gestion de l'alimentation des périphériques Wi-Fi. Sélectionnez **Disable** (Désactiver) pour désactiver cette fonctionnalité.
- **Reducing USB 3.0 interference (Réduire les interférences USB 3.0) :** Activer cette fonction assure les meilleures performances Wi-Fi sur la bande 2,4 GHz. Désactiver cette fonction augmente la vitesse de transfert des ports USB 3.0 et peut affecter la portée de la bande Wi-Fi 2,4 GHz.
- **Optimize AMPDU aggregation (Optimiser l'agrégation AMPDU):** Optimise le nombre maximal de MPDU dans un AMPDU et évite de perdre ou de corrompre les paquets pendant la transmission dans des canaux Wi-Fi sujets à des

erreurs

- **Optimize ack suppression (Optimiser la suppression des accusés de réception):** Optimise le nombre maximal d'accusés de réception à supprimer en une fois.
- **Turbo QAM:** Activer cette fonction permet de prendre en charge 256-QAM (MCS 8/9) sur la bande 2,4 GHz pour obtenir une meilleure portée et capacité de traitement sur cette fréquence.
- **Airtime Fairness:** Avec Airtime Fairness, la vitesse du réseau n'est pas déterminée par le trafic le plus lent. En allouant le même temps à tous les clients, Airtime Fairness permet d'effectuer chaque transfert à une vitesse optimale.
- **Explicit Beamforming (Beamforming explicite) :** L'adaptateur et le routeur WLAN du client prennent en charge la technologie de Beamforming. Cette technologie permet à ces périphériques de s'échanger des informations telles que l'estimation du canal et le sens de transmission pour améliorer le débit montant et descendant.
- **Universal Beamforming (Beamforming universel):** Pour les anciens adaptateurs réseau sans fil qui ne prennent pas en charge le Beamforming, le routeur estime le canal et détermine le sens de la transmission pour améliorer le débit descendant.
- **TX Power adjustment (Puissance TX):** La puissance TX correspond à la puissance en milliWatts (mW) requise pour alimenter le signal radio du routeur Wi-Fi. Entrez une valeur comprise entre 0 et 100.

REMARQUE : Utiliser une puissance TX trop élevée peut affecter la stabilité du réseau Wi-Fi.

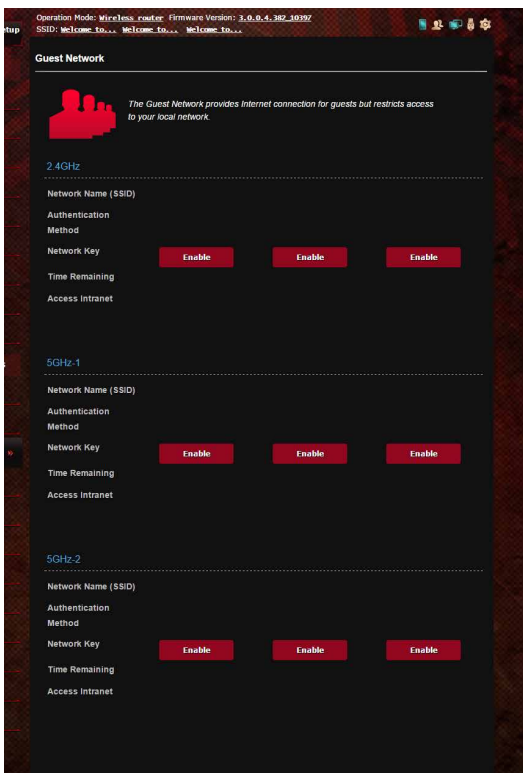
4.3 Créer un réseau invité

Un réseau invité permet d'offrir une connexion internet aux utilisateurs temporaires via l'accès à un SSID ou réseau séparé, et restreint l'accès au réseau local privé.

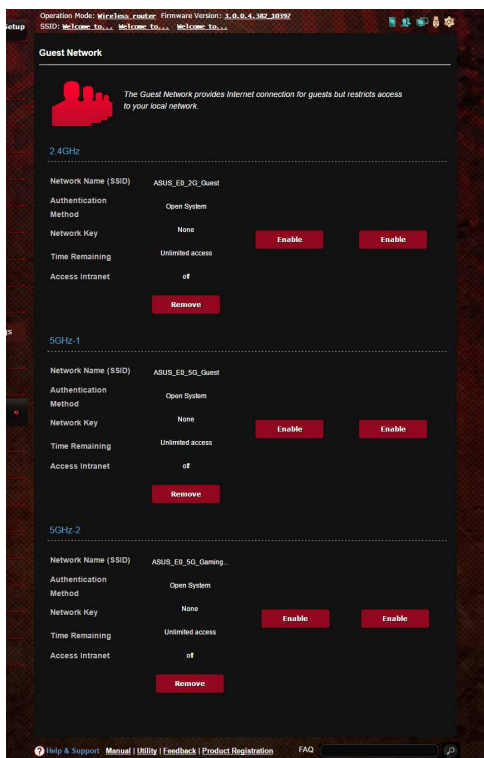
REMARQUE : Le GT-AC5300 prend en charge jusqu'à neuf SSID (trois pour chaque bande de fréquence, 2,4 GHz, 5 GHz-1 et 5 GHz-2).

Pour créer un réseau invité :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Guest Network** (Réseau invité).
2. Sélectionnez la bande de fréquence à utiliser (2,4 GHz ou 5 GHz) pour le réseau invité.
3. Cliquez sur **Enable** (Activer).



4. Pour modifier les paramètres invités, cliquez sur les paramètres invités que vous souhaitez modifier. Cliquez sur **Remove** (Supprimer) pour supprimer les paramètres invités.
5. Attribuez un nom Wi-Fi à votre réseau temporaire à partir du champ **Network Name (SSID)** (Nom réseau (SSID)).



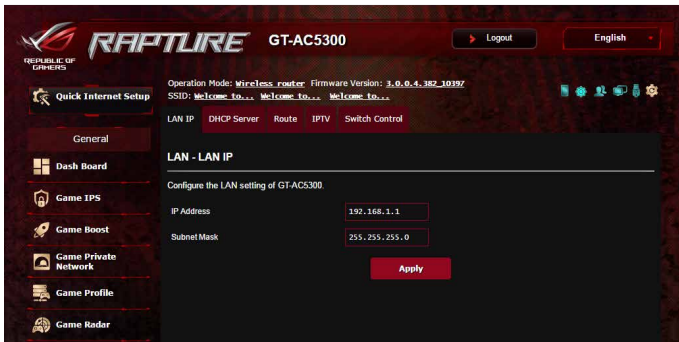
6. Sélectionnez une méthode d'authentification.
7. Si vous avez sélectionné une méthode d'authentification WPA, sélectionnez un chiffrement WPA.
8. Définissez les valeurs du champ Access time (Temps d'accès) ou cochez l'option **Limitless** (Illimité).
9. Sélectionnez l'option **Disable** (Désactiver) ou **Enable** (Activer) du champ Access Intranet (Accès au réseau local).
10. Une fois terminé, cliquez sur **Apply** (Appliquer).

4.4 Réseau local (LAN)

4.4.1 Adresse IP du routeur

L'onglet dédié à l'adresse IP du réseau local fait référence à l'adresse IP du routeur Wi-Fi.

REMARQUE : Toute modification de l'adresse IP locale influence certains réglages du serveur DHCP.

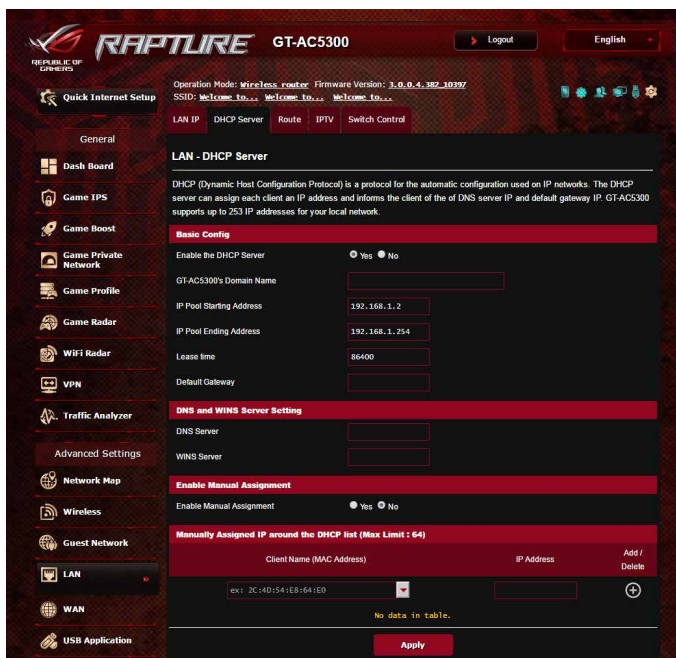


Pour modifier l'adresse IP du réseau local :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **LAN** (Réseau local) > onglet **LAN IP** (Adresse IP locale).
2. Remplissez les champs **IP address** (Adresse IP) et **Subnet Mask** (Masque de sous-réseau).
3. Une fois terminé, cliquez sur **Apply** (Appliquer).

4.4.2 Serveur DHCP

Votre routeur Wi-Fi utilise le protocole DHCP pour affecter automatiquement des adresses IP aux clients du réseau. Vous pouvez néanmoins spécifier une plage d'adresses IP et le délai du bail.



Pour configurer le serveur DHCP :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **LAN** (Réseau local) > onglet **DHCP Server** (Serveur DHCP).
2. Dans le champ **Enable the DHCP Server** (Activer le serveur DHCP), cochez **Yes** (Oui).
3. Dans la zone de texte **Domain Name** (Nom de domaine), attribuez un nom de domaine au routeur Wi-Fi.
4. Dans le champ **IP Pool Starting Address** (Adresse de départ de plage IP), entrez l'adresse IP de départ.

5. Dans le champ **IP Pool Ending Address** (Adresse de fin de plage IP), entrez l'adresse IP de fin.
6. Dans le champ **Lease Time** (Délai du bail), spécifiez le délai d'expiration (en secondes) du bail des adresses IP. Lorsque ce délai est atteint, le serveur DHCP renouvellera les adresses IP affectées.

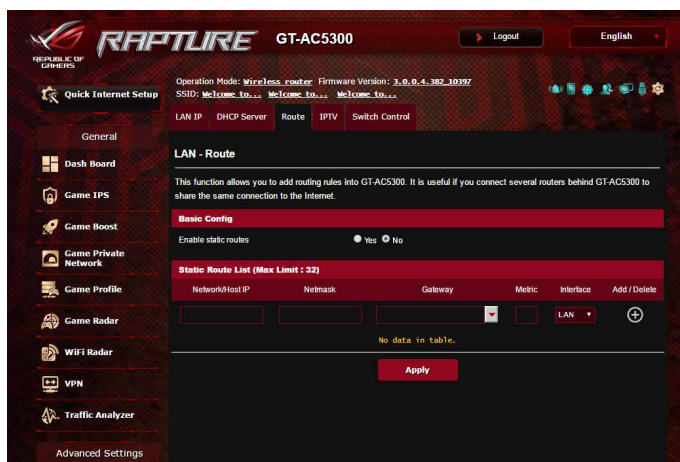
REMARQUES:

- Il est recommandé d'utiliser un format d'adresse IP de type 192.168.1.xxx (où xxx correspond à une valeur numérique comprise entre 2 et 254) lors de la saisie d'une plage d'adresses IP.
 - L'adresse de départ d'une plage IP ne peut pas être supérieure à l'adresse de fin.
-
7. Dans la zone **DNS and Server Settings** (Configuration des serveurs DNS et WINS), entrez, si nécessaire, les adresses dédiées au serveur DNS et WINS.
 8. Vous pouvez également affecter manuellement des adresses IP aux clients de votre réseau Wi-Fi. Dans le champ **Enable Manual Assignment** (Activer l'affectation manuelle), cochez **Yes** (Oui) pour affecter manuellement une IP à une adresse MAC spécifique du réseau. Jusqu'à 32 adresses MAC peuvent être ajoutées à la liste DHCP.

4.4.3 Routage

Si votre réseau est composé de plus d'un routeur Wi-Fi, vous pouvez configurer un tableau de routage permettant de partager le même service internet.

REMARQUE : Il est recommandé de ne pas modifier les paramètres de routage par défaut, sauf si vous possédez les connaissances suffisantes pour le faire.

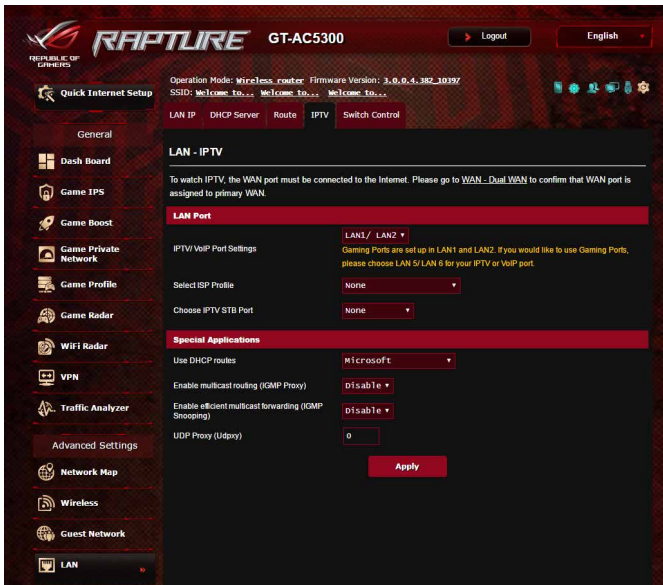


Pour configurer le tableau de routage :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **LAN** (Réseau local) > onglet **Route** (Routage).
2. Dans le champ **Enable static routes** (Activer le routage statique), cochez **Yes** (Oui).
3. Dans la zone **Static Route List** (Liste de routage statique), entrez les informations réseau des autres points d'accès. Cliquez sur le bouton **+** ou sur **-** pour ajouter ou supprimer un dispositif de la liste.
4. Cliquez sur **Apply** (Appliquer).

4.4.4 Télévision sur IP

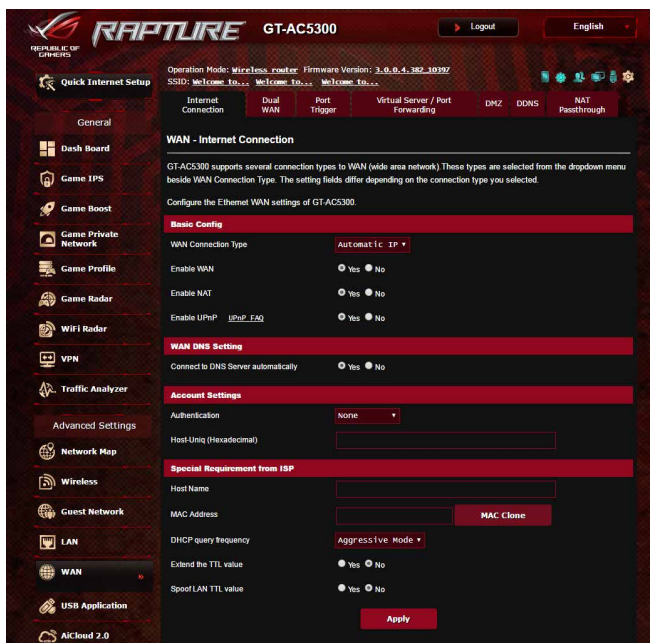
Le routeur Wi-Fi prend en charge la connexion à un service de télévision sur IP. L'onglet IPTV (Télévision sur IP) offre divers paramètres nécessaires à la configuration des protocoles IPTV, VoIP, multi-diffusion et UDP. Contactez votre fournisseur d'accès internet pour plus de détails sur ce service.



4.5 Réseau étendu (WAN)

4.5.1 Connexion internet

L'écran Internet Connection (Connexion internet) vous permet de configurer les paramètres de divers types de connexions au réseau étendu.



Pour configurer les paramètres de connexion au réseau étendu :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **WAN** (Réseau étendu) > onglet **Internet Connection** (Connexion internet).
2. Configurez les paramètres listés ci-dessous. Une fois terminé, cliquez sur **Apply** (Appliquer).
 - **WAN Connection Type (Type de connexion au réseau étendu)** : Sélectionnez votre type de connexion internet. Les choix suivants sont disponibles : **Automatic IP** (Adresse IP automatique), **PPPoE**, **PPTP**, **L2TP** et **static IP** (Adresse IP statique). Consultez votre FAI si le routeur n'est pas en mesure d'établir une connexion à Internet ou si vous n'êtes pas sûr du type de connexion à utiliser.

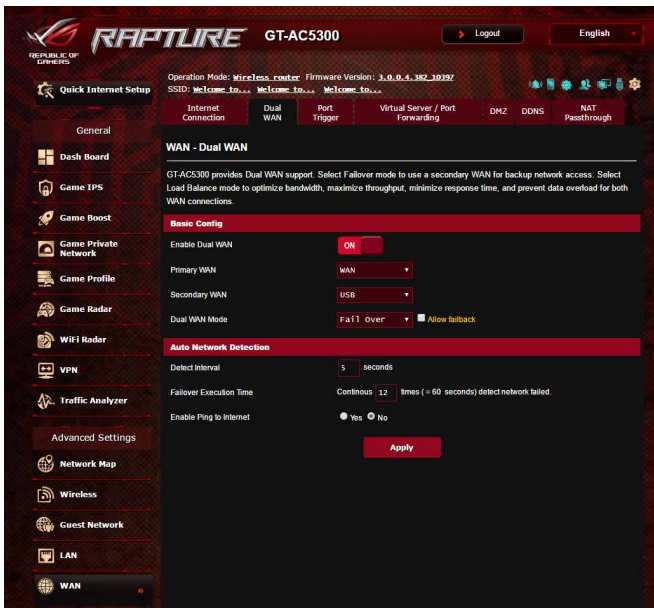
- **Enable WAN (Activer le réseau étendu):** Cochez **Yes** (Oui) pour autoriser un accès internet au routeur. Cochez **No** (Non) pour désactiver l'accès internet.
- **Enable NAT (Activer le NAT):** La fonction NAT (Network Address Translation) permet à une adresse IP publique (IP du réseau étendu) d'être utilisée pour fournir un accès internet aux clients disposant d'une adresse IP locale. L'adresse IP privée de chaque client est enregistrée dans le tableau NAT et est utilisée pour le routage des paquets entrants.
- **Enable UPnP (Activer le protocole UPnP) :** Le protocole UPnP (Universal Plug and Play) permet à de nombreux appareils (routeurs, téléviseurs, systèmes stéréo, consoles de jeu, téléphones portables, etc.) d'être contrôlés par le biais d'un réseau à IP (avec ou sans hub de contrôle central) via une passerelle. Le protocole UPnP connecte des ordinateurs de toute forme, afin d'offrir un réseau fluide pour la configuration distante et le transfert de fichiers. Grâce à l'UPnP, un périphérique réseau peut être automatiquement découvert. Une fois connectés au réseau, les périphériques peuvent être contrôlés à distance pour la prise en charge d'applications P2P, les jeux vidéo, les visioconférences et les serveurs Web ou proxy. Contrairement à la redirection de port, qui implique la configuration manuelle des ports, le protocole UPnP configure automatiquement le routeur de sorte que ce dernier accepte les connexions entrantes avant de rediriger les requêtes vers un client spécifique du réseau local.
- **Connect to DNS Server automatically (Obtenir automatiquement l'adresse de serveur DNS) :** Permet au routeur d'obtenir automatiquement les adresses des serveurs DNS auprès du FAI. Un DNS est un service permettant de traduire les noms de domaine internet en adresses IP numériques.
- **Authentication:** Authentication (Authentification). Cette option peut être requise par certains FAI. Si nécessaire, consultez votre FAI pour plus de détails.
- **Host Name (Nom d'hôte):** Permet d'attribuer un nom d'hôte au routeur. Ceci peut être requis par votre FAI. Si nécessaire, consultez votre FAI pour plus de détails.

