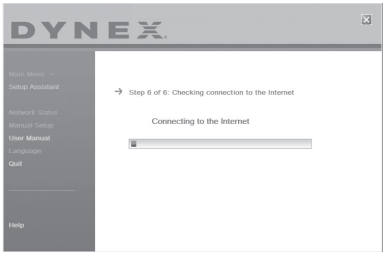
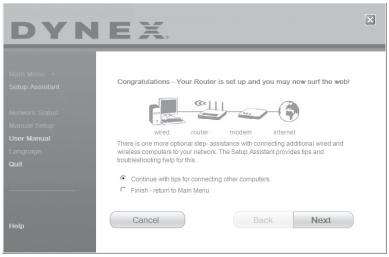
Une fois le routeur configuré, l'Assistant Configuration vérifie la connexion à l'Internet.



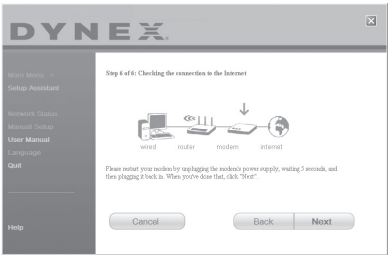
Ceci termine l'installation du routeur. L'écran *Congratulations* (Félicitations) s'affiche lorsque le routeur peut se connecter à l'Internet. Il est alors possible de commencer à surfer en ouvrant un navigateur Web et en se rendant sur n'importe quel site Web.



7 L'Assistant Configuration peut être utilisé pour configurer les autres ordinateurs câblés et sans fil, afin de les connecter à l'Internet, en cliquant sur **Next** (Suivant). Pour ajouter ultérieurement des ordinateurs au routeur, sélectionner **Exit the Assistant** (Quitter l'assistant), puis cliquer sur **Next** (Suivant).

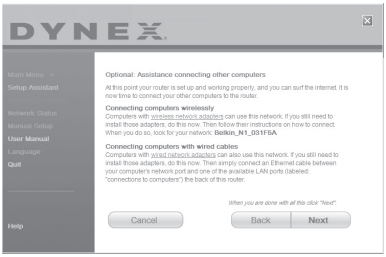
Pour identifier et résoudre les problèmes de configuration :

1 Si l'Assistant Configuration ne parvient pas à établir une connexion Internet, l'écran suivant s'affichera. Suivre les instructions à l'écran pour procéder à l'identification et à la résolution des problèmes.



Pour utiliser l'aide optionnelle pour connecter d'autres ordinateurs :

1. Cette étape optionnelle aide à connecter des ordinateurs câblés ou sans fil supplémentaires au réseau. Suivre les instructions affichées à l'écran.



À ce stade, le routeur est configuré et fonctionne correctement. Il est temps maintenant de connecter les autres ordinateurs.

Connexion d'ordinateurs sans fil

Des ordinateurs munis d'un adaptateur réseau sans fil peuvent utiliser ce réseau. Si ces adaptateurs n'ont pas encore été installés, le faire maintenant. Ensuite, suivre leurs instructions pour les connecter. Ce faisant, rechercher le réseau défini : domicile de Jean Wi-Fi.

Connexion d'ordinateurs câblés

Les ordinateurs munis d'un adaptateur réseau câblé peuvent utiliser ce réseau. Si ces adaptateurs n'ont pas encore été installés, le faire maintenant. Ensuite, connecter simplement un câble Ethernet du port réseau de l'ordinateur à un des ports LAN disponibles (étiquetés **connections to computers** [connexions aux ordinateurs]) au dos de ce routeur.

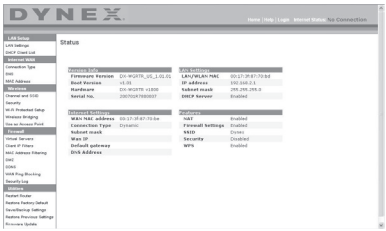
Une fois établi que les autres ordinateurs câblés et sans fil sont correctement connectés, le réseau est configuré et prêt à fonctionner. Il est maintenant possible de surfer sur Internet. Cliquer sur **Next** (Suivant) pour revenir au menu principal.

Configuration de la sécurité sans fil

Veiller à effectuer la configuration de base du routeur avant de configurer la sécurité. Vérifier que tous les ordinateurs (câblés et sans fil) peuvent se connecter sans problème à l'Internet par l'intermédiaire du routeur.

Pour configurer la sécurité :

1. Sur un ordinateur qui a une connexion câblée avec le routeur, ouvrir un navigateur Web. Dans le champ de l'adresse, saisir 192.168.2.1 (ou une autre adresse IP personnalisée), puis cliquer sur **Enter** (Entrée).



2 Dans le menu de gauche, aller à la section sans fil et cliquer sur **Security** (Sécurité). S'il est demandé d'ouvrir une session, saisir le mot de passe; si aucun mot de passe personnalisé n'a encore été configuré, laisser ce champ en blanc. Ensuite, cliquer sur **Submit** (Soumettre).

3 Il sera demandé de choisir le type de sécurité. Dynex recommande WPA2-PSK comme mode de sécurité et ensuite WPA-PSK+WPA2-PSK pour l'authentification, car c'est le mode le plus sûr et le plus facile à utiliser. Une fois le choix effectué, cliquer sur **Apply Changes** (Appliquer les modifications).

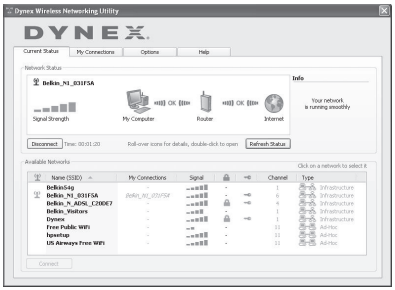
4 Dans le champ de la clé pré-partagée (PSK), saisir une clé de sécurité dont il sera facile de se souvenir. L'utilisation de ponctuation permettra d'améliorer la sécurité du réseau (par exemple, « Mon équipe favorite est celle des Canadiens de Montréal! »). Cliquer sur **Apply Changes** (Appliquer les modifications).

5 Maintenant, aller à chaque ordinateur sans fil. Utiliser l'utilitaire sans fil sur chacun d'entre eux pour effectuer les opérations suivantes (se reporter au manuel de l'utilisateur de l'adaptateur sans fil pour des instructions détaillées) :

a. Repérer le réseau sans fil et s'y connecter.

b. À l'invite, saisir la clé de sécurité créée à l'étape ci-dessus.

***Remarque** : Si un ordinateur n'accepte pas cette clé, il est probable qu'il ne prenne pas encore en charge le mode WPA/WPA2. Aller sur le site Web du fabricant de l'adaptateur sans fil et vérifier s'il existe une mise à jour pour le pilote.*



6 Si la mise à jour de l'adaptateur sans fil de l'ordinateur pour qu'il prenne en charge le mode WPA/WPA2 n'est pas souhaitée, retourner à l'étape 4 et choisir WEP. Se reporter au guide de l'utilisateur du routeur sans fil G de Dynex pour les instructions relatives à une configuration WEP.

Autre méthode de configuration

L'Interface utilisateur Web avancée est un outil qui peut être utilisé pour configurer le routeur sans utiliser l'Assistant Installation facile. Elle peut également être utilisée pour gérer les fonctions avancées du routeur. À partir de l'Interface utilisateur Web avancée, les tâches suivantes peuvent être réalisées :

- Visualiser les paramètres et l'état actuel du routeur
- Configurer le routeur afin qu'il se connecte au FSI, à l'aide des paramètres fournis par celui-ci
- Modifier les paramètres réseau en cours comme l'adresse IP interne, le pool d'adresses IP, les paramètres DHCP et bien plus encore
- Configurer le pare-feu du routeur afin qu'il fonctionne avec des applications spécifiques (réacheminement de port)
- Configurer des fonctions de sécurité, telles que la restriction des clients, le filtrage d'adresses MAC, le WEP et le WPA
- Activer la fonction DMZ (zone démilitarisée) pour un ordinateur unique du réseau
- Changer le mot de passe interne du routeur
- Activer/désactiver l'UPnP (Universal Plug-and-Play)
- Réinitialiser le routeur
- Sauvegarder les paramètres de configuration
- Rétablir les paramètres par défaut du routeur
- Mettre à jour le microprogramme du routeur.

Pour connecter le routeur (étape 1) :

1. Mettre le modem hors tension en débranchant le bloc d'alimentation du modem.
2. Repérer le câble réseau qui relie le modem à l'ordinateur. Le débrancher de l'ordinateur et laisser l'autre extrémité branchée sur le modem.
3. Brancher l'extrémité du câble ainsi débranchée sur le port marqué **Modem** à l'arrière du routeur.
4. Brancher un nouveau câble réseau (non fourni) pour connecter l'ordinateur à un des ports **1 à 4** sur le routeur. Remarque : Le numéro du port n'a pas d'importance.
5. Rebrancher le bloc d'alimentation du modem câble ou DSL pour l'allumer.
6. Brancher le cordon d'alimentation sur la prise secteur, puis sur la prise d'alimentation du routeur.
7. Vérifier que le modem est connecté au routeur en vérifiant les témoins lumineux à l'avant du routeur. Le témoin vert marqué **Modem** devrait être allumé si le modem est correctement branché sur le routeur. Si ce n'est pas le cas, vérifier de nouveau les connexions.
8. Vérifier que l'ordinateur est correctement connecté au routeur en vérifiant les témoins **1 à 4**. Le témoin correspondant au port connecté à l'ordinateur devrait être allumé si l'ordinateur est correctement connecté. Si ce n'est pas le cas, vérifier de nouveau les connexions.

Pour configurer les paramètres réseau de l'ordinateur de manière à ce qu'il fonctionne avec un serveur DHCP :

- Voir « Configuration manuelle des paramètres réseau » à la page 106 pour plus d'informations.

Configuration du routeur au moyen de l'Interface utilisateur Web avancée :

1. Ouvrir le navigateur Internet, puis accéder à l'Interface utilisateur Web avancée en saisissant « 192.168.2.1 » dans la barre d'adresse (il n'est pas nécessaire de taper autre chose, tel que « http:// » ou « www »). Ensuite, appuyer sur **Enter** (Entrée). La page d'accueil du routeur s'affiche.

   ***Remarque** : En cas de difficulté à accéder à l'Interface utilisateur Web avancée du routeur, aller à la section intitulée « Configuration manuelle des paramètres du réseau ».*

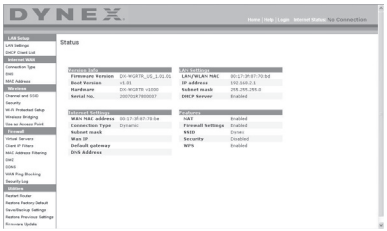
2. Pour apporter des modifications aux paramètres du routeur, il est nécessaire de se connecter. Cliquer sur **Login** (Connexion) ou sur tout autre lien sur la page d'accueil pour passer à l'écran de connexion.
3. Dans l'écran de connexion, laisser le mot de passe vide (aucun mot de passe n'est entré avant la livraison du routeur) et cliquer sur **Submit** (Soumettre) pour se connecter.

