

matériel

Routeur TpLink TL-MR3020 : Guide utilisateur

Apprenez à connaître votre Routeur

Présentation du produit

Pour répondre aux besoins sans fil de presque toutes les situations que vous pourriez rencontrer, le routeur portable TP-Link, avec plusieurs modes de fonctionnement, est conçu pour une utilisation à la maison et en voyage.

La taille portable du routeur signifie que vous pouvez le mettre dans votre poche et l'emporter avec vous partout où vous allez.

Apparence



Explication des voyants

LED	Statut	Indication
 (Power)	On	Le routeur est allumé.
	Off	Le routeur est éteint.
 (Internet)	On	Internet est disponible.
	Off	Internet n'est pas disponible.
 (Wireless)	On	Le réseau sans fil est activé.
	Off	Le réseau sans fil est désactivé.
 (WAN/LAN)	On	Le port Ethernet est connecté.
	Off	Le port Ethernet n'est pas connecté.
WPS/RESET	On	La connexion WPS a été établie.
	Clignotant	La connexion WPS est en cours d'établissement.
	Off	Aucune connexion WPS n'est établie.

Description des ports et des boutons

Élément	Description
Commutateur mode	Ce commutateur est utilisé pour déterminer le mode de fonctionnement du routeur.
Port WAN/LAN	LAN : 3G/4G (routeur 3G/4G), WISP, point d'accès, répéteur/pont WAN : 3G/4G (mode routeur 3G/4G avec sauvegarde Ewan, mode routeur sans fil, Mode routeur sans fil avec sauvegarde 3G/4G)
Port d'alimentation	Ce port est utilisé pour se connecter à l'adaptateur secteur.
Bouton WPS/RESET	Pour établir une connexion WPS, appuyez sur le bouton WPS de votre appareil, puis appuyez sur le bouton WPS/RESET de ce routeur. Pour réinitialiser le routeur, appuyez et maintenez ce bouton jusqu'à ce que tous les voyants s'allument puis relâchez-le
Port USB 3G/4G	Ce port est utilisé pour brancher un modem USB 3G/4G.

Connectez le matériel

Positionnez votre routeur

- Le produit ne doit pas être placé dans un endroit où il sera exposé à l'humidité ou chaleur excessive.
- Placez le routeur dans un endroit où il peut être connecté à plusieurs appareils ainsi qu'à une source d'alimentation.
- Assurez-vous que les câbles et le cordon d'alimentation sont placés en toute sécurité à l'écart afin qu'ils ne créent pas de risque de chute.
- Le routeur peut être placé sur une étagère ou un bureau.
- Tenez le produit éloigné des appareils présentant de fortes interférences électromagnétiques, tels que les appareils Bluetooth, les téléphones sans fil et les micro-ondes.

Connectez votre routeur

Ce routeur prend en charge cinq modes de fonctionnement : routeur 3G/4G, routeur sans fil, routeur WISP, point d'accès et répéteur/pont. Veuillez déterminer le mode de fonctionnement dont vous avez besoin et effectuer les étapes correspondantes.

Mode routeur 3G/4G

Créez instantanément un réseau sans fil privé et partagez le réseau 3G/4G avec des appareils locaux.

1. Basculez le mode de fonctionnement sur 3G/4G et connectez le matériel conformément aux étapes A à C.
2. Connectez votre appareil au routeur sans fil. Le SSID (nom du réseau sans fil) et le mot de passe se trouvent sur l'étiquette du routeur.



Mode routeur sans fil

En mode Routeur sans fil, le routeur partage l'accès Internet avec plusieurs appareils sans fil.

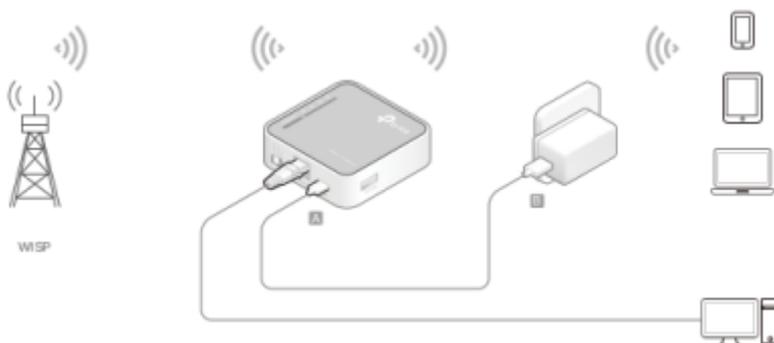
1. Basculez le mode de fonctionnement sur 3G/4G et connectez le matériel conformément aux étapes A à D.
2. Connectez votre appareil au routeur sans fil. Le SSID (nom du réseau sans fil) et le mot de passe se trouvent sur l'étiquette du routeur.



Mode routeur client WISP

En mode Routeur client WISP, le routeur permet à plusieurs utilisateurs de partager la connexion Internet à partir de WISP.

1. Basculez le mode de fonctionnement sur WISP et connectez le matériel conformément aux étapes A et B.
2. Connectez votre appareil au routeur sans fil ou via un câble Ethernet. Le SSID (nom du réseau sans fil) et le mot de passe se trouvent sur l'étiquette du routeur.



Mode point d'accès

Créez un réseau sans fil à partir d'une connexion Ethernet. Ce mode convient aux dortoirs ou aux maisons où il y a déjà un routeur filaire mais vous avez besoin d'une connexion sans fil.

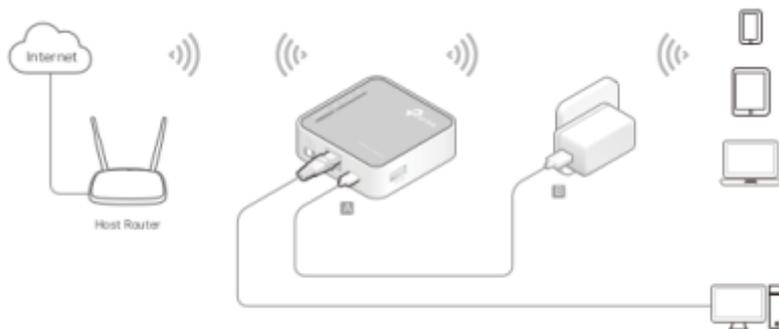
1. Basculez le mode de fonctionnement sur AP et connectez le matériel conformément aux étapes A à D.
2. Connectez sans fil votre appareil au routeur. Le SSID (nom du réseau sans fil) et le mot de passe se trouvent sur l'étiquette du routeur.



Mode Répéteur/Pont

Répète le signal d'un réseau sans fil existant. Ce mode est adapté pour étendre la couverture sans fil, en atteignant les appareils qui étaient auparavant trop éloignés de votre routeur hôte pour maintenir une connexion sans fil stable.

1. Basculez le mode de fonctionnement sur AP et connectez le matériel conformément aux étapes A et B.
2. Connectez votre appareil au routeur sans fil ou via un câble Ethernet. Le SSID (nom du réseau sans fil) et le mot de passe se trouvent sur l'étiquette du routeur.



Configurer la connexion Internet via l'assistant de configuration rapide

Connexion au routeur

Avec l'utilitaire Web, il est facile de configurer et de gérer le routeur. L'utilitaire Web peut être utilisé sur n'importe quel système d'exploitation Windows, Macintosh ou UNIX avec un navigateur Web, tel que Microsoft Internet Explorer, Mozilla Firefox ou Apple Safari.

Suivez les étapes ci-dessous pour vous connecter à votre routeur.

1. Configurez le protocole TCP/IP en mode Obtenir une adresse IP automatiquement sur votre ordinateur.
2. Visitez <http://tplinkwifi.net> et créez un mot de passe pour les futures connexions.

New Password

Low Middle High

Confirm Password

Let's Get Started

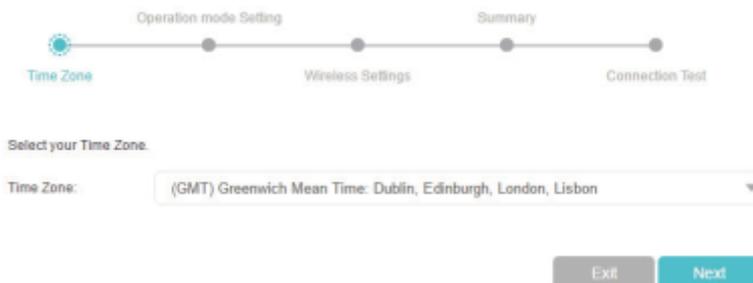


Si la fenêtre de connexion n'apparaît pas, veuillez vous référer à la section FAQ.

Configuration du routeur

Mode routeur 3G/4G

1. Sélectionnez votre fuseau horaire et cliquez sur Suivant.



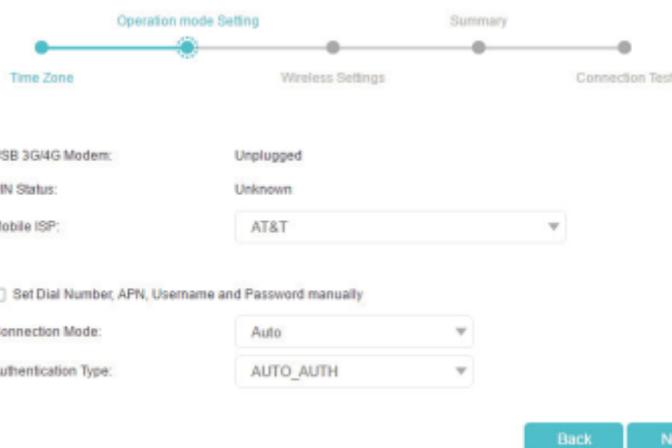
The screenshot shows a progress bar at the top with five steps: Time Zone, Operation mode Setting, Wireless Settings, Summary, and Connection Test. The 'Time Zone' step is highlighted with a blue circle. Below the progress bar, the text 'Select your Time Zone.' is followed by a dropdown menu labeled 'Time Zone:' with the selected option '(GMT) Greenwich Mean Time: Dublin, Edinburgh, London, Lisbon'. At the bottom right, there are two buttons: 'Exit' and 'Next'.

2. Sélectionnez Mode routeur 3G/4G et cliquez sur Suivant. ¹⁾



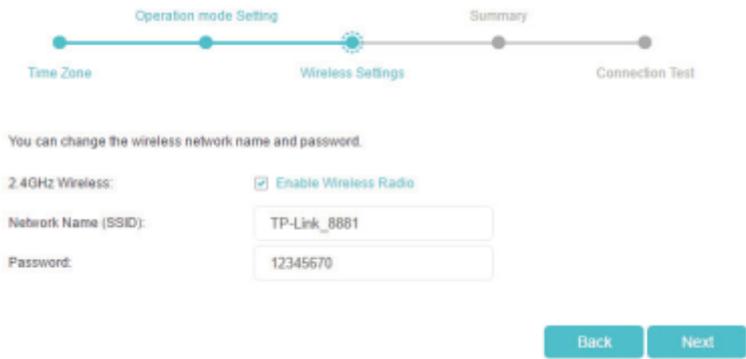
The screenshot shows the same progress bar as the previous step, but now the 'Operation mode Setting' step is highlighted with a blue circle. Below the progress bar, there are four radio button options: '3G/4G Router Mode' (selected), '3G/4G Router Mode With Ewan Backup', 'Wireless Router Mode', and 'Wireless Router Mode With 3G/4G Backup'. At the bottom right, there are two buttons: 'Back' and 'Next'.