- **MAC Address (Adresse MAC):** Une adresse MAC (Media Access Control) est un identifiant unique attribué aux appareils dotés d'une connectivité Wi-Fi. Certains FAI surveillent l'adresse MAC des appareils se connectant à leur service et peuvent rejeter toute tentative d'un appareil non enregistré d'établir une connexion. Pour surmonter le problème lié à une adresse MAC non enregistrée, vous pouvez :
 - Contacter votre FAI et mettre à jour l'adresse MAC associée à votre abonnement internet.
 - Cloner ou modifier l'adresse MAC de votre routeur Wi-Fi ASUS de sorte que celle-ci corresponde à celle enregistrée auprès de votre FAI.
- **DHCP query frequency (Fréquence d'interrogation DHCP):** Modifie l'intervalle de découverte DHCP pour éviter de surcharger le serveur DHCP.

4.5.2 Dual WAN (Double WAN)

Votre routeur ASUS prend en charge la fonctionnalité double WAN. Vous pouvez configurer cette fonctionnalité dans l'un des modes suivants :

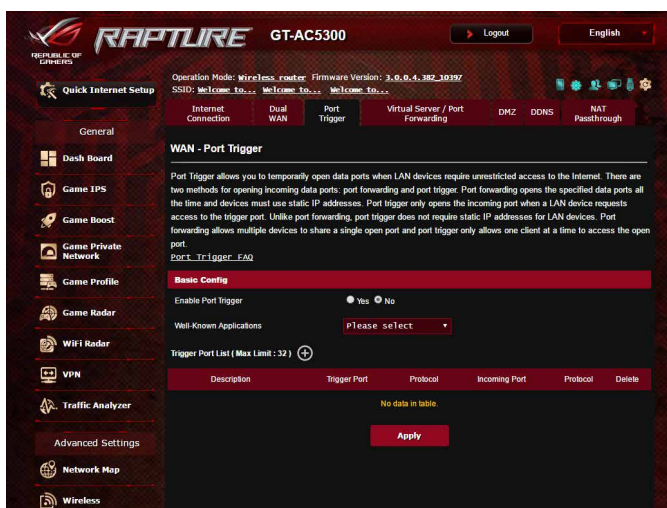
- **Failover Mode (Mode basculement) :** Sélectionnez ce mode pour utiliser le réseau étendu (WAN) secondaire comme connexion réseau de secours.
- **Load Balance Mode (Mode équilibrage de charge) :** Sélectionnez ce mode pour optimiser la bande passante, les délais de réponse et éviter les surcharges de données des deux WAN.



4.5.3 Déclenchement de port

Le déclenchement de port permet d'ouvrir un port entrant pré-déterminé pendant une période limitée lorsqu'un client du réseau local établit une connexion sortante vers un port spécifique. Le déclenchement de port est utilisé dans les cas suivants :

- Plus d'un client local requiert la redirection d'un port d'une même application à un moment différent.
- Une application nécessite des ports entrants spécifiques dissemblables des ports sortants.



Pour configurer le déclenchement de port :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **WAN** (Réseau étendu) > onglet **Port Trigger** (Déclenchement de port).
2. Dans le champ **Enable Port Trigger** (Activer le déclenchement de port), cochez **Yes** (Oui) pour activer le déclenchement de port.
3. Dans le champ **Well-Known Applications** (Applications connues), sélectionnez un jeu ou un service internet à ajouter à la liste de déclenchement de port.

4. Dans le tableau **Trigger Port List** (Liste des ports de déclenchement), spécifiez les informations suivantes :
 - **Description** : Entrez une description du service/jeu.
 - **Trigger Port (Port de déclenchement)** : Entrez le port à déclencher.
 - **Protocol (Protocole)** : Sélectionnez le protocole TCP ou UDP.
 - **Incoming Port (Port entrant)** : Spécifiez le port entrant recevant les données en provenance d'Internet.
 - **Protocol (Protocole)** : Sélectionnez le protocole TCP ou UDP.
5. Cliquez sur  pour ajouter les informations à la liste. Cliquez sur  pour supprimer une entrée de la liste.
6. Une fois terminé, cliquez sur **Apply** (Appliquer).

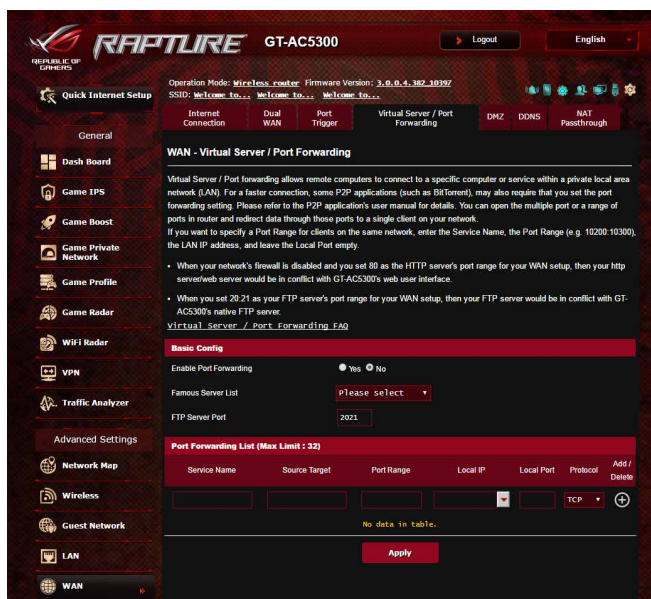
REMARQUES :

- Lors de la connexion à un serveur IRC, un PC client établit une connexion sortante par le biais de la plage de déclenchement 66660-7000. Le serveur IRC répond en vérifiant le nom d'utilisateur et en créant une nouvelle connexion au PC client via un port entrant.
 - Si le déclenchement de port est désactivé, le routeur met fin à la connexion car celui-ci n'est pas en mesure de déterminer quel ordinateur souhaite se connecter à un serveur IRC. Lorsque le déclenchement de port est activé, le routeur affecte un port entrant dédié à la réception des paquets. Ce port entrant est fermé après un certain temps car le routeur ne peut pas déterminer le moment auquel l'application a été arrêtée.
 - Le déclenchement de port ne permet qu'à un seul client à la fois d'utiliser un service et un port entrant spécifiques.
 - Il n'est pas possible d'utiliser la même application pour déclencher un port sur plus d'un ordinateur à la fois. Le routeur ne redirigera le port que vers le dernier ordinateur à avoir envoyé une requête.
-

4.5.4 Serveur virtuel et redirection de port

La redirection de port est une méthode permettant de diriger le trafic internet vers un port ou une plage de ports spécifique(s), et ensuite vers un ou plusieurs clients du réseau local. L'utilisation de la redirection de port sur le routeur autorise des ordinateurs extérieurs à un réseau d'accéder à des services répartis sur plusieurs ordinateurs de ce réseau.

REMARQUE : Lorsque la redirection de port est activée, le routeur ASUS bloque le trafic internet entrant non sollicité et n'autorise que les réponses à partir des requêtes sortantes en provenance du réseau local. Le client réseau ne dispose pas d'un accès direct à Internet, et vice versa.



Pour utiliser la redirection de port :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **WAN** (Réseau étendu) > onglet **Virtual Server / Port Forwarding** (Redirection de port).
2. Dans le champ **Enable Port Forwarding** (Activer la redirection de port), cochez **Yes** (Oui).

3. Dans le champ **Famous Server List** (Liste de serveurs), spécifiez le type de service auquel vous souhaitez accéder.
4. Dans le champ **Famous Game List** (Liste de jeux), sélectionnez l'une des options disponibles. Ce menu déroulant liste une liste de jeux et de services de jeu en ligne.
5. Dans le tableau **Port Forwarding List** (Liste des ports à rediriger), spécifiez les informations suivantes :
 - **Service Name (Nom du service)**: Spécifiez le nom du service.
 - **Port Range (Plage de ports)**: Si vous souhaitez spécifier une plage de ports pour des clients du même réseau, entrez le nom du service, la plage de ports (ex : 10200:10300), l'adresse IP locale et laissez le champ dédié au port local vide. Le champ spécifique à la plage de ports prend en charge plusieurs formats : 300:350, 566,789 ou 1015:1024,3021.

REMARQUES :

- Lorsque le pare-feu du réseau est désactivé et que vous utilisez le port 80 pour le protocole HTTP du réseau étendu, votre serveur http/Web entrera en conflit avec l'interface de gestion du routeur.
- Un réseau utilise les ports pour l'échange de données, chaque port étant doté d'une valeur numérique et d'une tâche spécifique. Par exemple, le port 80 est utilisé pour le protocole HTTP. Un port spécifique ne peut être utilisé que pour une seule application ou service à la fois. Ainsi, deux ordinateurs ne peuvent pas accéder simultanément aux données via un même port. Il n'est, par exemple, pas possible pour deux ordinateurs d'utiliser la redirection de port sur le port 100 au même moment.

-
- **Local IP (Adresse IP locale)**: Adresse IP locale du client.

REMARQUE : Utilisez une adresse IP statique pour le client local afin que la redirection de port puisse fonctionner correctement. Consultez la section **4.4 Réseau local** pour plus de détails.

- **Local Port (Port local):** Entrez un numéro de port spécifique dédié à la redirection des paquets. Laissez ce champ vide si vous souhaitez que les paquets entrants soient redirigés vers une plage de ports spécifique.
 - **Protocol (Protocole):** Sélectionnez un protocole. En cas d'incertitude, sélectionnez **BOTH** (Les deux).
5. Cliquez sur  pour ajouter les informations à la liste. Cliquez sur  pour supprimer une entrée de la liste.
 6. Une fois terminé, cliquez sur Apply (Appliquer).

Pour vérifier que la redirection de port a bien été configurée :

- Vérifiez que votre serveur ou que l'application est configuré(e) et prêt(e) à être utilisé(e).
- Un client en dehors du réseau local mais ayant accès à Internet (ou "Client internet") est nécessaire. Ce client ne doit pas être connecté au routeur ASUS.
- Sur le client internet, utilisez l'adresse IP du réseau étendu (WAN) du routeur pour accéder au serveur. Si la redirection de port fonctionne correctement, vous serez en mesure d'accéder aux fichiers ou aux applications souhaités.

Différences entre le déclenchement et la redirection de port :

- Le déclenchement de port peut être utilisé sans spécifier d'adresse IP locale. Contrairement à la redirection de port, nécessitant une adresse IP statique, le déclenchement de port autorise la redirection dynamique de port par le biais du routeur. Des plages de ports pré-déterminées sont configurées pour accepter les connexions entrantes pendant une période de temps spécifique. La redirection de port permet à plusieurs ordinateurs d'exécuter des applications nécessitant normalement la redirection manuelle des mêmes ports sur chaque ordinateur du réseau.
- Le déclenchement de port est plus sûr que la redirection de port dans la mesure où les ports entrants ne sont pas constamment ouverts. En effet, ceux-ci ne sont ouverts que lorsqu'une application effectue une connexion sortante par le biais du port déclencheur.

4.5.5 Zone démilitarisée

La zone démilitarisée (ou DMZ en anglais) est un sous-réseau exposant un client à Internet pour lui permettre de recevoir tous les paquets entrants acheminés sur le réseau local.

Le trafic en provenance d'Internet est normalement rejeté et acheminé vers un client spécifique si la redirection ou le déclenchement de port a été configuré sur le réseau. En configuration à zone démilitarisée, un client réseau reçoit tous les paquets entrants.

Le déploiement de cette fonctionnalité sur un réseau est particulièrement utile lorsque vous souhaitez ouvrir des ports entrants ou héberger un nom de domaine ou un serveur de messagerie électronique.

AVERTISSEMENT : L'ouverture de tous les ports d'un client au trafic internet rend le réseau vulnérable aux attaques extérieures. Veuillez prendre en compte les risques encourus lors de la configuration d'une zone démilitarisée.

Pour configurer la zone démilitarisée :

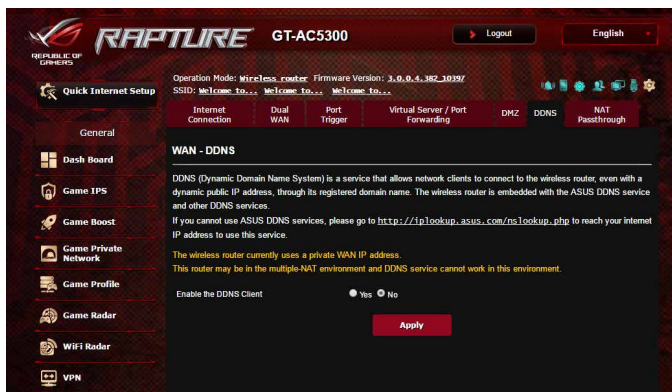
1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **WAN** (Réseau étendu) > onglet **DMZ** (Zone démilitarisée).
2. Configurez les paramètres listés ci-dessous. Une fois terminé, cliquez sur **Apply** (Appliquer).
 - **IP address of Exposed Station (Adresse IP du client) :** Entrez dans ce champ l'adresse IP du client hébergeant le service DMZ et exposé à Internet. Vérifiez que le client serveur possède une adresse IP statique.

Pour désactiver la zone démilitarisée :

1. Effacez l'adresse IP du client du champ **IP address of Exposed Station** (Adresse IP du client).
2. Une fois terminé, cliquez sur **Apply** (Appliquer).

4.5.6 Service DDNS

La configuration d'un serveur DDNS (DNS dynamique) vous permet d'accéder au routeur en dehors de votre réseau par le biais du service DDNS d'ASUS ou d'une société tierce.



Pour configurer le service DDNS :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **WAN** (Réseau étendu) > onglet **DDNS**.
2. Configurez les paramètres listés ci-dessous. Une fois terminé, cliquez sur **Apply** (Appliquer).
 - **Enable the DDNS Client (Activer le client DDNS):** Active l'accès à distance du routeur ASUS par le biais d'un nom de serveur DNS plutôt que de l'adresse IP du réseau étendu (WAN).
 - **Server (Serveur) et Host Name (Nom d'hôte):** Sélectionnez l'une des options disponibles. Si vous souhaitez utiliser le service de DDNS d'ASUS, spécifiez le nom d'hôte au format xxx.asuscomm.com (xxx correspondant à votre nom d'hôte).
 - Si vous choisissez un service DDNS différent, cliquez sur **Essai gratuit** pour être redirigé vers la page Web du service sélectionné. Remplissez les champs Nom d'utilisateur, Adresse email, Mot de passe et Clé DDNS.
 - **Enable wildcard (Utiliser une Wildcard):** Activez la Wildcard si le service DDNS utilisé requiert une Wildcard.

REMARQUES:

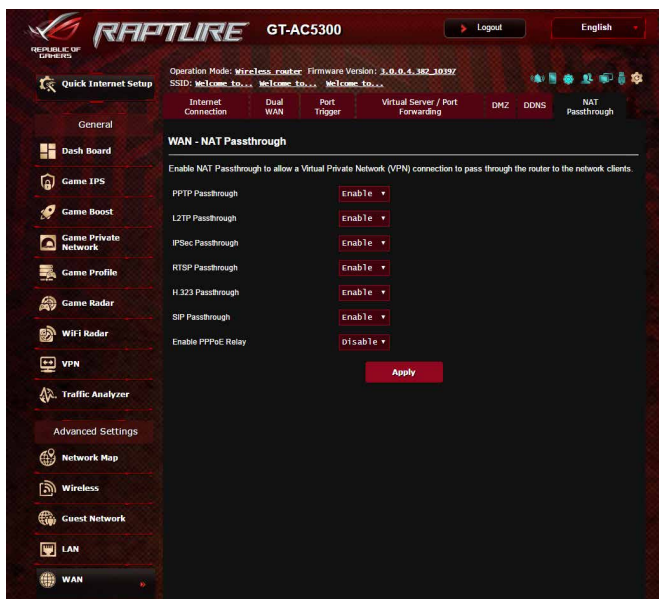
Le service DDNS ne peut pas fonctionner sous les conditions suivantes :

- Le routeur Wi-Fi utilise une adresse IP du réseau étendu (WAN) privée (de type 192.168.x.x, 10.x.x.x ou 172.16.x.x).
 - Le routeur fait partie d'un réseau utilisant plusieurs tableaux NAT.
-

4.5.7 NAT Passthrough

La fonction NAT Passthrough permet à une connexion VPN (réseau privé virtuel), d'être acheminée vers les clients du réseau par le biais du routeur. Les fonctionnalités PPTP Passthrough, L2TP Passthrough, IPsec Passthrough et RTSP Passthrough sont activées par défaut.

Pour activer ou désactiver la fonction NAT Passthrough, allez dans **Advanced Settings** (Paramètres avancés) > **WAN** (Réseau étendu) > onglet **NAT Passthrough**. Une fois terminé, cliquez sur **Apply** (Appliquer).



4.6 Utiliser les applications USB

La page des applications USB contient les sous-menus AiDisk, Servers Center (Centres de serveurs), Network Printer Server (Serveur d'impression réseau) et Download Master.