   Un seul ordinateur à la fois peut se connecter au routeur pour en modifier les paramètres.
4. Une fois l'utilisateur connecté pour apporter des modifications, il existe deux méthodes de déconnexion de l'ordinateur. Le fait de cliquer sur **Logout** (Déconnexion) déconnectera l'ordinateur.

   - OU -
5. La connexion se fermera automatiquement après une durée déterminée. Le délai avant déconnexion est par défaut de 10 minutes. Cette valeur peut être modifiée en choisissant une durée de 1 à 99 minutes. Pour plus d'informations, voir « Modification du paramètre de délai avant déconnexion » à la page 103.

Utilisation de l'Interface utilisateur Web avancée

La page d'accueil est la première page qui s'affiche lors de l'accès à l'interface utilisateur (IU) Web avancée. Cette page offre un aperçu rapide de l'état et des paramètres du routeur. Il est possible d'accéder à toutes les pages de configuration avancée depuis cette page.



Quick-Navigation Links (Liens de navigation rapide) – Il est possible de se rendre directement à n'importe laquelle des pages de l'IU du routeur en cliquant directement sur l'un de ces liens. Ils sont divisés en catégories logiques et groupés par onglets afin de faciliter la recherche d'un paramètre particulier. Pour obtenir une brève description de la fonction d'un onglet, cliquer sur l'en-tête violet de l'onglet.

Touche Home (Accueil) – La touche **Home** est disponible sur chaque page de l'IU. Appuyer sur cette touche pour revenir à la page d'accueil.

Internet Status Indicator (Témoin d'état Internet) – Ce témoin est visible sur toutes les pages de l'IU. Il indique l'état de la connexion du routeur. Lorsqu'il indique **connection OK** (Connexion OK) en vert, le routeur est connecté à l'Internet. Lorsque le routeur n'est pas connecté à l'Internet, l'indicateur affiche **no connection** (Pas de connexion) en rouge. L'indicateur est automatiquement mis à jour lors d'une modification des paramètres du routeur.

Touche Login/Logout (Connexion/Déconnexion) – Cette touche permet de se connecter et de se déconnecter du routeur en appuyant simplement sur une touche. Lorsque l'utilisateur est connecté au routeur, cette touche indique **Logout** (Déconnexion). Lors de la connexion au routeur, l'utilisateur accède à une page distincte où il doit entrer un mot de passe. Une fois connecté au routeur, il est possible de modifier les paramètres. Une fois les modifications apportées, l'utilisateur peut se déconnecter du routeur en cliquant sur **Logout** (Déconnexion).

Touche Help (Aide) – La touche **Help** permet d'accéder aux pages d'aide du routeur. Il est également possible d'obtenir de l'aide sur de nombreuses pages en cliquant sur **more info** (Plus d'infos) en regard de certaines sections de chaque page.

LAN Settings (Paramètres du réseau local) – Indique les paramètres du côté réseau local (LAN) du routeur. Pour modifier ces paramètres, cliquer sur l'un des liens (Adresse IP, Masque de sous-réseau, serveur DHCP) ou cliquer sur le lien **LAN - Quick Navigation** (LAN - Navigation rapide) sur le côté gauche de l'écran.

Features (Caractéristiques) – Indique l'état des fonctions NAT, pare-feu et sans fil du routeur. Pour modifier ces paramètres, cliquer sur l'un des liens ou sur les liens **Quick Navigation** (Navigation rapide) sur le côté gauche de l'écran.

Internet Settings (Paramètres Internet) – Affiche les paramètres du côté Internet/WAN du routeur qui se connecte à l'Internet. Pour modifier ces paramètres, cliquer sur l'un des liens ou sur le lien **Internet/WAN** - **Quick Navigation** (Internet/WAN - Navigation rapide) sur le côté gauche de l'écran.

Version Info (Informations sur la version) – Affiche la version du microprogramme, la version du code d'amorçage, la version du matériel ainsi que le numéro de série du routeur.

Page Name (Nom de la page) – La page sur laquelle se trouve l'utilisateur peut être identifiée par son nom. Ce guide de l'utilisateur fait parfois référence aux pages par leur nom. Par exemple, **LAN > LAN Settings** (LAN > Paramètres du réseau local) fait référence à la page LAN Settings (Paramètres LAN).

Configuration du routeur pour la connexion au fournisseur de service Internet (FSI)

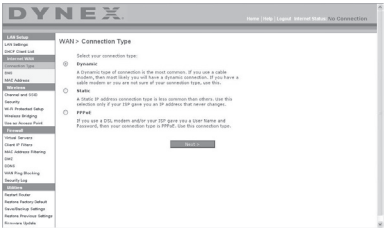
L'onglet **Internet/WAN** est l'endroit où l'utilisateur doit configurer le routeur pour qu'il se connecte à son fournisseur de service Internet (FSI). Le routeur peut se connecter pratiquement à n'importe quel système offert par un FSI, si bien sûr les paramètres du routeur ont été correctement configurés pour le type de connexion du FSI. Les paramètres de connexion au FSI sont fournis par ce dernier.

Pour configurer le routeur avec les paramètres fournis par le FSI :

1. Cliquer sur **Connection Type** (Type de connexion) sur le côté gauche de l'écran, puis sélectionner le type de connexion à employer.
2. Si le FSI a donné des paramètres DNS, cliquer sur **DNS** pour entrer l'adresse DNS pour les FSI qui nécessitent des paramètres particuliers.
3. Cliquer sur **MAC address** (Adresse MAC) pour cloner l'adresse MAC de l'ordinateur ou entrer une adresse WAN MAC spécifique, si cela est requis par le FSI.
4. Une fois les paramètres entrés, le témoin **Internet Status** (État Internet) affiche **connection OK** (Connexion OK) si le routeur est correctement configuré.

Pour définir le type de connexion :

1. Cliquer sur **Connection Type** (Type de connexion) dans le menu qui figure sur le côté gauche de l'écran. La page *Connection Type* (Type de connexion) s'affiche. À partir de cette page, sélectionner le type de connexion à utiliser en cliquant sur la touche qui se trouve en face du type de connexion, puis en cliquant sur **Next** (Suivant).



Réglage du type de connexion FSI comme « IP Dynamique »

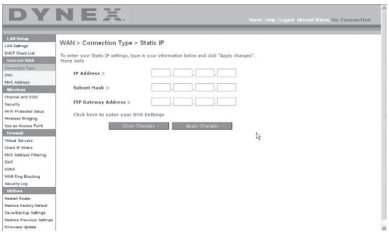
La connexion dynamique est le type le plus répandu sur les modems câble. Dans de nombreux cas, le simple fait de définir le type de connexion sur **dynamic** (Dynamique) suffit à effectuer la connexion avec le FSI. Certains types de connexion dynamique peuvent nécessiter un nom d'hôte. L'utilisateur peut entrer un nom d'hôte dans l'espace fourni à cet effet si un nom lui a été attribué. Le nom d'hôte est attribué par le FSI. Certaines connexions dynamiques peuvent nécessiter le clonage de l'adresse MAC du PC qui était, à l'origine, connecté au modem.

Modification de l'adresse MAC WAN

Si le FSI a besoin d'une adresse MAC spécifique pour la connexion au service, l'utilisateur peut entrer une adresse MAC particulière ou cloner l'adresse MAC de l'ordinateur en cours via ce lien.

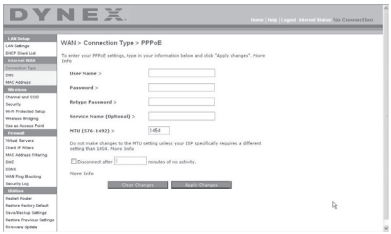
Réglage du type de connexion FSI comme « IP Statique »

Le type de connexion à adresse IP statique est moins répandu que les autres. Si le FSI utilise ce type d'adressage, il est nécessaire de connaître l'adresse IP, le masque de sous-réseau ainsi l'adresse de la passerelle du FSI. Ces informations sont disponibles auprès du FSI ou sur les documents qu'il distribue à ses abonnés. Entrer les informations, puis cliquer sur **Apply Changes** (Enregistrer les modifications). Une fois les modifications effectuées, le témoin **Internet Status** (État Internet) affiche **connection OK** (Connexion OK) si le routeur est correctement configuré.



Réglage du type de connexion FSI comme « PPPoE »

La plupart des fournisseurs de services DSL utilisent une connexion de type PPPoE. Si la connexion à l'Internet s'effectue au moyen d'un modem DSL, il est possible que le FSI utilise le protocole PPPoE pour fournir le service. Si une connexion Internet, à la maison ou dans une petite entreprise, n'utilise pas de modem, il est possible qu'elle utilise également le protocole PPPoE.



La connexion est de type PPPoE si :

- Le FSI a attribué un nom d'utilisateur et un mot de passe, qui sont requis pour se connecter à l'Internet;
- Le FSI a donné un logiciel tel que WinPOET ou Enternet300 à utiliser pour accéder à l'Internet; ou
- Il faut double-cliquer sur une icône du bureau, autre que celle du navigateur, pour accéder à l'Internet.

Saisir ce qui suit :

User Name (Nom d'utilisateur) – Cet espace est prévu pour saisir le nom d'utilisateur qui a été attribué par le FSI.

Password (Mot de passe) – Entrer le mot de passe et le retaper dans la zone *Retype Password* (Confirmer le mot de passe) pour le confirmer.

Service Name (Nom du service) – Un nom de service est rarement requis par un FSI. À moins d'avoir établi avec certitude que le FSI exige un nom de service, laisser ce champ vide.

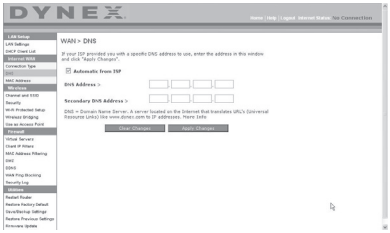
MTU – Le paramètre MTU ne devrait jamais être modifié, à moins que le FSI ne fournisse un paramètre MTU spécifique. Apporter des modifications aux valeurs MTU peut causer des problèmes pour la connexion à l'Internet, y compris déconnexion de l'Internet, accès lent à l'Internet et difficultés avec des applications Internet qui fonctionnaient correctement auparavant.

Disconnect after X minutes… (Déconnecter après X minutes...) – Cette fonction permet de déconnecter automatiquement le routeur du FSI en l'absence d'activité pendant une durée déterminée. Par exemple, si cette option est cochée et que la valeur **5** est entrée dans le champ des minutes, le routeur se déconnectera de l'Internet après 5 minutes d'inactivité Internet. Cette option devrait être utilisée si le service Internet est facturé à la minute.