3. Sélectionnez votre FAI mobile ou définissez-le manuellement si votre FAI n'est pas répertorié. Cliquez ensuite sur Suivant.

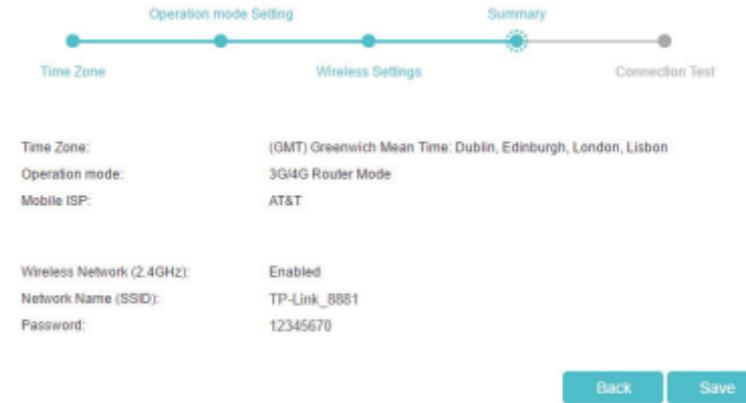


The screenshot shows the same progress bar, with 'Operation mode Setting' highlighted. Below the progress bar, there are several fields: 'USB 3G/4G Modem:' (Unplugged), 'PIN Status:' (Unknown), and 'Mobile ISP:' (AT&T). There is a checkbox for 'Set Dial Number, APN, Username and Password manually' which is unchecked. Below this, there are two dropdown menus: 'Connection Mode:' (Auto) and 'Authentication Type:' (AUTO_AUTH). At the bottom right, there are two buttons: 'Back' and 'Next'.

4. Personnalisez votre nom de réseau (SSID) et votre mot de passe ou conservez ceux par défaut, puis cliquez sur Suivant.



5. Vérifiez les paramètres sans fil et cliquez sur Enregistrer.

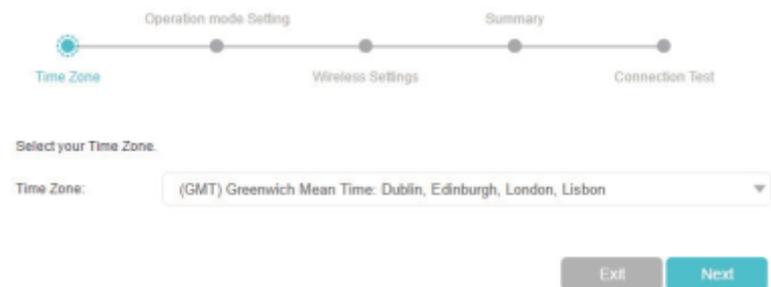


6. Cliquez sur Terminer pour terminer la configuration. Connectez maintenant vos appareils à Internet !

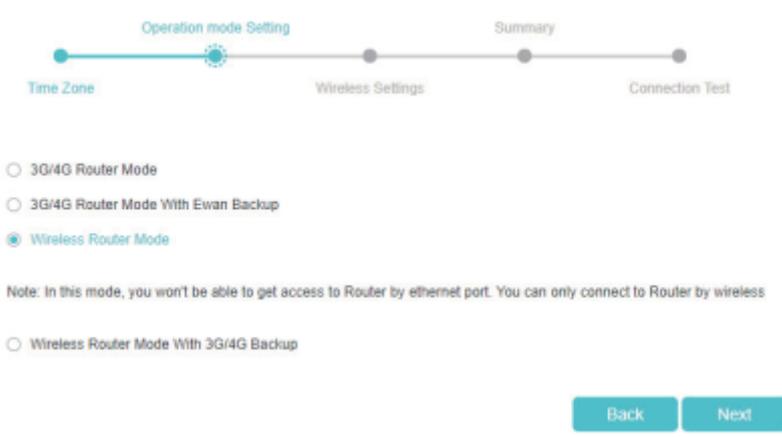


Mode routeur sans fil

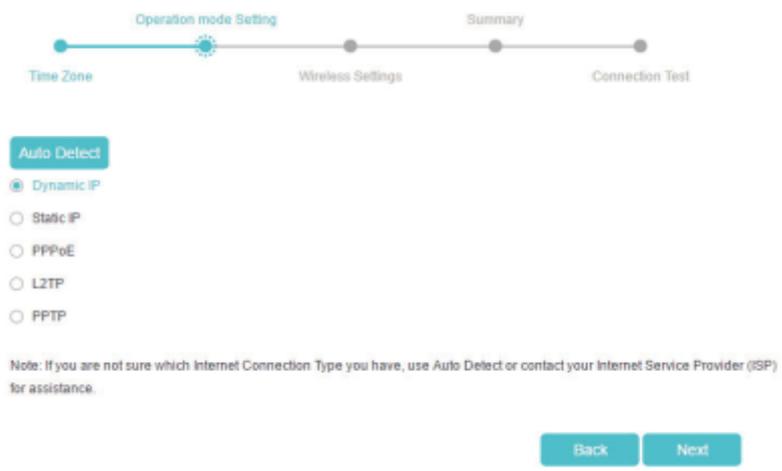
1. Sélectionnez votre fuseau horaire et cliquez sur Suivant.



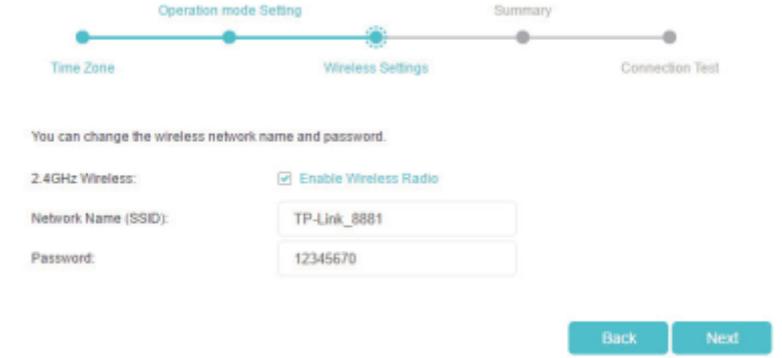
2. Sélectionnez Mode routeur sans fil et cliquez sur Suivant.²⁾



3. Sélectionnez le type de connexion Internet et entrez les paramètres correspondants. Si vous n'êtes pas sûr, cliquez sur Détection automatique. Cliquez ensuite sur Suivant et saisissez les paramètres correspondants.



4. Personnalisez votre nom de réseau (SSID) et votre mot de passe ou conservez ceux par défaut, puis cliquez sur Suivant.



5. Vérifiez les paramètres sans fil et cliquez sur Enregistrer.

Time Zone: (GMT) Greenwich Mean Time: Dublin, Edinburgh, London, Lisbon
Operation mode: Wireless Router Mode
Wan Connection Type: Dynamic IP

Wireless Network (2.4GHz): Enabled
Network Name (SSID): TP-Link_8881
Password: 12345670

Back Save

Mode routeur client WISP

1. Sélectionnez votre fuseau horaire et cliquez sur Suivant.

Select your Time Zone:
Time Zone: (GMT) Greenwich Mean Time: Dublin, Edinburgh, London, Lisbon

Exit Next

2. Cliquez sur Scan pour trouver le réseau correspondant de votre WISP. Saisissez le mot de passe du réseau sans fil sélectionné s'il est crypté. Cliquez ensuite sur Suivant.

Host 2.4GHz SSID: [input] Scan
Host 2.4GHz MAC: [input]
Security: No Security WPA/WPA2 Personal WEP

Back Next

3. Sélectionnez le type de connexion Internet. Cliquez ensuite sur Suivant et saisissez les paramètres correspondants.

Dynamic IP
 Static IP
 PPPoE
 L2TP
 PPTP

Back Next

4. Personnalisez votre nom de réseau (SSID) et votre mot de passe ou conservez ceux par défaut,

You can change the wireless network name and password.

2.4GHz Wireless: Enable Wireless Radio

Network Name (SSID):

Password:

puis cliquez sur Suivant.

5. Cliquez sur Enregistrer pour terminer la configuration.

Time Zone: (GMT) Greenwich Mean Time: Dublin, Edinburgh, London, Lisbon

Operation mode: WISP

Wan Connection Type: Dynamic IP

Host Network (2.4GHz): Enabled

Host Network Name (SSID): Deco test

Security: PSK2Authentication&AESEncryption

Password: 12345670

Wireless Network (2.4GHz): Enabled

Network Name (SSID): TP-Link_8881

Password: 12345670

Mode point d'accès

1. Sélectionnez votre fuseau horaire et cliquez sur Suivant.

Select your Time Zone.

Time Zone:

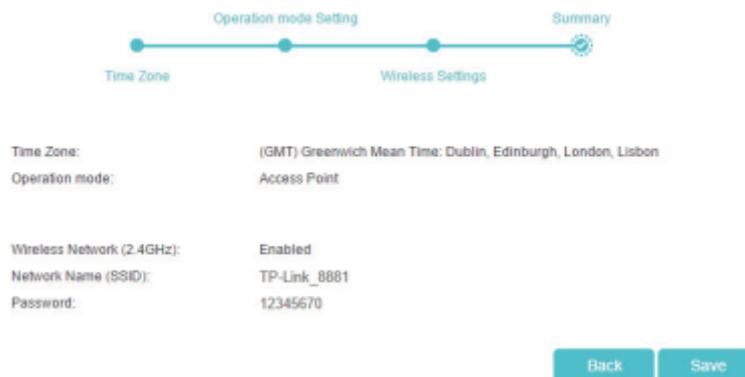
2. Sélectionnez Mode point d'accès et cliquez sur Suivant.



3. Personnalisez votre nom de réseau (SSID) et votre mot de passe ou conservez ceux par défaut, puis cliquez sur Suivant.

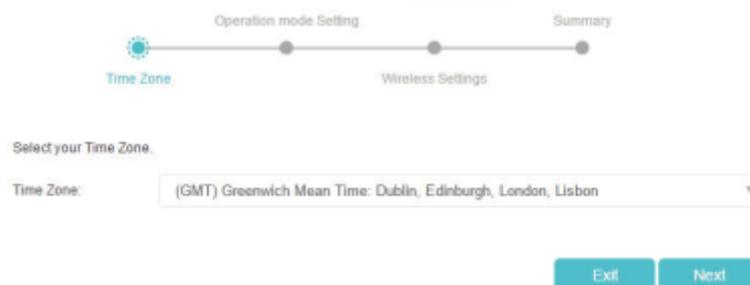


4. Cliquez sur Enregistrer pour terminer la configuration.



Mode Répéteur/Pont

1. Sélectionnez votre **fuseau horaire** et cliquez sur **Suivant**



2. Sélectionnez Mode Répéteur/Pont et cliquez sur Suivant.



3. Cliquez sur **Scan** pour trouver le réseau que vous souhaitez étendre. Saisissez le **mot de passe** du réseau sans fil sélectionné s'il est crypté. Cliquez ensuite sur **Suivant**.



4. Personnalisez votre **nom de réseau (SSID)** et votre **mot de passe** ou conservez ceux par défaut, puis cliquez sur **Suivant**.



5. Cliquez sur **Enregistrer** pour terminer la configuration.
6. Déplacez le routeur à mi-chemin entre votre routeur hôte et la zone morte Wi-Fi.