IMPORTANT ! Pour utiliser la fonction de serveur multimédia, vous devez connecter un périphérique de stockage USB (ex : disque dur ou clé USB) au port USB 2.0 situé à l'arrière du routeur Wi-Fi. Assurez-vous que le périphérique de stockage USB est formaté et correctement partitionné. Rendez-vous sur le site internet d'ASUS sur <http://event.asus.com/2009/networks/disksupport/> pour plus de détails.

The screenshot displays the ASUS Rapture GT-AC5300 web interface. At the top, the logo 'RAPTURE' and model 'GT-AC5300' are visible, along with 'Logout' and 'English' buttons. The main content area is titled 'USB Application' and includes a warning: 'To remove the hard disk from the router, click the USB icon at the upper right corner of your screen.' Below this, several application options are listed with circular icons and brief descriptions:

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

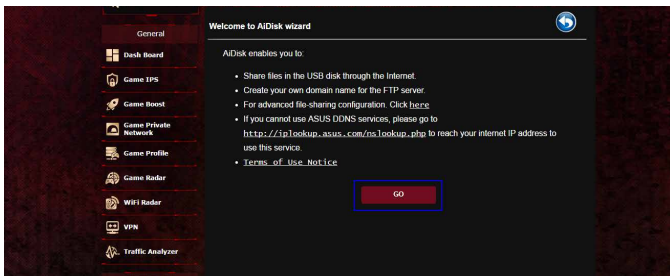
A left-hand navigation menu is visible, listing various settings categories such as 'General', 'Advanced Settings', and 'Network Tools'. The 'USB Application' menu item is currently selected and highlighted.

4.6.1 Utiliser AiDisk

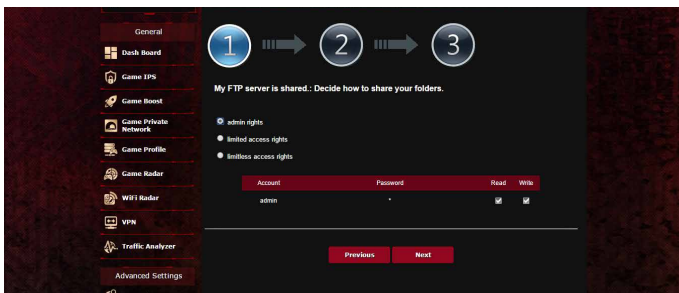
AiDisk vous permet de partager les fichiers contenus sur un périphérique de stockage USB connecté au routeur via Internet. AiDisk offre aussi la possibilité de configurer le service DDNS d'ASUS ou un serveur FTP.

Pour utiliser AiDisk :

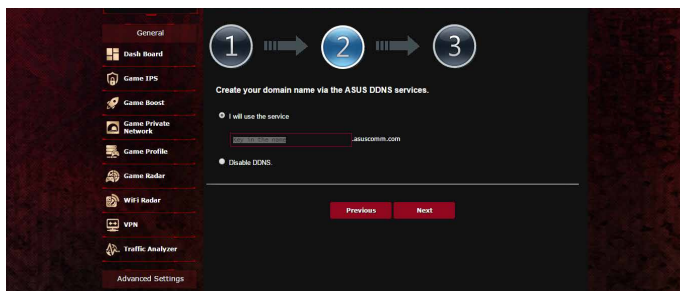
1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **USB application** (Applications USB) > icône **AiDisk**.
2. À partir de l'écran Welcome to AiDisk wizard (Bienvenue sur l'assistant AiDisk), cliquez sur **Go** (Démarrer).



3. Définissez les droits d'accès des différents clients accédant aux données partagées.



4. Si vous souhaitez créer votre propre nom de domaine dédié au serveur FTP grâce au service DDNS d'ASUS, sélectionnez **I will use the service and accept the Terms of service** (Je souhaite utiliser ce service et en accepte les conditions) et spécifiez le nom de votre domaine. Cliquez sur **Next** (Suivant).



Vous pouvez aussi sélectionner **Skip ASUS DDNS settings** (Ignorer la configuration du service DDNS ASUS), puis cliquez sur **Next** (Suivant) pour ignorer cette étape.

5. Cliquez sur **Finish** (Terminé) pour terminer la configuration.
6. Pour accéder au site FTP que vous venez de créer, ouvrez votre navigateur internet ou un client FTP tiers et saisissez l'adresse suivante : (**ftp ://<nom de domaine>.asuscomm.com**).

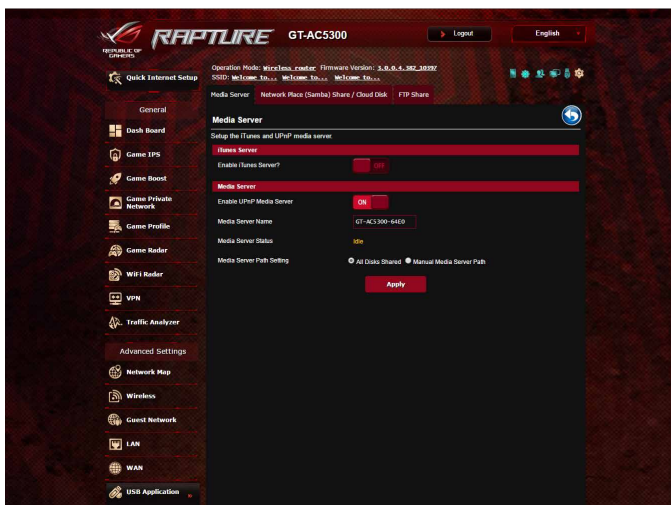
4.6.2 Utiliser les centres de serveurs

Les centres de serveurs vous permettent de partager vos fichiers à partir d'un disque USB par le biais des protocoles DLNA, Samba et FTP. Vous pouvez aussi configurer d'autres paramètres pour le disque USB dans les centres de serveurs.

Utiliser le service de partage DLNA

Votre routeur Wi-Fi autorise les appareils compatibles avec le protocole DLNA à accéder aux fichiers multimédia stockés sur un disque de stockage USB connecté au routeur.

REMARQUE : Avant d'utiliser le partage de fichiers via le protocole DLNA, connectez votre appareil au réseau du routeur Wi-Fi.

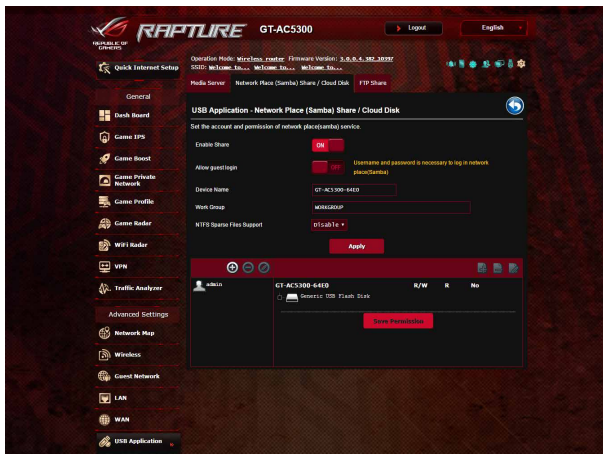


Pour utiliser le service de partage DLNA, allez dans **Advanced Settings** (Paramètres avancés) > **USB application** (Applications USB) > **Media Services and Servers** (Services et serveurs multimédia) > onglet **Media Servers** (Serveurs multimédia). Vous trouverez ci-dessous une description de chacun des champs disponibles :

- **Enable iTunes Server? (Activer le serveur iTunes ?) ?**: Déplacez l'interrupteur ON/OFF pour activer ou désactiver le serveur iTunes.
- **Enable DLNA Media Server (Activer le serveur DLNA) :** Déplacez l'interrupteur ON/OFF pour activer ou désactiver cette fonctionnalité.
- **Media Server Status (État du serveur):** Affiche l'état du serveur.
- **Media Server Path Setting (Répertoire de partage):** Sélectionnez le répertoire du serveur multimédia et cliquez sur Apply (Appliquer) pour partager le contenu d'un répertoire du disque USB avec les clients du réseau.

Utiliser le service de partage Samba

Le partage Samba vous permet de configurer des comptes de partage et leurs permissions d'accès au service Samba.




Pour utiliser le partage Samba :

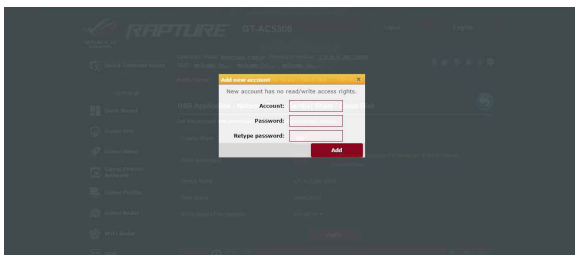
1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **USB application** (Applications USB) > **Media Services and Servers** (Services et serveurs multimédia) > onglet **Network Place (Samba) Share / Cloud Disk** (Partage de favoris réseau / Cloud Disk).

REMARQUE : Le partage Samba est activé par défaut.


2. Suivez les instructions suivantes pour ajouter, supprimer ou modifier un compte de partage.

Pour créer un nouveau compte :


- a) Cliquez sur  pour ajouter un compte.
- b) Remplissez les champs **Account** (Compte) et **Password** (Mot de passe). Ressaisissez le mot de passe pour le confirmer. Cliquez sur **Add** (Ajouter) pour ajouter le compte.

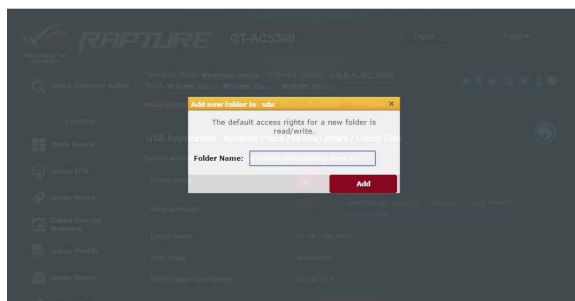


Pour supprimer un compte existant :

- a) Sélectionnez le compte à supprimer.
- b) Cliquez sur .
- c) À l'apparition de la fenêtre de confirmation, cliquez sur **Delete** (Supprimer) pour confirmer la suppression.

Pour ajouter un dossier :

- a) Cliquez sur .
- b) Spécifiez le nom du dossier, et cliquez sur **Add** (Ajouter). Le dossier créé sera ajouté à la liste des dossiers partagés.



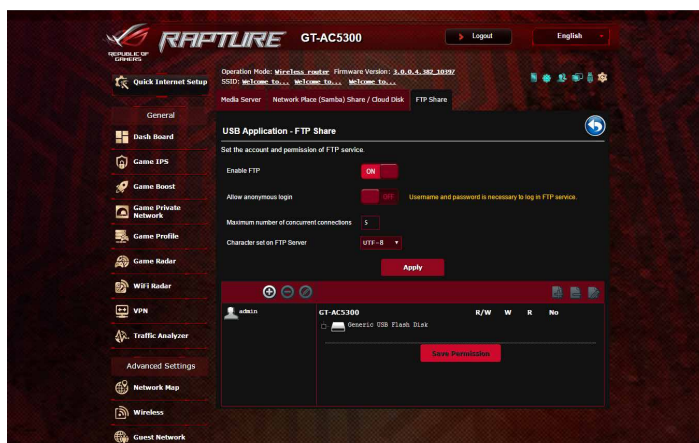
3. Dans la liste des fichiers/dossiers, sélectionnez le type de droits d'accès à affecter aux différents types de fichiers/dossiers :
 - **R/W** : Sélectionnez cette option pour affecter un droit de lecture/écriture à un type spécifique de fichier/dossier.
 - **R** : Sélectionnez cette option pour affecter un accès en lecture seule à un type spécifique de fichier/dossier.
 - **No (Non)**: Sélectionnez cette option si vous ne souhaitez pas partager un type spécifique de fichier/dossier.
4. Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications.

Utiliser le service de partage FTP

Le routeur Wi-Fi ASUS vous permet de partager les fichiers contenus sur un périphérique de stockage USB, via un serveur FTP, avec d'autres ordinateurs du réseau local, via Internet.

IMPORTANT :

- Assurez-vous de retirer le périphérique USB en toute sécurité. Une mauvaise éjection du périphérique de stockage USB peut endommager les données contenues sur le disque.
- Pour plus de détails sur l'éjection en toute sécurité d'un lecteur USB, consultez la sous-section **Éjecter un disque USB** de la section **4.1.3 Surveiller un périphérique USB**.



Pour utiliser le service de partage FTP :

REMARQUE : Assurez-vous d'avoir configuré votre serveur FTP avec AiDisk. Pour plus de détails, consultez la section **4.6.1 Utiliser AiDisk**.

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **USB application** (Applications USB) > **Media Services and Servers** (Services et serveurs multimédia) > **Servers Center** (Centres de serveurs) > onglet **FTP Share** (Partage FTP).
2. Dans la liste des fichiers/dossiers, sélectionnez le type de droits d'accès à affecter aux différents types de fichiers/dossiers :
 - **R/W**: Sélectionnez cette option pour affecter un droit de lecture/écriture à un type spécifique de fichier/dossier.
 - **W**: Sélectionnez cette option pour affecter un accès en écriture seule à un type spécifique de fichier/dossier.
 - **R**: Sélectionnez cette option pour affecter un accès en lecture seule à un type spécifique de fichier/dossier.
 - **No (Non)**: Sélectionnez cette option si vous ne souhaitez pas partager un type spécifique de fichier/dossier.
3. Vous pouvez également autoriser les connexions anonymes en déplaçant l'interrupteur du champ **Allow anonymous login** (Autoriser les connexions anonymes) sur **ON** (OUI).
4. Dans le champ **Maximum number of concurrent connections** (Nombre maximum de connexions simultanées), entrez le nombre maximum d'appareils pouvant se connecter simultanément au serveur FTP.
5. Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications.
6. Pour accéder au serveur FTP, entrez le lien ftp **ftp://<nomd'hôte>.asuscomm.com** ainsi que votre nom d'utilisateur et mot de passe dans la barre d'adresse de votre navigateur internet ou d'un client FTP tiers.

4.6.3 3G/4G

Des modems 3G/4G USB peuvent être connectés au routeur Wi-Fi pour permettre un accès à Internet.

REMARQUE : Rendez-vous sur le site <http://event.asus.com/2009/networks/3gsupport/> pour consulter la liste des modems compatibles.

Pour configurer une connexion internet 3G/4G :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **USB application** (Applications USB) > **3G/4G**.
2. Dans le champ **Enable USB Modem** (Activer le modem USB), cochez **Yes** (Oui).
3. Réglez les options suivantes :
 - **Location (Emplacement) :** Sélectionnez l'emplacement de votre fournisseur de service 3G/4G.
 - **ISP (FAI) :** Sélectionnez votre FAI (Fournisseur d'accès internet).
 - **APN (Access Point Name) service (optional) (Service d'accès internet Wi-Fi (optionnel)) :** Contactez votre fournisseur d'accès 3G/4G pour plus de détails.
 - **Dial Number (Numéro à composer) et PIN code (Code PIN) :** Entrez le numéro d'accès et le code PIN de votre fournisseur d'accès 3G/4G.

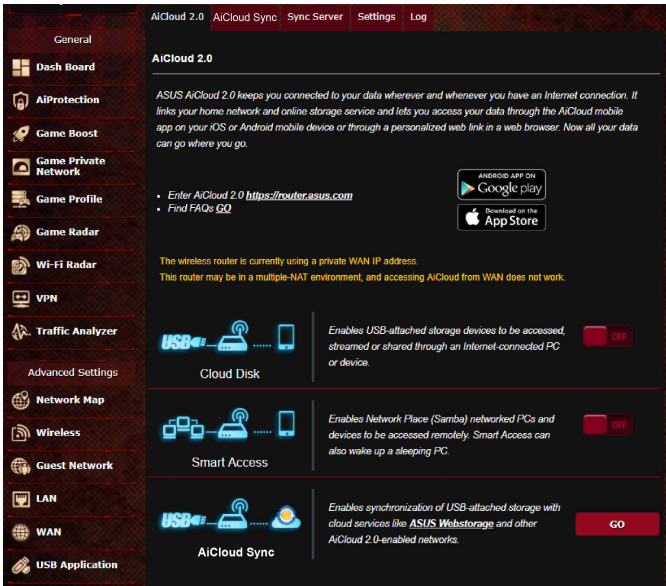
REMARQUE : Le code PIN peut varier en fonction du fournisseur d'accès.

- **Username / Password (Nom d'utilisateur / Mot de passe) :** Entrez le nom d'utilisateur et le mot de passe fournis par votre fournisseur d'accès 3G/4G.
 - **USB Adapter (Adaptateur USB) :** Choisissez votre adaptateur 3G / 4G USB à partir du menu déroulant. Si vous n'êtes pas certain du modèle ou si celui-ci n'apparaît pas dans la liste, sélectionnez **Auto**.
4. Cliquez sur **Apply** (Appliquer).

REMARQUE : Le routeur doit redémarrer pour que les modifications puissent prendre effet.

4.7 Utiliser AiCloud 2.0

AiCloud 2.0 est une application dans le Cloud vous permettant de sauvegarder, de synchroniser, de partager et d'accéder à distance à vos fichiers.



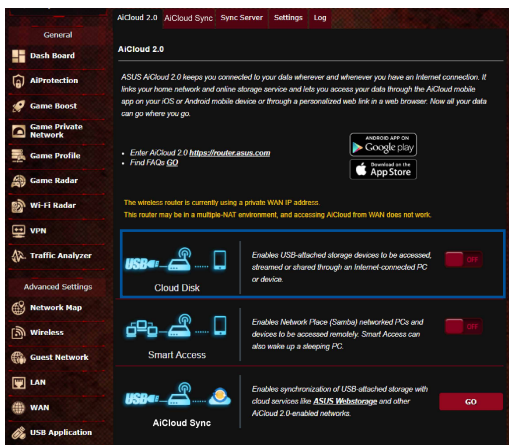
Pour utiliser AiCloud :

1. Téléchargez et installez l'application ASUS AiCloud sur votre appareil mobile à partir de la boutique en ligne Google Play ou Apple Store.
2. Connectez l'appareil mobile à votre réseau. Suivez les instructions pour effectuer la configuration d'AiCloud.