Définition des paramètres personnalisés du serveur de noms de domaine (DNS)

Un serveur de noms de domaine (*Domain Name Server*) est un serveur situé sur Internet qui traduit les URL (Universal Resource Locators), telles que « www.dynex.com », en adresses IP. La plupart des FSI n'exigent pas que cette information soit entrée dans le routeur. La case **Automatic from ISP** (Obtenir automatiquement du FSI) doit être cochée si le FSI n'a pas fourni d'adresse DNS particulière. En cas d'utilisation d'un type de connexion avec adresse IP statique, il pourra être nécessaire d'entrer une adresse DNS particulière, ainsi qu'une adresse DNS secondaire, pour que la connexion fonctionne correctement. Si la connexion est de type dynamique ou PPPoE, il ne sera probablement pas nécessaire d'entrer une adresse DNS. Laisser la case **Automatic from ISP** (Obtenir automatiquement du FSI) cochée. Pour entrer

les paramètres d'adresse DNS, désélectionner la case **Automatic from ISP** (Obtenir automatiquement du FSI) et entrer les numéros DNS dans les espaces fournis à cet effet. Cliquer sur **Apply Changes** (Enregistrer les modifications) pour enregistrer les paramètres.



Configuration de l'adresse MAC (Media Access Controller) WAN

Tous les composants réseau, y compris les cartes, les adaptateurs et les routeurs, possèdent un « numéro de série » unique appelé une adresse MAC. Il est possible qu'un FSI enregistre l'adresse MAC de l'adaptateur d'un ordinateur et n'autorise que cet ordinateur à accéder à l'Internet. Après l'installation du routeur, c'est sa propre adresse MAC qui sera « vue » par le FSI, ce qui risque de faire échouer la connexion. Dynex permet de cloner (copier) l'adresse MAC de l'ordinateur sur le routeur. Cette adresse MAC, à son tour, sera vue par le système du FSI comme l'adresse MAC d'origine et permettra la connexion. Si la politique du FSI à l'égard de l'adresse MAC d'origine n'est pas connue, cloner simplement l'adresse MAC de l'ordinateur qui était au départ connecté au modem. Le clonage de l'adresse ne causera aucun problème au niveau du réseau.

Pour cloner l'adresse MAC :

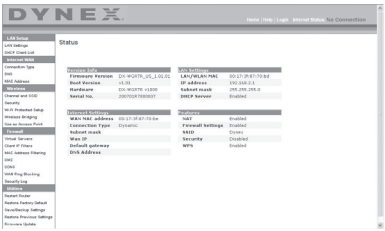
1. Veiller à utiliser l'ordinateur qui était CONNECTÉ À L'ORIGINE au modem avant que le routeur ne soit installé.
2. Cliquer sur **Clone** (Cloner), puis sur **Apply Changes** (Enregistrer les modifications). L'adresse MAC est désormais clonée sur le routeur.

Pour entrer une adresse MAC spécifique :

- Entrer une adresse MAC dans les espaces fournis à cet effet, puis cliquer sur **Apply Changes** (Enregistrer les modifications) pour enregistrer les changements. L'adresse MAC WAN du routeur est alors remplacée par l'adresse MAC spécifiée.

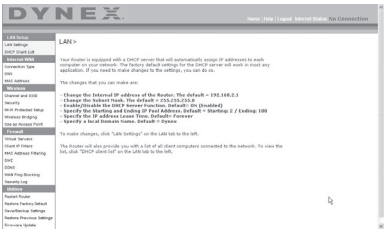
Utilisation de l'Interface utilisateur Web avancée

Grâce au navigateur Internet, il est possible d'accéder à l'Interface utilisateur Web avancée du routeur. Ouvrir le navigateur et entrer **192.168.2.1** (n'entrer aucun autre élément, comme « http:// » ou « www »), puis appuyer sur **Enter** (Entrée). La page d'accueil du routeur s'affiche dans le navigateur.



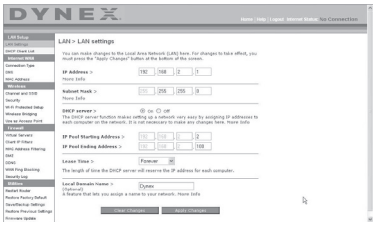
Affichage des paramètres LAN

Cliquer sur l'onglet intitulé **LAN Setup** (Configuration du réseau local) pour accéder à la page d'accueil correspondante. Celle-ci contient une brève description des fonctions. Pour afficher les paramètres ou modifier un des paramètres du réseau local, cliquer sur **LAN Settings** (Paramètres du réseau local) ou, pour afficher la liste des ordinateurs connectés, cliquer sur **DHCP Client List** (Liste des clients DHCP).



Modifications des paramètres LAN

Tous les paramètres de configuration du réseau local interne du routeur peuvent être affichés ou modifiés sur cette page.



IP Address (Adresse IP) – *IP address* représente l'adresse IP interne du routeur. L'adresse IP par défaut est **192.168.2.1**. Pour accéder à l'Interface utilisateur Web avancée, entrer cette adresse IP dans la barre d'adresse du navigateur. Si besoin, cette adresse peut être modifiée. Pour modifier l'adresse IP, entrer la nouvelle adresse, puis cliquer sur **Apply Changes** (Enregistrer les modifications). L'adresse IP choisie doit être une adresse IP non-acheminable.

Exemples d'IP non-acheminables : 192.168.x.x (où x est un nombre compris entre 0 et 255) et 10.x.x.x (où x est un nombre compris entre 0 et 255).

Subnet Mask (Masque de sous-réseau) – Il est inutile de modifier le masque de sous-réseau. Il s'agit d'une fonctionnalité unique et avancée du routeur Dynex. Il est possible de changer le masque de sous-réseau, si nécessaire. Toutefois, ne PAS le modifier à moins d'avoir une raison particulière de le faire. La valeur par défaut est **255.255.255.0**.

DHCP Server (Serveur DHCP) – La fonction de serveur DHCP facilite grandement la configuration du réseau grâce à l'attribution automatique d'adresses IP à tous les ordinateurs du réseau. La valeur par défaut est **On** (Activé). Le serveur DHCP peut être désactivé, si nécessaire. Toutefois, pour le désactiver, il faut définir manuellement une adresse IP statique pour chaque ordinateur du réseau. Pour désactiver le serveur DHCP, sélectionner l'option **Off** (Désactivé), puis cliquer sur **Apply Changes** (Enregistrer les modifications).

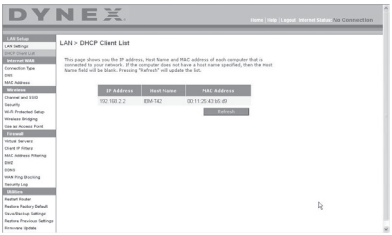
IP Pool (Pool d'adresses IP) – Plage d'adresses IP mises de côté pour l'affectation dynamique aux ordinateurs du réseau. La valeur par défaut est 2–100 (99 ordinateurs). Pour changer ce nombre, entrer de nouvelles adresses IP de début et de fin, puis cliquer sur **Apply Changes** (Enregistrer les modifications). Le serveur DHCP peut attribuer automatiquement 100 adresses IP. Cela signifie qu'il n'est pas possible de spécifier un pool d'adresses IP supérieur à 100 ordinateurs. Par exemple, si on commence à 50, cela signifie qu'il faut terminer à 150 ou à moins, de manière à ne pas dépasser la limite des 100 clients. L'adresse IP de début doit avoir un numéro inférieur à celui de l'adresse IP de fin.

Lease Time (Durée du bail) – Durée pendant laquelle le serveur DHCP réserve l'adresse IP de chaque ordinateur. Dynex conseille de laisser la durée du bail à **Forever** (Toujours). La valeur par défaut est **Forever** (Toujours), ce qui signifie que chaque fois que le serveur DHCP attribue une adresse IP à un ordinateur, cette adresse ne changera pas pour l'ordinateur. L'affectation en tant que durées de bail d'intervalles plus courts, comme un jour ou une heure, permet de libérer les adresses IP une fois la durée écoulée. Cela signifie également que l'adresse IP d'un ordinateur peut changer. Si d'autres fonctionnalités avancées du routeur ont été définies, comme la DMZ ou les filtres IP de clients, elles dépendent de l'adresse IP. Pour cette raison, il n'est pas recommandé que l'adresse IP change.

Local Domain Name (Nom du domaine local) – Le paramètre par défaut est **Dynex**. Il est possible de définir un nom de domaine local (nom de réseau) pour le réseau. Il est inutile de changer ce paramètre à moins d'avoir un réel besoin de le faire. Il est possible de donner n'importe quel nom au réseau (« MON RÉSEAU », par exemple).

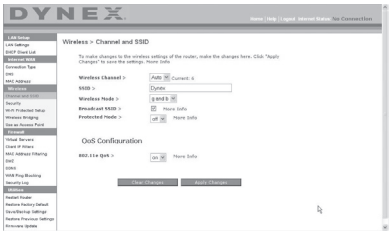
Affichage de la liste des clients DHCP

Il est possible d'afficher la liste des ordinateurs (appelés des clients) qui sont connectés au réseau. Il est possible d'afficher l'adresse IP de l'ordinateur, le nom d'hôte (si l'ordinateur en a un) ainsi que l'adresse MAC de la carte d'interface réseau (NIC) de l'ordinateur. Cliquer sur **Refresh** (Actualiser) pour mettre la liste à jour. Si des changements ont eu lieu, la liste sera mise à jour.



Configuration des paramètres du réseau sans fil

Cliquer sur l'onglet intitulé **Wireless** (Sans fil) pour accéder à la page *Wireless* (Sans fil). Sous l'onglet **Wireless** (Sans fil) se trouvent des liens qui permettent de modifier les paramètres du réseau sans fil.



Modification du nom du réseau sans fil (SSID)

Un SSID (Service Set Identifier) est utilisé pour identifier le réseau sans fil. Le SSID par défaut du routeur est « Dynex ». L'utilisateur est libre de choisir ce qu'il veut ou de le laisser inchangé. Si d'autres réseaux sans fil fonctionnent dans le secteur, il faudra s'assurer que le SSID est unique (qu'il ne correspond pas à celui d'un autre réseau sans fil de la zone). Pour modifier le SSID, entrer le SSID souhaité dans le champ **SSID** et cliquer sur **Apply Changes** (Enregistrer les informations). Le changement est immédiat. En cas de changement du SSID, les ordinateurs sans fil devront également être reconfigurés pour se connecter au nouveau nom du réseau. Se reporter à la documentation de l'adaptateur réseau sans fil pour obtenir des informations sur la procédure à suivre pour effectuer cette modification.

Utilisation du commutateur de mode sans fil

Le routeur est en mesure de fonctionner sous trois modes sans fil différents : « g and b », « g only » et « b only ». Ces différents modes sont décrits ci-dessous.

Mode « g and b » – Dans ce mode, le routeur est compatible avec des clients sans fil 802.11b et 802.11g, de façon simultanée. Ce mode est le mode par défaut, et il assure un bon fonctionnement avec tous les dispositifs Wi-Fi compatibles. Si le réseau comprend à la fois des clients 802.11b et 802.11g, Dynex recommande le mode « g and b » pour le routeur. Ne pas modifier ce paramètre à moins d'avoir une raison particulière de le faire.

Mode « g only » – Ce mode ne fonctionne qu'avec des clients 802.11g. Ce mode n'est recommandé que pour empêcher les clients 802.11b d'accéder au réseau. Pour changer de mode, sélectionner le mode souhaité dans la liste **Wireless Mode** (Mode sans fil), puis cliquer sur **Apply Changes** (Enregistrer les modifications).