Réseau invité

Cette fonction vous permet de fournir un accès Wi-Fi aux invités sans divulguer votre réseau principal. Lorsque vous avez des invités dans votre maison, appartement ou lieu de travail, vous pouvez créer un réseau d'invités pour eux. De plus, vous pouvez personnaliser les options du réseau invité pour garantir la sécurité et la confidentialité du réseau. Le réseau invité n'est pris en charge que par le mode routeur.

Créer un réseau pour les invités

1. Visitez <http://tplinkwifi.net> et connectez-vous avec le mot de passe que vous avez défini pour le routeur.
2. Allez à **Avancé > Réseau invité**. Localisez la section **Sans fil**.
3. Créez un réseau d'invités comme voulu.
 1. Cochez la case **Activer le réseau invité**.
 2. Personnalisez le SSID. Ne sélectionnez pas **Masquer le SSID** sauf si vous souhaitez que vos invités saisissent manuellement le SSID pour l'accès au réseau invité.
 3. Définissez **Sécurité** sur **WPA/WPA2 Personnel**, conservez les valeurs par défaut **Version** et **Cryptage** et personnalisez votre propre mot de passe.

The screenshot shows the 'Wireless' settings page. Under '2.4GHz Wireless:', the 'Enable Guest Network' checkbox is checked. The 'Network Name (SSID):' field contains 'TP-Link_Guest_28ED' and the 'Hide SSID' checkbox is unchecked. The 'Security:' section has 'WPA/WPA2-Personal' selected. The 'Version:' section has 'Auto' selected. The 'Encryption:' section has 'Auto' selected. The 'Password:' field contains '12345670'. A 'Save' button is located at the bottom right of the form.

4. Cliquez sur **Enregistrer**. Vos invités peuvent désormais accéder à votre réseau invité en utilisant le SSID et le mot de passe que vous avez définis !

Personnaliser les options du réseau invité

1. Visitez <http://tplinkwifi.net> et connectez-vous avec le mot de passe que vous avez défini pour le routeur.
2. Accédez à **Avancé > Réseau d'invités**. Localisez la section **Paramètres**.
3. Personnalisez les options du réseau invité selon vos besoins.

The screenshot shows the 'Settings' page for guest network options. There are three checkboxes: 'Allow Guests to Access Each Other' (checked), 'Allow Guests to Access My Local Network' (unchecked), and 'Enable guest network bandwidth control' (unchecked). A 'Save' button is located at the bottom right of the form.

- **Autoriser les invités à se connecter les uns aux autres** : Cochez cette case si vous souhaitez autoriser les clients sans fil de votre réseau invité à communiquer entre eux via des méthodes telles que le voisinage réseau et Ping.
- **Autoriser les invités à accéder à mon réseau local (en mode routeur)** : Cochez cette case si vous souhaitez autoriser les clients sans fil sur votre réseau invité à communiquer avec les appareils connectés aux ports LAN de votre routeur ou au réseau principal via des méthodes telles que le voisinage réseau et Ping.
- **Activer le contrôle de la bande passante du réseau invité** : Cochez cette case si vous souhaitez appliquer les paramètres de contrôle de la bande passante aux périphériques sans fil de votre réseau invité.

4. Cliquez sur Enregistrer. Vous pouvez désormais garantir la sécurité et la confidentialité du réseau !

Contrôle parental

Cette fonction vous permet de bloquer les sites Web inappropriés, explicites et malveillants, et de contrôler l'accès à des sites Web spécifiés à une heure spécifiée. Le contrôle parental n'est pris en charge que par le mode Routeur.

Je veux Contrôler les heures de la journée où mes enfants ou d'autres utilisateurs du réseau domestique sont autorisés à accéder à Internet et même aux types de sites Web qu'ils peuvent visiter.

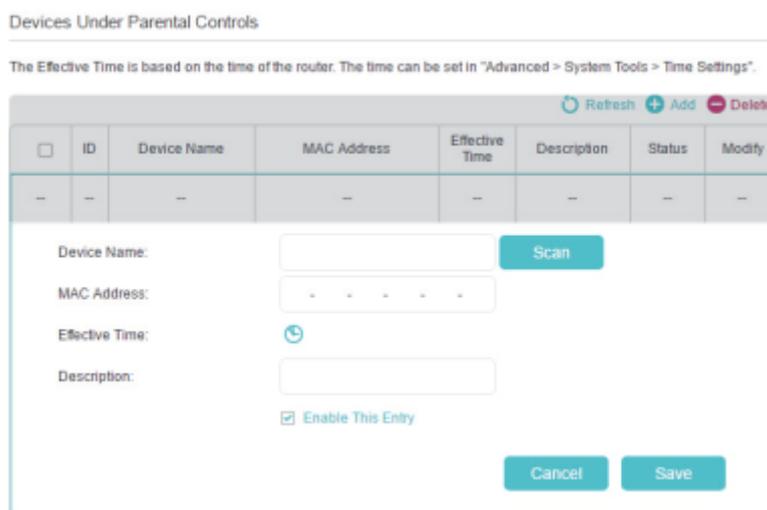
Par exemple, je souhaite autoriser les appareils de mes enfants (par exemple un ordinateur ou une tablette) à accéder uniquement à www.tp-link.com et Wikipedia.org de 18h00 à 22h00 le week-end et pas d'autres fois.

Pour cela :

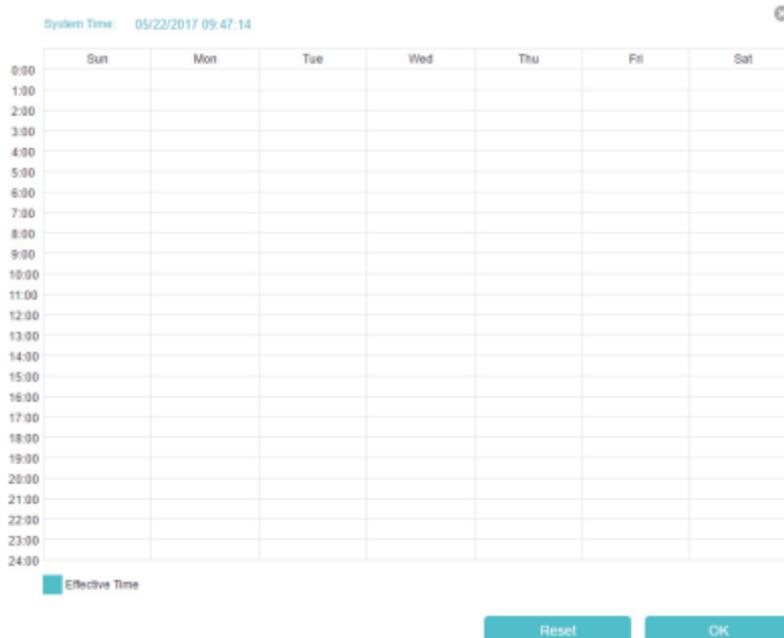
1. Visitez <http://tplinkwifi.net> et connectez-vous avec le mot de passe que vous avez défini pour le routeur.
2. Allez dans **Avancé > Contrôle Parental** et activez le **Contrôle Parental**.



3. Cliquez sur Ajouter. Et puis cliquez sur Scan, et sélectionnez le périphérique d'accès. Ou saisissez manuellement le nom du périphérique et l'adresse MAC.

A screenshot of the 'Devices Under Parental Controls' section. It shows a table with columns: ID, Device Name, MAC Address, Effective Time, Description, Status, and Modify. Below the table is a form to add a new device. The form includes fields for 'Device Name', 'MAC Address', 'Effective Time' (with a clock icon), and 'Description'. There is a 'Scan' button next to the Device Name field, an 'Enable This Entry' checkbox, and 'Cancel' and 'Save' buttons at the bottom.

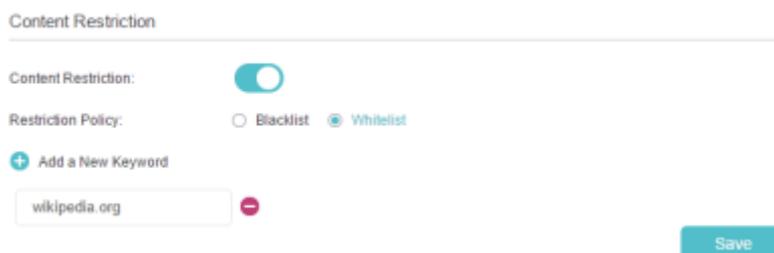
4. Cliquez sur l'icône ⌚ pour définir l'heure d'accès à Internet. Faites glisser le curseur sur la ou les cellules appropriées et cliquez sur OK.



- 5. Saisissez une **description** pour l'entrée, cochez la case **Activer cette entrée**, puis cliquez sur **OK**.
- 6. Sélectionnez **Liste blanche** comme stratégie de restriction.



- Lorsque **liste noire** est sélectionnée, les appareils contrôlés ne peuvent accéder à aucun site Web contenant les mots-clés spécifiés pendant la période d'accès Internet.
 - Lorsque **liste blanche** est sélectionnée, les appareils contrôlés ne peuvent accéder qu'aux sites Web contenant les mots-clés spécifiés pendant la période d'accès Internet.
7. Cliquez sur **+ Add a New Keyword** . Entrez un site Web et cliquez sur Enregistrer. Vous pouvez ajouter jusqu'à 32 mots-clés pour la liste noire ou la liste blanche. Vous trouverez ci-dessous quelques exemples d'entrées pour autoriser l'accès.
- Pour la liste blanche : saisissez une adresse Web (par exemple, wikipedia.org) pour autoriser l'accès uniquement à ses sites Web connexes. Si vous souhaitez bloquer tout accès à la navigation Internet, n'ajoutez aucun mot-clé à la liste blanche.
 - Pour la liste noire : spécifiez une adresse Web (par exemple, wikipedia.org), un mot-clé d'adresse Web (par exemple, wikipedia) ou un suffixe de domaine (par exemple, .edu ou .org) pour bloquer l'accès uniquement aux sites Web contenant ce mot-clé ou ce suffixe.



Terminé ! Vous pouvez désormais contrôler l'accès Internet de vos enfants selon les

besoins.

Contrôle de bande passante

Ce chapitre explique comment définir des limites de bande passante afin de minimiser l'impact causé lorsque la connexion est soumise à une charge importante. Le contrôle de la bande passante n'est pris en charge que par le mode Routeur.

Définir la bande passante montante et descendante

1. Visitez <http://tplinkwifi.net> et connectez-vous avec le mot de passe que vous avez défini pour le routeur.
2. Accédez à **Avancé > Contrôle de la bande passante**.
3. Activez **Contrôle de la bande passante** et saisissez la **Bande passante totale en amont** et la **Bande passante totale en aval**.

Bandwidth Control

Bandwidth Control: Enable

Total Upstream Bandwidth: Kbps

Total Downstream Bandwidth: Kbps

Save

4. Cliquez sur **Enregistrer**.

Règles de contrôle

1. Visitez <http://tplinkwifi.net> et connectez-vous avec le mot de passe que vous avez défini pour le routeur.
2. Accédez à **Avancé > Contrôle de la bande passante**.
3. Cliquez sur **Ajouter** et remplissez les champs.

Controlling Rules

<input type="checkbox"/>	IP Range/Port Range	Priority	Up (min/max)	Down (min/max)	Status	Modify
--	--	--	--	--	--	--

IP Range: -

Port Range: - (1-65535)

Protocol: ALL ▾

Priority: 5 ▾ (1 means the highest priority.)

