

MENU AIDE

- De base
- Avancé
- Outils
- État
- Glossaire

AIDE DE BASE

- Assistant
- WAN
- Réseau
- DHCP
- Sans fil (Wi-Fi)

AIDE AVANCEE

- Serveur virtuel
- Applications spéciales
- Jeux
- Mise en forme de trafic
- Routage
- Contrôle des accès
- Filtre Web
- Filtre d'adresse MAC
- Paramètres du pare-feu
- Filtre entrant
- Sans-fil Avancé
- WISH
- Wi-Fi Protected Setup (WEP)
- Réseau avancé
- Reprise

AIDE SUR LES OUTILS

- Paramètres d'administrateur
- Heure
- Syslog
- Paramètres de courriel
- Système
- Microprogramme
- DNS dynamique
- Vérification de système
- Horaires

AIDE SUR L'ETAT

- Info routeur
- Sans fil (Wi-Fi)
- Routage
- Journaux
- Statistiques
- Sessions actives
- Sessions WISH

AIDE DE BASE

- Assistant
- WAN
- Réseau
- DHCP
- Sans fil (Wi-Fi)

ASSISTANT

Assistant d'installation

Si le monde du réseautage ne vous est pas familier et si vous n'avez jamais configuré de routeur, cliquez sur **Assistant de configuration**. Cet assistant vous guidera à travers les étapes de configuration de votre réseau.

WAN

La section Grand réseau (WAN) vous permet de configurer votre type de connexion cellulaire ou câblée à Internet.

Authentification PPP du modem cellulaire (facultatif)

Certains fournisseurs de services sans fil demandent un nom d'utilisateur et un mot de passe pour vous connecter sur PPP (protocole Point par Point). En général, les valeurs par défaut du routeur seront opérationnelles et vous ne devrez les modifier que si votre fournisseur vous le demande.

Type de connexion WAN câblée

Les divers types de connexion sont: IP statique, DHCP, PPPoE, PPTP et L2TP. Si vous n'êtes pas certain de la méthode de connexion utilisée, veuillez communiquer avec votre fournisseur d'accès Internet. Remarque : Si vous utilisez l'option PPPoE, vous devrez vous assurer que tout logiciel client PPPoE sur vos ordinateurs est supprimé ou désactivé.

Mode Grand réseau statique

Cette fonction est utilisée lorsque le FSI vous fournit une adresse IP prédéfinie qui ne change pas. Les données IP sont entrées manuellement dans vos paramètres de configuration IP. Vous devez entrer le **Adresse IP**, **Masque de sous-réseau**, et **Passerelle**. Votre FAI vous fournit toutes ces informations.

Mode WAN DHCP

Méthode de connexion où le FSI attribue votre adresse IP lorsque votre routeur en demande une au serveur du FSI. Certains FSI exigent que vous effectuiez une certaine configuration avant que votre routeur ne puisse se connecter à Internet.

Nom de l'hôte: Certains FAI peuvent vérifier le nom d'hôte de votre ordinateur. Le nom d'hôte identifie votre système auprès du serveur du FAI. Cette méthode permet de déterminer que votre ordinateur est admissible à recevoir une adresse IP. Autrement dit, cela permet de déterminer que vous payez pour les services offerts par le FAI.

Utiliser la monodiffusion: Cette option est désactivée par défaut et devrait le rester tant que le serveur DHCP du côté réseau étendu fournit correctement une adresse IP au routeur. Toutefois, si le routeur ne réussit pas à obtenir du serveur DHCP une adresse IP, ce serveur pourrait être un modèle qui fonctionne mieux avec des réponses unicast (point à point). Dans ce cas, activez l'option Unicasting et regardez si le routeur peut obtenir une adresse IP. Dans ce mode, le routeur accepte les réponses unicast du serveur DHCP au lieu des réponses broadcast (diffusion multiple).

PPPoE

Sélectionnez cette option si votre FAI vous demande d'utiliser une connexion PPPoE (Point to Point Protocol over Ethernet). Les fournisseurs de connexion DSL utilisent en général cette option. Avec cette méthode de connexion vous devez saisir un **nom d'utilisateur** et un **mot de passe** (fourni par votre FAI) pour obtenir un accès Internet. Les protocoles d'authentification pris en charge sont PAP et CHAP.

IP dynamique: Si les serveurs du FAI attribuent l'adressage IP du routeur à l'établissement de la connexion, sélectionnez cette option.

IP statique: Si votre FAI vous a attribué une adresse IP statique, sélectionnez cette option. Le FAI fournit la valeur **Adresse IP**.

Nom du service: Certains FSI pourraient exiger d'entrer un nom de service. Entrez un nom de service seulement si votre FSI l'exige.

Mode de reconnexion: En général les connexions PPPoE ne sont pas activées de manière permanente. Le routeur vous permet de régler le mode de reconnexion. Les paramètres sont :

- **Toujours activé:** Une connexion à Internet est toujours gardée ouverte.
- **Sur demande:** Une connexion à Internet est effectuée si nécessaire.
- **Mode manuel:** Vous devez ouvrir l'interface de gestion Web et cliquer sur le bouton Connecter chaque fois que vous désirez vous connecter à Internet.

Temps d'inactivité max.: Intervalle de temps durant lequel la machine peut rester inactive avant l'arrêt de la connexion PPPoE. La valeur de temps d'inactivité maximum ne s'applique qu'aux modes de reconnexion «Sur demande» et «Manuel».

PPTP

PPTP (Point-to-Point Tunneling Protocol, ou protocole de tunnellation point à point) utilise un réseau privé virtuel pour se connecter à votre FSI. Cette méthode de connexion est utilisée principalement en Europe. Cette méthode de connexion exige d'entrer un **nom d'utilisateur** et un **mot de passe** (fournis par votre fournisseur de services Internet) pour accéder à Internet. Les protocoles d'authentification pris en charge sont PAP et CHAP.