Mode « b only » – Il n'est PAS recommandé d'utiliser ce mode à moins d'avoir une raison très particulière de le faire. Ce mode existe dans l'unique but de résoudre les problèmes pouvant survenir avec certains adaptateurs 801.11b et n'est PAS nécessaire pour assurer l'interopérabilité entre les normes 802.11b et 802.11g.

Quand utiliser le mode « b only » – Parfois, des clients 802.11b plus anciens peuvent ne pas être compatibles avec le sans fil 802.11g. Ces adaptateurs sont généralement de qualité inférieure et peuvent utiliser des pilotes ou des technologies plus anciennes. Le choix de ce mode peut résoudre certains problèmes rencontrés avec ces clients. Si le client utilisé semble faire partie de cette catégorie d'adaptateurs, vérifier d'abord auprès du fabricant de l'adaptateur s'il existe une mise à jour des pilotes. En l'absence de mise à jour disponible, il se peut que l'utilisation du mode « b only » puisse résoudre le problème. Noter que l'utilisation du mode « b only » diminuera les performances du réseau 802.11g.

Configuration QoS (Quality of Service) – QoS établit la priorité des données sur le réseau, telles que le contenu multimédia et la téléphonie Internet (VoIP), de manière à éviter les interférences avec d'autres données transmises sur le réseau. Basé sur 802.11e, il est possible d'activer ou de désactiver cette fonction en la sélectionnant dans le menu déroulant (3) et en choisissant le mode d'accusé de réception souhaité. S'il est prévu d'accéder en flux continu à du contenu multimédia ou d'utiliser la téléphonie Internet sur le réseau, Dynex recommande d'activer la fonction QoS.

Modification du canal sans fil

Il est possible de choisir entre plusieurs canaux de fonctionnement. Aux États-Unis, il existe 11 canaux. En Australie, au Royaume-Uni et dans la plupart des pays européens, il existe 13 canaux. Dans un petit nombre d'autres pays, les exigences concernant les canaux sont différentes. Le routeur est configuré de façon à fonctionner sur les canaux appropriés pour le pays de résidence de l'utilisateur. Le canal par défaut est 11 (à moins que l'utilisateur ne réside dans un pays où le canal 11 est interdit). Si besoin est, le canal peut être modifié. Si d'autres réseaux sans fil fonctionnent dans le secteur, le réseau doit être configuré de manière à fonctionner sur un canal différent de celui des autres réseaux sans fil. Pour un bon fonctionnement, utiliser un canal qui se trouve au moins à cinq canaux d'écart d'un autre réseau sans fil. Par exemple, si un autre réseau fonctionne sur le canal 11, choisir le canal 6 ou inférieur pour celui-ci. Pour changer de canal, sélectionner le canal souhaité dans la liste, puis cliquer sur **Apply Changes** (Enregistrer les modifications). Le changement est immédiat.

Utilisation de la fonction Broadcast SSID (Diffusion du SSID)

Remarque : *Cette fonctionnalité avancée doit uniquement être employée par des utilisateurs expérimentés.*

Pour plus de sécurité, choisir de ne pas diffuser le SSID du réseau. Ainsi, le nom du réseau demeurera caché pour les ordinateurs qui recherchent la présence de réseaux sans fil. Pour désactiver la diffusion du SSID, désélectionner la case en regard de **Broadcast SSID** (Diffusion du SSID), puis cliquer sur **Apply Changes** (Enregistrer les modifications). Le changement est immédiat. Chaque ordinateur doit maintenant être configuré pour se connecter au SSID spécifique. Le paramètre **ANY** (TOUS) pour le SSID ne sera plus accepté. Se reporter à la documentation de l'adaptateur réseau sans fil pour obtenir des informations sur la procédure à suivre pour effectuer cette modification.

Protected Mode Switch (Commutateur en mode protégé) – Faisant partie de la spécification 802.11g, le mode protégé assure un fonctionnement satisfaisant des clients et points d'accès 802.11g en présence d'un trafic 802.11b dense dans l'environnement d'exploitation. Lorsque le mode protégé est **ON** (Activé), le 802.11g effectue un balayage pour détecter le trafic d'autres réseaux sans fil avant de transmettre les données. Par conséquent, l'utilisation de ce mode dans un environnement avec un trafic 802.11b DENSE ou comportant des interférences permet d'obtenir les meilleurs résultats. Dans un environnement avec très peu, voire pas du tout, de trafic issu d'autres réseaux sans fil, les meilleures performances seront obtenues en désactivant le mode protégé (**OFF**).

Sécurisation du réseau Wi-Fi[MD]

Voici quelques façons d'optimiser la sécurité du réseau sans fil et de protéger les données des yeux et oreilles indiscrets. Cette section est destinée aux utilisateurs de réseaux sans fil à domicile ou dans de petites entreprises.

À la date de publication de ce manuel, quatre méthodes de cryptage sont disponibles.

	Wired Equivalent Privacy 64 bits	**Wired Equivalent Privacy 128 bits**	**Wi-Fi Protected Access-TKIP**	**Wi-Fi Protected Access 2**
Acronyme	WEP 64 bits	WEP 128 bits	WPA-TKIP/AES (ou juste WPA)	WPA2-AES (ou juste WPA2)
Sécurité	Bonne	Meilleure	Optimale	Optimale
Fonctionnalités	Clés statiques	Clés statiques	Cryptage à clé dynamique et authentification réciproque.	Cryptage à clé dynamique et authentification réciproque.
	Clés de cryptage basées sur l'algorithme RC4 (généralement clés de 40 bits).	Plus sûr que le WEP 64 bits en utilisant une longueur de clé de 104 bits plus 24 bit supplémentaires de données générées par le système.	TKIP (Temporal Key Integrity Protocol) ajouté afin que les clés soient permutées et le cryptage renforcé.	AES (Advanced Encryption Standard) ne cause aucune perte de débit

WEP (Wired Equivalent Privacy)

Le WEP est un protocole courant qui fournit une sécurité à tous les produits sans fil compatibles Wi-Fi. Le WEP donne aux réseaux sans fil un niveau de protection équivalent à celui d'un réseau câblé comparable.

WEP 64 bits – Le WEP 64 bits a été introduit la première fois avec un cryptage sur 64 bits, ce qui comprend une clé de 40 bits plus 24 bits supplémentaires composés de données générées par le système (64 bits au total). Certains fabricants parlent de cryptage sur 40 bits lorsqu'ils font référence au cryptage sur 64 bits. Peu après le lancement de la technologie, des chercheurs ont découvert que le cryptage sur 64 bits était trop simple à décoder.

Cryptage 128 bits – Pour contrer la faille de sécurité du WEP 64 bits, une méthode de cryptage plus sécurisée, le WEP 128 bits, a été créée. Le WEP 128 bits comprend une clé de 104 bits plus 24 bits supplémentaires composés de données générées par le système (128 bits au total). Certains fabricants parlent de cryptage sur 104 bits lorsqu'ils font référence au cryptage sur 128 bits. La plupart des nouveaux dispositifs sans fil disponibles sur le marché aujourd'hui prennent en charge le cryptage WEP 64 bits et 128 bits, mais il se peut que des dispositifs plus anciens ne prennent en charge que le WEP 64 bits. Tous les produits sans fil de Dynex prennent en charge le WEP 64 bits et 128 bits.

WEP Encryption Keys (Clés de cryptage WEP) – Après avoir sélectionné le mode de cryptage WEP 64 bits ou 128 bits, il est essentiel de générer une clé de cryptage. Si la clé de cryptage n'est pas la même dans tout le réseau sans fil, les dispositifs du réseau sans fil ne pourront pas communiquer les uns avec les autres. La clé peut être saisie en tapant manuellement la clé hexadécimale, ou en tapant un mot de passe dans le champ **Passphrase** (Mot de passe), puis en cliquant sur **Generate** (Générer) pour créer une clé. Une clé hexadécimale est une combinaison de chiffres et de lettres de A à F et de 0 à 9. Pour le mode WEP 64 bits, il faut entrer 10 caractères hexadécimaux. Pour le mode WEP 128 bits, il faut entrer 26 caractères hexadécimaux.

Par exemple :

AF 0F 4B C3 D4 = clé pour WEP 64 bits

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = clé pour WEP 128 bits

Le mot de passe WEP n'est PAS la même chose que la clé WEP. La carte utilise ce mot de passe pour générer les clés WEP, mais différents fabricants de matériel peuvent avoir différentes méthodes pour générer les clés. Si le réseau comporte des équipements de différentes marques, le plus simple est d'utiliser la clé WEP hexadécimale du routeur sans fil et de l'entrer manuellement dans le tableau des clés WEP hexadécimales de l'écran de configuration de la carte.

Synchronisation de sécurité (WPS)

La routeur est équipé de la dernière norme de sécurité, appelée *Wi-Fi Protected Access* (WPA2), et de l'ancienne norme de sécurité, appelée *Wired Equivalent Privacy* (WEP). Il prend également en charge la spécification *Wi-Fi Protected Setup* (WPS), qui simplifie la configuration d'un réseau sans fil. WPS utilise des méthodologies familières, comme saisir un *numéro d'identification personnel* (NIP) ou appuyer sur une touche, pour permettre aux utilisateurs de configurer automatiquement les noms des réseaux et les protocoles WPA/WPA2 de cryptage et d'authentification des données. Par défaut, la sécurité sans fil est

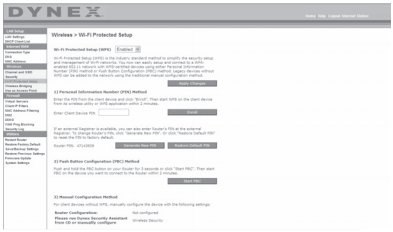
désactivée. Pour activer la sécurité, il faut d'abord déterminer quelle norme sera utilisée. Pour accéder aux paramètres de sécurité de la carte, cliquer sur **Security** (Sécurité) sous l'onglet **Wireless** (Sans fil).

Utilisation de la synchronisation de sécurité (WPS)

La synchronisation de sécurité (WPS) utilise WPA2 pour le cryptage. Elle ne fournit aucune sécurité supplémentaire, mais standardise la méthode de sécurisation du réseau sans fil. Il est possible d'utiliser soit la méthode de configuration du bouton-poussoir (PBC), soit la méthode NIP pour permettre à un dispositif d'accéder au réseau sans fil. Conceptuellement, les deux méthodes fonctionnent comme suit :

PBC : Appuyer sur la touche de synchronisation de sécurité (WPS), située sur le dessus du routeur, sans la relâcher pendant trois secondes. Entamer ensuite la procédure de synchronisation de sécurité (WPS) sur le client au cours des deux minutes suivantes. Le client échangera automatiquement les informations de sécurité et sera ajouté au réseau sans fil. Le client a maintenant été ajouté de façon sécurisée au réseau sans fil. Le fait d'appuyer sur la touche de synchronisation de sécurité activera automatiquement WPS. La méthode PBC peut également être lancée depuis un ordinateur portatif.