Upstream: to Kbps

Downstream: to Kbps

Enable This Entry

Cancel Save

- **Plage IP** : saisissez la plage IP de vos appareils auxquels vous souhaitez appliquer le contrôle de la bande passante.
- **Plage de ports** : saisissez la plage de ports des protocoles.
- **Protocole** : sélectionnez les protocoles des services que vous souhaitez contrôler.
- **Priorité** : Sélectionnez la priorité de 1 à 5. 1 signifie la priorité la plus élevée.
- **montant/descendant** : saisissez la bande passante minimale et maximale montante/descendante que vous souhaitez allouer.
- Cliquez sur **Enregistrer**.

Sécurité réseau

Ce chapitre vous explique comment protéger votre réseau domestique contre les cyberattaques et les utilisateurs non autorisés en mettant en œuvre ces trois fonctions de sécurité réseau. Vous pouvez protéger votre réseau domestique contre les attaques DoS (Denial of Service), inondation de votre réseau par des demandes de serveur à l'aide de la protection DoS, bloquer ou autoriser des périphériques clients spécifiques à accéder à votre réseau à l'aide du contrôle d'accès, ou vous pouvez empêcher l'usurpation d'identité ARP et les attaques ARP à l'aide d'IP & Liaison MAC. Certaines fonctionnalités ne sont prises en charge que par un certain mode.

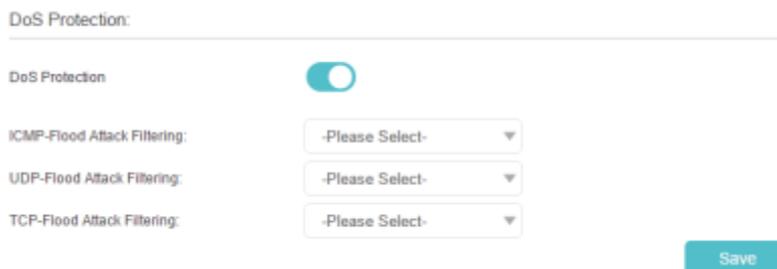
Protéger le réseau contre les cyberattaques

Le pare-feu SPI (Stateful Packet Inspection) et la protection DoS (Denial of Service) protègent le routeur des cyberattaques.

Le pare-feu SPI peut empêcher les cyberattaques et valider le trafic qui passe via le routeur en fonction du protocole. Cette fonction est activée par défaut, et il est recommandé de conserver les paramètres par défaut.

La protection DoS peut protéger votre réseau domestique contre les attaques DoS qui inondent votre réseau de requêtes de serveur. Suivez les étapes ci-dessous pour configurer la protection DoS.

1. Visitez <http://tplinkwifi.net> et connectez-vous avec le mot de passe que vous avez défini pour le routeur.
2. Allez à **Avancé > Sécurité > Pare-feu et protection DoS**.
3. Activez la **Protection DoS**.



4. Réglez le niveau (faible, moyen ou élevé) de protection pour le **filtrage d'attaque ICMP-FLOOD**, le **filtrage des attaques UDP-FLOOD** et le **filtrage des attaques TCP-SYN-FLOOD**.³⁾
 - **Filtrage des attaques ICMP-FLOOD** - Activer pour empêcher l'attaque par inondation ICMP (Internet Control Message Protocol).
 - **UDP-FLOOD Attack Filtering** - Activer pour empêcher l'attaque par inondation UDP (User Datagram Protocol).
 - **Filtrage des attaques TCP-SYN-FLOOD** - Activer pour empêcher l'attaque par inondation TCP-SYN (Transmission Control Protocol-Synchronize).

Blocked DoS Host List

Host Number: 0 Refresh Delete

<input type="checkbox"/>	ID	IP Address	MAC Address
<input type="checkbox"/>	--	--	--

- Cliquez sur Enregistrer.

Filtrage des services

Le filtrage de service est utilisé pour empêcher certains utilisateurs d'accéder à un service spécifique. Il peut même empêcher un utilisateur d'accéder à Internet.

1. Visitez <http://tplinkwifi.net> et connectez-vous avec le mot de passe que vous avez défini pour le routeur.
2. Allez dans Avancé > **Sécurité > Filtrage des services**.
3. Activez le filtrage des services.



4. Cliquez sur Ajouter.

Filtering List

<input type="checkbox"/>	ID	Service Type	Port	IP Address	Status	Modify
--	--	--	--	--	--	--

Refresh + Add - Delete

Service Type: Any(ALL)

Protocol: TCP/UDP

Starting Port: 1 (1-65535)

Ending Port: 65535 (1-65535)

Service Type: Any(ALL)

Filter Service For: Single IP Address IP Address Range All IP Addresses

Cancel Save

- Sélectionnez un type de service dans la liste déroulante et les paramètres correspondants seront automatiquement renseignés. Sélectionnez Personnalisé si le type de service souhaité n'est pas répertorié et entrez les paramètres correspondants.
- Spécifiez la ou les adresses IP auxquelles cette règle de filtrage sera appliquée.
- Cliquez sur Enregistrer.

Contrôle d'accès

Le contrôle d'accès est utilisé pour bloquer ou autoriser des périphériques clients spécifiques à accéder à votre réseau (via filaire ou sans fil) en fonction d'une liste de périphériques bloqués (liste noire) ou d'une liste de périphériques autorisés (liste blanche).

Comment bloquer ou autoriser des périphériques clients spécifiques à accéder à mon réseau (avec ou sans fil) ?

- Visitez <http://tplinkwifi.net> et connectez-vous avec le mot de passe que vous avez défini pour le routeur.
- Accédez à Avancé > Sécurité > Contrôle d'accès ou Paramètres > Sécurité > Contrôle d'accès.
- Activez le contrôle d'accès.

Access Control

Access Control:

- Sélectionnez le mode d'accès pour bloquer (recommandé) ou autoriser le(s) périphérique(s) dans la liste.
 - Pour bloquer un ou plusieurs appareils spécifiques :
 - Sélectionnez Liste noire et cliquez sur Enregistrer.

Access Mode

Default Access Mode: Blacklist Whitelist

Save

2. Sélectionnez le ou les appareils à bloquer dans le tableau Appareils en ligne en cochant la ou les cases.
3. Cliquez sur Bloquer au-dessus du tableau Appareils en ligne. Les appareils sélectionnés seront automatiquement ajoutés aux appareils de la liste noire.



The screenshot shows a table titled 'Online Devices' with columns: ID, Device Name, IP Address, MAC Address, Connection Type, and Modify. There are two rows of data. The first row is selected with a checkmark in the ID column. A 'Block' button is highlighted in a red box in the top right corner of the table area.

ID	Device Name	IP Address	MAC Address	Connection Type	Modify
1	Roses iPhone	192.168.0.175	1C-1A-C0-3B-28-4B	Wireless	
2	ADMIN PC	192.168.0.157	C0-4A-00-1A-C3-45	Wireless	

2. Pour autoriser des appareils spécifiques :
 1. Sélectionnez la liste blanche et cliquez sur Enregistrer



The screenshot shows the 'Access Mode' form. It has a 'Default Access Mode' section with two radio buttons: 'Blacklist' and 'Whitelist'. The 'Whitelist' radio button is selected. There is a 'Save' button at the bottom right.

2. Cliquez sur Ajouter dans la section Appareils dans la liste blanche. Saisissez le nom de l'appareil et l'adresse MAC (vous pouvez copier et coller les informations de la liste des appareils en ligne si l'appareil est connecté à votre réseau).



The screenshot shows the 'Devices In Whitelist' form. It has a table with columns: ID, Device Name, MAC Address, and Modify. Below the table are input fields for 'Device Name' and 'MAC Address'. There are 'Cancel' and 'OK' buttons at the bottom right.

3. Click OK

Terminé ! Vous pouvez désormais bloquer ou autoriser des périphériques clients spécifiques à accéder à votre réseau (avec ou sans fil) à l'aide de la liste noire ou de la liste blanche.

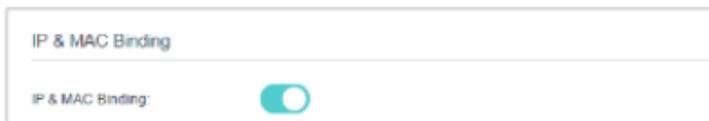
Liaison IP et MAC

La liaison IP et MAC, à savoir la liaison ARP (Address Resolution Protocol), est utilisée pour lier l'adresse IP du périphérique réseau à son adresse MAC. Cela empêchera l'usurpation ARP et d'autres attaques ARP en refusant

l'accès réseau à un périphérique avec une adresse IP correspondante dans la liste de liaison, mais une adresse MAC non reconnue.

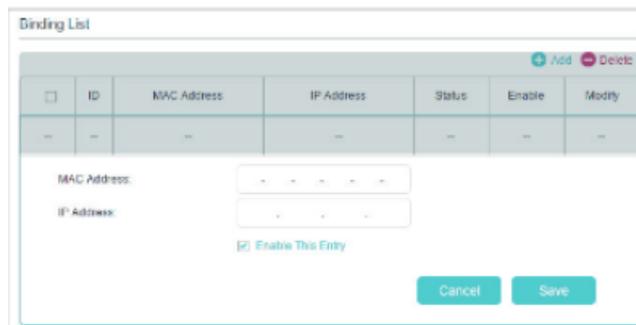
Pour empêcher l'usurpation d'identité ARP et les attaques ARP :

1. Visitez <http://tplinkwifi.net> et connectez-vous avec le mot de passe que vous avez défini pour le routeur.
2. Accédez à Avancé > Sécurité > Liaison IP et MAC.
3. Activez la liaison IP et MAC.



4. Liez votre ou vos appareils en fonction de vos besoins. Pour lier l'appareil ou les appareils connectés : Cliquez pour ajouter l'appareil correspondant à la liste de liaison. Pour lier l'appareil non connecté :

1. Cliquez sur Ajouter dans la section Liste de liaison.



2. Saisissez l'adresse MAC et l'adresse IP que vous souhaitez lier.
3. Cochez la case Activer cette entrée et cliquez sur Enregistrer.

Terminé ! Désormais, vous n'avez plus à vous soucier de l'usurpation d'identité ARP et des attaques ARP !

Transfert NAT

La fonction NAT (Network Address Translation) du routeur permet aux appareils du réseau local d'utiliser la même adresse IP publique pour communiquer avec les appareils sur Internet, ce qui protège le réseau local en masquant les adresses IP des appareils. Cependant, cela pose également le problème qu'un hôte externe ne peut pas initier une communication de manière initiative avec un

périphérique spécifié sur le réseau local.

Grâce à la fonction de transfert, le routeur peut pénétrer l'isolement de NAT et permet aux appareils sur Internet de communiquer de manière initiative avec des appareils sur le réseau local, réalisant ainsi certaines fonctions spéciales.

Le routeur TP-Link prend en charge quatre règles de transfert. Si deux règles ou plus sont définies, la priorité de mise en œuvre de haut en bas est Serveurs virtuels, Déclenchement de port, UPNP et DMZ.

Le transfert NAT n'est pris en charge que par le mode Routeur.

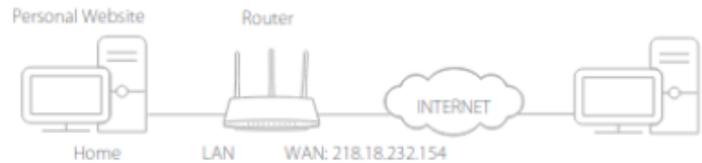
Partager des ressources locales sur Internet par des serveurs virtuels

Lorsque vous créez un serveur sur le réseau local et que vous souhaitez le partager sur Internet, les serveurs virtuels peuvent réaliser le service et le fournir aux internautes. Dans le même temps, les serveurs virtuels peuvent protéger le réseau local, car les autres services sont toujours invisibles sur Internet.