IP dynamique: Si les serveurs du FAI attribuent l'adressage IP du routeur à l'établissement de la connexion, sélectionnez cette option.

IP statique: Si votre FSI a attribué une adresse IP fixe, sélectionnez cette option. Le FSI fournit les valeurs des champs suivants : **Adresse IP PPTP**, **Masque de sous-réseau PPTP**, et **Adresse IP de la passerelle PPTP**.

Adresse IP du serveur PPTP: Le FAI fournit ce paramètre, si requis. La valeur peut être la même que celle de l'adresse IP de la passerelle.

Reconnecter le mode: En général les connexions PPTP ne sont pas activées de manière permanente. Le routeur vous permet de régler le mode de reconnexion. Les paramètres sont :

- **Toujours activé:** Une connexion à Internet est toujours gardée ouverte.
- **Sur demande:** Une connexion à Internet est effectuée si nécessaire.
- **Mode manuel:** Vous devez ouvrir l'interface de gestion Web et cliquer sur le bouton Connecter chaque fois que vous désirez vous connecter à Internet.

Temps d'inactivité max.: Intervalle de temps durant lequel la machine peut rester inactive avant que la connexion PPTP soit coupée. La valeur maximale de temps d'inactivité n'est utilisée qu'avec les modes de reconnexion «Sur demande» et «Manuel».

Protocole L2TP

L2TP (Layer Two Tunneling Protocol) utilise un réseau privé virtuel pour la connexion à votre FSI. Cette méthode de connexion exige d'entrer un **nom d'utilisateur** et un **mot de passe** (fournis par votre fournisseur de services Internet) pour accéder à Internet. Les protocoles d'authentification pris en charge sont PAP et CHAP.

IP dynamique: Si les serveurs du FAI attribuent l'adressage IP du routeur à l'établissement de la connexion, sélectionnez cette option.

IP statique: Si votre FSI a attribué une adresse IP fixe, sélectionnez cette option. Le FSI fournit les valeurs des champs suivants : **Adresse IP L2TP**, **Masque de sous-réseau L2TP**, et **Adresse IP de la passerelle L2TP**.

Adresse IP du serveur L2TP: Le FAI fournit ce paramètre, si requis. La valeur peut être la même que celle de l'adresse IP de la passerelle.

Mode de reconnexion: En général les connexions L2TP ne sont pas activées de manière permanente. Le routeur vous permet de régler le mode de reconnexion. Les paramètres sont :

- **Toujours activé :** Une connexion à Internet est toujours gardée ouverte.
- **Sur demande:** Une connexion à Internet est effectuée si nécessaire.
- **Mode manuel:** Vous devez ouvrir l'interface de gestion Web et cliquer sur le bouton Connecter chaque fois que vous désirez vous connecter à Internet.

Temps d'inactivité max.: Intervalle de temps durant lequel la machine peut rester inactive avant que le système mette fin à la connexion P2TP. La valeur de temps d'inactivité maximum s'applique aux modes de reconnexion «Sur demande» et «Manuel».

Les options suivantes s'appliquent à tous les modes grand réseau.

MTU: Le paramètre Maximum Transmission Unit (MTU) définit la taille maximale d'un paquet (en octets) que le routeur enverra au réseau étendu. Si les périphériques LAN envoient des paquets plus gros, le routeur les fractionnera en paquets plus petits. Idéalement, vous devriez régler cette valeur en concordance avec la valeur MTU de la connexion de votre FAI. Les valeurs courantes sont de 1 500 octets pour une connexion Ethernet et de 1 492 octets pour une connexion PPPoE. Si la MTU du routeur est réglée à une trop forte valeur, les paquets seront fragmentés en aval. Si la MTU a une valeur trop basse, le routeur fragmentera les paquets sans nécessité et, dans les cas extrêmes, sera incapable d'établir des connexions. Dans un cas comme dans l'autre, les performances du réseau seront affectées.

Adresse MAC: Chaque périphérique de réseautage dispose de son adresse MAC unique, attribuée par le fabricant. Certains FAI peuvent vérifier l'adresse MAC de votre ordinateur. Certains FAI enregistrent l'adresse MAC de la carte réseau de l'ordinateur ou du routeur, utilisée pour la connexion initiale au service. Le FAI n'autorise par la suite l'accès à Internet qu'aux requêtes qui proviennent d'un ordinateur ou d'un routeur affichant cette adresse MAC précise. L'adresse MAC de ce routeur diffère de l'adresse MAC de l'ordinateur ou du routeur utilisé à l'origine pour établir la connexion au FAI. Si vous devez changer l'interface Ethernet de grand réseau du routeur, tapez une adresse MAC alternative (par exemple, l'adresse MAC du routeur qui s'est connecté initialement au FSI) ou copiez l'adresse MAC d'un ordinateur. Pour copier l'adresse MAC de l'ordinateur qui s'est connecté initialement au FSI, connectez-vous au routeur au moyen de cet ordinateur, puis cliquez sur le bouton **Cloner l'adresse MAC de votre PC**. L'interface de grand réseau utilisera alors l'adresse MAC de la carte réseau de votre ordinateur.

RÉSEAU

Paramètres du routeur

Ce sont les paramètres d'interface du réseau local (LAN) pour le routeur. La configuration des paramètres LAN du routeur est basée sur l'adresse IP et le masque de sous-réseau indiqués dans cette section. L'adresse IP est également utilisée pour l'accès à cette interface de gestion sur Web. Si vous n'avez pas de réseau existant, il est recommandé d'utiliser les valeurs par défaut.

Adresse IP

Adresse IP de votre routeur sur le réseau local. Les paramètres de votre réseau local sont basés sur l'adresse attribuée ici. Par exemple, 192.168.0.1.

Masque de sous-réseau

Le masque de sous-réseau de votre routeur de réseau local.