NIP : Le périphérique client est doté d'un numéro NIP (de quatre ou huit caractères) qui est associé à WPS. Activer WPS au moyen de l'interface utilisateur illustrée ci-dessous. Entrer le NIP du client dans le registre interne du routeur (accessible au moyen de cette IU). Le client sera automatiquement admis dans le réseau sans fil en moins de deux minutes.



1. Wi-Fi Protected Setup (WPS) : Enabled (Activé) ou Disabled (Désactivé).
2. Méthode du numéro d'identification personnel (NIP) : Avec cette méthode, un client sans fil souhaitant accéder au réseau doit fournir au routeur un NIP de 4 ou 8 caractères. Après avoir cliqué sur « Enroll » (Inscription), il faut démarrer le protocole de transfert WPS à partir du client au cours des deux minutes suivantes.
3. NIP du routeur : Si un registre externe est disponible, il est possible d'entrer le NIP du routeur dans le registre. Cliquer sur **Generate New PIN** (Générer nouveau NIP) pour remplacer la valeur par défaut du NIP, ou cliquer sur **Restore Default PIN** (Rétablir NIP par défaut) pour réinitialiser la valeur du NIP.
4. Méthode de configuration du bouton-poussoir (PBC) : PBC est une autre méthode permettant de se connecter à un réseau WPS. Appuyer sur la touche de synchronisation de sécurité, située au dos du routeur, pendant trois secondes, puis initier la configuration PBC sur le périphérique client. Il est également possible de cliquer sur « Start PBC » (Démarrer PBC) pour démarrer ce processus.

5. Méthode de configuration manuelle : Cette section indique les paramètres de sécurité par défaut si WPS n'est pas utilisé.

Le routeur est équipé de WPA2, qui est la deuxième génération de la norme 802.11i basée sur le WPA. Elle offre un niveau plus élevé de sécurité sans fil en combinant des méthodes avancées d'authentification de réseau et des méthodes de cryptage AES (Advanced Encryption Standard) plus robustes.

WPA (Wi-Fi Protected Access)

Le WPA est une nouvelle norme Wi-Fi qui apporte des améliorations aux caractéristiques de sécurité du WEP. Pour utiliser la sécurité WPA, les pilotes et le logiciel des appareils sans fil doivent être mis à niveau pour en assurer la prise en charge. Ces mises à niveau se trouvent sur le site Web du fournisseur des appareils sans fil. Il existe trois types de sécurité WPA : WPA-PSK (pas de serveur), WPA (avec serveur RADIUS) et WPA2.

WPA-PSK (pas de serveur) utilise en tant que clé de réseau ce que l'on appelle une clé pré-partagée. Une clé de réseau est un mot de passe qui comporte de 8 à 63 caractères. Cela peut être une combinaison de lettres, de chiffres ou de caractères. Chaque client utilise la même clé de réseau pour accéder au réseau. Généralement, il s'agit du mode utilisé dans un environnement familial.

WPA (avec serveur RADIUS) est un système dans lequel un serveur RADIUS distribue automatiquement la clé du réseau aux clients. Ceci se trouve généralement dans un environnement professionnel.

WPA2 utilise AES (Advanced Encryption Standard) pour le cryptage des données, offrant ainsi une sécurité bien supérieure à WPA. Le WPA utilise à la fois le protocole TKIP (Temporal Key Integrity Protocol) et AES pour le cryptage.

La plupart des produits Wi-Fi sont expédiés sans qu'aucune sécurité ne soit activée. Aussi, une fois que le réseau fonctionne, il faut activer le WEP ou le WPA et vérifier que tous les dispositifs sans fil partagent la même clé de réseau.

***IMPORTANT**: Il faut maintenant configurer toutes les cartes réseau pour qu'elles correspondent à ces paramètres.*

Partage des clés réseau

La plupart des produits Wi-Fi sont expédiés sans qu'aucune sécurité ne soit activée. Aussi, une fois que le réseau fonctionne, il faut activer le WEP ou le WPA et vérifier que tous les dispositifs de réseau sans fil partagent la même clé de réseau.

La carte réseau sans fil G pour ordinateur de bureau ne peut pas accéder au réseau parce qu'elle utilise une clé réseau différente de celle configurée sur le routeur sans fil G.

Utilisation d'une clé hexadécimale

Une clé hexadécimale est un mélange de chiffres et de lettres de A à F et de 0 à 9. Les clés de 64 bits sont constituées de cinq nombres de deux chiffres. Les clés de 128 bits sont constituées par 13 nombres de deux chiffres.

Par exemple :

AF 0F 4B C3 D4 = clé 64 bits

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = clé 128 bits

Remarque pour les utilisateurs de Mac : *Les produits AirPort*[MD] *d'Apple*[MD] *de première génération ne prennent en charge que le cryptage sur 64 bits. Les produits Apple AirPort 2 prennent en charge le cryptage sur 64 bits ou 128 bits. Vérifier le produit pour savoir quelle est la version utilisée. S'il n'est pas possible de configurer le réseau avec le cryptage sur 128 bits, essayer le cryptage sur 64 bits.*

Configuration du WEP

Pour configurer le cryptage WEP 64 bits :

1. Cliquer sur **Security** (Sécurité) sous l'en-tête **Wireless** (Sans fil) du menu de gauche. La page *Wireless* > *Security* (Sans fil > Sécurité) s'affiche.
2. Sélectionner **64-bit WEP** (WEP 128 bits) dans la liste **Security Mode** (Mode de sécurité).
3. Entrer la clé en saisissant manuellement la clé hexadécimale, ou cocher la case **Passphrase** (Mot de passe), puis saisir le mot de passe.
4. Cliquer sur **Generate** (Générer) pour générer quatre clés hexadécimales différentes.

   Une clé hexadécimale est une combinaison de chiffres et de lettres de A à F et de 0 à 9. Pour le mode WEP 64 bits, il faut entrer 10 clés hexadécimales.

   Par exemple : AF 0F 4B C3 D4 = clé pour WEP 64 bits
5. Cliquer sur **Apply Changes** (Enregistrer les modifications) pour enregistrer les paramètres.

   Attention *: Si le routeur sans fil ou le point d'accès sans fil G est configuré à partir d'un ordinateur doté d'un client sans fil, il faut s'assurer que la sécurité est activée (ON) pour ce client sans fil. Sinon, le client perdra sa connexion sans fil.*

Pour configurer le cryptage WEP 128 bits :

Remarque pour les utilisateurs de Mac : *L'option de mot de passe ne fonctionne pas avec Apple AirPort. Pour configurer le cryptage sur un ordinateur Mac, utiliser la méthode manuelle décrite dans la section suivante.*

1. Cliquer sur **Security** (Sécurité) sous l'en-tête **Wireless** (Sans fil) du menu de gauche. La page *Wireless* > *Security* (Sans fil > Sécurité) s'affiche.
2. Sélectionner **128-bit WEP** (WEP 128 bits) dans la liste **Security Mode** (Mode de sécurité).
3. Entrer la clé en saisissant manuellement la clé hexadécimale, ou cocher la case **Passphrase** (Mot de passe), puis saisir le mot de passe.
4. Cliquer sur **Generate** (Générer) pour générer quatre clés hexadécimales différentes.

Une clé hexadécimale est une combinaison de chiffres et de lettres de A à F et de 0 à 9. Pour le mode WEP 128 bits, il faut entrer 26 clés hexadécimales.

Par exemple : C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = clé pour WEP 128 bits

5 Cliquer sur **Apply Changes** (Enregistrer les modifications) pour enregistrer les paramètres.

***Attention** : Si le routeur sans fil ou le point d'accès sans fil G est configuré à partir d'un ordinateur doté d'un client sans fil, il faut s'assurer que la sécurité est activée (ON) pour ce client sans fil. Sinon, le client perdra sa connexion sans fil.*

Modification des paramètres de sécurité sans fil

Le routeur comprend la toute dernière norme de sécurité, appelée WPA (Wi-Fi Protected Access). En outre, il prend en charge les normes de sécurité plus anciennes telles que le WEP (Wired Equivalent Privacy). Par défaut, la sécurité sans fil est désactivée. Pour activer la sécurité, il faut d'abord déterminer quelle norme sera utilisée. Pour accéder aux paramètres de sécurité, cliquer sur **Security** (Sécurité) sous l'onglet **Wireless** (Sans fil).

Configuration du WPA

***Remarque** : Pour utiliser la sécurité WPA, tous les clients doivent être mis à jour avec les logiciels et les pilotes qui la prennent en charge. À la date de publication de ce manuel, un correctif de sécurité est disponible pour téléchargement gratuit, auprès de Microsoft*[MD]*. Ce correctif ne fonctionne qu'avec Windows XP. Il faudra également télécharger sur le site d'assistance technique de Dynex le pilote le plus récent pour la carte réseau sans fil G de Dynex pour ordinateur de bureau ou portatif. À l'heure actuelle, les autres systèmes d'exploitation ne sont pas pris en charge. Le correctif de Microsoft ne prend en charge que les dispositifs avec pilotes compatibles WPA, tels que les produits 802.11g de Dynex.*

Le WPA utilise ce qu'on appelle une « clé pré-partagée » en tant que clé de sécurité. Une clé pré-partagée est en fait un mot de passe composé de 8 à 63 caractères. Elle peut être une combinaison de lettres, de chiffres et d'autres caractères. Chaque client utilise la même clé pour accéder au réseau. Généralement, ce mode est utilisé dans un environnement familial.

Le WPA2, c'est le WPA de seconde génération. Il offre une technique de cryptage plus avancée que le WPA.

Pour configurer le WPA/WPA2 :

1 Cliquer sur **Security** (Sécurité) sous l'en-tête **Wireless** (Sans fil) du menu de gauche. La page *Wireless* > *Security* (Sans fil > Sécurité) s'affiche.

2 Sélectionner **WPA/WPA2-Personal (PSK)** dans la liste **Security Mode** (Mode de sécurité).

3 Sélectionner **WPA-PSK** pour une simple authentification WPA, ou **WPA2-PSK** pour une simple authentification WPA2; il est également possible de sélectionner **WPA-PSK + WPA2-PSK** pour choisir WPA et WPA2 comme type d'authentification.

4 Entrer la clé pré-partagée. Elle peut contenir de 8 à 63 caractères, qui peuvent être des lettres, des chiffres ou des symboles. Cette même clé doit être utilisée sur tous les clients qui seront configurés. Cette clé pré-partagée donnera aux utilisateurs un accès complet au réseau, y compris aux fichiers et imprimantes partagés.

5 Cliquer sur **Apply Changes** (Appliquer les modifications) pour terminer. Il faut maintenant configurer tous les clients avec ces paramètres, suivant le type d'accès souhaité pour chacun d'eux.

Remarque : *Si une carte sans fil n'est pas équipée d'un logiciel compatible WPA, un fichier de Microsoft, appelé* ***Windows XP Support Patch for Wireless Protected Access****, peut être téléchargé gratuitement.*

Le fichier mis à disposition par Microsoft fonctionne uniquement avec Windows XP. À l'heure actuelle, les autres systèmes d'exploitation ne sont pas pris en charge.