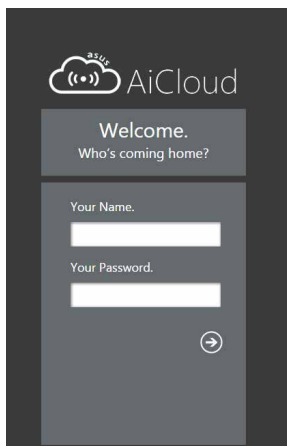
4.7.1 Cloud Disk

Pour créer un disque de stockage dans le Cloud :

1. Insérez un périphérique de stockage USB sur l'un des ports USB de votre routeur Wi-Fi.
2. Activez **Cloud Disk**.

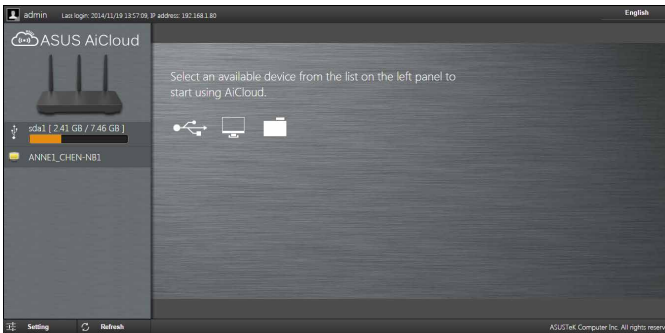


3. Rendez-vous sur <https://router.asus.com> et entrez les identifiants de connexion de votre routeur. Pour améliorer votre expérience d'utilisation, il est recommandé d'utiliser **Google Chrome** ou **Firefox**.



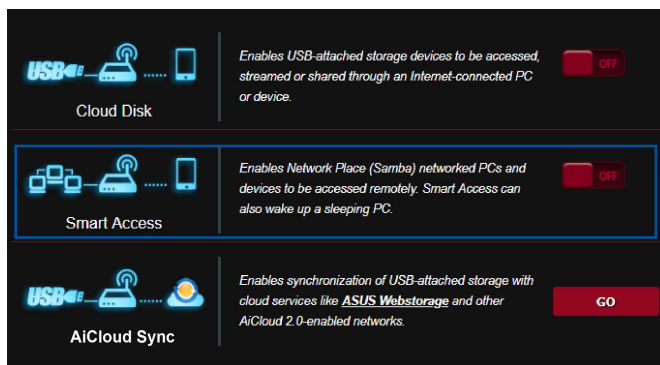
4. Vous pouvez dès lors accéder aux fichiers Cloud Disk des appareils connectés au réseau.

REMARQUE : Lorsque vous accédez aux appareils connectés au réseau, vous devez saisir manuellement le nom d'utilisateur et le mot de passe de l'appareil. Pour des raisons de sécurité, AiCloud ne mémorise pas vos identifiants de connexion.



4.7.2 Smart Access

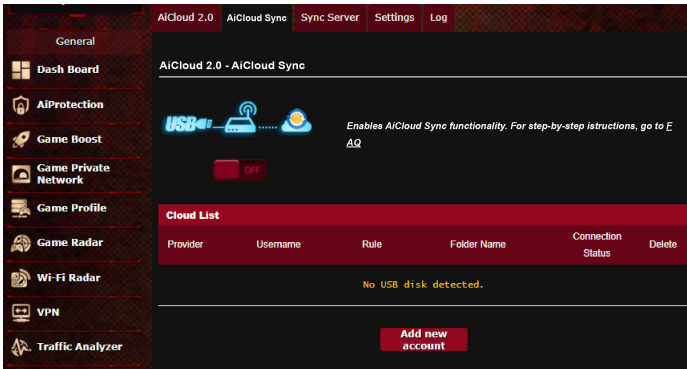
La fonctionnalité Smart Access vous permet d'accéder aisément à votre réseau domestique par le biais du nom de domaine de votre routeur.



REMARQUES :

- Vous pouvez créer un nom de domaine pour votre routeur grâce au service DDNS d'ASUS. Pour plus de détails, consultez la section **4.5.6 DDNS**.
 - Par défaut, AiCloud offre une connexion HTTPS sécurisée. Entrez **[https://\[nomduDDNSASUS\].asuscomm.com](https://[nomduDDNSASUS].asuscomm.com)** pour une utilisation extrêmement sûre des fonctionnalités Cloud Disk et Smart Access.
-

4.7.3 AiCloud Sync

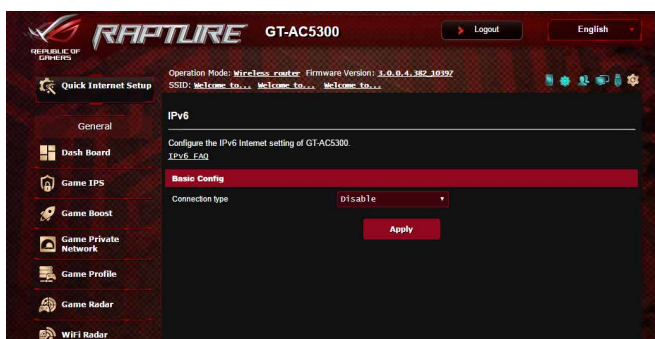


Pour utiliser AiCloud Sync :

1. Lancez AiCloud, cliquez sur **AiCloud Sync** > **Go**.
2. Sélectionnez **ON** (Activé) pour activer AiCloud Sync.
3. Cliquez sur **Add new account** (Ajouter un compte).
4. Entrez votre nom d'utilisateur et mot de passe ASUS WebStorage et sélectionnez le répertoire à synchroniser avec WebStorage.
5. Cliquez sur **Apply** (Appliquer).

4.8 IPv6 (Protocole IPv6)

Ce routeur Wi-Fi est compatible avec le protocole d'adressage IPv6, un protocole disposant d'un espace d'adressage bien plus important que l'IPv4. Cette norme n'étant pas encore largement utilisée, contactez votre FAI pour en confirmer sa prise en charge. Contactez votre FAI si votre connexion Internet est compatible IPv6.



Pour configurer le protocole IPv6 :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **IPv6**.
2. Dans le menu déroulant **Connection Type** (Type de connexion), sélectionnez le type de connexion. Les options de configuration apparaissant ensuite peuvent varier selon le type de connexion choisi.
3. Entrez les informations IPv6 et de serveur DNS.
4. Cliquez sur **Apply** (Appliquer).

REMARQUE : Consultez votre FAI en cas de doute sur les informations nécessaires à la configuration de l'adressage IPv6.

4.9 Pare-feu

Le routeur Wi-Fi peut faire office de pare-feu matériel sur votre réseau.

REMARQUE : Le pare-feu est activé par défaut sur votre routeur.

4.9.1 General (Général)

Pour configurer les paramètres de base du pare-feu :


1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Firewall** (Pare-feu) > onglet **General** (Général).
2. Dans le champ **Enable Firewall** (Activer le pare-feu), cochez **Yes** (Oui).
3. Dans le champ **Enable DoS Protection** (Activer la protection contre les attaques DoS), cochez **Yes** (Oui) pour protéger votre réseau contre les attaques de déni de service (DoS). Veuillez toutefois noter que l'activation de cette fonctionnalité peut affecter les performances du routeur.
4. Vous pouvez aussi surveiller l'échange de paquets entre le réseau local (LAN) et le réseau étendu (WAN). Dans le menu déroulant **Logged packets** (Types de paquets), sélectionnez **Dropped** (Ignorés), **Accepted** (Acceptés) ou **Both** (Les deux).
5. Cliquez sur **Apply** (Appliquer).

4.9.2 Filtrage d'URL

Le routeur Wi-Fi offre la possibilité de filtrer l'accès à certaines adresses internet (URL).

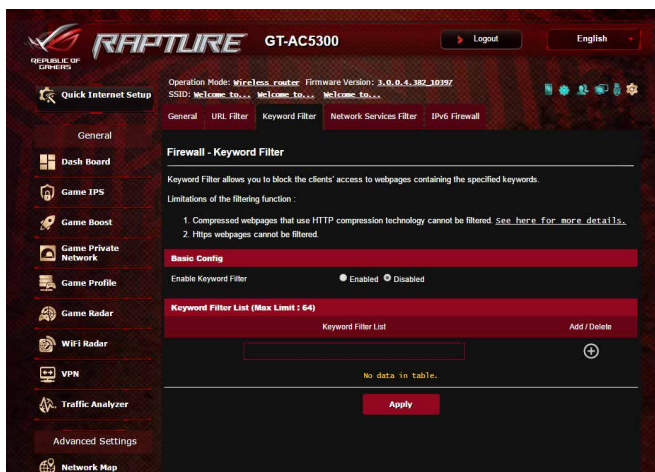
REMARQUE : Le filtrage d'URL est fondé sur les requêtes DNS. Si un client du réseau a déjà accédé à un site internet, celui-ci ne sera pas bloqué (un cache DNS stockant une liste des sites internet visités). Pour résoudre ce problème, effacez la mémoire cache dédiée au DNS avant d'utiliser le filtrage d'URL.

Pour configurer le filtrage d'URL :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Firewall** (Pare-feu) > onglet **URL Filter** (Filtrage d'URL).
2. Dans le champ **Enable URL Filter** (Activer le filtrage d'URL), cochez **Enabled** (Activer).
3. Entrez une adresse URL et cliquez sur le bouton .
4. Cliquez sur **Apply** (Appliquer).

4.9.3 Filtrage de mots-clés

Vous pouvez bloquer l'accès à des sites internet contenant certains mots clés.



Pour configurer le filtrage de mots clés :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Firewall** (Pare-feu) > onglet **Keyword Filter** (Filtrage de mots clés).
2. Dans le champ **Enable Keyword Filter** (Activer le filtrage de mots clés), cochez **Enabled** (Activer).

- Entrez un mot ou une phrase, puis cliquez sur le bouton **Add** (Ajouter).
- Cliquez sur **Apply** (Appliquer).

REMARQUES :


- Le filtrage de mots clés est fondé sur les requêtes DNS. Si un client du réseau a déjà accédé à un site internet, celui-ci ne sera pas bloqué (un cache DNS stockant une liste des sites internet visités). Pour résoudre ce problème, effacez la mémoire cache dédiée au DNS avant d'utiliser le filtrage de mots clés.
- Les pages internet compressées au format HTTP ne peuvent pas être filtrées. Les pages utilisant le standard HTTPS ne peuvent également pas être filtrées.

4.9.4 Filtrage de services réseau

Le filtrage de services réseau permet de bloquer l'échange de paquets entre le réseau local (LAN) et le réseau étendu (WAN), et de restreindre l'accès des clients à certains services internet (ex : Telnet ou FTP).

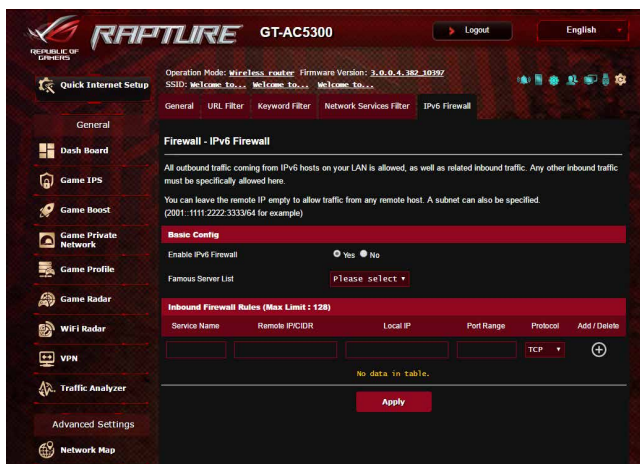
The screenshot shows the Rapture GT-AC5300 web interface. The left sidebar contains navigation options: Quick Internet Setup, General, Game Board, Game IPS, Game Boost, Game Private Network, Game Profile, Game Radar, WiFi Radar, VPN, Traffic Analyzer, Advanced Settings, Network Map, Wireless, Guest Network, LAN, WAN, USB Application, AiCloud 2.0, IPv6, and Firewall. The main content area is titled "Firewall - Network Services Filter". It includes a description of the filter, a "Network Services Filter" section with a "Filter table type" dropdown set to "Block List", and a "Network Services Filter Table" with columns for Source IP, Port Range, Destination IP, Port Range, Protocol, and Add/Delete. The table currently shows "No data in table." and an "Apply" button is at the bottom.

Pour configurer le filtrage de services réseau :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Firewall** (Pare-feu) > onglet **Network Services Filter** (Filtrage de services réseau).
2. Dans le champ **Enable Network Services Filter** (Activer le filtrage de services réseau), cochez **Yes** (Oui).
3. Sélectionnez ensuite le type de filtrage. **L'option Black List** (Liste noire) bloque les services réseau spécifiés bloque les services réseau spécifiés. **White List** (Liste blanche) limite l'accès à certains services réseau uniquement.
4. Si nécessaire, spécifiez les jours et les horaires d'activité du filtre.
5. Remplissez ensuite le tableau de filtrage. Cliquez sur le bouton .
6. Cliquez sur **Apply** (Appliquer).

4.9.5 Pare-feu IPv6

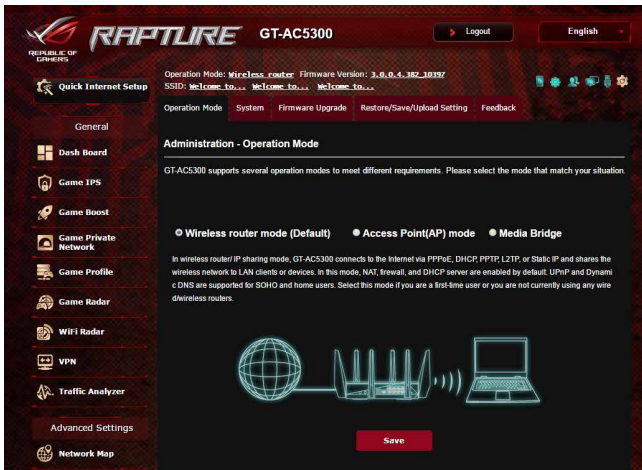
Par défaut, votre routeur ASUS bloque tout le trafic entrant non sollicité. La fonction de pare-feu IPv6 permet toutefois d'autoriser le trafic entrant en provenance de services spécifiques.



4.10 Administration

4.10.1 Mode de fonctionnement

Le routeur Wi-Fi dispose de plusieurs modes de fonctionnement offrant une plus grande flexibilité d'utilisation, selon vos besoins.



Pour définir le mode de fonctionnement du routeur :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Administration** > onglet **Operation Mode** (Mode de fonctionnement).
2. Sélectionnez l'un des modes disponibles :
 - **Wireless router mode (default) (Routeur Wi-Fi (Mode de fonctionnement par défaut))**: Ce mode permet d'établir une connexion à Internet et d'en ouvrir l'accès aux clients disponibles sur le réseau local du routeur.
 - **Access Point mode (Point d'accès)** : Ce mode permet de créer un nouveau réseau Wi-Fi à partir d'un réseau existant.
 - **Media Bridge (Pont média)** : La sélection de ce mode nécessite deux routeurs Wi-Fi. Le second routeur faisant office de pont multimédia sur lequel divers appareils (TV connectée, console de jeu, etc.) peuvent être connectés par le réseau Ethernet.
3. Cliquez sur **Apply** (Appliquer).

REMARQUE : Le changement de mode de fonctionnement requiert un redémarrage du routeur.

4.10.2 Système

L'onglet **System** (Système) permet de configurer certains paramètres système du routeur Wi-Fi.

Pour configurer les paramètres système du routeur :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Administration** > onglet **System** (Système).
2. Configurez les paramètres listés ci-dessous :
 - **Change router login password (Modification des identifiants de connexion du routeur)**: Cette zone vous permet de modifier le nom d'utilisateur et le mot de passe d'accès à l'interface de gestion du routeur Wi-Fi.
 - **Time Zone (Fuseau horaire)**: Sélectionnez votre fuseau horaire.
 - **NTP Server (Serveur NTP)**: Le routeur peut accéder à un serveur NTP (Network time Protocol) pour synchroniser l'heure.
 - **Enable Telnet (Activer le protocole Telnet)**: Cochez **Yes** (Oui) / **No** (Non) pour activer / désactiver le protocole Telnet.
 - **Authentication Method (Méthode d'authentification)**: Les protocoles d'authentification HTTP, HTTPS aident à sécuriser le routeur.
 - **Enable Web Access from WAN (Autoriser l'accès au routeur depuis Internet)**: Cochez **Yes** (Oui) / **No** (Non) pour autoriser / ne pas autoriser l'accès à l'interface de gestion du routeur depuis Internet. Sélectionnez **No** (Non) pour empêcher l'accès.
 - **Allow only specified IP address (Filtrage d'adresse IP)**: Cochez **Yes** (Oui) si vous souhaitez spécifier les adresses IP des clients pouvant accéder à l'interface de gestion du routeur depuis Internet.
 - **Client List (Liste des clients)**: Entrez les adresses IP du réseau étendu (WAN) des clients autorisés à accéder à l'interface de gestion du routeur depuis Internet. Cette liste ne sera utilisée que si vous avez coché **Yes** (Oui) pour l'option précédente.
3. Cliquez sur **Apply** (Appliquer).

4.10.3 Mise à niveau du firmware

REMARQUE : Téléchargez la dernière version du firmware sur le site internet d'ASUS : <http://www.asus.com>

Pour mettre à niveau le firmware :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Administration** > onglet **Firmware Upgrade** (Mise à jour du firmware).
2. Dans le champ **New Firmware File** (Nouveau fichier de firmware), cliquez sur **Browse** (Parcourir) pour localiser le fichier téléchargé.
3. Cliquez sur **Upload** (Charger).

REMARQUES:

- Une fois le processus de mise à niveau terminé, patientez quelques instants le temps que le routeur redémarre.
- Si la mise à niveau échoue, le routeur bascule automatiquement en mode de secours et le voyant d'alimentation situé en façade du routeur clignote lentement. Pour restaurer le routeur, consultez la section **5.2 Firmware Restoration (Restauration du firmware)**.

4.10.4 Restaurer/Sauvegarder/Transférer les paramètres de configuration

Pour restaurer/sauvegarder/transférer les paramètres de configuration du routeur :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Administration** > **Restore/Save/Upload Setting** (Restauration/Sauvegarde/Transfert de paramètres).
2. Sélectionnez une tâche :
 - Pour restaurer la configuration d'usine du routeur, cliquez sur **Restore** (Restaurer) puis sur **OK** lorsque le message de confirmation apparaît.
 - Pour effectuer une copie de sauvegarde des paramètres du routeur, cliquez sur **Save** (Sauvegarder), sélectionnez le dossier souhaité et cliquez sur **Save** (Sauvegarder).
 - Pour restaurer le routeur à partir d'un fichier de configuration précédent, cliquez sur **Browse** (Parcourir) et localisez le fichier, puis cliquez sur **Upload** (Charger).