Nom de domaine local

Cette entrée est facultative. Entrez un nom de domaine pour le réseau local. Les ordinateurs du réseau local utiliseront ce nom de domaine lorsqu'ils obtiendront une adresse du serveur DHCP intégré du routeur. Par exemple, si vous entrez **monréseau.net** ici et que vous disposez d'un ordinateur portable côté réseau local nommé **christian**, cet ordinateur sera désigné sous le nom **christian.monréseau.net**. Notez cependant que le nom de domaine entré peut être remplacé par celui obtenu auprès du serveur DHCP de liaison ascendante du routeur.

Relais DNS

Lorsque la fonction de relais DNS est activée, le routeur joue le rôle d'un serveur DNS. Les requêtes DNS transmises au routeur sont réacheminées au serveur DNS du FAI. Cette méthode permet aux ordinateurs du réseau local d'utiliser une adresse DNS constante, même lorsque le routeur obtient une adresse de serveur DNS différente d'un FAI lors du rétablissement d'une connexion au grand réseau. Il est recommandé de désactiver la fonction de relais DNS si vous prévoyez utiliser un serveur DNS côté réseau local en tant que serveur virtuel.

Serveur DNS principal, serveur DNS auxiliaire

Entrez les adresses IP des serveurs DNS. Laissez le champ du serveur secondaire vide s'il n'est pas utilisé.

RIP (Routing Information Protocol) (protocole d'information de routage)

Utilisée pour diffuser des données de routage parmi les routeurs.

Activer le protocole RIP

Activez RIP si cela est indiqué par le FSI, si le réseau local comporte plusieurs routeurs ou si le réseau comporte des périphériques avec adresse IP automatique.

Mode d'exploitation RIP

Ce routeur prend en charge les versions 2 et 1 de la spécification RIP.

V1. Utiliser cette version si aucun routeur ne prend en charge la version 2.

V2 Broadcast. À utiliser si certains routeurs prennent en charge la version 2; d'autres n'acceptent que la version 1.

Multidiffusion V2. Utilisez cette option s'il s'agit du seul routeur sur le réseau local ou si tous les routeurs prennent en charge la version 2.

Router Metric (métrologie du routeur)

Coût additionnel de routage d'un paquet passant à travers ce routeur. La valeur habituelle d'un simple réseau est 1. Cette valeur métrique s'ajoute aux routes apprises des autres routeurs; elle ne s'ajoute pas aux routes statiques ou du système.

Fonctionne comme routeur par défaut

Faire de ce routeur la destination préférée des paquets qui n'y sont pas normalement destinés.

Accepter les mises à jour WAN

Pour des raisons de sécurité, désactivez cette option, sauf demande contraire de votre FAI.

Mot de passe RIP

RIP version 2 prend en charge l'utilisation d'un mot de passe pour limiter l'accès aux routeurs par le protocole RIP. Si le FSI ou un routeur de réseau local exige un mot de passe RIP, entrez-le ici.

DHCP

Paramètres du serveur DHCP

DHCP signifie Dynamic Host Configuration Protocol (protocole de configuration dynamique de l'hôte). La section DHCP permet de configurer le serveur DHCP pour qu'il attribue des adresses IP aux ordinateurs et aux autres périphériques sur le réseau local.

Activer le serveur DHCP

Une fois que votre routeur sera correctement configuré et cette option activée, le serveur DHCP gèrera les adresses IP et autres données de configuration réseau pour les ordinateurs et les autres périphériques connectés à votre réseau local. Vous n'aurez pas à vous en occuper.

Les ordinateurs (et autres périphériques) connectés à votre réseau local ont également besoin d'une configuration TCP/IP réglée à «DHCP» ou «Obtenir une adresse IP automatiquement».

Lorsque vous choisissez **Activer le serveur DHCP**, les options suivantes sont affichées.

Plage d'adresses IP du serveur DHCP

Ces deux valeurs IP (*de* et *à*) définissent la plage des adresses IP utilisées par la serveur DHCP lors de l'affectation d'adresses aux ordinateurs et périphériques du réseau local. Les adresses hors plage ne sont pas gérées par le serveur DHCP et peuvent, par conséquent, être utilisées pour les périphériques configurés de façon manuelle ou les périphériques qui ne peuvent pas recourir à DHCP pour obtenir automatiquement les informations d'adresse réseau.

Un ordinateur ou un appareil manuellement configuré peut avoir une adresse résidant dans cette plage. Dans ce cas, l'adresse doit être réservée (voir *Réservation DHCP* ci-dessous), afin que le serveur DHCP sache que cette adresse particulière ne peut être utilisée que par un ordinateur ou un appareil spécifique.

Votre routeur, par défaut, possède une adresse IP statique de 192.168.0.1. Ceci signifie que les adresses de 192.168.0.2 à 192.168.0.254 sont disponibles pour allocation par le serveur DHCP.

Exemple:

Votre routeur utilise 192.168.0.1 comme adresse IP. Vous avez attribué l'adresse IP statique 192.168.0.3 à un ordinateur que vous souhaitez désigner à titre de serveur Web. Vous avez attribué l'adresse IP statique 192.168.0.4 à un autre ordinateur que vous souhaitez désigner à titre de serveur FTP. Par conséquent, l'adresse IP de début de la plage d'adresses IP DHCP doit être 192.168.0.5 ou plus élevée.

Exemple:

Supposons que vous configurez le serveur DHCP pour gérer les adresses comprises entre 192.168.0.100 et 192.168.0.199. Cela signifie que les adresses de 192.168.0.3 à 192.168.0.99 et de 192.168.0.200 à 192.168.0.254 ne sont PAS gérées par le serveur DHCP. Les ordinateurs et les périphériques qui utilisent des adresses comprises dans ces plages non gérées doivent être configurés manuellement. Supposons que vous avez un serveur Web utilisant l'adresse 192.168.0.100, qui a été configurée manuellement. Comme cette adresse est comprise dans la plage « gérée », vous devez créer une réservation pour cette adresse et établir la correspondance avec l'ordinateur approprié (voir Client DHCP statique ci-dessous).