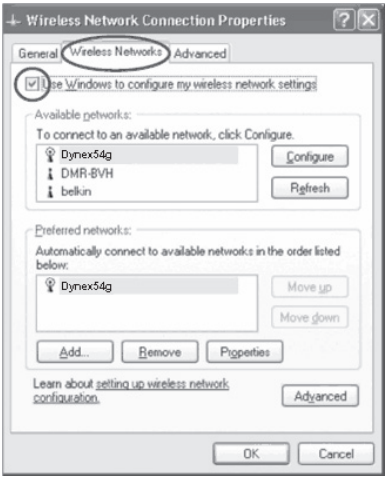
Important *: Il faudra également vérifier que le fabricant de la carte sans fil prend en charge le WPA et que le pilote le plus récent a été téléchargé à partir de son site Web et installé.*

Configuration de l'utilitaire réseau sans fil de Windows XP pour utiliser le WPA-PSK :

1 Sous Windows XP, cliquer sur **Start** (Démarrer), **Control Panel** (Panneau de configuration) et **Network Connections** (Connexions réseau).

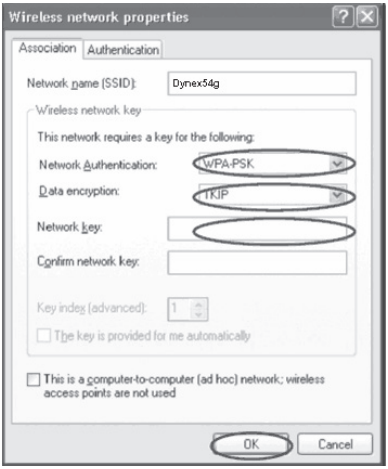
2 Cliquer à l'aide du bouton droit de la souris sur **Wireless Network Connection** (Connexion réseau sans fil), puis sur **Properties** (Propriétés).

3 Cliquer sur l'onglet **Wireless Networks** (Réseaux sans fil). L'écran suivant s'affiche.



4 Vérifier que la case **Use Windows to configure my wireless network settings** (Utiliser Windows pour configurer mes paramètres réseau sans fil) est cochée.

5 Cliquer sur l'onglet **Wireless Networks** (Réseaux sans fil), puis sur **Configure** (Configurer). L'écran suivant s'affiche.



6 Pour un utilisateur de réseau familial ou de petite entreprise, sélectionner **WPA-PSK** sous **Network Authentication** (Authentification de réseau).

***Remarque**: Sélectionner **WPA** si cet ordinateur est utilisé pour se connecter à un réseau d'entreprise qui prend en charge un serveur d'authentification tel qu'un serveur RADIUS. Consulter l'administrateur réseau pour de plus amples informations.*

7 Sélectionner **TKIP** ou **AES** sous **Data Encryption** (Cryptage des données). Ce paramètre doit être identique à celui configuré sur le routeur.

8 Entrer la clé de cryptage dans la boîte **Network Key** (Clé de réseau).

***Important** : Entrer la clé pré-partagée. Elle peut contenir de 8 à 63 caractères, qui peuvent être des lettres, des chiffres ou des symboles. Cette même clé doit être utilisée sur tous les clients qui seront configurés.*

9 Cliquer sur **OK** pour enregistrer les modifications.

Utilisation du mode Point d'accès

***Remarque** : Cette fonctionnalité avancée doit uniquement être employée par des utilisateurs expérimentés. Il est possible de configurer le routeur pour qu'il fonctionne comme un point d'accès réseau sans fil. L'utilisation de ce mode bloque la fonction de partage IP NAT et de serveur DHCP. En mode « Point d'Accès » (AP), le routeur doit être configuré avec une adresse IP qui doit se trouver dans le même sous-réseau que le reste du réseau vers lequel une passerelle sera établie. L'adresse IP par défaut est 192.168.2.254 et le masque de sous-réseau est 255.255.255.0. Ces adresses peuvent être modifiées au besoin.*

Pour utiliser le mode Point d'accès :

1. Cliquer sur **Use as Access Point only** (Utiliser uniquement comme point d'accès) sous l'en-tête **Wireless** (Sans fil) du menu de gauche. La page *Wireless > Use as Access Point* (Sans fil > Utiliser comme point d'accès) s'affiche.

2. Sélectionner **Enable** (Activer). Lorsque cette option est sélectionnée, elle permet de modifier les paramètres IP.
3. Configurer les paramètres IP de manière à ce qu'ils correspondent à ceux du réseau, puis cliquer sur **Apply Changes** (Enregistrer les Modifications).
4. Connecter un câble depuis le port modem du routeur sur le réseau existant.

   Le routeur joue maintenant le rôle de point d'accès. Pour accéder de nouveau à l'Interface utilisateur Web avancée du routeur, taper l'adresse IP spécifiée dans la barre d'adresse du navigateur. Les paramètres de cryptage, le filtrage des adresses MAC, le SSID et le canal peuvent être configurés normalement.

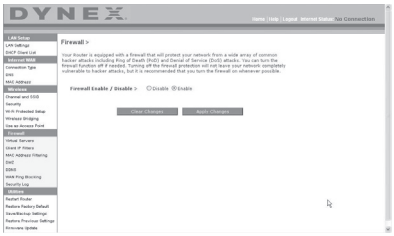
Configuration du pare-feu

Le routeur est équipé d'un pare-feu qui protégera le réseau contre un grand nombre d'attaques habituelles de pirates, notamment :

- Usurpation d'adresse IP (IP Spoofing)
- SYN flood
- Attaque Land
- UDP flooding
- Ping de la mort (PoD)
- Attaque Teardrop
- Déni de service (DoS)
- Défaut ICMP
- IP de longueur nulle
- Défaut RIP
- Attaque Smurf
- Fragment flooding
- TCP Null Scan

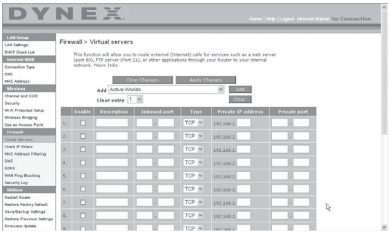
Le pare-feu masque également les ports habituels qui sont fréquemment utilisés pour attaquer les réseaux. Ces ports apparaissent en tant que *stealth* (furtifs), ce qui veut dire en d'autres termes qu'ils n'existent pas pour un pirate potentiel. Si nécessaire, la fonction de

pare-feu peut-être désactivée. Toutefois, Dynex conseille de la laisser activée. La désactivation de la protection par pare-feu ne laissera pas le réseau complètement vulnérable aux attaques des pirates, mais il est conseillé de laisser le pare-feu activé.



Configuration des paramètres de retransmission interne

La fonction *Virtual Servers* (Serveurs virtuels) permet de diriger les appels de service externes (Internet) tels qu'un serveur Web (port 80), un serveur FTP (port 21) ou toute autre application via le routeur vers le réseau interne. Étant donné que les ordinateurs internes sont protégés par un pare-feu, les ordinateurs situés hors du réseau (sur Internet) ne peuvent pas y accéder parce qu'ils ne sont pas *visibles*. Contacter le fournisseur de l'application pour déterminer quels paramètres de ports sont nécessaires.



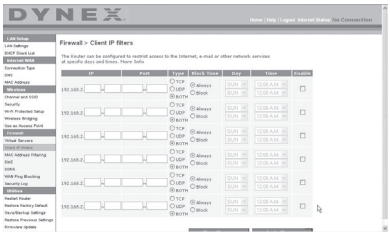
Pour entrer des paramètres dans le serveur virtuel :

1. Ouvrir la page *Virtual Servers* (Serveurs virtuels), puis entrer l'adresse IP dans le champ prévu pour la machine (serveur) interne et les ports requis pour la transmission.
2. Sélectionner le type de port (TCP ou UDP), cliquer sur la case **Enable** (Activer), puis sur **Apply Changes** (Enregistrer les Modifications).

   Chaque entrée de port d'entrée possède deux champs, pouvant contenir cinq caractères maximum. Ces champs délimitent le début et la fin de la plage, soit [xxxxx]-[xxxxx]. Pour chaque entrée, il est possible d'entrer une seule valeur de port en remplissant les deux champs avec la même valeur (par exemple, [7500]-[7500]) ou une plage étendue (par exemple, [7500]-[9000]). Pour sélectionner plusieurs ports uniques, ou plusieurs plages et une valeur unique, il faut utiliser plusieurs entrées, jusqu'à un maximum de 20 (par exemple : 1. [7500]-[7500], 2. [8023]-[8023], 3. [9000]-[9000]). Il est possible de transmettre un seul port par adresse IP interne. L'ouverture de ports dans le pare-feu risque de créer un problème de sécurité. Les paramètres peuvent être activés ou désactivés très rapidement. Aussi, Dynex recommande de les désactiver lorsqu'une application particulière n'est pas utilisée.

Configuration des filtres IP de clients

Il est possible de configurer le routeur de manière à limiter l'accès à l'Internet, à la messagerie électronique ou à d'autres services réseau certains jours et à certaines heures. La restriction peut être définie pour un seul ordinateur, une plage d'ordinateurs ou plusieurs ordinateurs.

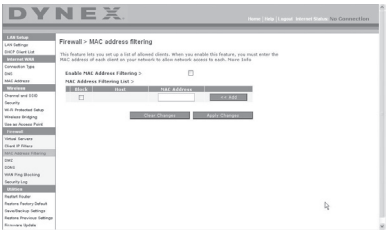


Pour limiter l'accès à l'Internet à un seul ordinateur :

1. Ouvrir la page *Firewall* > *Client IP filters* (Pare-feu > Filtres IP de clients), puis entrer l'adresse IP de l'ordinateur auquel sera limité l'accès dans les champs IP.
2. Entrer **80** dans chaque champ de port, sélectionner **Both** (Les deux), puis sélectionner **Block** (Bloquer). Il est aussi possible de sélectionner **Always** (Toujours) pour bloquer l'accès en permanence.
3. Sélectionner le jour de début en haut, l'heure de début en haut, le jour de fin en bas et l'heure de fin en bas.
4. Sélectionner **Enable** (Activer), puis cliquer sur **Apply Changes** (Enregistrer les modifications). L'ordinateur répondant à l'adresse IP indiquée sera désormais bloqué et ne pourra plus accéder à l'Internet aux heures mentionnées. Veiller à avoir sélectionné le fuseau horaire approprié dans **Utilities**> **System Settings**> **Time Zone** (Utilitaires > Paramètres système > Fuseau horaire).

Configuration du filtrage d'adresses MAC

Le filtrage d'adresses MAC est une fonction de sécurité puissante qui permet de spécifier les ordinateurs autorisés sur le réseau. Tout ordinateur qui tente d'accéder au réseau alors qu'il ne figure pas dans la liste ne pourra pas y accéder. Lorsque cette fonction est activée, il faut entrer l'adresse MAC de chaque client (ordinateur) du réseau pour permettre à chacun d'accéder au réseau.



Pour activer le filtrage d'adresses MAC :

1. Ouvrir la page *Firewall* > *MAC Address filters* (Pare-feu > Filtres d'adresses MAC), puis cliquer sur **Enable MAC Address Filtering** (Activer le filtrage d'adresses MAC).