REMARQUE : En cas de défaillance du routeur, chargez la dernière version du firmware. Ne restaurez pas la configuration d'usine du routeur.

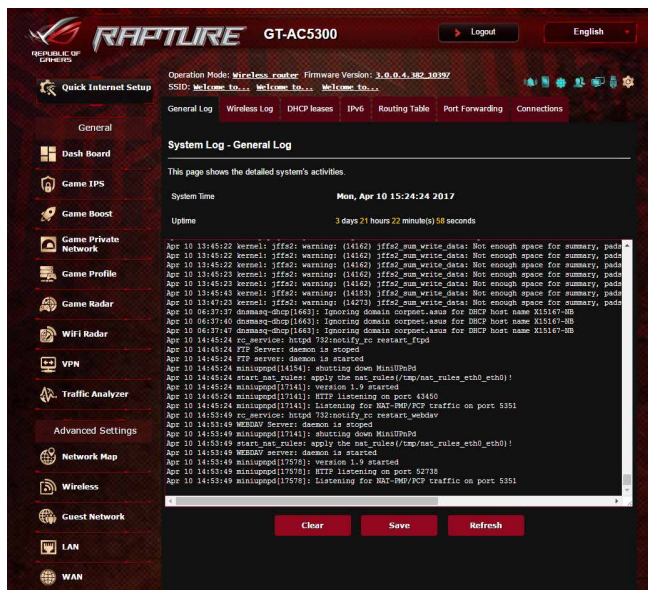
4.11 Journal système

Le journal système contient les activités du réseau enregistrées par le routeur.

REMARQUE : Le journal système est réinitialisé à chaque extinction ou redémarrage du routeur.

Pour afficher le journal système :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **System Log** (Journal système).
2. Les activités du réseau sont répertoriées dans les 5 onglets suivants :
 - General Log (Général)
 - DHCP Leases (Baux DHCP)
 - Wireless Log (Réseau Wi-Fi)
 - Port Forwarding (Redirection de port)
 - Routing Table (Tableau de routage)



The screenshot shows the Rapture GT-AC5300 web interface. The main content area is titled "System Log - General Log" and displays a list of system activities. The log entries include:

- Apr 10 13:45:22 kernel: jffs2: warning: (14162) jffs2_sum_write_data: Not enough space for summary, page
- Apr 10 13:45:22 kernel: jffs2: warning: (14162) jffs2_sum_write_data: Not enough space for summary, page
- Apr 10 13:45:23 kernel: jffs2: warning: (14162) jffs2_sum_write_data: Not enough space for summary, page
- Apr 10 13:45:23 kernel: jffs2: warning: (14162) jffs2_sum_write_data: Not enough space for summary, page
- Apr 10 13:45:43 kernel: jffs2: warning: (14153) jffs2_sum_write_data: Not enough space for summary, page
- Apr 10 13:47:23 kernel: jffs2: warning: (14273) jffs2_sum_write_data: Not enough space for summary, page
- Apr 10 06:37:07 dnsmasq-dhcp[1463]: Ignoring domain corrupt-ansu for DHCP host name X15167-08
- Apr 10 06:37:47 dnsmasq-dhcp[1463]: Ignoring domain corrupt-ansu for DHCP host name X15167-08
- Apr 10 14:45:24 rc_service: httpd_732:notify_rc: restart_fupd
- Apr 10 14:45:24 PFS server: daemon is stopped
- Apr 10 14:45:24 FTP server: daemon is started
- Apr 10 14:45:24 miniupnpd[14154]: shutting down MiniUPnPd
- Apr 10 14:45:24 miniupnpd[17141]: version 1.9 started
- Apr 10 14:45:24 miniupnpd[17141]: HTTP listening on port 5349
- Apr 10 14:45:24 miniupnpd[17141]: Listening for NAT-PMP/PCP traffic on port 5351
- Apr 10 14:53:49 rc_service: httpd_732:notify_rc: restart_webdav
- Apr 10 14:53:49 WREDV server: daemon is stopped
- Apr 10 14:53:49 miniupnpd[17141]: shutting down MiniUPnPd
- Apr 10 14:53:49 miniupnpd[17141]: version 1.9 started
- Apr 10 14:53:49 miniupnpd[17141]: HTTP listening on port 5349
- Apr 10 14:53:49 WREDV server: daemon is started
- Apr 10 14:53:49 miniupnpd[17178]: version 1.9 started
- Apr 10 14:53:49 miniupnpd[17178]: HTTP listening on port 52738
- Apr 10 14:53:49 miniupnpd[17178]: Listening for NAT-PMP/PCP traffic on port 5351

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

4.12 Smart Connect

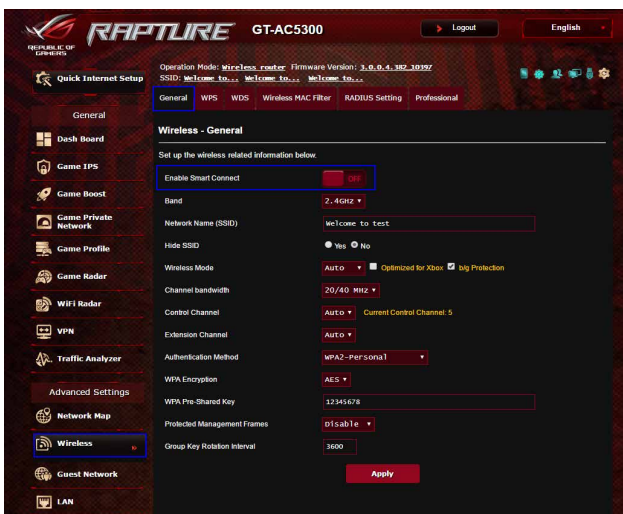
Smart Connect est conçu pour diriger automatiquement les clients vers l'une des trois bandes (une 2,4 GHz, une 5 GHz bande basse, une 5 GHz bande haute) pour optimiser l'utilisation de la bande passante.

4.12.1 Configurer Smart Connect

Vous pouvez activer Smart Connect depuis l'interface de gestion des deux façons suivantes :

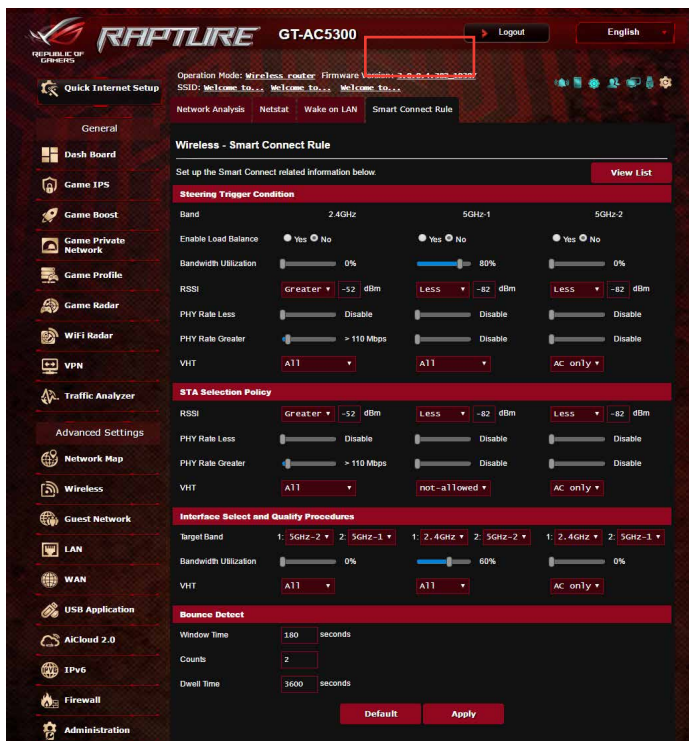
- **Via l'écran sans fil**

1. Dans la barre d'adresse de votre navigateur internet, entrez l'adresse IP par défaut de votre routeur Wi-Fi : <http://router.asus.com>.
2. Dans la fenêtre de connexion, saisissez le nom d'utilisateur par défaut (**admin**) et le mot de passe (**admin**), puis cliquez sur **OK**. L'assistant de configuration internet s'exécute automatiquement.
3. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **Wireless** (Wi-Fi) > onglet **General** (Général).
4. Déplacez l'interrupteur de l'élément **Enable Smart Connect** (Activer Smart Connect) sur **ON** (OUI) pour activer cette fonction permettant de connecter automatiquement les clients Wi-Fi à la bande de fréquence appropriée pour une vitesse optimale. Cette fonction permet de connecter automatiquement les clients Wi-Fi à la bande de fréquence appropriée pour une vitesse optimale.



4.12.2 Règles de Smart Connect

ASUSWRT fournit des paramètres par défaut pour déclencher le mécanisme de commutation. Vous pouvez également modifier les conditions de déclenchement en fonction de l'environnement de mise en réseau. Pour modifier les paramètres, allez dans l'onglet **Règles de Smart Connect** dans la section Network Tools (Outils réseau).

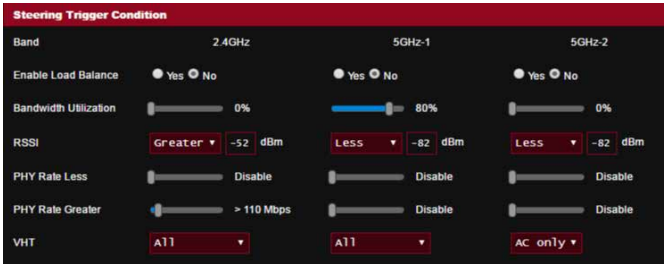


Les commandes des règles de Smart Connect sont divisées en quatre sections :

- Steering Trigger Condition (Conditions de déclenchement de redirection)
- STA Selection Policy (Politique de sélection de la station STA)
- Interface Select and Qualify Procedures (Sélection de l'interface et procédures de qualité)
- Bounce Detect (Détecteur de rebonds)

Steering Trigger Condition (Conditions de déclenchement de redirection)

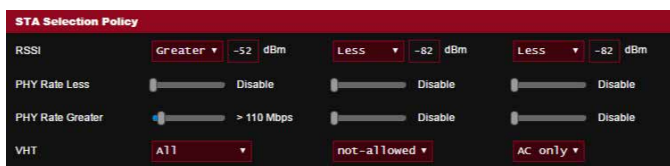
Cet ensemble de commandes définit les critères pour lancer la redirection de bande.



- **Bandwidth Utilization (Utilisation de bande passante)**
Si l'utilisation de la bande passante dépasse ce pourcentage, la redirection est lancée. La documentation Broadcom ne précise pas comment l'utilisation est mesurée.
- **Enable Load Balance (Activer l'équilibrage des charges)**
Cet élément contrôle l'équilibrage des charges. La documentation Broadcom n'indique pas comment l'équilibrage est effectué.
- **RSSI**
Si le niveau du signal reçu répond à ce critère, la redirection est déclenchée.
- **PHY Rate Less (Réduire le taux PHY) / PHY Rate Greater (Augmenter le taux PHY)**
Ces commandes déterminent le taux des liaisons STA pour déclencher la redirection de bande.
- **VHT**
Cette commande détermine comment les clients 802.11ac et non ac sont traités.
 - **ALL (TOUS)** (par défaut) signifie que tous les types de clients peuvent déclencher la redirection.
 - **AC only (AC uniquement)** signifie qu'un client doit prendre en charge 802.11ac pour déclencher la redirection.
 - **Not-allowed (Non autorisé)** signifie que seuls les clients non 802.11ac déclenchent la redirection, tels que 802.11a/b/g/n.

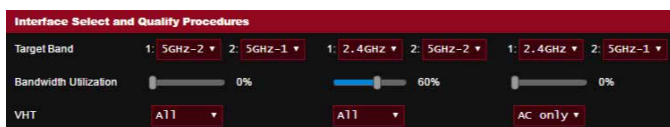
STA Selection Policy (Politique de sélection de la station STA)

Une fois la redirection déclenchée, ASUSWRT suit la politique de sélection STA pour sélectionner un client (STA) qui va être redirigé vers la bande la plus appropriée.



Interface Select and Qualify Procedures (Sélection de l'interface et procédures de qualité)

Ces commandes déterminent où le client redirigé aboutira. Les commandes **Target Band** (Bande cible) spécifient le premier et le deuxième choix de redirection. Les clients répondant aux critères de sélection STA pour la radiodiffusion seront orientés vers la première cible si la **Bandwidth Utilization** (Utilisation de la bande passante) est inférieure à la valeur définie. Dans le cas contraire, le client sera envoyé à la deuxième cible.



Bounce Detect (Détecteur de rebonds)

Cet ensemble de commandes détermine la fréquence à laquelle un client peut être redirigé. Ceci est destiné à éviter aux clients de se déplacer constamment. Cependant, cela n'empêche pas les clients de se déconnecter de leur propre initiative, ou de se compter eux-mêmes comme un rebond. Chaque client peut être redirigé **N Counts** (fois) dans la **Window Time** (Fenêtre de temps). Si le nombre limite est atteint, le client ne sera pas redirigé pendant le **Dwell Time** (Temps d'arrêt).



5 Utilitaires

REMARQUES :

- Téléchargez et installez les utilitaires Wi-Fi du routeur à partir du site ASUS :
 - Device Discovery (v1.4.7.1) : <http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Discovery.zip>
 - Firmware Restoration (v1.9.0.4) : <http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Rescue.zip>
 - Restauration du firmware (v1.0.5.5) : <http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Printer.zip>
 - Les utilitaires ne sont pas compatibles avec le système d'exploitation MAC OS.
-

5.1 Device Discovery (Détection d'appareils)

Détection d'appareils est un utilitaire Wi-Fi ASUS qui détecte les routeurs Wi-Fi ASUS et permet de les configurer facilement.

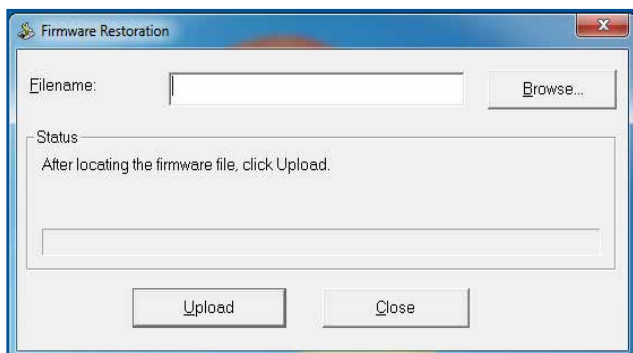
Pour lancer l'utilitaire Détection d'appareils :

- Depuis le Bureau de votre ordinateur, cliquez sur **Start** (Démarrer) > **All Programs** (Tous les programmes) > **ASUS Utility** (Utilitaire ASUS) > **GT-AC5300 Wireless Router** (Routeur Wi-Fi GT-AC5300) > **Device Discovery** (Détection d'appareils).

REMARQUE : Lorsque le routeur fonctionne en mode point d'accès, cet utilitaire est nécessaire pour obtenir l'adresse IP du routeur.

5.2 Firmware Restoration (Restauration du firmware)

Restauration du firmware est un utilitaire qui recherche automatiquement les routeurs Wi-Fi ASUS dont la mise à jour du firmware a échoué, puis restaure ou charge le firmware que vous avez spécifié. Cela télécharge le firmware que vous avez choisi. Le processus prend de 3 à 4 minutes.



IMPORTANT : Placez le routeur en mode de secours avant de lancer l'utilitaire Restauration du firmware.

REMARQUE : Cet utilitaire n'est pas compatible avec le système d'exploitation MAC OSX.

Pour basculer le routeur en mode de secours et utiliser l'utilitaire Restauration du firmware :

1. Débranchez la source d'alimentation de votre routeur Wi-Fi.
2. Maintenez enfoncé le bouton de réinitialisation situé à l'arrière du routeur et rebranchez l'adaptateur secteur au routeur. Relâchez le bouton de réinitialisation une fois que le voyant d'alimentation en façade se met à clignoter lentement pour indiquer que le routeur est en mode de secours.

3. Configurez une adresse IP statique sur votre ordinateur et utilisez les éléments suivants pour configurer les paramètres TCP/IP :

Adresse IP: 192.168.1.x

Masque de sous-réseau: 255.255.255.0

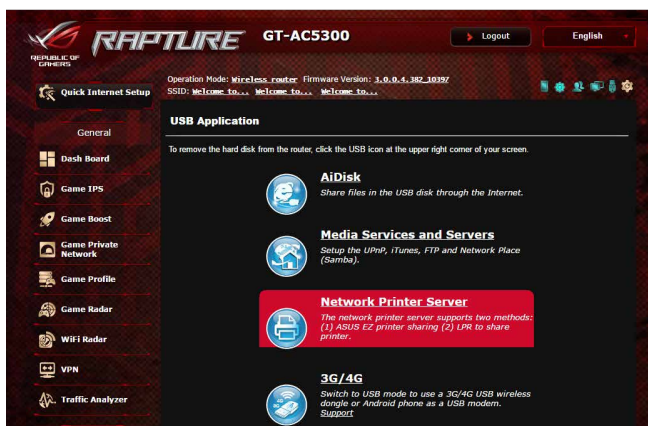
4. Depuis le Bureau de votre ordinateur, cliquez sur **Start** (Démarrer) > **All Programs** (Tous les programmes) > **ASUS Utility GT-AC5300 Wireless Router** (Utilitaire ASUS Routeur Wi-Fi GT-AC5300) > **Firmware Restoration** (Restauration du firmware).
5. Spécifiez un fichier de firmware, puis cliquez sur **Upload** (Charger).

REMARQUE : Cet utilitaire n'est pas un outil de mise à niveau du firmware et ne doit pas être utilisé avec un routeur Wi-Fi ASUS fonctionnant normalement. Les mises à niveau du firmware doivent être effectuées via l'interface de gestion du routeur. Consultez le **Chapitre 4 : Configurer les paramètres avancés** pour plus de détails.

5.3 Configurer un serveur d'impression

5.3.1 Utilitaire ASUS EZ Printer Sharing

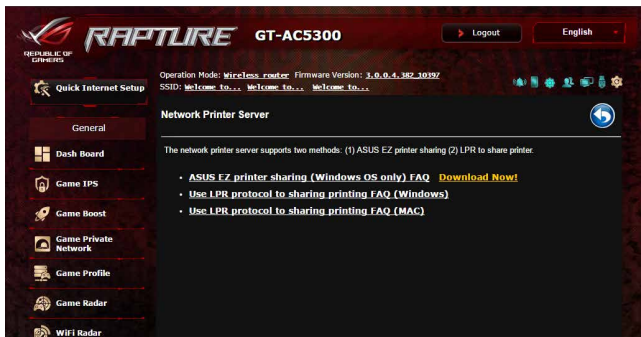
L'utilitaire ASUS EZ Printing Sharing vous permet de connecter une imprimante réseau au port USB du routeur et de configurer un serveur d'impression. Ceci permet aux clients du réseau d'imprimer et de scanner des fichiers en passant par le Wi-Fi.