Les serveurs virtuels peuvent être utilisés pour configurer des services publics sur votre réseau local, tels que HTTP, FTP, DNS, POP3/SMTP et Telnet. Différents services utilisent différents ports de service. Le port 80 est utilisé dans le service HTTP, le port 21 dans le service FTP, le port 25 dans le service SMTP et le port 110 dans le service POP3. Veuillez vérifier le numéro de port de service avant la configuration.

Je veux partager mon site Web personnel que j'ai construit sur mon réseau local avec mes amis via Internet.

Par exemple, le site Web personnel a été créé sur mon PC personnel (192.168.1.100). J'espère que mes amis sur Internet pourront visiter mon site Web d'une manière ou d'une autre. Le PC est connecté au routeur avec l'adresse IP WAN 218.18.232.154.



Comment faire cela ?

1. Attribuez une adresse IP statique à votre PC, par exemple 192.168.1.100.
2. Visitez <http://tplinkwifi.net> et connectez-vous avec le mot de passe que vous avez défini pour le routeur.
3. Accédez à Avancé > Transfert NAT > Serveurs virtuels.
4. Cliquez sur Ajouter. Cliquez sur Afficher les services existants et sélectionnez HTTP. Le port externe, le port interne et le protocole seront automatiquement renseignés. Saisissez l'adresse IP du PC 192.168.0.100 dans le champ IP interne.
5. Cliquez sur OK.

ID	Service Type	External Port	Internal IP	Internal Port	Protocol	Status	Modify
--	--	--	--	--	--	--	--

Service Type: [View Existing Services](#)

External Port: (XX-XXX or XXX)

Internal IP:

Internal Port: (XX or Blank, 1-65535)

Protocol:

Enable This Entry

- Il est recommandé de conserver les paramètres par défaut du port et du protocole internes si vous n'êtes pas sûr du port et du protocole à utiliser.



- Si le service que vous souhaitez utiliser n'est pas dans le type de service, vous pouvez saisir les paramètres correspondants manuellement. Vous devez vérifier le numéro de port dont le service a besoin.



- Vous pouvez ajouter plusieurs règles de serveur virtuel si vous souhaitez fournir plusieurs services dans un routeur. Veuillez noter que le port externe ne doit pas se chevaucher.

Terminé ! Les utilisateurs sur Internet peuvent saisir <http://WAN IP> (dans cet exemple : <http://218.18.232.154>) pour visiter votre site Web personnel.

- L'adresse IP WAN devient une adresse IP publique. Pour que l'IP WAN soit attribuée dynamiquement par le FAI, il est recommandé d'appliquer et d'enregistrer un nom de domaine pour le WAN en se référant à **Configurer un compte de service DNS dynamique**. Les utilisateurs sur Internet peuvent alors utiliser <http://nom de domaine> pour visiter le site Web.
- Si vous avez modifié le port externe par défaut, vous devez utiliser <http://WAN IP:port externe> ou <http://nom de domaine:port externe> pour visiter le site Web.

Ouvrir des ports dynamiquement par déclenchement de port

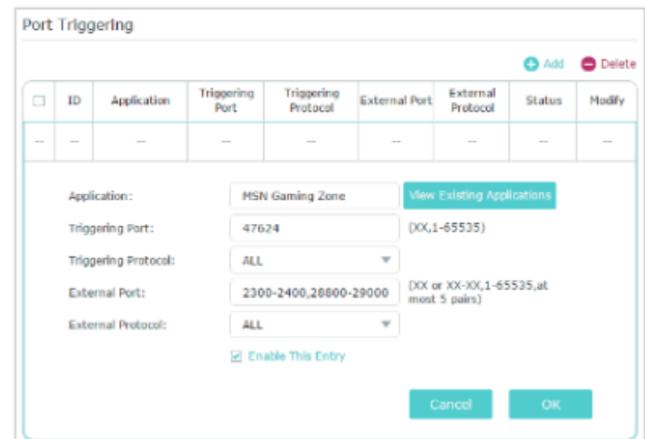
Le déclenchement de port peut spécifier un port de déclenchement et ses ports externes correspondants. Lorsqu'un hôte sur le réseau local initie une connexion au port de déclenchement, tous les ports externes seront ouverts pour les connexions suivantes. Le routeur peut enregistrer l'adresse IP de l'hôte. Lorsque les données d'Internet retournent aux ports externes, le routeur peut les transmettre à l'hôte correspondant. Le déclenchement de port est principalement appliqué aux jeux en ligne, aux VoIP, aux lecteurs vidéo et aux applications courantes, notamment MSN Gaming Zone, Dialpad et Quick Time 4, etc.

Suivez les étapes ci-dessous pour configurer les règles de déclenchement de port :

1. Visitez <http://tplinkwifi.net> et connectez-vous

avec le mot de passe que vous avez défini pour le routeur.

2. Accédez à Avancé > Transfert NAT > Déclenchement de port et cliquez sur Ajouter.
3. Cliquez sur Afficher les applications existantes et sélectionnez l'application souhaitée. Le port de déclenchement, le port externe et le protocole seront automatiquement renseignés. L'image suivante prend comme exemple l'application MSN Gaming Zone.
4. Cliquez sur OK.



ID	Application	Triggering Port	Triggering Protocol	External Port	External Protocol	Status	Modify
--	--	--	--	--	--	--	--

Application: MSN Gaming Zone [View Existing Applications](#)

Triggering Port: 47624 (XX,1-65535)

Triggering Protocol: ALL

External Port: 2300-2400,28800-29000 (XX or XX-XX,1-65535,at most 5 pairs)

External Protocol: ALL

Enable This Entry

Cancel OK

- Vous pouvez ajouter plusieurs règles de déclenchement de port en fonction des besoins de votre réseau.
- Les ports de déclenchement ne peuvent pas se chevaucher.
- Si l'application dont vous avez besoin n'est pas répertoriée dans la liste Applications existantes, veuillez saisir les paramètres manuellement. Vous devez d'abord vérifier les ports externes que l'application utilise et les saisir dans le champ Port externe en fonction du format affiché par la page.



Rendre les applications exemptes de restriction de port par DMZ

Lorsqu'un PC est configuré pour être un hôte DMZ (zone démilitarisée) sur le réseau local, il est totalement exposé à Internet, ce qui peut réaliser la communication bidirectionnelle illimitée entre les hôtes internes et les hôtes externes. L'hôte DMZ devient un serveur virtuel avec tous les ports ouverts. Lorsque vous ne savez pas exactement quels ports ouvrir dans certaines applications spéciales, telles qu'une caméra IP et un logiciel de base de données, vous pouvez configurer le PC en tant qu'hôte DMZ.



Lorsque DMZ est activé, l'hôte DMZ est totalement exposé à Internet, ce qui peut entraîner des risques potentiels pour la sécurité. Si la DMZ n'est pas utilisée, veuillez la désactiver à temps.

Je souhaite que le PC domestique rejoigne le jeu en ligne sur Internet sans restriction de port.

Par exemple, en raison de certaines restrictions de port, lorsque vous jouez aux jeux en ligne, vous pouvez vous connecter normalement mais ne pouvez pas rejoindre une équipe avec d'autres joueurs. Pour résoudre ce problème, configurez votre PC en tant qu'hôte DMZ avec tous les ports ouverts.

Comment puis je faire ça?

1. Attribuez une adresse IP statique à votre PC, par exemple 192.168.1.100.
2. Visitez <http://tplinkwifi.net> et connectez-vous avec le mot de passe que vous avez défini pour le routeur.
3. Accédez à Avancé > Transfert NAT > DMZ et sélectionnez Activer DMZ.
4. Saisissez l'adresse IP 192.168.1.100 dans le champ DMZ Host IP Address.



5. Cliquez sur Enregistrer.

Terminé! La configuration est terminée. Vous avez configuré votre PC sur un hôte DMZ et vous pouvez maintenant former une équipe pour jouer avec d'autres joueurs.

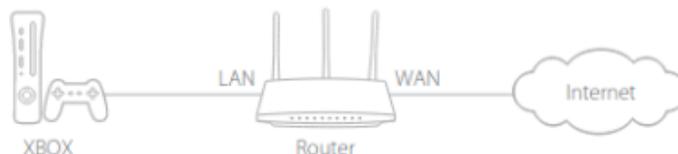
Faites en sorte que les jeux en ligne Xbox fonctionnent en douceur grâce à UPnP

Le protocole UPnP (Universal Plug and Play) permet aux applications ou aux périphériques hôtes de trouver automatiquement le périphérique NAT frontal et de lui envoyer une demande d'ouverture des ports correspondants. Lorsque l'UPnP est activé, les applications ou les périphériques hôtes sur le réseau local et Internet peuvent communiquer librement les uns avec les autres, réalisant ainsi la connexion transparente du réseau. Vous devrez peut-être activer l'UPnP si vous souhaitez utiliser des applications pour les jeux multijoueurs, les connexions peer-to-peer, la communication en temps réel (telle que la VoIP ou la conférence téléphonique) ou l'assistance à distance, etc.



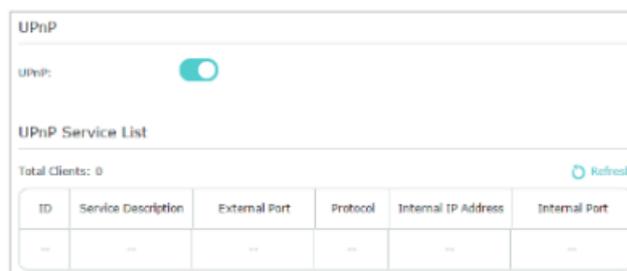
- UPnP est activé par défaut sur ce routeur.
- Seule l'application prenant en charge le protocole UPnP peut utiliser cette fonctionnalité.
- La fonction UPnP nécessite la prise en charge du système d'exploitation (par exemple, Windows Vista/Windows 7/Windows 8, etc. Certains systèmes d'exploitation doivent installer les composants UPnP).

Par exemple, lorsque vous connectez votre Xbox au routeur qui s'est connecté à Internet pour jouer à des jeux en ligne, UPnP enverra une demande au routeur pour ouvrir les ports correspondants permettant aux données suivantes pénétrant le NAT de transmettre. Par conséquent, vous pouvez jouer à des jeux en ligne Xbox sans accroc.



Si nécessaire, vous pouvez suivre les étapes pour modifier l'état de l'UPnP.

1. Visitez <http://tplinkwifi.net> et connectez-vous avec le mot de passe que vous avez défini pour le routeur.
2. Allez dans Avancé > Transfert NAT > UPnP et activez ou désactivez selon vos besoins.



VPN

La fonction VPN (Virtual Private Networking) vous permet d'accéder à votre réseau domestique de manière sécurisée via Internet lorsque vous n'êtes pas chez vous.

Le VPN n'est pris en charge que par le mode Routeur.

Avec IPSec VPN, vous pouvez accéder au réseau en toute sécurité lorsque vous n'êtes pas chez vous. Pour utiliser le service VPN, vous devez configurer le service DNS dynamique ou attribuer une adresse IP statique au port WAN du routeur. Et l'heure système doit être synchronisée avec Internet.