Temps de bail DHCP

Période durant laquelle un ordinateur peut posséder une adresse IP avant que le système lui demande de renouveler le bail. Le bail fonctionne exactement comme un bail de location d'appartement. Le bail initial indique la durée du bail jusqu'à expiration. Si le «locataire» souhaite garder l'adresse lorsque le bail est venu à expiration, un nouveau bail est établi. Si le bail expire et que son utilisateur n'a plus besoin de l'adresse, celle-ci peut alors être allouée à un autre locataire.

Toujours Broadcast

Cette option peut demeurer désactivée si tous les ordinateurs du réseau réussissent à obtenir leurs adresses IP du serveur DHCP du routeur, tel que prévu. Si l'un des ordinateurs du réseau n'obtient pas d'adresse IP du serveur DHCP du routeur, il se peut qu'il utilise un ancien client DHCP qui désactive l'indicateur de diffusion des paquets DHCP. L'activation de cette option permet au routeur de toujours diffuser ses réponses à tous les clients et de contourner ainsi le problème, au détriment d'une augmentation de trafic de diffusion sur le réseau local.

Information du NetBIOS

Cochez cette case pour autoriser le serveur DHCP à fournir des paramètres de configuration NetBIOS aux hôtes du réseau local. NetBIOS permet aux hôtes du réseau local de découvrir tous les autres ordinateurs au sein du réseau, par ex. dans le voisinage réseau.

Obtenir l'information NetBIOS du WAN

Si l'option d'avertissement NetBIOS est activée, activer ce paramètre entraîne l'acquisition de l'information WINS du côté réseau à distance, si disponible. Désactivez ce paramètre pour effectuer une configuration manuelle.

Adresse IP du serveur WINS primaire

Configurer l'adresse IP du serveur WINS préféré. Les serveurs WINS stockent des informations sur les hôtes du réseau, ce qui permet aux hôtes de s'enregistrer et de découvrir les autres hôtes disponibles, par exemple pour une utilisation avec le voisinage réseau. Ce paramètre n'a aucun effet si l'option Obtenir les informations NetBIOS du grand réseau est activée.

Adresse IP du serveur WINS secondaire

Configurez l'adresse IP du serveur WINS de secours, le cas échéant. Ce paramètre n'a aucun effet si l'option Obtenir les informations NetBIOS du grand réseau est activée.

Portée NetBIOS

Ce champ concerne un paramètre avancé et il est généralement laissé vide. Permet de configurer un nom de domaine NetBIOS sous lequel les hôtes du réseau fonctionnent. Ce paramètre n'a aucun effet si l'option Obtenir les informations NetBIOS du grand réseau est activée.

Mode d'enregistrement du NetBIOS

Indique quels hôtes du réseau exécuteront l'enregistrement et la recherche de nom NetBIOS.

Nœud H, indiquant un mode hybride de fonctionnement. Une première tentative est effectuée avec les serveurs WINS, s'il en existe, suivie par une diffusion au réseau local. Ce mode est généralement préférable si vous avez configuré des serveurs WINS.
Nœud M (valeur par défaut), indiquant un mode mixte de fonctionnement. La première opération de diffusion vise à enregistrer les hôtes et à découvrir d'autres hôtes; si l'opération échoue, une tentative est effectuée avec les serveurs WINS, s'il en existe. Ce mode favorise l'opération de diffusion, qui peut être préférable si les serveurs WINS sont accessibles par un lien réseau lent et si la majorité des services réseau (serveurs, imprimantes, etc.) sont sur le réseau local.

P-Node; indication de n'utiliser que des serveurs WINS UNIQUEMENT. Ce paramètre est utile pour forcer tout transfert NetBIOS à s'exécuter sur les serveurs WINS configurés. Vous devez avoir configuré au moins l'adresse IP du serveur WINS primaire pour qu'elle pointe vers un serveur WINS en fonction.

B-Node, ceci indique d'utiliser le mode broadcast (diffusion générale) sur le réseau local UNIQUEMENT. Ce paramètre est utile lorsqu'il n'existe aucun serveur WINS disponible; il est toutefois conseillé d'essayer d'abord l'option M-Node.
Ce paramètre n'a aucun effet si l'option Obtenir les informations NetBIOS du grand réseau est activée.

Nombre de clients DHCP dynamique

Dans cette section, vous pouvez voir quels sont les périphériques de réseau local qui louent actuellement des adresses IP.

Revoke

L'option **Revoke** est disponible pour le cas où la table de baux est pleine ou presque pleine, que vous avez besoin de récupérer de l'espace pour de nouvelles entrées, et que vous savez que certaines adresses allouées ne sont plus nécessaires. Cliquer sur **Revoke** annule le bail d'un périphérique LAN particulier et libère une entrée dans la table des baux. N'utilisez cette option que si le périphérique n'a plus besoin de l'adresse IP car, par exemple, il a été retiré du réseau.

Réserver

L'option de **Réserver** convertit cette attribution d'adresse IP dynamique en une réservation DHCP et ajoute l'entrée correspondante dans la liste de réservations DHCP.

Ajouter/modifier une réservation DHCP

Cette option permet de réserver des adresses IP et d'assigner la même adresse IP au périphérique réseau, avec l'adresse MAC spécifiée, chaque fois que celui-ci demande une adresse IP. Cette option revient pratiquement à utiliser une adresse IP statique pour le périphérique, sauf que celui-ci doit quand même obtenir une adresse IP auprès du routeur. Le routeur attribue chaque fois la même adresse IP au périphérique. Les réservations DHCP sont utiles pour les serveurs sur le réseau local qui hébergent des applications (Web et FTP, par exemple). Les serveurs de votre réseau doivent utiliser une adresse IP statique ou bien vous devez activer cette option.

Nom de l'ordinateur

Vous pouvez attribuer un nom pour chaque ordinateur disposant d'une adresse IP réservée. Cette méthode pourrait vous aider à identifier les ordinateurs auxquels les adresses sont attribuées. Exemple : **Serveur de jeu**.