REMARQUE : Les serveurs d'impression ne sont pris en charge que sous Windows® XP, Windows® Vista et Windows® 7.

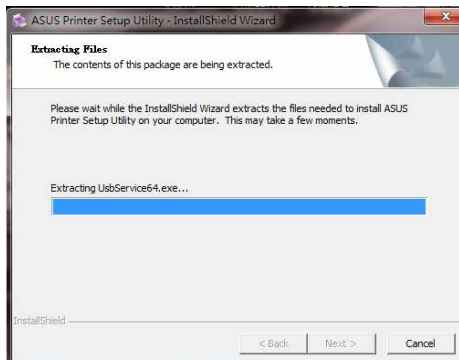
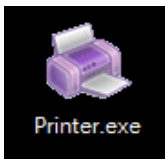
Pour partager une imprimante avec EZ Printer :

1. À partir du volet de navigation, cliquez sur **Advanced Settings** (Paramètres avancés) > **USB application** (Applications USB) > **Network Printer Server** (Serveur d'impression réseau).
2. Cliquez sur **Download Now!** (Télécharger maintenant!) pour télécharger l'utilitaire pour imprimante réseau.

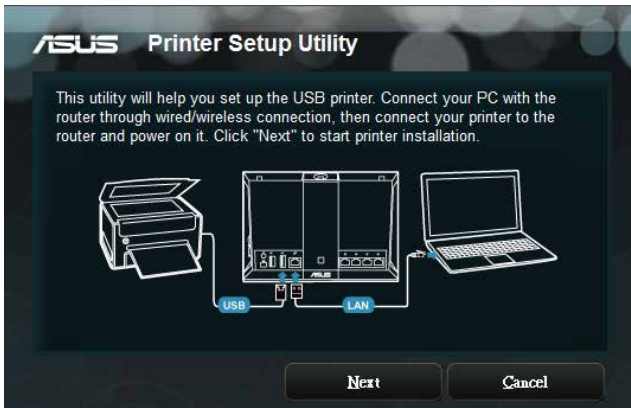


REMARQUE : L'utilitaire d'imprimante réseau est pris en charge sur Windows® XP, Windows® Vista et Windows® 7 uniquement. Pour installer l'utilitaire sur Mac OS, sélectionnez **Use LPR protocol for sharing printer** (Utiliser le protocole LPR pour partager une imprimante).

3. Décompressez le fichier téléchargé et cliquez sur l'icône représentant une imprimante pour exécuter le programme de configuration d'imprimante réseau.



4. Suivez les instructions apparaissant à l'écran pour configurer le matériel, puis cliquez sur **Next** (Suivant).

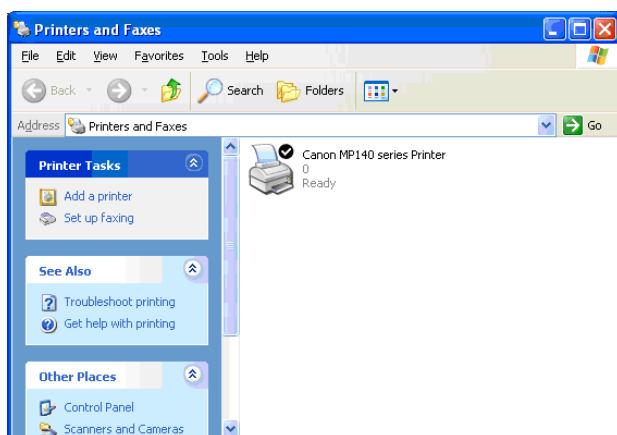


5. Patientez quelques minutes le temps que la configuration initiale se termine. Cliquez sur **Next** (Suivant).
6. Cliquez sur **Finish** (Terminé) pour conclure l'installation.

7. Suivez les instructions du système d'exploitation Windows® pour installer le pilote de l'imprimante.



8. Une fois le pilote installé, les clients du réseau pourront utiliser l'imprimante.



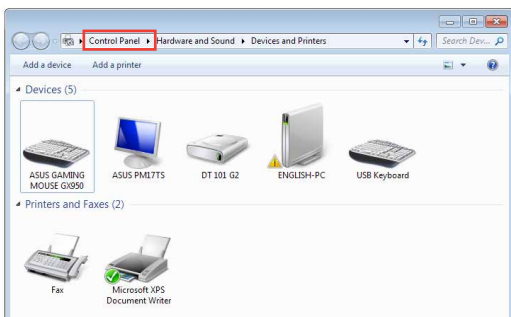
5.3.2 Utiliser le protocole LPR pour partager une imprimante

Vous pouvez utiliser les protocoles LPR/LPD (Line Printer Remote/ Line Printer Daemon) pour partager votre imprimante sous Windows® et MAC OS.

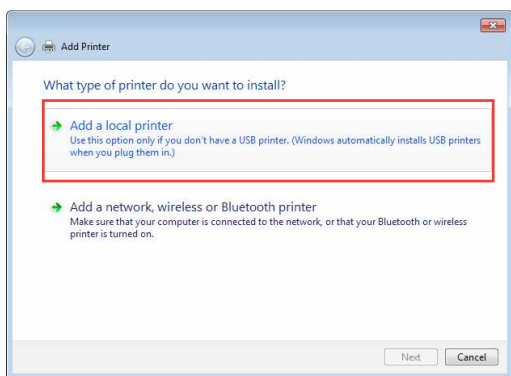
Partage d'imprimante LPR :

Pour partager une imprimante via le protocole LPR :

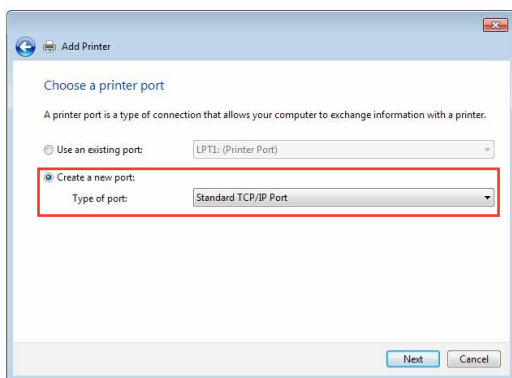
1. À partir du Bureau de Windows®, cliquez sur **Start** (Démarrer) > **Devices and Printers** (Périphériques et imprimantes) > **Add Printer Wizard** (Ajouter une imprimante).



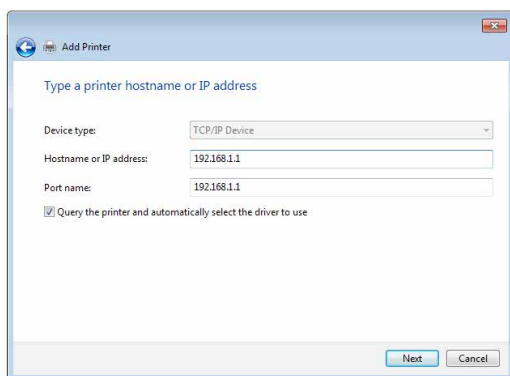
2. Sélectionnez **Add a local printer** (Ajouter une imprimante locale) et cliquez sur **Next** (Suivant).



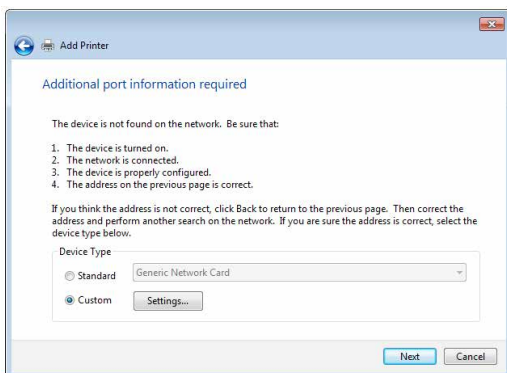
3. Sélectionnez **Create a new port** (Créer un nouveau port) puis sélectionnez l'option **Standard TCP/IP Port** (Port TCP/IP standard) du menu déroulant **Type of Port** (Type de port). Cliquez sur **New Port** (Nouveau port).



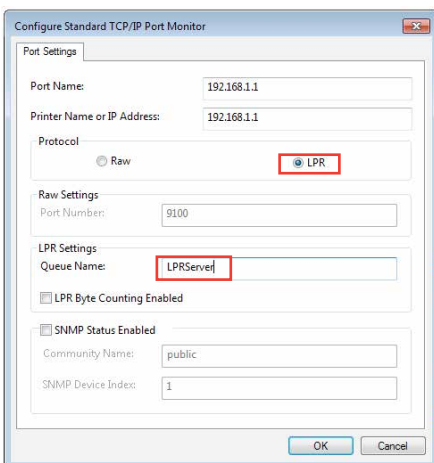
4. Dans le champ **Hostname or IP address** (Nom d'hôte ou adresse IP), entrez l'adresse IP du routeur Wi-Fi et cliquez sur **Next** (Suivant).



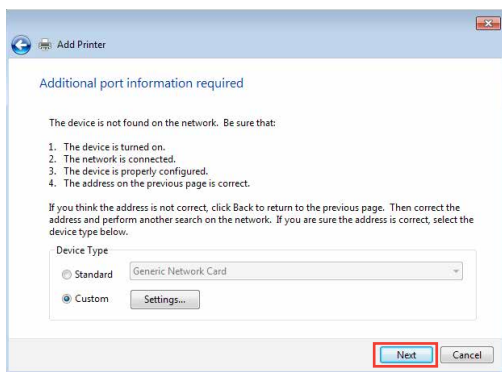
5. Sélectionnez **Custom** (Personnalisé) puis cliquez sur **Settings** (Paramètres).



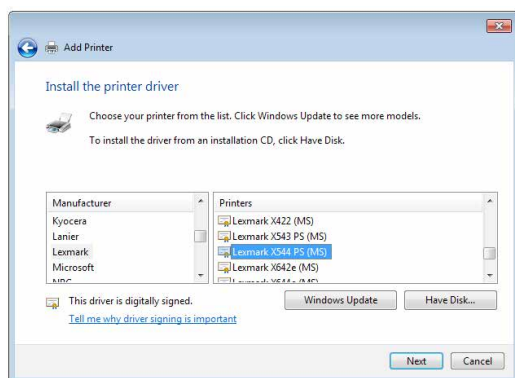
6. Réglez le **Protocol** (Protocole) sur **LPR**. Dans le champ **Queue Name** (Nom de la file d'attente), entrez **LPRServerj** puis cliquez sur **OK** pour continuer.



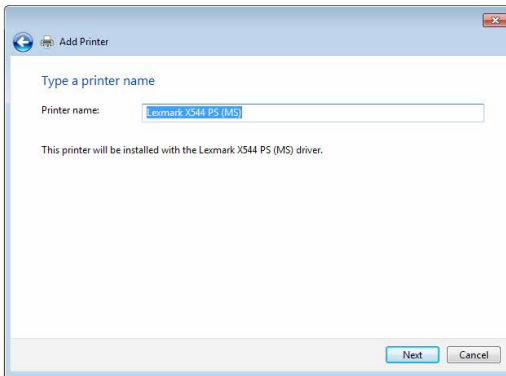
7. Cliquez sur **Next** (Suivant) pour terminer la configuration TCP/IP.



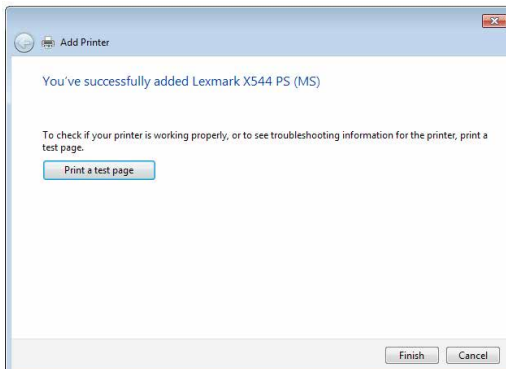
8. Installez le pilote d'impression à partir de la liste. Si votre imprimante ne figure pas dans la liste, cliquez sur **Have Disk** (Disque fourni) pour installer le pilote à partir d'un disque optique ou d'un fichier.



9. Cliquez sur **Next** (Suivant) pour accepter le nom par défaut de l'imprimante.



10. Cliquez sur **Finish** (Terminé) pour conclure l'installation.



5.4 Download Master

Download Master est un utilitaire vous permettant de télécharger des fichiers même lorsque votre ordinateur est éteint.

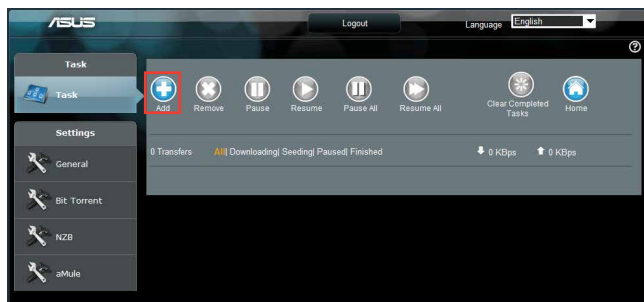
REMARQUE : Un périphérique de stockage USB doit être connecté au routeur Wi-Fi pour pouvoir utiliser Download Master.

Pour utiliser Download Master :

1. Cliquez sur **Advanced Settings** (Paramètres avancés) > **USB application** (Applications USB) > **Download Master** pour télécharger et installer l'utilitaire.

REMARQUE : Si plus d'un périphérique de stockage USB est relié au routeur Wi-Fi, sélectionnez celui sur lequel vous souhaitez télécharger vos fichiers.

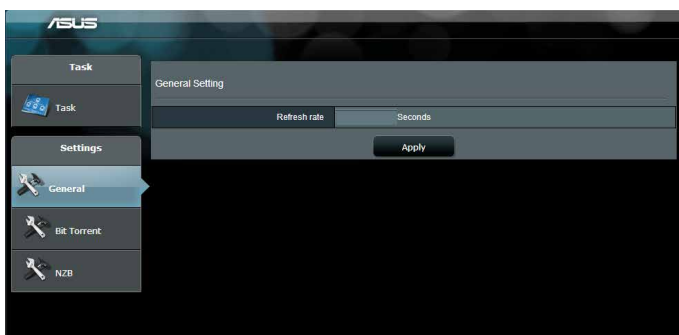
2. Une fois le téléchargement terminé, cliquez sur l'icône Download Master pour commencer à l'utiliser.
3. Cliquez sur **Add** (Ajouter) pour ajouter une tâche à télécharger.



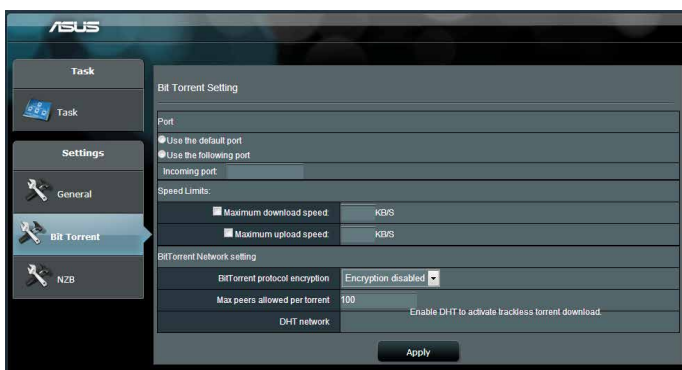
4. Sélectionnez un type de téléchargement, soit BitTorrent, HTTP, ou FTP. Spécifiez un fichier torrent ou une URL pour lancer le téléchargement.

REMARQUE : Pour plus de détails sur le protocole BitTorrent, consultez la section **5.4.1 Configurer les paramètres BitTorrent**.

5. Utilisez le panneau de navigation pour configurer les paramètres avancés.



5.4.1 Configurer les paramètres BitTorrent

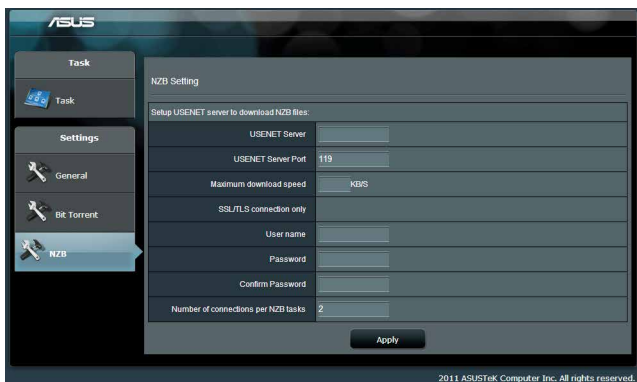


Pour configurer les paramètres de téléchargement BitTorrent :

1. Dans le panneau de navigation de Download Master, cliquez sur **BitTorrent**.
2. Sélectionnez un port de téléchargement spécifique.
3. Pour éviter les congestions réseau, vous pouvez limiter les vitesses de téléchargement en amont ou en aval sous l'élément **Speed Limits** (Limites de vitesse).
4. Vous pouvez aussi limiter le nombre maximum de clients autorisés et activer ou désactiver le chiffrement lors des téléchargements.

5.4.2 Paramètres NZB

Vous pouvez utiliser un serveur USENET pour télécharger des fichiers NZB. Après avoir configuré les paramètres USENET, cliquez sur **Apply** (Appliquer).



6 Dépannage

Ce chapitre offre des solutions aux problèmes pouvant survenir lors de l'utilisation de votre routeur. Si vous rencontrez un problème non traité dans ce chapitre, rendez-vous sur le site d'assistance d'ASUS sur : <https://www.asus.com/support/> pour plus d'informations sur votre produit et obtenir les coordonnées du service technique d'ASUS.

6.1 Dépannage de base

Si votre routeur ne fonctionne pas correctement, essayez les solutions de dépannage de base suivantes.

Mettez à jour le firmware.

1. Ouvrez l'interface de gestion du routeur. Cliquez sur **Advanced Settings** (Paramètres avancés) > **Administration** > onglet **Firmware Upgrade** (Mise à jour du firmware). Cliquez sur **Check** (Vérifier) pour vérifier si une mise à jour du firmware est disponible.
2. Si c'est le cas, rendez-vous sur http://www.asus.com/Networks/Wireless_Routers/GTAC5300/#download pour télécharger le dernier firmware disponible.
3. Dans l'onglet **Firmware Upgrade** (Mise à jour du firmware), cliquez sur **Browse** (Parcourir) pour localiser le fichier téléchargé.
4. Cliquez sur **Upload** (Charger) pour lancer le processus de mise à niveau du firmware.