2 Entrer l'adresse MAC de chaque ordinateur du réseau en cliquant sur le champ prévu et en entrant l'adresse MAC de l'ordinateur à ajouter à la liste.

3 Cliquer sur **Add** (Ajouter), puis sur **Apply Changes** (Enregistrer les modifications) pour enregistrer les paramètres. La liste de filtrage d'adresses MAC peut comprendre jusqu'à 32 ordinateurs.

***Remarque** : Il n'est pas possible de supprimer l'adresse MAC de l'ordinateur qui est utilisé pour accéder aux fonctions d'administration du routeur (celui qui est actuellement en cours d'utilisation).*

Activation de la zone démilitarisée (DMZ)

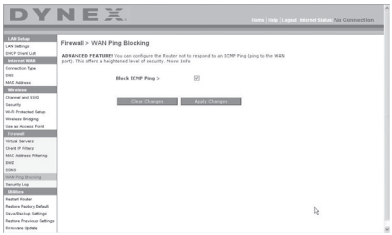
La fonctionnalité DMZ permet de désigner un ordinateur du réseau qui sera placé hors du pare-feu. Ceci peut être nécessaire si le pare-feu cause des problèmes avec une application telle qu'un jeu ou une application de vidéoconférence. Cette fonctionnalité doit être utilisée de façon temporaire. L'ordinateur de la DMZ n'est PAS protégé contre les attaques de pirates. Si l'abonnement auprès du FSI prévoit des adresses IP publiques (WAN) supplémentaires, des ordinateurs supplémentaires peuvent être placés en dehors du pare-feu à condition que chaque ordinateur utilise une adresse IP publique (WAN) différente.

Pour établir une DMZ pour un ordinateur :

- Ouvrir la page *Firewall > DMZ* (Pare-feu > DMZ) et entrer les derniers chiffres de l'adresse IP de l'ordinateur dans le champ **IP**, cliquer sur **Enable** (Activer), puis sur **Apply Changes** (Enregistrer les modifications) pour que le changement entre en vigueur.

Blocage du ping WAN

Les pirates informatiques utilisent l'envoi de *ping* pour trouver des victimes potentielles sur Internet. En émettant un ping sur une certaine adresse IP et en recevant une réponse de celle-ci, un pirate informatique peut décider de s'intéresser à ce qui se trouve derrière cette adresse. Le routeur peut être défini de façon à ne pas répondre à un ping ICMP provenant de l'extérieur. Ceci accroît le niveau de sécurité du routeur.

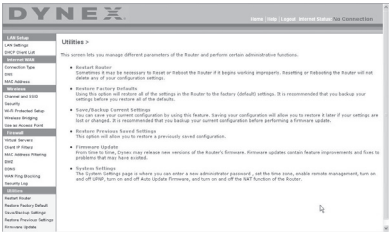


Pour désactiver la réponse au ping

- Ouvrir la page *Firewall* > *WAN Ping Blocking* (Pare-feu > Blocage de ping WAN) et sélectionner Block ICMP Ping (Bloquer le ping ICMP), puis cliquer sur **Apply Changes** (Enregistrer les modifications). Le routeur ne répondra pas à un ping ICMP.

Onglet Utilities (Utilitaires)

Cet écran permet de gérer divers paramètres du routeur et de réaliser certaines fonctions d'administration.

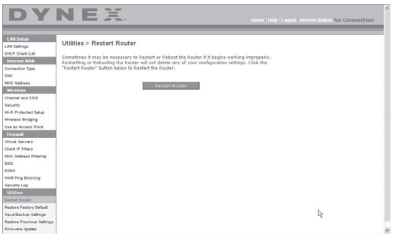


Redémarrage du routeur

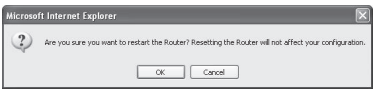
Il est parfois nécessaire de redémarrer ou de réamorcer le routeur s'il commence à fonctionner de façon incorrecte. Le redémarrage ou le réamorçage du routeur ne supprimera AUCUN des paramètres de configuration.

Pour redémarrer le routeur afin de rétablir un fonctionnement normal :

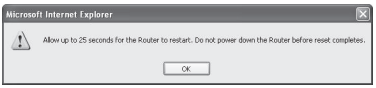
1. Sous l'en-tête **Utilities** (Utilitaires) dans le menu de gauche, cliquer sur **Restart Router** (Redémarrer le routeur). La page *Restart Router* (Redémarrer le routeur) s'affiche.



2. Cliquer sur **Restart Router** (Redémarrer le routeur). Le message suivant s'affiche.



3. Cliquer sur **OK**. Le message suivant s'affiche.



4 Cliquer sur **OK**. Le redémarrage du routeur peut prendre jusqu'à 25 secondes. Il est important de ne pas mettre le routeur hors tension pendant le redémarrage.

Un compte à rebours de 25 secondes s'affiche à l'écran. Lorsqu'il parvient à zéro, le routeur est redémarré. La page d'accueil du routeur doit s'afficher automatiquement. Dans le cas contraire, taper l'adresse du routeur (par défaut = 192.168.2.1) dans la barre de navigation du navigateur.

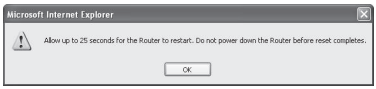
Rétablissement des paramètres par défaut du constructeur

Cette option permet de rétablir tous les paramètres d'usine (par défaut) du routeur. Il est recommandé de sauvegarder les paramètres avant de rétablir les valeurs par défaut.

Pour rétablir les paramètres par défaut du constructeur :

1 Sous l'en-tête **Utilities** (Utilitaires) dans le menu de gauche, cliquer sur **Restore Defaults** (Rétablir les paramètres par défaut). L'avertissement suivant s'affiche.

2 Cliquer sur **OK**. Le message suivant s'affiche.



3 Cliquer sur **OK**. Le rétablissement des paramètres par défaut exige un redémarrage du routeur. Le redémarrage du routeur peut prendre jusqu'à 25 secondes. Il est important de ne pas mettre le routeur hors tension pendant le redémarrage.

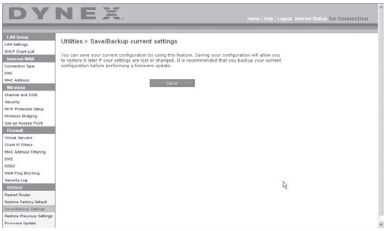
Un compte à rebours de 25 secondes s'affiche à l'écran. Lorsqu'il parvient à zéro, le routeur est redémarré. La page d'accueil du routeur doit s'afficher automatiquement. Dans le cas contraire, taper l'adresse du routeur (par défaut = 192.168.2.1) dans la barre de navigation du navigateur.

Enregistrement de la configuration en cours

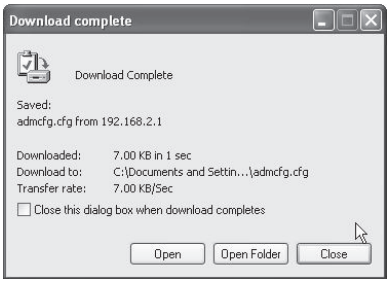
Il est possible d'enregistrer la configuration en cours en utilisant cette fonction. L'enregistrement de la configuration permettra de la rétablir ultérieurement si les paramètres sont perdus ou modifiés. Il est recommandé de sauvegarder la configuration en cours avant d'effectuer une mise à jour du microprogramme.

Pour enregistrer une configuration en cours :

1. Sous l'en-tête **Utilities** (Utilitaires) dans le menu de gauche, cliquer sur **Save/ Backup Settings** (Enregistrer/sauvegarder les paramètres). La page *Save/Backup Settings* (Enregistrer/sauvegarder les paramètres) s'affiche.



2. Cliquer sur **Save** (Enregistrer). La fenêtre File Download (Téléchargement de fichier) s'affiche.
3. Cliquer sur **Save** (Enregistrer). Une fenêtre s'affiche, permettant de sélectionner l'emplacement où sera enregistré le fichier de configuration.
4. Choisir un emplacement. Il est possible de donner n'importe quel nom au fichier, ou d'utiliser le nom par défaut : « Config. ». Veiller à donner au fichier un nom qui permettra de le retrouver ultérieurement. Après la sélection de l'emplacement et du nom du fichier, cliquer sur **Save** (Enregistrer).
5. Une fois l'enregistrement terminé, la fenêtre ci-dessous s'affiche.



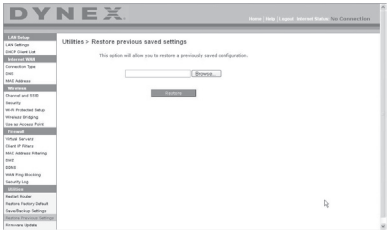
6. Cliquer sur **Close** (Fermer). La configuration est maintenant enregistrée.

Rétablissement d'une configuration antérieure

Cette option permet de rétablir une configuration enregistrée préalablement.

Pour rétablir une configuration enregistrée préalablement :

1. Sous l'en-tête **Utilities** (Utilitaires) dans le menu de gauche, cliquer sur **Restore Previous Settings** (Rétablir des paramètres antérieurs). La page *Restore Previous Settings* (Rétablir des paramètres antérieurs) s'affiche.



2. Cliquer sur **Browse** (Parcourir). Une fenêtre s'affiche, permettant de sélectionner l'emplacement du fichier de configuration. Tous les fichiers de configuration se terminent par l'extension « .bin ». Rechercher le fichier de configuration à rétablir, puis double-cliquer sur celui-ci. Le message suivant s'affiche à l'écran.

3. Cliquer sur **OK**. Une fenêtre de rappel s'affiche.

Le rétablissement de la configuration peut prendre jusqu'à 35 secondes.

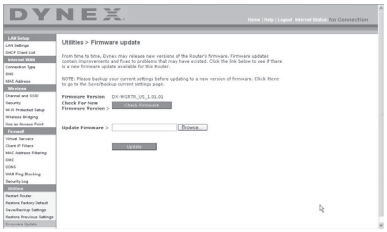
4. Cliquer sur **OK**. Un compte à rebours de 35 secondes s'affiche à l'écran. Lorsqu'il parvient à zéro, la configuration du routeur est rétablie. La page d'accueil du routeur doit s'afficher automatiquement. Dans le cas contraire, taper l'adresse du routeur (par défaut = 192.168.2.1) dans la barre de navigation du navigateur.

Mise à jour du microprogramme

De temps en temps, Dynex peut publier de nouvelles versions du microprogramme du routeur. Ces mises à jour peuvent contenir des améliorations et des solutions aux problèmes existants. Lorsque Dynex publie un nouveau microprogramme, il est possible de le télécharger depuis le site Web des mises à jour de Dynex et d'actualiser le microprogramme du routeur avec la toute dernière version.