Adresse IP:

Adresse du réseau local que vous désirez réserver.

Adresse MAC

Pour entrer l'adresse MAC de votre système, saisissez-la manuellement ou connectez-vous à l'interface de gestion WEB du routeur sur le système et cliquez sur le bouton **Copier l'adresse MAC de votre PC**.

Une adresse MAC est généralement indiquée sur une étiquette placée sous un périphérique de réseau. L'adresse MAC comprend douze chiffres. Chaque paire de chiffres hexadécimaux est séparée par des tirets ou des deux points, par ex. : 00-0D-88-11-22-33 ou 00:0D:88:11:22:33. Si le périphérique est un ordinateur et qu'il intègre déjà une carte réseau, vous pouvez vous connecter au routeur par le biais du PC. Cliquez ensuite sur le bouton **Copier l'adresse MAC de votre PC** pour saisir l'adresse MAC de la machine.

Vous pourriez également repérer une adresse MAC dans un système d'exploitation visé en suivant les étapes ci-dessous :

Windows 98 Windows Me	Allez au menu Démarrer, sélectionnez Exécuter, tapez winiipcfg , puis appuyez sur Entrée. Une fenêtre instantanée s'affiche. Sélectionnez dans le menu déroulant l'adaptateur approprié pour afficher son adresse à l'écran. C'est l'adresse MAC de l'appareil.
Windows 2000 Windows XP	Au menu Démarrer, sélectionnez Programmes, Accessoires, puis Invite de commandes. À l'invite, tapez ipconfig /all et appuyez sur Entrée. L'adresse physique affichée pour la carte de connexion au routeur est l'adresse MAC.
Mac OS X	Allez au menu Apple, sélectionnez l'option Préférences système, puis Réseau, puis l'adaptateur Ethernet qui assure la connexion au routeur. Cliquez sur le bouton Ethernet; l'ID Ethernet apparaît dans la liste. C'est le même que l'adresse MAC.

Activer

Indique si l'entrée sera active ou inactive.

Enregistrer/Mettre à jour

Enregistrez les modifications apportées dans la liste suivante.

Effacer

Réinitialisez cette zone de l'écran en annulant toute modification que vous avez apportée.

Liste des réservations DHCP

Montre les clients pour lesquels vous avez spécifié que les adresses DHCP sont réservées. Cochez la case à gauche «Activer» pour activer ou désactiver directement la valeur saisie. Il est possible de changer une entrée en cliquant sur l'icône Modifier, ou de l'éliminer en cliquant sur l'icône Supprimer. Si vous cliquez sur l'icône Modifier, l'élément est mis en surbrillance et la section de modification de réservation DHCP est activée pour modification.

SANS FIL (WI-FI)

La section Sans fil permet de configurer les paramètres de votre routeur. Veuillez noter que les modifications apportées dans cette section pourraient devoir être dupliquées sur les clients sans fil que vous souhaitez connecter à votre réseau sans fil.

Pour protéger votre confidentialité, utilisez le mode de sécurité sans fil pour configurer les fonctions connexes. Cet appareil est compatible avec les trois modes de sécurité sans fil suivantes : WEP, WPA Personnel et WPA Entreprise. WEP est la norme de chiffrement sans fil d'origine. WPA offre un plus haut niveau de sécurité. WPA Personnel ne nécessite aucun serveur d'authentification. L'option WPA Entreprise nécessite un serveur d'authentification RADIUS.

Ajouter des périphériques sans fil avec l'assistant WPS (Wi-Fi Protected Setup)

Cet assistant vous aide à ajouter des périphériques sans fil au réseau à l'aide du protocole Wi-Fi Protected Setup.

L'assistant vous demandera d'entrer le NIP de l'appareil, ou d'appuyer sur le bouton de configuration de cet appareil. Si l'appareil prend en charge la fonction Wi-Fi Protected Setup et qu'il possède un bouton de configuration, vous pouvez ajouter cet appareil au réseau en appuyant sur son bouton puis sur celui du routeur dans les 60 secondes qui suivent. Le voyant d'état du routeur clignotera trois fois si l'appareil a été ajouté avec succès au réseau.

Il existe plusieurs façons d'ajouter un dispositif sans fil à votre réseau. L'accès au réseau sans fil est géré par un registraire. Le registraire n'autorise l'accès d'un dispositif au réseau sans fil que si vous avez entré le NIP ou appuyé sur le bouton Configuration de l'accès Wi-Fi protégé du dispositif. Le routeur agit à titre de registraire pour le réseau, bien que d'autres dispositifs puissent également jouer ce rôle.

Activer le sans fil

Cette option active ou désactive la fonction de connexion sans fil du routeur. Lorsque vous activez cette option, les paramètres suivants sont en vigueur.

Nécessite une ouverture de session utilisateur

Cette option désactive et active la fonction de nom d'utilisateur du routeur. Si l'option est activée, l'utilisateur doit entrer un mot de passe pour pouvoir accéder à Internet. Cette option limite également l'accès Internet à un maximum de 32 clients simultanés.

Nom du réseau sans fil

Nom qui s'affiche dans la liste lorsque vous recherchez les réseaux sans fil disponibles (à moins que l'état de visibilité ne soit réglé à Invisible, voir plus bas). Ce nom est également connu sous le nom de SSID. Il est fortement recommandé, à des fins de sécurité, de changer le nom de réseau prédéfini.

Activer l'option Scan canal auto

Si vous sélectionnez cette option, le routeur trouvera automatiquement le canal subissant le moins d'interférences et l'utilisera pour le réseau sans fil. Si vous désactivez cette option, le routeur utilisera le canal que vous avez indiqué à l'aide de l'option **Canal sans fil** suivante.