1. Visitez <http://tplinkwifi.net> et connectez-vous avec le mot de passe que vous avez défini pour le routeur.

2. Allez dans Avancé > VPN > VPN IPsec.
3. Activez la détection des pairs morts.

IPsec VPN

Dead Peer Detection:



4. Cliquez sur Ajouter et entrez les paramètres correspondants.

<input type="checkbox"/>	Connection Name	Remote Gateway	Local Address	Remote Address	Status	Enable	Modify
--	--	--	--	--	--	--	--

+ Add - Delete

IPsec Connection Name:

Remote IPsec Gateway (URL):

Tunnel access from local IP addresses:

IP Address for VPN:

Subnet Mask:

Tunnel access from remote IP addresses:

IP Address for VPN:

Subnet Mask:

Key Exchange Method:

Authentication Method:

Pre-Shared Key:

Perfect Forward Secrecy:

Advanced

- Nom de la connexion IPsec : saisissez un nom pour la connexion VPN IPsec.
- Passerelle IPsec distante (URL) : saisissez l'adresse IP de la passerelle de destination qui est l'adresse IP publique du WAN ou le nom de domaine du point de terminaison du serveur VPN distant.
- Accès au tunnel à partir d'adresses IP locales : sélectionnez Adresse de sous-réseau si vous souhaitez que l'ensemble du réseau local rejoigne le réseau VPN, ou sélectionnez Adresse unique si vous souhaitez qu'une seule adresse IP rejoigne le réseau VPN.
- Adresse IP pour VPN : Saisissez l'adresse IP de votre réseau local.
- Masque de sous-réseau : saisissez le masque de sous-réseau de votre réseau local.
- Accès tunnel à partir d'adresses IP distantes : sélectionnez Adresse de sous-réseau si vous souhaitez que l'ensemble du réseau local distant rejoigne le réseau VPN, ou sélectionnez Adresse unique si

vous souhaitez qu'une seule adresse IP rejoigne le réseau VPN.

- Adresse IP pour VPN : saisissez l'adresse IP du réseau local distant.
- Masque de sous-réseau IP : saisissez le masque de sous-réseau du réseau local distant.
- Méthode d'échange de clés : sélectionnez Auto (IKE) ou Manuel à utiliser pour authentifier les pairs IPSec.
- Méthode d'authentification : sélectionnez la clé pré-partagée (recommandée).
- Clé pré-partagée : créez une clé pré-partagée à utiliser pour l'authentification.
- Perfect Forward Secrecy : sélectionnez Activer ou Désactiver comme protocole de sécurité supplémentaire pour la clé pré-partagée.
Vous pouvez configurer les paramètres avancés selon vos besoins. Il est recommandé de conserver les valeurs par défaut. Si vous souhaitez modifier ces paramètres, assurez-vous que les deux points de terminaison du serveur VPN utilisent les mêmes algorithmes de chiffrement, algorithme d'intégrité, groupe Diffie-Hellman et durée de vie de la clé en phase1 et en phase2.
- Cliquez sur Enregistrer.

Personnalisez vos paramètres réseau

Ce chapitre vous explique comment configurer les fonctionnalités réseau avancées. Certaines fonctionnalités ne sont prises en charge que par un certain mode.

Modifier les paramètres du réseau local

Le routeur est prédéfini avec une IP LAN par défaut 192.168.1.1, que vous pouvez utiliser pour vous connecter à sa page de gestion Web.

L'adresse IP LAN ainsi que le masque de sous-réseau définissent également le sous-réseau sur lequel se trouvent les appareils connectés. Si l'adresse IP est en conflit avec un autre appareil sur votre réseau local ou si votre réseau nécessite un sous-réseau IP spécifique, vous pouvez le modifier.

1. Visitez <http://tplinkwifi.net> et connectez-vous avec le mot de passe que vous avez défini pour le routeur.
2. Accédez à Réseau > Paramètres LAN.
3. Saisissez une nouvelle adresse IP adaptée à vos besoins. Et laissez le masque de sous-réseau comme paramètres par défaut.

DHCP Server

IP Version: IPv4 IPv6

MAC Address: 50-C7-BF-44-88-81

IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255.255.255.0

IGMP Snooping: Enable

Second IP: Enable

DHCP: Enable

Save

4. Cliquez sur Enregistrer.

Spécifier les paramètres du serveur DHCP

Par défaut, le serveur DHCP (Dynamic Host Configuration Protocol) est activé et le routeur agit comme un serveur DHCP ; il attribue dynamiquement des paramètres TCP/IP aux périphériques clients à partir du pool d'adresses IP. Vous pouvez modifier les paramètres du serveur DHCP si nécessaire et vous pouvez réserver des adresses IP LAN pour les périphériques clients spécifiés. En mode Point d'accès, sélectionnez SmartIP dans la plupart des cas.

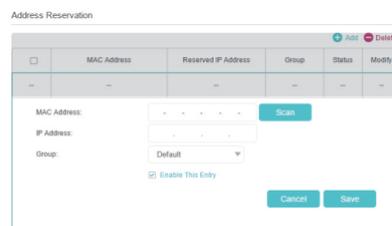
1. Visitez <http://tplinkwifi.net> et connectez-vous avec le mot de passe que vous avez défini pour le routeur.
2. Allez dans Réseau > Paramètres LAN.
 1. **Pour spécifier l'adresse IP que le routeur attribue :**



1. Activez le serveur DHCP.
2. Saisissez les adresses IP de début et de fin dans le pool d'adresses IP.
3. Saisissez d'autres paramètres si le FAI le propose. La passerelle par défaut est automatiquement renseignée et correspond à l'adresse IP LAN du routeur.
4. Cliquez sur Enregistrer.

2. Pour réserver une adresse IP pour un appareil client spécifié :

1. Cliquez sur Ajouter dans la section Réservez une adresse.



2. Cliquez sur Scan pour trouver un appareil connecté auquel vous souhaitez appliquer cette règle. Vous pouvez également saisir manuellement l'adresse MAC de l'appareil s'il est actuellement déconnecté du routeur.
3. Saisissez l'adresse IP à réserver pour l'appareil client.
4. Cochez la case Activer cette entrée et cliquez sur Enregistrer.

Configurer un compte de

service DNS dynamique

La plupart des FAI attribuent une adresse IP dynamique au routeur et vous pouvez utiliser cette adresse IP pour accéder à votre routeur à distance. Cependant, l'adresse IP peut changer de temps en temps et vous ne savez pas quand elle change. Dans ce cas, vous pouvez appliquer la fonctionnalité DDNS (Dynamic Domain Name Server) sur le routeur pour vous permettre, ainsi qu'à vos amis, d'accéder à votre routeur et aux serveurs locaux (FTP, HTTP, etc.) en utilisant un nom de domaine sans vérifier et mémoriser l'IP adresse.



Le DDNS ne fonctionne pas si le FAI attribue une adresse IP WAN privée (telle que 192.168.1.x) au routeur.

1. Visitez <http://tplinkwifi.net> et connectez-vous avec le mot de passe que vous avez défini pour le routeur.
2. Allez dans Avancé > Réseau > DNS dynamique.
3. Sélectionnez le fournisseur de service DDNS : NO-IP ou DynDNS. Si vous n'avez pas de compte DDNS, vous devez d'abord vous inscrire en cliquant sur Aller pour vous inscrire. Saisissez ensuite le nom d'utilisateur, le mot de passe et le nom de domaine de votre compte.

Dynamic DNS Settings

Service Provider: DynDNS NO-IP [Go to register...](#)

Username:

Password:

Domain Name:

4. Cliquez sur Se connecter et Enregistrer.



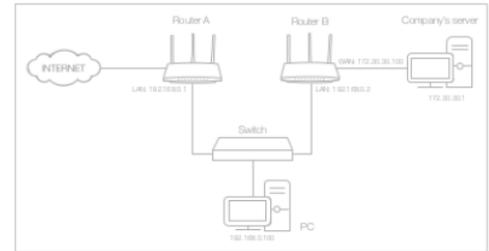
Si vous souhaitez utiliser un nouveau compte DDNS, veuillez d'abord cliquer sur Déconnexion, puis connectez-vous avec un nouveau compte.

Créer des routes statiques

Le routage statique est une forme de routage configurée manuellement par un administrateur réseau ou un utilisateur en ajoutant des entrées dans une table de routage. Les informations de routage configurées manuellement guident le routeur dans le transfert des paquets de données vers la destination spécifique.

Je veux visiter plusieurs réseaux et serveurs en même temps.

Par exemple, dans un petit bureau, mon PC peut surfer sur Internet via le routeur A, mais je souhaite également visiter le réseau de mon entreprise. J'ai maintenant un commutateur et un routeur B. Je connecte les appareils comme indiqué dans la figure suivante afin que la connexion physique entre mon PC et le serveur de mon entreprise soit établie. Pour surfer sur Internet et visiter le réseau de mon entreprise en même temps, je dois configurer le routage statique.



1. Remplacez les adresses IP LAN des routeurs par deux adresses IP différentes sur le même sous-réseau. Désactivez la fonction DHCP du routeur B.
2. Visitez <http://tplinkwifi.net> et connectez-vous avec le mot de passe que vous avez défini pour le routeur A.
3. Allez dans Avancé > Réseau > Routage avancé.
4. Cliquez sur Ajouter et terminez les réglages selon les explications suivantes :

ID	Network Destination	Subnet Mask	Gateway	Status	Modify
--	--	--	--	--	--

Network Destination: 172 . 30 . 30 . 1
 Subnet Mask: 255 . 255 . 255 . 255
 Gateway: 192 . 168 . 0 . 2
 Interface: LAN

Enable This Entry

Cancel Save

1. **Destination réseau** : l'adresse IP de destination que vous souhaitez attribuer à une route statique. Cette adresse IP ne peut pas être sur le même sous-réseau que l'IP WAN ou l'IP LAN du routeur A. Dans l'exemple, l'adresse IP du réseau d'entreprise est l'adresse IP de destination, entrez donc ici 172.30.30.1.
2. **Masque de sous-réseau** : détermine le réseau de destination avec l'adresse IP de destination. Si la destination est une adresse IP unique, saisissez

255.255.255.255 ;
sinon, entrez le masque de sous-réseau de l'IP réseau correspondant. Dans l'exemple, le réseau de destination est une adresse IP unique, entrez donc ici 255.255.255.255.

3. **Passerelle par défaut** : l'adresse IP du périphérique de passerelle auquel les paquets de données seront envoyés. Cette adresse IP doit être sur le même sous-réseau que l'IP du routeur qui envoie les données. Dans l'exemple, les paquets de données seront envoyés au port LAN du routeur B, puis au serveur, la passerelle par défaut doit donc être 192.168.0.2.

4. **Interface** : déterminé par le port (WAN/LAN) qui envoie les paquets de données. Dans l'exemple, les données sont envoyées à la passerelle via le port LAN du routeur A, donc LAN doit être sélectionné.

5. Cliquez sur Enregistrer.

6. Vérifiez la table de routage du système ci-dessous. Si vous pouvez trouver l'entrée que vous avez définie, le routage statique est défini avec succès.

System Routing Table

Active Routes Number: 3 [Refresh](#)

ID	Network Destination	Subnet Mask	Gateway	Interface
1	172.30.30.1	255.255.255.255	192.168.0.2	lan
2	192.168.0.0	255.255.255.0	0.0.0.0	lan
3	192.168.0.2	255.255.255.255	0.0.0.0	lan

Terminé ! Ouvrez un navigateur Web sur votre PC. Saisissez l'adresse IP du serveur de l'entreprise pour visiter le réseau de l'entreprise.