Réinitialisez votre réseau dans l'ordre suivant :

1. Éteignez le modem.
2. Débranchez la prise d'alimentation du modem.
3. Éteignez le routeur et les ordinateurs connectés.
4. Branchez la prise d'alimentation du modem.
5. Allumez le modem et patientez environ 2 minutes.
6. Allumez le routeur et patientez environ 2 minutes.
7. Allumez vos ordinateurs.

Vérifiez que les câbles réseau Ethernet sont correctement branchés.

- Lorsque le câble Ethernet connectant le routeur au modem est correctement branché, le témoin lumineux du routeur dédié au réseau internet (WAN) s'allume.
- Lorsque le câble Ethernet connectant un ordinateur sous tension au routeur est correctement branché, le témoin lumineux du routeur dédié au réseau local (LAN) s'allume.

Vérifiez que les paramètres de connexion Wi-Fi de l'ordinateur correspondent à ceux du routeur.

- Lorsque vous tentez d'établir une connexion Wi-Fi entre un ordinateur et le routeur, assurez-vous que le SSID (nom du réseau Wi-Fi), la méthode de chiffrement et le mot de passe sont corrects.

Vérifiez que les paramètres de configuration du réseau sont corrects.

- Chaque client du réseau se doit de posséder une adresse IP valide. Il est recommandé d'utiliser le serveur DHCP du routeur pour affecter automatiquement les adresses IP aux clients du réseau.
- Certains fournisseurs d'accès internet au câble requièrent l'adresse MAC de l'ordinateur enregistré sur leur réseau. Vous pouvez obtenir l'adresse MAC d'un client à partir de l'interface de gestion du routeur, en cliquant sur **Network Map** (Carte du réseau) > page **Clients**. Placez le curseur de souris au-dessus d'un client pour visualiser son adresse MAC.

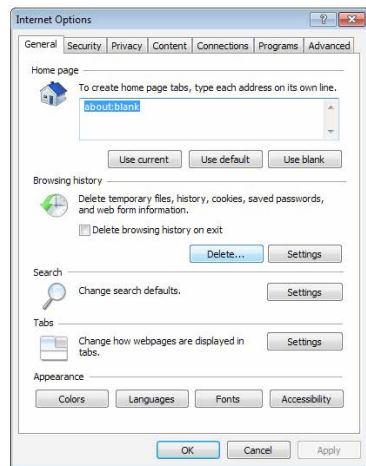


6.2 Foire aux questions (FAQ)

Impossible d'accéder à l'interface de gestion du routeur

- Si vous utilisez une connexion filaire, vérifiez le câble Ethernet et l'état des différents voyants lumineux tel qu'expliqué dans la section précédente.
- Assurez-vous d'utiliser les bons identifiants de connexion. Le nom d'utilisateur/mot de passe par défaut est "admin". Vérifiez également que la touche de verrouillage des majuscules n'a pas été activée.
- Supprimez les cookies et les fichiers temporaires de votre navigateur internet. Pour Internet Explorer, suivez les instructions suivantes :

1. Ouvrez Internet Explorer, puis cliquez sur **Tools** (Outils) > **Internet Options** (Options internet).
2. Dans l'onglet **General** (Général), sous **Browsing history** (Historique de navigation), cliquez sur **Delete...** (Supprimer...), sélectionnez **Temporary Internet Files** (Fichiers internet temporaires) et **Cookies** puis cliquez sur **Delete** (Supprimer).



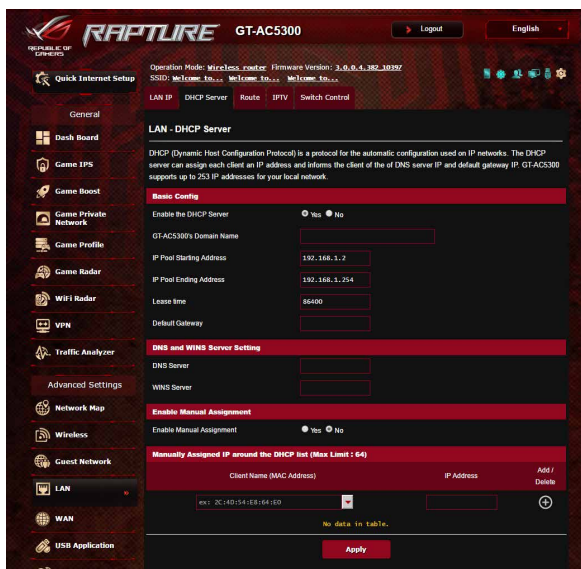
REMARQUES :

- Les options de suppression des cookies et des fichiers temporaires peuvent varier en fonction du navigateur internet utilisé.
- Si applicable, désactivez votre proxy, la numérotation de votre connexion à distance, et configurez les paramètres TCP/IP de sorte à obtenir une adresse IP automatiquement. Pour plus de détails, consultez le chapitre 1 de ce manuel.
- Assurez-vous d'utiliser des câbles réseau Ethernet de catégorie 5 ou 6.

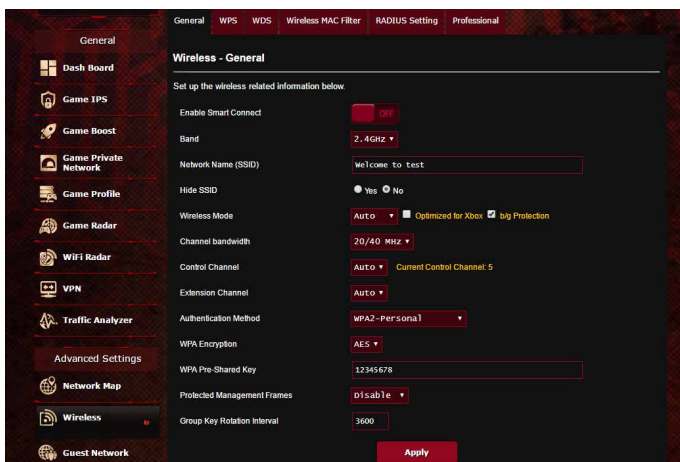
Le client ne peut pas établir de connexion Wi-Fi avec le routeur.

REMARQUE : Si vous rencontrez des problèmes de connexion au réseau 5 GHz, assurez-vous que votre appareil soit compatible avec cette bande de fréquence.

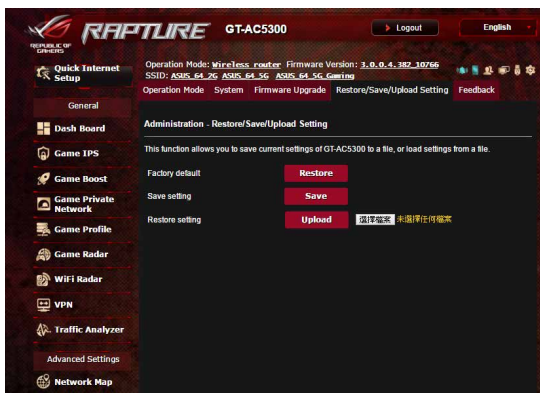
- **Hors de portée :**
 - Rapprochez le routeur du client.
 - Si disponibles, essayez d'ajuster l'angle des antennes du routeur. Pour plus de détails, consultez la section **1.4 Placer votre routeur**.
- **Serveur DHCP désactivé :**
 1. Ouvrez l'interface de gestion du routeur. Dans l'interface de gestion du routeur, cliquez sur **Advanced Settings** (Paramètres avancés) > **Network Map** (Carte du réseau) > icône **Clients**.
 2. Si l'appareil n'apparaît pas dans la liste, cliquez sur **Advanced Settings** (Paramètres avancés) > **LAN** (Réseau local) > onglet **DHCP Server** (Serveur DHCP), et vérifiez que la case **Yes** (Oui) du champ **Enable the DHCP Server** (Activer le serveur DHCP) est bien cochée.



- Le SSID est masqué. Si votre appareil est en mesure de détecter d'autres réseaux Wi-Fi sauf celui de votre routeur, allez dans **Advanced Settings** (Paramètres avancés) > **Wireless** (Wi-Fi) > onglet **General** (Général), cochez l'option **No** (Non) du champ **Hide SSID** (Masquer le SSID), et l'option **Auto** du champ **Control Channel** (Canal).



- Si vous utilisez une carte Wi-Fi, vérifiez que le canal Wi-Fi utilisé est disponible dans votre pays/région. Dans ce cas, modifiez le canal et les autres paramètres Wi-Fi appropriés.
- Si vous ne parvenez toujours pas à établir une connexion Wi-Fi au routeur, restaurez sa configuration d'usine. Pour ce faire, dans l'interface de gestion du routeur, allez dans **Administration** > onglet **Restore/Save/Upload Setting** (Restauration/Sauvegarde/Transfert de paramètres) et cliquez sur **Restore** (Restaurer).



Internet n'est pas accessible.

- Vérifiez que votre routeur peut se connecter à l'adresse IP du réseau étendu (WAN) de votre FAI. Pour ce faire, dans l'interface de gestion du routeur, allez dans **Advanced Settings** (Paramètres avancés) > **Network Map** (Carte du réseau) et vérifiez **l'état de la connexion internet**.
- Si votre routeur ne peut pas se connecter à Internet, essayez de réinitialiser le réseau comme décrit à la sous-section **Réinitialisez votre réseau dans l'ordre suivant** sous **Dépannage de base**.



- Le client a été bloqué par la fonctionnalité de contrôle parental. Rendez-vous dans **General** (Général) > **Game IPS** > onglet **Parental Controls** (Contrôle parental) et vérifiez que l'appareil figure dans la liste. Si c'est le cas, utilisez le bouton **Supprimer** pour retirer le client de la liste, ou modifiez les horaires de blocage.
- Si Internet n'est toujours pas accessible, essayez de redémarrer l'ordinateur et vérifiez son adresse IP et de passerelle.
- Vérifiez les témoins lumineux du modem ADSL et du routeur Wi-Fi. Si le voyant lumineux dédié au réseau étendu (WAN) du routeur est éteint, vérifiez l'état de connexion des câbles.

Oubli du SSID (nom du réseau) ou du mot de passe de connexion au réseau

- Configurez un nouveau SSID et une nouvelle clé de chiffrement par le biais d'une connexion filaire (câble Ethernet). Ouvrez l'interface de gestion du routeur, allez sur la page **Network Map** (Carte du réseau), spécifiez un nouveau SSID ainsi qu'une nouvelle clé de chiffrement, puis cliquez sur **Apply** (Appliquer).
- Restaurer la configuration d'usine du routeur. Pour ce faire, dans l'interface de gestion du routeur, allez dans **Administration** > onglet **Restore/Save/Upload Setting** (Restauration/Sauvegarde/Transfert de paramètres) et cliquez sur **Restore** (Restaurer). Le nom d'utilisateur / mot de passe par défaut est "admin".

Restauration des paramètres par défaut du routeur ?

- Allez dans **Administration** > onglet **Restore/Save/Upload Setting** (Restauration/Sauvegarde/Transfert de paramètres) et cliquez sur **Restore** (Restaurer).

Les éléments suivants sont les paramètres par défaut du routeur :

| | |
|--------------------------------|---|
| Nom d'utilisateur : | admin |
| Mot de passe : | admin |
| Serveur DHCP : | Activé (Si le câble WAN est branché) |
| Adresse IP : | http://router.asus.com (ou 192.168.1.1) |
| Nom de domaine : | (aucun) |
| Masque de sous-réseau : | 255.255.255.0 |
| Serveur DNS 1 : | 192.168.1.1 |
| Serveur DNS 2 : | (aucun) |
| SSID (2,4 GHz) : | ASUS |
| SSID (5 GHz) : | ASUS_5G |

Échec de la mise à jour du firmware.

Placez le routeur en mode de secours et exécutez l'utilitaire Restauration du firmware. Consultez la section **5.2 Firmware Restoration (Restauration du firmware)** pour en savoir plus sur l'utilisation de cet utilitaire.

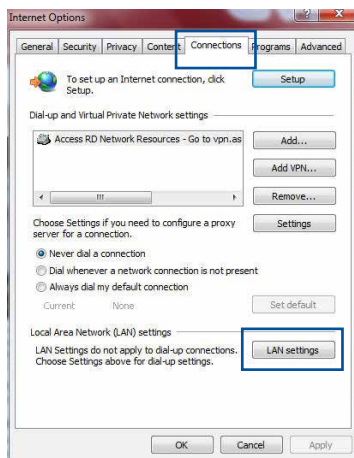
Impossible d'accéder à l'interface de gestion de routeur

Avant de configurer votre routeur Wi-Fi, suivez les instructions suivantes pour votre ordinateur hôte et les autres clients du réseau.

A. Désactivez le serveur proxy si celui-ci est activé.

Sous Windows® 7

1. Cliquez sur **Start** (Démarrer) > **Internet Explorer** pour ouvrir le navigateur.
2. Cliquez sur **Tools** (Outils) > **Internet options** (Options internet) > onglet **Connections** (Connexions) > **LAN settings** (Paramètres réseau).

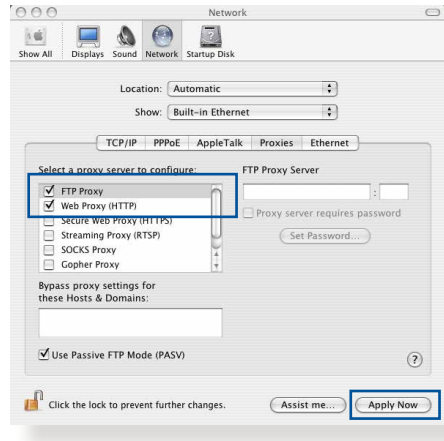


3. À partir de l'écran des paramètres du réseau local, décochez l'option **Use a proxy server for your LAN** (Utiliser un serveur proxy pour votre réseau local).
4. Cliquez sur **OK** une fois terminé.



Sous MAC OS

1. Dans votre navigateur Safari, cliquez sur **Safari > Preferences** (Préférences) > **Advanced** (Avancées) > **Change Settings** (Modifier les réglages).
2. Dans la liste des protocoles, décochez les options **FTP Proxy** (Proxy FTP) et **Web Proxy (HTTP)** (Proxy web sécurisé (HTTP)).
3. Cliquez sur **Apply Now** (Appliquer maintenant) une fois terminé.

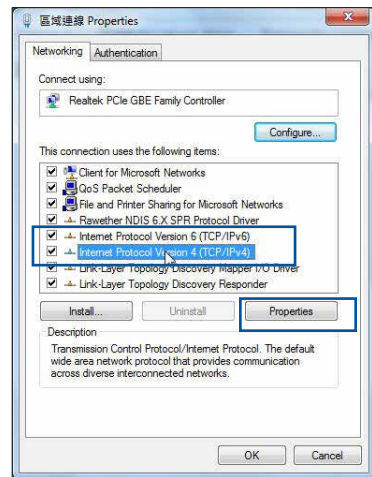


REMARQUE : Consultez le fichier d'aide de votre navigateur internet pour plus de détails sur la désactivation du serveur proxy.

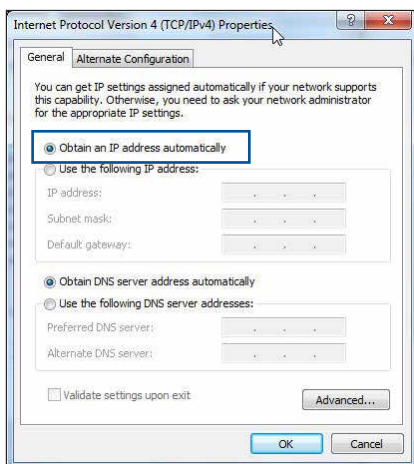
B. Configurez les paramètres TCP/IP pour l'obtention automatique d'une adresse IP.

Sous Windows® 7


1. Cliquez sur **Start** (Démarrer) > **Control Panel** (Panneau de configuration) > **Network and Internet** (Réseau et Internet) > **Network and Sharing Center** (Centre réseau et partage) > **Manage network connections** (Gérer les connexions réseau).
2. Sélectionnez **Internet Protocol Version 4 (TCP/IPv4)** (Protocole internet version 4 (TCP/IPv4)) ou **Internet Protocol Version 6 (TCP/IPv6)** (Protocole internet version 6 (TCP/IPv6)), puis cliquez sur **Properties** (Propriétés).

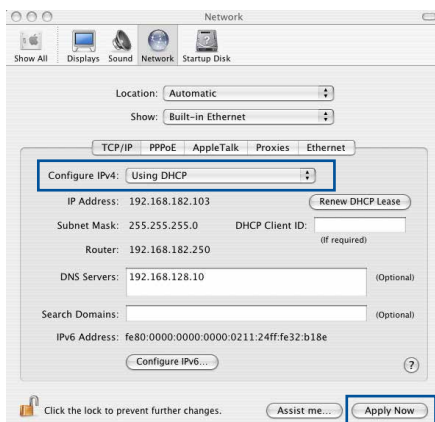


3. Pour obtenir une adresse IP IPv4, cochez l'option **Obtain an IP address automatically** (Obtenir une adresse IP automatiquement).
Pour obtenir une adresse IP IPv6, cochez l'option **Obtain an IPv6 address automatically** (Obtenir une adresse IPv6 automatiquement).
4. Cliquez sur **OK** une fois terminé.



Sous MAC OS

1. Cliquez sur l'icône Apple  située en haut à gauche de votre écran.
2. Cliquez sur **System Preferences** (Préférences Système) > **Network** (Réseau) > **Configure...** (Configurer...).
3. Dans l'onglet **TCP/IP**, sélectionnez **Using DHCP** (Via DHCP) dans le menu déroulant **Configure IPv4** (Configurer IPv4).
4. Cliquez sur **Apply Now** (Appliquer maintenant) une fois terminé.

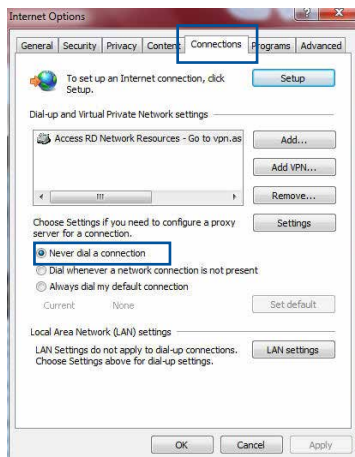


REMARQUE : Consultez l'aide de votre système d'exploitation pour plus de détails sur la configuration des paramètres TCP/IP de votre ordinateur.