Canal sans fil

Un réseau sans fil utilise des canaux particuliers dans le spectre du sans-fil pour traiter les communications entre clients. Certains canaux utilisés dans votre zone peuvent subir des interférences générées par d'autres dispositifs électroniques. Choisissez le canal le plus clair pour aider à optimiser les performances et la couverture de votre réseau sans fil.

Mode 802.11

Si tous les périphériques sans fil que vous désirez connecter à ce routeur peuvent utiliser pour cela le même mode de transmission, il vous est possible d'améliorer un peu les performances en choisissant le mode «Seulement» approprié. Si certains de vos périphériques utilisent un mode de transmission différent, choisissez le mode «Mixe» approprié.

Largeur de canal

L'option Auto 20/40 MHz est habituellement préférable. Les autres options servent pour des circonstances spéciales.

Débit de transmission

Par défaut, le débit de transmission le plus élevé est sélectionné. Vous avez la possibilité de sélectionner la vitesse, si nécessaire.

État visibilité

L'option Invisible vous permet de masquer votre réseau sans fil. Lorsque cette option est réglée sur Visible, le nom de votre réseau sans fil est diffusé à tous les utilisateurs situés dans la portée de votre signal. Si vous n'utilisez aucun mode de chiffrement ils pourront se connecter à votre réseau. Lorsque le mode Invisible est activé, vous devez entrer manuellement sur le système client le nom du réseau sans fil (SSID) pour vous connecter au réseau.

Mode de sécurité

Si aucun de ces modes de chiffrement n'est sélectionné, les transmissions sans fil en provenance ou à destination de votre réseau sans fil pourront être interceptées et interprétées facilement par des utilisateurs non autorisés.

WEP

Méthode de chiffrement des données pour les communications sans fil visant à fournir le même niveau de confidentialité qu'un réseau câblé. Le chiffrement WEP est moins sûr que le chiffrement WPA. Pour obtenir l'accès à un réseau WEP, vous devez connaître la clé. La clé est une chaîne de caractères que vous créez. Si vous utilisez le WEP, vous devez définir le niveau de chiffrement. La longueur de la clé varie en fonction du type de chiffrement. Un chiffrement à 128 bits nécessite une clé plus longue que le chiffrement à 64 bits. Les clés sont définies en entrant une chaîne au format HEX (hexadécimal - en utilisant des caractères de 0-9 et de A-F) ou ASCII (American Standard Code for Information Interchange - caractères alphanumérique). Le format ASCII est fourni pour vous permettre de saisir une chaîne plus facile à mémoriser. La chaîne ASCII est convertie au format HEX pour utilisation sur le réseau. Vous pouvez définir jusqu'à quatre clés afin de pouvoir en changer facilement. Une clé par défaut est choisie pour le réseau.

Exemple:

Les clés hexadécimales de 64 bits comportent exactement 10 caractères. (12345678FA est une chaîne de 10 caractères valide pour le chiffrement 64 bits.)

Les clés hexadécimales de 128 bits comportent exactement 26 caractères. (456FBCDF123400122225271730 est une chaîne de 26 caractères valide pour le cryptage 128 bits.)

Les clés ASCII de 64 bits comprennent jusqu'à 5 caractères maximum (DMODE est une chaîne valide de 5 caractères pour le chiffrement 64 bits).

Les clés ASCII de 128 bits comportent jusqu'à 13 caractères (2002HALOSWIN1 est une chaîne de 13 caractères valide pour le chiffrement 128 bits.)

Prenez note que si vous entrez moins de caractères que nécessaire pour la clé WEP, la partie manquante est automatiquement remplie avec des zéros.

WPA-Personal et WPA-Enterprise

Ces deux options sélectionnent une variante de WPA (Wi-Fi Protected Access) -- normes de sécurité créées par la Wi-Fi Alliance. Le **mode WPA** raffine encore la variante que le routeur doit utiliser.

Mode WPA: WPA est le standard le plus ancien. Sélectionnez cette option si les clients qui seront utilisés avec le routeur ne prennent en charge que WPA. WPA2 est une version plus récente de la spécification IEEE 802.11i. Si vous choisissez l'option WPA2, le routeur tente d'utiliser WPA2 dans un premier temps, puis passe à WPA si le client ne prend en charge que cette version. Si vous choisissez l'option WPA2 seulement, le routeur n'accepte que les clients prenant en charge la sécurité WPA2.

Type de cryptage: Algorithme de chiffrement utilisé pour assurer la protection des communications de données. La fonction TKIP (Temporal Key Integrity Protocol), basé sur le WEP, génère une clé par paquet périodiquement modifiée. L'AES (Advanced Encryption Standard) est un algorithme de chiffrement très sûr basé sur le bloc de 128 bits. Avec l'option «TKIP et AES» activée, le routeur négocie le type de chiffre avec le client et utilise AES, le cas échéant.

Intervalle de mise à jour de la clé de groupe: Période avant que la clé de groupe utilisée pour les données de diffusion et de multidiffusion ne soit modifiée.

WPA-Personal

Cette option utilise l'authentification WPA (Wi-Fi Protected Access) avec une clé pré-partagée (PSK).

Clé partagée: La clé est entrée en tant que phrase de vérification d'un maximum de 63 caractères alphanumériques au format ASCII (American Standard Code for Information Interchange), aux deux extrémités de la liaison sans fil. Cette clé ne peut compter moins de huit caractères. Toutefois, pour assurer une sécurité suffisante, celle-ci doit être plus longue et il ne doit pas s'agir d'une phrase triviale. Cette phrase est utilisée pour générer des clés de session uniques pour chaque client sans fil.

Exemple:

La technologie de réseau sans fil permet la communication en tout lieu

WPA-Enterprise

Cette option fonctionne avec un serveur RADIUS pour authentifier les clients sans fil. Les clients sans fil doivent avoir établi les attestations nécessaires avant de tenter de s'authentifier sur le serveur par le biais de cette passerelle. De plus, il sera peut-être nécessaire de configurer le serveur RADIUS pour permettre à cette passerelle d'authentifier les utilisateurs.