Spécifier les paramètres sans fil

Le nom de réseau sans fil (SSID) et le mot de passe du routeur ainsi que l'option de sécurité sont prédéfinis en usine. Le SSID et le mot de passe prédéfinis se trouvent sur l'étiquette du routeur.

Vous pouvez personnaliser les paramètres sans fil en fonction de vos besoins.

Visitez <http://tplinkwifi.net> et connectez-vous avec le mot de passe que vous avez défini pour le routeur.

1. Pour activer ou désactiver la fonction sans fil :

1. Accédez à Basic > Sans fil, Paramètres > Sans fil > Paramètres sans fil ou Paramètres > Sans fil > Réseau étendu.
2. La radio sans fil est activée par défaut. Si vous souhaitez désactiver la fonction sans fil du routeur, décochez simplement la case Activer. Dans ce cas, tous les paramètres

sans fil seront
invalides.

2. **Pour modifier le nom du réseau sans fil (SSID) et le mot de passe sans fil :**

1. Accédez à De base > Sans fil, Paramètres > Sans fil > Paramètres sans fil ou Paramètres > Sans fil > Réseau étendu.
2. Créez un nouveau SSID dans Network Name (SSID) et personnalisez le mot de passe du réseau dans Password. La valeur est sensible à la casse.⁴⁾

3. **Pour masquer le SSID :**

1. Accédez à Basic > Sans fil, Paramètres > Sans fil > Paramètres sans fil ou Paramètres > Sans fil > Réseau étendu.
2. Sélectionnez Masquer le SSID et votre SSID ne s'affichera pas lorsque vous recherchez des réseaux sans fil locaux sur votre appareil sans fil et que vous devez vous connecter

4. Pour modifier

l'option de sécurité :

1. Accédez à Avancé > Sans fil > Paramètres sans fil, Paramètres > Sans fil > Paramètres sans fil ou Paramètres > Sans fil > Réseau étendu.
2. Sélectionnez une option dans la liste déroulante Sécurité. Nous vous recommandons de ne pas modifier les paramètres par défaut, sauf si nécessaire. Si vous sélectionnez d'autres options, configurez les paramètres associés en fonction de la page d'aide.

5. en plus

- Mode - Sélectionnez un mode de transmission en fonction de vos périphériques clients sans fil. Il est recommandé de le laisser par défaut.
- Largeur de canal - Sélectionnez une largeur de canal (bande passante) pour le réseau sans fil.
- Canal - Sélectionnez un canal d'exploitation

pour le réseau sans fil. Il est recommandé de laisser le canal sur Auto, si vous ne rencontrez pas de problème de connexion sans fil intermittent.

Étendre le réseau hôte

Si vous souhaitez étendre un autre réseau hôte après la configuration rapide lorsque le routeur fonctionne comme un prolongateur de portée, vous pouvez vous référer à cette section.

1. Visitez <http://tplinkwifi.net> et connectez-vous avec le mot de passe que vous avez défini pour le routeur.
2. Allez dans Paramètres > Sans fil > Se connecter au réseau.
3. Activez Connect to 2.4GHz Network et cliquez sur Scan pour trouver tous les réseaux disponibles.
4. Sélectionnez le réseau hôte que



vous souhaitez étendre.

Remarque : Si le réseau que vous souhaitez étendre est sur mais n'est pas répertorié, veuillez essayer les étapes suivantes.

- Rapprochez le routeur de votre routeur hôte et cliquez sur Actualiser dans le coin supérieur droit de la liste.
- Vous pouvez saisir manuellement le SSID (nom du réseau) et le mot de passe du réseau que vous souhaitez étendre, puis cliquer sur Enregistrer.

5. Une fois qu'un réseau hôte est sélectionné, son SSID, son adresse MAC et son type de sécurité seront automatiquement renseignés. S'il est crypté, saisissez le mot de passe dans le champ Mot de passe.

6. Cliquez sur Enregistrer.

Utiliser WPS pour la connexion sans fil

Wi-Fi Protected Setup (WPS) offre une approche plus simple pour configurer une connexion Wi-Fi sécurisée.

1. Visitez <http://tplinkwifi.net> et connectez-vous avec le mot de passe que vous avez défini pour le routeur.
2. Accédez à Avancé > Sans fil > WPS ou Paramètres > Sans fil > WPS.

Utiliser l'assistant WPS pour les connexions Wi-Fi

1. Cliquez sur le bouton Démarrer WPS à l'écran. Dans les deux minutes,

appuyez sur le bouton WPS sur le périphérique client.



- Succès** apparaîtra sur l'écran ci-dessus et le voyant WPS du routeur restera allumé pendant cinq minutes si le client a été ajouté avec succès au réseau.

Utiliser le code PIN pour les connexions Wi-Fi

Le code PIN du routeur est activé par défaut pour permettre aux appareils sans fil de se connecter au routeur à l'aide du code PIN. Vous pouvez utiliser celui par défaut ou en générer un nouveau.



Vous pouvez également saisir le code PIN de l'appareil que

vous souhaitez
connecter au Wi-
Fi.

Router's PIN Client's PIN
Enter the client's PIN:

S
i
v
o
u
s
s
o
u
h
a
i
t
e
z
a
c
t
i
v
e
r
/
d
é
s
a
c
t
i
v
e
r
l
a
f
o
n
c
t
i
o





S
e
z
l
a
s
e
c
t
i
o
n
W
P
S
e
t
c
o
c
h
e
z
o
u
d
é
c
o
c
h
e
z
l
a
c
a
s
e
A
c
t
i
v
e
r
.
P





I
N
(
P
e
r
s
o
n
a
l
I
d
e
n
t
i
f
i
c
a
t
i
o
n
N
u
m
b
e
r
)
e
s
t
u
n
n
u
m
é
r
o
d
i
d
e
n
t
i
f



C
a
t
i
o
n
à
h
u
i
t
c
a
r
a
c
t
è
r
e
s
p
r
é
d
é
f
i
n
i
p
o
u
r
c
h
a
q
u
e
r
o
u
t
e
u
r
. L
e



S
a
p
p
a
r
e
i
l
s
c
o
m
p
a
t
i
b
l
e
s
W
P
S
p
e
u
v
e
n
t
s
e
c
o
n
n
e
c
t
e
r
à
v
o
t
r
e
r
o
u



t
e
u
r
a
v
e
c
l
e
c
o
d
e
P
I
N
·
L
e
c
o
d
e
P
I
N
p
a
r
d
é
f
a
u
t
e
s
t
i
m
p
r
i
m
é
s
u
r



Programmez votre fonction sans fil

Le réseau sans fil peut être automatiquement désactivé à un moment précis lorsque vous n'avez pas besoin de la connexion sans fil.

1. Visitez <http://tplinkwifi.net> et connectez-vous avec le mot de passe que vous avez défini pour le routeur.
2. Accédez à

Avancé >
Sans fil >
Programmation sans fil.

3. Activer la programmation sans fil.
4. Cliquez sur Ajouter pour définir l'heure d'arrêt sans fil. Spécifiez la période et les jours pendant lesquels le réseau sans fil sera désactivé.



5. Cliquez sur Enregistrer.

Gérer le routeur

Ce chapitre vous montrera la configuration pour la gestion et la maintenance de votre routeur. Certaines fonctionnalités ne sont prises en charge que par un certain mode.

Configurer l'heure du système

L'heure système

est l'heure affichée pendant que le routeur fonctionne. L'heure système que vous configurez ici sera utilisée pour d'autres fonctions basées sur l'heure comme le contrôle parental.

1. Visitez <http://tplinkwifi.net> et connectez-vous avec le mot de passe que vous avez défini pour le routeur.
2. Accédez à Outils système > Paramètres d'heure.
 1. **Pour obtenir le temps à partir du PC:**
 2. Cliquez sur **Obtenir du PC.**
 3. Cliquez sur **Enregistrer.**
 1. **Pour obtenir le**

temps par Internet :

1. Sélectio
nnez
votre
refuse
au
horai
re
local
dans
sua
lis

t
e
d
é
r
o
u
l
a
n
t
e
:
2.
D
a
n
s
l
e
c
h
a
m
p
N
T
P
S
e
r
v
e
r
l
,
s
a
i
s
i
s
s
e
z
l
,
a
d
r
e

S
S
e
l
P
o
u
l
e
n
o
m
d
e
d
o
m
a
i
n
e
d
u
s
e
r
v
e
u
r
N
T
P
s
o
u
h
a
i
t
é
.
3.
(
F
a
c
u
l

t
a
t
i
f
)
D
a
n
s
l
e
c
h
a
m
p
N
T
P
S
e
r
v
e
r
l
l
,
s
a
i
s
i
s
s
e
z
l
,
a
d
r
e
s
s
e
l
P
o
u

I
e
n
o
m
d
e
d
o
m
a
i
n
e
d
u
d
e
u
x
i
è
m
e
s
e
r
v
e
u
r
N
T
P
.
4.
C
l
i
q
u
e
z
s
u
r
O
b
t

e
n
i
r
d
e
p
u
i
s
l
n
t
e
r
n
e
t
e
t
c
l
i
q
u
e
z
s
u
r
E
n
r
e
g
i
s
t
r
e
r
.

2. **Pour
confi
gure
r
l'heu
re
d'été**
:

1. S
é
l
e
c
t
i
o
n
n
e
z
A
c
t
i
v
e
r
i
h
e
u
r
e
d
é
t
é

2. S
é
l
e
c
t
i
o
n
n
e
z
l
a
d

a
t
e
e
t
l
,
h
e
u
r
e
d
e
d
é
b
u
t
c
o
r
r
e
c
t
e
s
l
o
r
s
q
u
e
l
,
h
e
u
r
e
d
,
é
t
é
c
o
m
m

e
n
c
e
à
v
o
t
r
e
f
u
s
e
a
u
h
o
r
a
i
r
e
l
o
c
a
l
.
3.

S
é
l
e
c
t
i
o
n
n
e
z
l
a
d
a
t
e
e

t
l
,
h
e
u
r
e
d
e
f
i
n
c
o
r
r
e
c
t
e
s
l
o
r
s
q
u
e
l
,
h
e
u
r
e
d
,
é
t
é
s
e
t
e
r
m
i
n
e
d
a

n
s
v
o
t
r
e
f
u
s
e
a
u
h
o
r
a
i
r
e
l
o
c
a
l
.
4.
C
l
i
q
u
e
z
s
u
r
E
n
r
e
g
i
s
t
r
e
r
.

Tester la connectivité réseau

Les diagnostics sont utilisés pour tester la connectivité entre le routeur et l'hôte ou d'autres périphériques réseau.

1. Visitez [http://](#)

t
p
l
i
n
k
w
i
f
i
·
n
e
t
e
t
c
o
n
n
e
c
t
e
z
-
v
o
u
s
a
v
e
c
l
e
m
o
t
d
e
p
a
s
s
e
q
u
e
v

o
u
s
a
v
e
z
d
é
f
i
n
i
p
o
u
r
l
e
r
o
u
t
e
u
r
.
2.
A
l
l
e
z
d
a
n
s
A
v
a
n
c
é
>
O
u
t
i
l
i
s
s
y

s
t
è
m
e
>
D
i
a
g
n
o
s
t
i
c
s
.
3.
C
l
i
q
u
e
z
s
u
r
D
é
m
a
r
r
e
r
p
o
u
r
l
a
n
c
e
r
l
e

S
d
i
a
g
n
o
s
t
i
c
s
.

**Met
tre
à
nive
au
le
micr
olog
iciel**

TP-
Link
vise à
offrir
une
meille
ure
expér
ience
résea
u aux
utilisa
teurs.