C. Désactivez la numérotation de votre connexion à distance (si applicable).

Sous Windows® 7

1. Cliquez sur **Start** (Démarrer) > **Internet Explorer** pour ouvrir le navigateur.
2. Cliquez sur **Tools** (Outils) > **Internet options** (Options internet) > onglet **Connections** (Connexions).
3. Cochez l'option **Never dial a connection** (Ne jamais établir de connexion).
4. Cliquez sur **OK** une fois terminé.



REMARQUE : Consultez le fichier d'aide de votre navigateur internet pour plus de détails sur la désactivation d'une connexion à distance.

Annexes

Notices

Services de reprise et de recyclage

Les programmes de recyclage et de reprise d'ASUS découlent de nos exigences en terme de standards élevés de respect de l'environnement. Nous souhaitons apporter à nos clients des solutions permettant de recycler de manière responsable nos produits, batteries et autres composants ainsi que nos emballages. Veuillez consulter le site <http://csr.asus.com/english/Takeback.htm> pour plus de détails sur les conditions de recyclage en vigueur dans votre pays.

REACH

En accord avec le cadre réglementaire REACH (Enregistrement, Evaluation, Autorisation, et Restriction des produits chimiques), nous publions la liste des substances chimiques contenues dans nos produits sur le site ASUS REACH :

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

Rapport de la Commission Fédérale des Communications (FCC)

Cet appareil est conforme à l'alinéa 15 des règles établies par la FCC. Son utilisation est sujette aux deux conditions suivantes :

- Cet appareil ne doit pas créer d'interférences nuisibles, et.
- Cet appareil doit tolérer tout type d'interférences, y compris celles susceptibles de provoquer un fonctionnement non souhaité de l'appareil.

Cet appareil a été testé et déclaré conforme aux limites relatives aux appareils numériques de classe B, en accord avec la Section 15 de la réglementation de la Commission Fédérale des Communications (FCC). Ces limites sont conçues pour offrir une protection raisonnable contre les interférences nuisibles en installation résidentielle.

Cet appareil génère, utilise et peut émettre de l'énergie de radiofréquence et, s'il n'est pas installé et utilisé en accord

avec les instructions, peut créer des interférences nuisibles aux communications radio. Cependant, il n'y a pas de garantie que des interférences ne surviendront pas dans une installation particulière. Si cet appareil crée des interférences nuisibles à la réception de la radio ou de la télévision (il est possible de le déterminer en éteignant puis en rallumant l'appareil), l'utilisateur est encouragé à essayer de corriger les interférences par l'une ou plusieurs des mesures suivantes :

- Réorienter ou repositionner l'antenne de réception.
- Augmenter la distance de séparation entre l'appareil et le récepteur.
- Brancher l'appareil sur une prise secteur d'un circuit différent de celui auquel le récepteur est branché.
- Consulter le revendeur ou un technicien radio/TV qualifié pour obtenir de l'aide.

Rapport de la Commission Fédérale des Communications

Cet appareil a été testé et s'est avéré conforme aux limites établies par la FCC en matière d'exposition aux radiations dans un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 31 cm de distance entre la source de rayonnement et votre corps.

IMPORTANT ! Cet appareil est restreint à une utilisation en intérieur.

AVERTISSEMENT!

- Tout changement ou modification non expressément approuvé(e) par le responsable de la conformité peut annuler le droit de l'utilisateur à faire fonctionner cet appareil.
 - Les utilisateurs ne sont pas autorisés à modifier l'appareil. Les changements ou modifications apportés à cette unité n'étant pas expressément approuvés par la partie responsable de la conformité (FCC) peuvent annuler le droit de l'utilisateur à faire fonctionner cet appareil.
 - Pour les produits disponibles aux États-Unis et au Canada, seuls les canaux 1 à 11 peuvent être utilisés. La sélection d'autres canaux n'est pas possible.
-

Interdiction de colocalisation

Cet appareil et son ou ses antenne(s) ne doivent pas être situés près de ou utilisés conjointement avec une autre antenne ou un autre émetteur.

Consignes de sécurité

Cet appareil a été testé et s'est avéré conforme aux limites établies par la FCC en matière d'exposition aux radiations dans un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 31 cm de distance entre la source de rayonnement et votre corps.

Déclaration de conformité (Directive R et TTE 1999/5/CE)

Exigences essentielles selon l'[Article 3]

Exigences de protection pour la santé et la sécurité selon l'[Article 3.1a]

Test de la sécurité électrique en conformité avec l'EN 60950-1. Des tests ont été conduits et leurs résultats sont considérés comme pertinents et suffisants.

Exigences de protection pour la compatibilité électromagnétique selon l'[Article 3.1b]

Test de la compatibilité électromagnétique selon l'[EN 301 489-1] et l'[EN 301 489-17]. Des tests ont été conduits et leurs résultats sont considérés comme pertinents et suffisants.

Utilisation efficace du spectre des radiofréquences selon l'[Article 3.2]

Test radio selon l'[EN 300 328] et l'[EN 301 893]. Des tests ont été conduits et leurs résultats sont considérés comme pertinents et suffisants.

Seule une utilisation en intérieur pour les bandes de fréquence 5150-5250 MHz est autorisée.

Avvertimento concernente il marchio CE

Ceci est un produit de classe B. Dans un environnement domestique, ce produit peut créer des interférences radio, auquel cas l'utilisateur pourra être amené à prendre les mesures adéquates.

Cet appareil peut être utilisé dans les pays suivants : AT, BE, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IE, IT, LU, MT, NL, PL, PT, SK, SL, ES, SE, GB, IS, LI, NO, CH, BG, RO, RT.

Canada, Industry Canada (IC) Notices

This device complies with Industry Canada license-exempt RSS standard(s).

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Informations concernant l'exposition aux fréquences radio (RF)

Cet équipement a été testé et s'est avéré conforme aux limites établies par Industrie Canada en matière d'exposition aux radiations dans un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 31 cm de distance entre la source de rayonnement et votre corps.

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 31 cm de distance entre la source de rayonnement et votre corps.

Canada, avis d'Industrie Canada (IC)

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

Son utilisation est sujette aux deux conditions suivantes : (1) Cet appareil ne doit pas créer d'interférences nuisibles, et

(2) Cet appareil doit tolérer tout type d'interférences, y compris celles susceptibles de provoquer un fonctionnement non souhaité de l'appareil.

AVERTISSEMENT !

- Le présent émetteur radio (3568A-RTGZ00) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.
- Le présent émetteur radio (3568A-RTGZ00) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Tableau de l'antenne déposée

| Ant. | Marque | Nom du modèle | Type d'antenne | Connecteur | Gain (dBi) | |
|------|--------|---------------|----------------|-------------|------------|-------|
| | | | | | 2,4 GHz | 5 GHz |
| 1 | Whayu | C660-510391-A | Antenne dipôle | SMA-inversé | 2.14 | 2.98 |
| 2 | Whayu | C660-510391-A | Antenne dipôle | SMA-inversé | 2.14 | 2.98 |
| 3 | Whayu | C660-510391-A | Antenne dipôle | SMA-inversé | 2.14 | 2.98 |
| 4 | Whayu | C660-510391-A | Antenne dipôle | SMA-inversé | 2.14 | 2.98 |
| 5 | Whayu | C660-510391-A | Antenne dipôle | SMA-inversé | 2.14 | 2.98 |
| 6 | Whayu | C660-510391-A | Antenne dipôle | SMA-inversé | 2.14 | 2.98 |
| 7 | Whayu | C660-510391-A | Antenne dipôle | SMA-inversé | 2.14 | 2.98 |
| 8 | Whayu | C660-510391-A | Antenne dipôle | SMA-inversé | 2.14 | 2.98 |

- Pour les produits disponibles aux États-Unis et au Canada, seuls les canaux 1 à 11 peuvent être utilisés. La sélection d'autres canaux n'est pas possible.
- Pour les produits disponibles aux États-Unis et au Canada, seuls les canaux 1 à 11 peuvent être exploités. La sélection d'autres canaux n'est pas possible.
- Cet appareil et son ou ses antenne(s) ne doivent pas être situés près de ou utilisés conjointement avec une autre antenne ou un autre émetteur.
- Cet appareil et son antenne ne doivent pas être co-localisés ou fonctionner en association avec une autre antenne ou transmetteur.
- Les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement à une utilisation en intérieur afin de réduire les risques d'interférence préjudiciables aux systèmes de satellites mobiles utilisant les mêmes canaux ;
- Les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement à une utilisation en intérieur afin de réduire les risques d'interférence préjudiciables aux systèmes de satellites mobiles utilisant les mêmes canaux.

NCC

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

「產品之限用物質含有情況」之相關資訊，請參考下表：

| 單元 | 限用物質及其化學符號 | | | | | |
|-------------------------------------|------------|---|---|-----|---------------|-----------------|
| | 鉛 | 汞 | 鎳 | 六價鉻 | 多溴聯苯 (PBB) | 多溴二苯醚 (PBDE) |
| 印刷電路板及電子組件 | - | ○ | ○ | ○ | ○ | ○ |
| 外殼 | ○ | ○ | ○ | ○ | ○ | ○ |
| 天線 | - | ○ | ○ | ○ | ○ | ○ |
| 其他及其配件 | ○ | ○ | ○ | ○ | ○ | ○ |
| 備考1. “○” 係指該項限用物質之百分比含量未超出百分比含量基準值。 | | | | | | |
| 備考2. “-” 係指該項限用物質為排除項目。 | | | | | | |

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. We include a copy of the GPL with every CD shipped with our product. 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

Pour la Turquie

Distributeurs autorisés pour la Turquie :

BOGAZICI BIL GISAYAR SAN. VE TIC. A.S.

Téléphone : +90 212 3311000

Adresse : AYAZAGA MAH. KEMERBURGAZ CAD. NO.10
AYAZAGA/ISTANBUL

CIZGI Elektronik San. Tic. Ltd. Sti.

Téléphone : +90 212 3567070

Adresse : CEMAL SURURI CD. HALIM MERIC IS MERKEZI
No : 15/C D:5-6 34394 MECIDIYEKOY/
ISTANBUL

KOYUNCU ELEKTRONİK BİLGİ İŞLEM SİST. SAN. VE DİSTİC. A.S.

Téléphone : +90 216 5288888

Adresse : EMEK MAH.ORDU CAD. NO:18, SARIGAZI,
SANCAKTEPE ISTANBUL

AEEE Yönetmeliğine Uygundur.

Informations de contact ASUS

ASUSTeK COMPUTER INC. (Asie Pacifique)

Adresse 4F, No. 150, Li Te Rd., Peitou, Taipei 112, Taiwan
Site internet www.asus.com.tw

Support technique

Téléphone +886228943447
Fax +886228907698
Support en ligne www.asus.com/support/

ASUS COMPUTER INTERNATIONAL (Amérique)

Adresse 48720 Kato Rd., Fremont, CA 94538, USA
Téléphone +15107393777
Fax +15106084555
Site internet usa.asus.com
Support en ligne www.asus.com/support/

ASUS COMPUTER GmbH (Allemagne et Autriche)

Adresse Harkort Str. 21-23, D-40880 Ratingen, Germany
Fax +49-2102-959931
Site internet asus.com/de
Contact en ligne eu-rma.asus.com/sales

Support technique

Téléphone (Composants) +49-2102-5789555
Téléphone Allemagne
(System/Notebook/Eee/LCD) +49-2102-5789557
Téléphone Autriche
(System/Notebook/Eee/LCD) +43-820-240513
Support Fax +49-2102-959911
Support en ligne www.asus.com/support/

Centres d'appel mondiaux

| Région | Pays | Numéro de téléphone | Horaires | |
|-----------------|------------------------|---------------------------------|--|--|
| Europe | Chypre | 800-92491 | 09:00-13:00 ; 14:00-18:00 Lun.-Vend | |
| | France | 0033-170949400 | 09:00-18:00 Lun.-Vend | |
| | Allemagne | 0049-1805010920 | | |
| | | 0049-1805010923 (composants) | | 09:00-18:00 Lun.-Vend 10:00-17:00 Lun.-Vend |
| | | 0049-2102959911 (Fax) | | |
| | Hongrie | 0036-15054561 | 09:00-17:30 Lun.-Vend | |
| | Italie | 199-400089 | 09:00-13:00 ; 14:00-18:00 Lun.-Vend | |
| | Grèce | 00800-44142044 | 09:00-13:00 ; 14:00-18:00 Lun.-Vend | |
| | Autriche | 0043-820240513 | 09:00-18:00 Lun.-Vend | |
| | Pays-Bas Luxembourg | 0031-591570290 | 09:00-17:00 Lun.-Vend | |
| | Belgique | 0032-78150231 | 09:00-17:00 Lun.-Vend | |
| | Norvège | 0047-2316-2682 | 09:00-18:00 Lun.-Vend | |
| | Suède | 0046-858769407 | 09:00-18:00 Lun.-Vend | |
| | Finlande | 00358-969379690 | 10:00-19:00 Lun.-Vend | |
| | Danemark | 0045-38322943 | 09:00-18:00 Lun.-Vend | |
| | Pologne | 0048-225718040 | 08:30-17:30 Lun.-Vend | |
| | Espagne | 0034-902889688 | 09:00-18:00 Lun.-Vend | |
| | Portugal | 00351-707500310 | 09:00-18:00 Lun.-Vend | |
| | Slovaquie | 00421-232162621 | 08:00-17:00 Lun.-Vend | |
| | République Tchèque | 00420-596766888 | 08:00-17:00 Lun.-Vend | |
| | Suisse-Allemand | 0041-848111010 | 09:00-18:00 Lun.-Vend | |
| Suisse-Français | 0041-848111014 | 09:00-18:00 Lun.-Vend | | |
| Suisse-Italien | 0041-848111012 | 09:00-18:00 Lun.-Vend | | |
| Royaume-Uni | 0044-1442265548 | 09:00-17:00 Lun.-Vend | | |
| Irlande | 0035-31890719918 | 09:00-17:00 Lun.-Vend | | |
| Russie et CIS | 008-800-100-ASUS | 09:00-18:00 Lun.-Vend | | |
| Ukraine | 0038-0445457727 | 09:00-18:00 Lun.-Vend | | |

Centres d'appel mondiaux

| Région | Pays | Numéro de téléphone | Horaires |
|----------------------|-----------------------|--|---|
| Asie-Pacifique | Australie | 1300-278788 | 09:00-18:00 Lun.-Vend |
| | Nouvelle Zélande | 0800-278788 | 09:00-18:00 Lun.-Vend |
| | Japon | 0800-1232787 | 09:00-19:00 Lun.-Dim |
| | | 0081-570783886 (Payant) | 09:00-19:00 Lun.-Dim |
| | Corée du Sud | 0082-215666868 | 09:30-17:00 Lun.-Vend |
| | Thaïlande | 0066-24011717 | 09:00-18:00 Lun.-Vend |
| | | 1800-8525201 | |
| | Singapour | 0065-64157917 | 11:00-19:00 Lun.-Vend |
| | | 0065-67203835 | 11:00-19:00 Lun.-Vend |
| | | (Vérification du statut de réparation) | 11:00-13:00 Samedi |
| | Malaisie | 1300-88-3495 | 9:00-18:00 Lun.-Vend |
| | Philippines | 1800-18550163 | 09:00-18:00 Lun.-Vend |
| | Inde | 1800-2090365 | 09:00-18:00 Lun.-Sam |
| 09:00-21:00 Lun.-Dim | | | |
| Indonésie | 0062-2129495000 | 09:30-17:00 Lun.-Vend | |
| | 500128 (Numéro local) | 9:30 – 12:00 Samedi | |
| Vietnam | 1900-555581 | 08:00-12:00 13:30-17:30 Lun.-Sam | |
| Hong Kong | 00852-35824770 | 10:00-19:00 Lun.-Sam | |
| Amérique | États-Unis | 1-812-282-2787 | 8:30-12:00 HNE Lun.-Vend |
| | Canada | | 9:00-18:00 HNE Sam.-Dim |
| | Mexique | 001-8008367847 | 08:00-20:00 CST Lun.-Vend 08:00-15:00 CST Samedi |

Centres d'appel mondiaux

| Région | Pays | Numéro de téléphone | Horaires |
|-------------------------------|--------------------|--|--|
| Moyen Orient + Afrique | Égypte | 800-2787349 | 09:00-18:00 Dim.-Jeu |
| | Arabie Saoudite | 800-1212787 | 09:00-18:00 Sam.-Mer |
| | EAU | 00971-42958941 | 09:00-18:00 Dim.-Jeu |
| | Turquie | 0090-2165243000 | 09:00-18:00 Lun.-Vend |
| | Afrique du Sud | 0861-278772 | 08:00-17:00 Lun.-Vend |
| | Israël | *6557/00972-39142800 *9770/00972-35598555 | 08:00-17:00 Dim.-Jeu 08:30-17:30 Dim.-Jeu |
| Pays des Balkans | Roumanie | 0040-213301786 | 09:00-18:30 Lun.-Vend |
| | Bosnie Herzégovine | 00387-33773163 | 09:00-17:00 Lun.-Vend |
| | Bulgarie | 00359-70014411 | 09:30-18:30 Lun.-Vend |
| | | 00359-29889170 | 09:30-18:00 Lun.-Vend |
| | Croatie | 00385-16401111 | 09:00-17:00 Lun.-Vend |
| | Monténégro | 00382-20608251 | 09:00-17:00 Lun.-Vend |
| | Serbie | 00381-112070677 | 09:00-17:00 Lun.-Vend |
| Slovénie | 00368-59045400 | 08:00-16:00 Lun.-Vend | |
| | 00368-59045401 | | |
| Pays Baltes | Estonie | 00372-6671796 | 09:00-18:00 Lun.-Vend |
| | Lettonie | 00371-67408838 | 09:00-18:00 Lun.-Vend |
| | Lituanie-Kaunas | 00370-37329000 | 09:00-18:00 Lun.-Vend |
| | Lituanie-Vilnius | 00370-522101160 | 09:00-18:00 Lun.-Vend |

REMARQUE : Pour plus d'informations, rendez-vous sur le site internet officiel d'ASUS sur : <https://www.asus.com/support>

| | | |
|---------------------------------------|------------------------------|--|
| Fabricant : | ASUSTeK Computer Inc. | |
| | Tél : | +886-2-2894-3447 |
| | Adresse : | 4F, No. 150, LI-TE RD., PEITOU, TAIPEI 112, TAIWAN |
| Représentant légal en Europe : | ASUS Computer GmbH | |
| | Adresse : | HARKORT STR. 21-23, 40880 RATINGEN, GERMANY |