Expiration du délai d'authentification: Période avant que le système ne demande au client de s'authentifier de nouveau.

Adresse de serveur RADIUS: Adresse IP du serveur d'authentification.

Port de serveur RADIUS: Numéro de port utilisé pour la connexion au serveur d'authentification.

Mode Secret partagé du serveur RADIUS: Phrase d'entrée qui doit correspondre avec le serveur d'authentification

Authentification d'adresse MAC: Lorsque cette option est sélectionnée, l'utilisateur doit se connecter à partir du même ordinateur chaque fois qu'il ouvre une session sur le réseau sans fil.

Avancé:

Serveur RADIUS de sauvegarde facultatif

Cette option permet de configurer un deuxième serveur RADIUS facultatif qui peut être utilisé comme serveur de secours pour le serveur RADIUS primaire. Ce second serveur n'est consulté que lorsque le serveur RADIUS primaire n'est pas disponible ou qu'il ne répond pas. Les champs **Adresse IP du second serveur RADIUS**, **Port du serveur RADIUS**, **Secret partagé du second serveur RADIUS** et **Deuxième authentification d'adresse MAC** fournissent les paramètres du serveur RADIUS secondaire.

AIDE AVANCEE

- Serveur virtuel
- Applications spéciales
- Jeux
- Mise en forme de trafic
- Routage
- Contrôle des accès
- Filtre Web
- Filtre d'adresse MAC
- Paramètres du pare-feu
- Filtre entrant
- Sans-fil Avancé
- WISH
- Wi-Fi Protected Setup (WEP)
- Réseau avancé
- Reprise

SERVEUR VIRTUEL

L'option Serveur virtuel donne aux utilisateurs Internet l'accès aux services de votre réseau local. Cette fonction permet d'héberger des services en ligne comme FTP, Web ou des serveurs de jeux. Pour chaque serveur virtuel, vous définissez un port public sur votre routeur pour réacheminement vers une adresse IP et un port d'un réseau local interne.

Exemple:

Vous hébergez un serveur Web sur un PC ayant l'adresse IP LAN de 192.168.0.50, mais votre FAI a bloqué le port 80.

1. Donnez un nom au serveur virtuel (par exemple : **Serveur Web**)
2. Entrez l'adresse IP de l'appareil sur votre réseau local (par exemple : **192.168.0.50**).
3. Entrez [80] pour le port privé
4. Entrez [8888] pour le port public
5. Sélectionnez le protocole (par exemple **TCP**).
6. Vérifiez que la programmation est réglée à **Toujours**
7. Cliquez sur **Enregistrer** pour ajouter les paramètres dans la liste de serveurs virtuels.
8. Répétez ces étapes pour chaque règle de serveur virtuel que vous désirez ajouter.

Cette entrée de serveur virtuel permet de réacheminer tout le trafic Internet du port 8888 vers le port 80 de votre serveur Web interne, à l'adresse IP 192.168.0.50.

Ajouter/modifier un serveur virtuel

Activer

Indique si l'entrée sera active ou inactive.

Nom

Attribuez un nom significatif au serveur virtuel, par exemple **Serveur Web**. Plusieurs types de serveur virtuel connus sont disponibles dans la zone de liste déroulante Nom de l'application. Vous pouvez sélectionner l'une de ces options pour remplir automatiquement certains des champs de paramètre à l'aide de valeurs standard pour le type de serveur visé.

Adresse IP

Adresse IP du système sur votre réseau interne qui fournira le service virtuel, par exemple **192.168.0.50**. Vous pouvez sélectionner un ordinateur dans la liste des clients DHCP du menu déroulant Nom de l'ordinateur, ou entrer manuellement l'adresse IP du serveur.

Protocole

Sélectionnez le protocole qu'utilise le service. Les protocoles communs -- UDP, TCP et les deux choix UDP et TCP sont à sélectionner dans le menu déroulant. Pour spécifier tout autre protocole, sélectionnez « Autre » dans la liste, puis entrez le numéro de protocole correspondant (tel qu'attribué par l'IANA) dans la case **Protocole**.

Port de réseau privé

Port qui sera utilisé sur votre réseau interne.

Port public

Port d'accès aux données Internet

Programmation

Sélectionnez une programmation pour l'activation du service. Si la programmation dont vous avez besoin ne figure pas dans la liste, accédez à l'écran Outils → Programmation et créez une nouvelle programmation de plage horaire.

Filtre entrant

Sélectionnez un filtre qui contrôle l'accès, tel que requis pour ce serveur virtuel. Si le filtre dont vous avez besoin ne figure pas dans la liste de filtres, accédez à l'écran Avancé → Filtre de données entrantes et créez un nouveau filtre.

Enregistrer/Mettre à jour

Enregistrez les modifications apportées dans la liste suivante.

Effacer

Réinitialisez cette zone de l'écran en annulant toute modification que vous avez apportée.

Liste de serveurs virtuels

C'est une liste des serveurs virtuels définis. Cochez la case à gauche «Activer» pour activer ou désactiver directement la valeur saisie. Il est possible de changer une entrée en cliquant sur l'icône Modifier, ou de l'éliminer en cliquant sur l'icône Supprimer. Lorsque vous cliquez sur l'icône Modifier, l'article visé est mis en évidence et la section «Modifier les serveurs virtuels» est activée pour permettre la modification.

Remarque: Vous éprouvez peut-être des difficultés à accéder à un serveur virtuel au moyen de son identité publique (adresse IP de la passerelle côté réseau étendu ou son nom DNS dynamique) sur une machine du réseau local. Votre requête ne reboucle pas ou vous êtes redirigé vers la page «Interdit».

Cette situation peut se produire si une règle de contrôle d'accès est définie pour cet appareil du réseau local.

Les requêtes de la machine LAN ne peuvent reboucler si l'accès Internet est bloqué au moment de l'accès. Pour résoudre le problème, accédez à la machine LAN en utilisant son identité côté LAN.