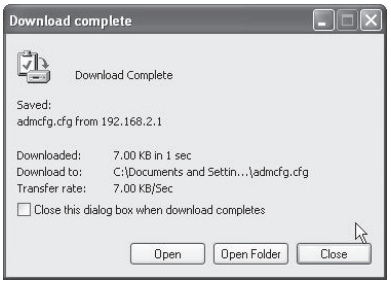
Pour rechercher et télécharger une nouvelle version du microprogramme :

1. Sous l'en-tête **Utilities** (Utilitaires) dans le menu de gauche, cliquer sur **Firmware Update** (Mise à jour du microprogramme). La page *Utilities > Firmware updates* (Utilitaires > Mises à jour du microprogramme) s'affiche.



2. Cliquer sur **Check Firmware** (Vérifier le microprogramme). L'utilitaire vérifie si une mise à jour du microprogramme est disponible.
3. Si une nouvelle version du microprogramme est disponible, une fenêtre s'affiche, permettant de sélectionner l'emplacement où sera enregistré le fichier du microprogramme. Choisir un emplacement. Il est possible de donner n'importe quel nom au fichier, ou d'utiliser le nom par défaut. Veiller à enregistrer le fichier à un endroit où il sera possible de le retrouver ultérieurement. Une fois l'emplacement sélectionné, cliquer sur **Save** (Enregistrer).

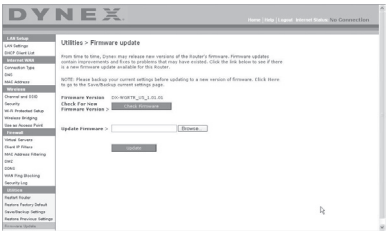
   ***Remarque** : Dynex suggère de l'enregistrer sur le bureau afin de le retrouver facilement.*
4. Une fois l'enregistrement terminé, la fenêtre ci-dessous s'affiche.



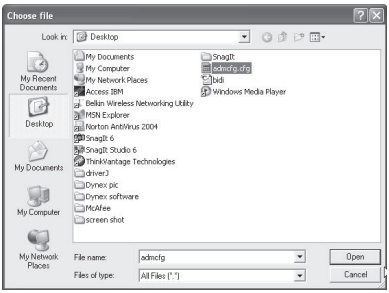
5. Cliquer sur **Close** (Fermer). Le téléchargement est terminé. Pour mettre le microprogramme à jour, procéder comme indiqué dans la section **Pour mettre à jour le microprogramme du routeur**.

Pour mettre à jour le microprogramme du routeur :

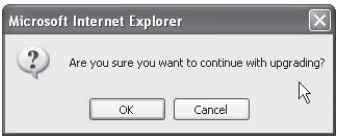
1. Sur la page *Firmware Update* (Mise à jour du microprogramme), cliquer sur **Browse** (Parcourir). Une fenêtre s'affiche, permettant de sélectionner l'emplacement du fichier de mise à jour du microprogramme.



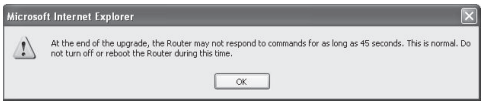
2. Accéder au fichier du microprogramme qui a été téléchargé, puis le sélectionner en double-cliquant sur son nom.



3. La boîte de dialogue **Update Firmware** (Mise à jour du microprogramme) affiche maintenant l'emplacement et le nom du fichier sélectionné. Cliquer sur **Update** (Mettre à jour). Un message demande confirmation avant de continuer.



4. Cliquer sur **OK**. Un autre message s'affiche. Ce message indique que le routeur peut ne pas répondre pendant une minute, car le microprogramme est en cours de chargement et que le routeur doit être redémarré.



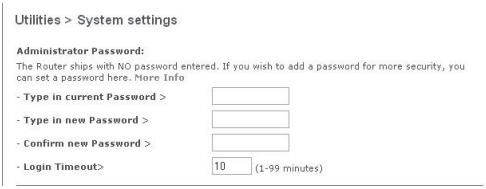
5 Cliquer sur **OK**. Un compte à rebours de 60 secondes s'affiche à l'écran. Lorsqu'il parvient à zéro, la mise à jour du microprogramme du routeur est terminée. La page d'accueil du routeur doit s'afficher automatiquement. Dans le cas contraire, taper l'adresse du routeur (par défaut = 192.168.2.1) dans la barre de navigation du navigateur.

La mise à jour du microprogramme est terminée.

Modifications des paramètres du système

La page *System Settings* (Paramètres du système) est l'endroit où il est possible d'entrer un nouveau mot de passe d'administrateur, définir le fuseau horaire, activer la gestion à distance et activer ou désactiver la fonction NAT du routeur.

Définition ou modification du mot de passe d'administrateur



AUCUN mot de passe n'est entré avant la livraison du routeur. Si l'utilisateur souhaite ajouter un mot de passe pour plus de sécurité, il peut en définir un ici. Noter le mot de passe et le garder en lieu sûr car il sera indispensable pour se connecter au routeur à l'avenir. Il est également recommandé de définir un mot de passe s'il est prévu d'utiliser la fonction de gestion du routeur à distance.

Modification du paramètre de délai avant déconnexion

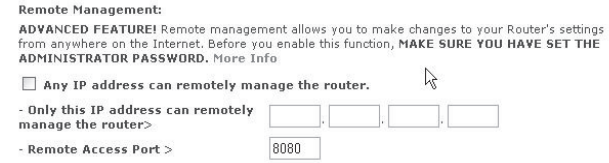
L'option de délai avant déconnexion permet de définir la durée pendant laquelle l'utilisateur peut rester connecté à l'Interface utilisateur Web avancée du routeur. Le temporisateur démarre lorsqu'il n'y a plus d'activité. Par exemple, des modifications ont été apportées au moyen de l'Interface utilisateur Web avancée, puis l'utilisateur a quitté l'ordinateur sans cliquer sur « Logout » (Déconnexion). Si le délai de déconnexion est de 10 minutes, 10 minutes après le départ de l'utilisateur, la session prendra fin. L'utilisateur devra de nouveau se connecter au routeur pour procéder à d'autres modifications. L'option de délai de déconnexion a été créée dans un but de sécurité. La valeur par défaut est de 10 minutes.

***Remarque** : Un seul ordinateur à la fois peut être connecté à l'Interface utilisateur Web avancée du routeur.*

Réglage de l'heure et choix d'un fuseau horaire

Le routeur marque l'heure en se connectant à un serveur SNTP (Simple Network Time Protocol). Cela lui permet de synchroniser l'horloge système du routeur avec Internet. L'horloge synchronisée du routeur est employée pour enregistrer le journal de sécurité et contrôler le filtrage des clients. Sélectionner un fuseau horaire. Si l'utilisateur vit dans une région qui passe à l'heure d'été, cocher la case située à côté de **Automatically Adjust Daylight Saving** (Régler automatiquement à l'heure d'été). Il se peut que l'horloge système ne soit pas mise à jour immédiatement. Laisser au minimum 15 minutes au routeur pour contacter les serveurs horaires sur Internet et obtenir une réponse. Il n'est pas possible de régler l'horloge manuellement.

Activation de la gestion à distance



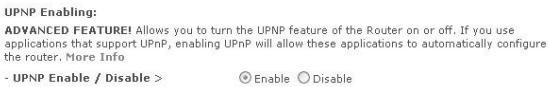
Avant d'activer cette fonctionnalité avancée du routeur, VÉRIFIER QU'UN MOT DE PASSE D'ADMINISTRATEUR A BIEN ÉTÉ DÉFINI. La gestion à distance permet de modifier les paramètres du routeur depuis Internet. Il existe deux méthodes de gestion à distance du routeur. La première consiste à accéder au routeur depuis un endroit quelconque d'Internet en sélectionnant **Any IP address can remotely manage the Router** (Toute adresse IP peut gérer le routeur à distance). Après avoir tapé l'adresse IP WAN depuis un ordinateur quelconque relié à l'Internet, un écran de connexion s'affichera, demandant d'entrer le mot de passe du routeur. La seconde méthode consiste à autoriser une seule adresse IP spécifique à gérer le routeur à distance. Cette méthode est plus sûre, mais moins pratique. Pour utiliser cette méthode, entrer l'adresse IP autorisée à accéder au routeur dans le champ fourni à cet effet, puis sélectionner **Only this IP address can remotely manage the Router** (Seule cette adresse IP est autorisée à gérer le routeur à distance). Avant d'activer cette fonction, Dynex CONSEILLE VIVEMENT de définir un mot de passe d'administrateur. Si le mot de passe reste vide, le routeur sera potentiellement vulnérable à des intrusions.

Activation/Désactivation de la traduction d'adresses réseau (NAT)

***Remarque** : Cette fonctionnalité doit uniquement être modifiée par des utilisateurs expérimentés.*

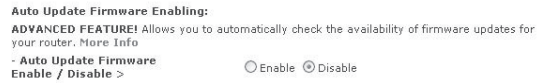
La traduction d'adresses réseau (Network Address Translation, ou NAT) est la méthode selon laquelle le routeur partage l'adresse IP unique attribuée par le FSI avec les autres ordinateurs du réseau. Cette fonction est activée par défaut. Elle ne doit être désactivée que si le FSI attribue plusieurs adresses IP ou s'il est nécessaire de la désactiver pour une configuration système avancée. Si l'utilisateur dispose d'une seule adresse IP et que la fonction NAT est désactivée, les ordinateurs du réseau ne pourront pas accéder à l'Internet. D'autres problèmes risquent également de survenir. La désactivation de NAT désactive les fonctions du pare-feu.

Activation/Désactivation de l'UPnP



UPnP (Universal Plug-and-Play) est une autre fonctionnalité avancée offerte par ce routeur. C'est une technologie qui offre un fonctionnement transparent de la messagerie vocale et vidéo, des jeux et d'autres applications compatibles avec l'UPnP. Certaines applications exigent que le pare-feu du routeur soit configuré d'une certaine manière pour fonctionner correctement. Ceci demande habituellement l'ouverture des ports TCP et UDP. Une application compatible UPnP peut communiquer avec le routeur en lui « disant » comment le pare-feu doit être configuré. Au départ, la fonction UPnP du routeur est désactivée. Lors de l'utilisation d'applications compatibles UPnP, activer la fonction UPnP pour profiter de leurs fonctionnalités UPnP. Sélectionner **Enable** (Activer) dans la section **UPnP Enabling** (Activation UPnP) de la page *Utilities* (Utilitaires), puis cliquer sur **Apply Changes** (Enregistrer les modifications) pour enregistrer les modifications.

Activation/Désactivation de la mise à jour automatique du microprogramme



Cette innovation permet au routeur, grâce à une fonction intégrée, de vérifier automatiquement l'existence d'une nouvelle version du microprogramme et d'avertir l'utilisateur lorsqu'elle est disponible. Lors de la connexion à l'Interface utilisateur Web avancée du routeur, ce dernier effectue une vérification pour savoir s'il existe une nouvelle version du microprogramme. Si tel est le cas, l'utilisateur en est informé. Il est alors possible de télécharger la nouvelle version ou d'ignorer le message. Au départ, cette fonction du routeur est activée. Pour la désactiver, sélectionner **Disable** (Désactiver), puis cliquer sur **Apply Changes** (Enregistrer les modifications).