Nous
vous
infor
mero
ns via
la
page
de
gestio
n
Web

si une mise à jour du micrologiciel est disponible pour votre routeur. De plus, le dernier firmware sera publié sur le site officiel de TP-Link www.tp-link.com, et vous pouvez télécharger gratuitement à partir de la page d'assistance.

• A
s
s
u
r
e
z
-
v
o
u
s
d
e
r
e
t
i
r
e
r
t
o
u
s
l
e
s
p
é
r
i
p
h
é
r
i
q
u
e
s
U
S
B
c
o
n
n
e



c
t
é
s
d
u
r
o
u
t
e
u
r
a
v
a
n
t
l
a
m
i
s
e
à
i
n
i
v
e
a
u
d
u
m
i
c
r
o
l
o
g
i
c
i
e
l
p
o
u



r
é
v
i
t
e
r
t
o
u
t
e
p
e
r
t
e
d
e
d
o
n
n
é
e
s
.
•
S
a
u
v
e
g
a
r
d
e
z
l
a
c
o
n
f
i
g
u
r
a
t
i



o
n
d
e
v
o
t
r
e
r
o
u
t
e
u
r
a
v
a
n
t
l
a
m
i
s
e
à
n
i
v
e
a
u
d
u
m
i
c
r
o
l
o
g
i
c
i
e
l



• N
'
é
t
e
i
g
n
e
z
P
A
S
l
e
r
o
u
t
e
u
r
p
e
n
d
a
n
t
l
a
m
i
s
e
à
n
i
v
e
a
u
d
u
m
i
c
r
o





1. T é l é c h a r g e z l e d e r n i e r f i c h i e r d e f i r m w a r e p o u

r
l
e
r
o
u
t
e
u
r
à
p
a
r
t
i
r
d
e
h
t
t
p
:
/
/
w
w
w
.
t
p
-
l
i
n
k
.
c
o
m
.
2.
V
i
s
i
t
e
z
h

t
t
p
:
/
/
t
p
l
i
n
k
w
i
f
i
.
n
e
t
e
t
c
o
n
n
e
c
t
e
z
-
v
o
u
s
a
v
e
c
l
e
m
o
t
d
e
p
a
s

S
e
q
u
e
v
o
u
s
a
v
e
z
d
é
f
i
n
i
p
o
u
r
l
e
r
o
u
t
e
u
r
.

3. A
c
c
é
d
e
z
à
O
u
t
i
l
s
s
y
s
t

è
m
e
> M
i
s
e
à
n
i
v
e
a
u
d
u
m
i
c
r
o
l
o
g
i
c
i
e
l
.
4. C
l
i
q
u
e
z
s
u
r
P
a
r
c
o
u
r

i
r
p
o
u
r
l
o
c
a
l
i
s
e
r
l
e
n
o
u
v
e
a
u
f
i
c
h
i
e
r
d
e
f
i
r
m
w
a
r
e
t
é
l
é
c
h
a
r
g
é
,
p

u
i
s
c
l
i
q
u
e
z
s
u
r
M
e
t
t
r
e
à
n
i
v
e
a
u
.
5.
A
t
t
e
n
d
e
z
q
u
e
l
q
u
e
s
m
i
n
u
t

e
s
q
u
e
l
a
m
i
s
e
à
n
i
v
e
a
u
e
t
l
e
r
e
d
é
m
a
r
r
a
g
e
s
e
t
e
r
m
i
n
e
n
t
.

**Sau
veg
arde**

r et rest aure r les para mèt res de con figu rati on

Les paramètres de configuration sont stockés sous forme de fichier de configuration dans le routeur. Vous pouvez sauvegarder le fichier de configuration sur

votre ordinateur pour une utilisation future et restaurer le routeur à des paramètres antérieurs à partir du fichier de sauvegarde si nécessaire. De plus, si nécessaire, vous pouvez effacer les paramètres actuels et réinitialiser le routeur aux

para
mètre
s
d'usin
e par
défau
t.

1. [V
i
s
i
t
e
z
h
t
t
p
:
/
/
t
p
l
i
n
k
w
i
f
i
.
n
e
t
e
t
c
o
n
n
e
c
t
e
z
-
v
o](https://www.netcettez.com/necettez-vo)

u
s
a
v
e
c
l
e
m
o
t
d
e
p
a
s
s
e
q
u
e
v
o
u
s
a
v
e
z
d
é
f
i
n
i
p
o
u
r
l
e
r
o
u
t
e
u
r
.

2.

A
c

C
é
d
e
z
à
O
u
t
i
l
s
s
y
s
t
è
m
e
>
S
a
u
v
e
g
a
r
d
e
e
t
r
e
s
t
a
u
r
a
t
i
o
n
.
3.
**P
o
u**

r
s
a
u
v
e
g
a
r
d
e
r
l
e
s
p
a
r
a
m
è
t
r
e
s
d
e
c
o
n
f
i
g
u
r
a
t
i
o
n

:
C
l
i
q
u
e
z
s
u
r

S
a
u
v
e
g
a
r
d
e
r
p
o
u
r
e
n
r
e
g
i
s
t
r
e
r
u
n
e
c
o
p
i
e
d
e
s
p
a
r
a
m
è
t
r
e
s
a
c

t
u
e
l
s
s
u
r
v
o
t
r
e
o
r
d
i
n
a
t
e
u
r
l
o
c
a
l
.
U
n
f
i
c
h
i
e
r
«

.
b
i
n

»
d
e
s
p
a
r

a
m
è
t
r
e
s
a
c
t
u
e
l
s
s
e
r
a
s
t
o
c
k
é
s
u
r
v
o
t
r
e
o
r
d
i
n
a
t
e
u
r
.
4.
**P
o
u
r**

e
s
t
a
u
r
e
r
l
e
s
p
a
r
a
m
è
t
r
e
s
d
e
c
o
n
f
i
g
u
r
a
t
i
o
n

:

1.

C
l
i
q
u
e
z
s
u
r
P
a
r

C
O
U
R
I
R
P
O
U
R
L
O
C
A
L
I
S
E
R
L
E
F
I
C
H
I
E
R
D
E
C
O
N
F
I
G
U
R
A
T
I
O
N
D
E
S
A
U
V
E
G

a
r
d
e
s
t
o
c
k
é
s
u
r
v
o
t
r
e
o
r
d
i
n
a
t
e
u
r
,
p
u
i
s
c
l
i
q
u
e
z
s
u
r
R
e
s
t
a
u
r
e

r
.
2.
A
t
t
e
n
d
e
z
q
u
e
l
q
u
e
s
m
i
n
u
t
e
s
p
o
u
r
l
a
r
e
s
t
a
u
r
a
t
i
o
n
e
t
l
e
r

e
d
é
m
a
r
r
a
g
e
.
R
e
m
a
r
q
u
e
:
p
e
n
d
a
n
t
l
e
p
r
o
c
e
s
s
u
s
d
e
r
e
s
t
a
u
r
a
t
i
o

n
,
n
,
é
t
e
i
g
n
e
z
p
a
s
e
t
n
e
r
é
i
n
i
t
i
a
l
i
s
e
z
p
a
s
l
e
r
o
u
t
e
u
r
.

5.
**P
o
u**

r
r
é
i
n
i
t
i
a
l
i
s
e
r
l
e
r
o
u
t
e
u
r
a
u
x
p
a
r
a
m
è
t
r
e
s
d
'
u
s
i
n
e
p
a
r
d
é
f
a
u

t
:

1.

C
l
i
q
u
e
z
s
u
r
F
a
c
t
o
r
y
R
e
s
t
o
r
e
p
o
u
r
r
é
i
n
i
t
i
a
l
i
s
e
r
l
e
r
o

u
t
e
u
r
.
2.
A
t
t
e
n
d
e
z
q
u
e
l
q
u
e
s
m
i
n
u
t
e
s
p
o
u
r
l
a
r
é
i
n
i
t
i
a
l
i
s
a
t
i

o
n
e
t
l
e
r
e
d
é
m
a
r
r
a
g
e
.
R
e
m
a
r
q
u
e
:
:

R
e
d
é
m
a
r
r
a
g
e
a
u
t
o
m
a
t
i
q
u
e

L
e
r
e

d
é
m
a
r
r
a
g
e
a
u
t
o
m
a
t
i
q
u
e
v
o
u
s
p
e
r
m
e
t
d
e
s
p
é
c
i
fi
e
r
u
n
e
h
e
u
r
e
à
l
a

q
u
e
l
l
e
l
e
r
o
u
t
e
u
r
r
e
d
é
m
a
r
r
e
r
a
a
u
t
o
m
a
t
i
q
u
e
m
e
n
t
.



C
h
a
n
g
e
r
l
e
m
o
t
d
e
p
a
s
s
e
d
e
c
o
n
n
e
x
i
o

n

L
a
f
o
n
c
t
i
o
n
d
e
g
e
s
t
i
o
n
d
e
c
o
m
p
t
e
v
o
u
s
p
e
r
m
e
t
d
e
m
o
d
i
fi
e
r
v
o

t
r
e
m
o
t
d
e
p
a
s
s
e
d
e
c
o
n
n
e
x
i
o
n
d
e
l
a
p
a
g
e
d
e
g
e
s
t
i
o
n
W
e
b
.



a
l
e

L
a
g
e
s
t
i
o
n
l
o
c
a
l
e
p
e
r
m
e
t
a
u
x
p
é
r
i
p
h
é
r
i
q
u
e
s
l
o
c
a
u
x
d

r
a
c
c
é
d
e
r
a
u
r
o
u
t
e
u
r
e
t
d
e
l
e
g
é
r
e
r
.
P
a
r
d
é
f
a
u
t
,
t
o
u
s
l
e
s
p
é
r
i
p

h
é
r
i
q
u
e
s
l
o
c
a
u
x
p
e
u
v
e
n
t
a
c
c
é
d
e
r
e
t
g
é
r
e
r
l
e
r
o
u
t
e
u
r
v
i
a
H
T

S
i
u
n
a
v
e
r
t
i
s
s
e
m
e
n
t
a
p
p
a
r
a
î
t
l
o
r

s
q
u
e
v
o
u
s
v
i
s
i
t
e
z
h
t
t
p
s
:
/
/
t
p
l
i
n
k
w
i
f
.
n
e
t
,
c
l
i
q
u
e
z
s
u
r
T
r
u
s

t
(
o
u
u
n
e
o
p
t
i
o
n
s
i
m
i
l
a
i
r
e
)
p
o
u
r
c
o
n
t
i
n
u
e
r
.

**G
e
s
t
i
o**

n
à
d
i
s
t
a
n
c
e

L
a
g
e
s
t
i
o
n
à
d
i
s
t
a
n
c
e
p
e
r
m
e
t
t
a
u
x
p
é
r
i
p
h
é
r
i
q
u

e
s
d
i
s
t
a
n
t
s
d
'
a
c
c
é
d
e
r
a
u
r
o
u
t
e
u
r
e
t
d
e
l
e
g
é
r
e
r
.
P
a
r
d
é
f
a
u
t

,
t
o
u
s
l
e
s
a
p
p
a
r
e
i
l
s
d
i
s
t
a
n
t
s
n
e
p
e
u
v
e
n
t
p
a
s
a
c
c
é
d
e
r
a
u
r
o
u
t
e







Statut	Description
...	...
...	...
...	...
...	...
...	...
...	...
...	...
...	...
...	...
...	...