Les demandes peuvent être redirigées vers la page « Interdit » si l'accès Internet d'un appareil du réseau local est restreint par une règle de contrôle d'accès. Ajoutez l'identification du grand réseau (adresse IP de grand réseau du routeur ou son nom de serveur DNS dynamique) à l'écran *Avancé* → *Filtre Web* pour contourner ce problème.

JEUX

Des connexions multiples sont requises par certaines applications, telles de jeux sur Internet, de conférence vidéo, de téléphonie Internet, etc. Ces applications éprouvent des difficultés à fonctionner via le NAT (traduction d'adresses de réseau). Cette section est utilisée pour ouvrir plusieurs ports ou une plage de ports sur votre routeur et réacheminer les données au moyen de ces ports vers un seul ordinateur de votre réseau. Vous pouvez entrer les ports sous différents formats :

Plage (50 à 100)
 Individuel (80, 68, 888)
 Mixe (1020-5000, 689)

Exemple :

Supposons que vous hébergez un serveur de jeu en ligne sur un ordinateur utilisant l'adresse IP privée 192.168.0.50. Ce jeu nécessite d'ouvrir plusieurs ports (6159 à 6180, 99) sur le routeur pour que les utilisateurs puissent se connecter par Internet.

Ajouter/Modifier la règle de jeux

Utilisez cette section pour ajouter une règle applicable aux jeux dans la liste ci-dessous, ou pour modifier une règle existante.

Activer

Indique si l'entrée sera active ou inactive.

Nom

Attribuez à la règle un nom significatif, par exemple **Serveur de jeux**. Vous pouvez également sélectionner une option de la liste des jeux populaires pour que le système remplisse automatiquement plusieurs des champs de configuration restants. Vous devrez remplir le champ d'adresse IP et il est recommandé de vérifier si les valeurs de port ont été modifiées depuis la création de la liste.

Adresse IP

Entrez l'adresse IP du réseau local du système hébergeant le serveur, par exemple **192.168.0.50**. Vous pouvez sélectionner un ordinateur dans la liste des clients DHCP du menu déroulant Nom de l'ordinateur, ou entrer manuellement l'adresse IP du serveur.

Ports TCP

Entrez les ports TCP à ouvrir (par exemple **6159-6180, 99**).

Ports UDP

Entrez les ports UDP à ouvrir (par exemple **6159-6180, 99**).

Programmation

Choisissez une programmation durant laquelle cette règle est en vigueur. Si vous ne voyez pas la programmation pertinente dans la liste des plages horaires, allez à l'écran Outils → Horaires et créez une nouvelle programmation.

Filtre entrant

Pour cette règle, sélectionnez un filtre qui contrôle l'accès selon les besoins. Si le filtre dont vous avez besoin ne figure pas dans la liste de filtres, accédez à l'écran Avancé → Filtre de données entrantes et créez un nouveau filtre.

Enregistrer/Mettre à jour

Enregistrez les modifications apportées dans la liste suivante.

Effacer

Réinitialisez cette zone de l'écran en annulant toute modification que vous avez apportée.

Avec les exemples de valeurs saisies ci-dessus et cette règle de jeux activée, tout le trafic TCP et UDP sur les ports 6159 à 6180 et le port 99 traverse le routeur et est redirigé vers l'adresse IP privée interne 192.168.0.50. de votre serveur de jeux.

Veillez noter que des ordinateurs LAN différents ne peuvent être associés aux règles de jeux ayant des ports en commun; de telles règles se contrediraient mutuellement.

Règles de jeux

Il s'agit d'une liste de règles de jeux définies. Cochez la case à gauche «Activer» pour activer ou désactiver directement la valeur saisie. Il est possible de changer une entrée en cliquant sur l'icône Modifier, ou de l'éliminer en cliquant sur l'icône Supprimer. Lorsque vous cliquez sur l'icône Modifier, l'article visé est mis en évidence et la section «Modifier la règle de jeux» est activée pour permettre la modification.

REGLES D'APPLICATIONS

Une règle d'application est utilisée pour ouvrir un ou plusieurs ports sur votre routeur, lorsque le routeur détecte des données envoyées sur Internet à partir d'un port ou d'une plage de ports désignés comme « déclencheurs ». La règle d'application est valable pour tous les ordinateurs de votre réseau interne.

Ajouter/Modifier règle d'applications

Exemple:

Vous devez configurer le routeur de façon à permettre aux applications qui s'exécutent sur tout ordinateur de votre réseau de se connecter à un serveur Web ou à l'ordinateur d'un autre utilisateur sur Internet.

Activer

Indique si l'entrée sera active ou inactive.

Nom

Attribuez un nom significatif à la règle d'application spéciale, par exemple **App jeux**, pour en faciliter l'identification ultérieure. Vous pouvez également sélectionner une option dans la liste des applications courantes **Applications**.

Application

Vous pouvez, au lieu d'attribuer un nom à la règle d'application spéciale, sélectionner une option de la liste des applications courantes pour que le système remplisse automatiquement les champs de configuration restants.

Port de déclenchement

Entrez la plage de ports sortants utilisée par votre application (par exemple **6500-6700**).

Type de trafic de déclenchement

Sélectionnez le protocole sortant utilisé par votre application (par exemple **Les deux**).

Port pare-feu

Entrez la plage de ports à ouvrir pour le trafic Internet (par exemple, **6000-6200**).

Type de trafic pare-feu

Sélectionnez le protocole utilisé par le trafic Internet réacheminé au routeur par le biais de la plage de port ouverts (par exemple **Les deux**).

Programmation

Choisissez une programmation pour l'application de cette règle. Si vous ne voyez pas la programmation pertinente dans la liste des plages horaires, allez à l'écran Outils → Horaires et créez une nouvelle programmation.

Enregistrer/Mettre à jour

Enregistrez les modifications apportées dans la liste suivante.

Effacer

Réinitialisez cette zone de l'écran en annulant toute modification que vous avez apportée.

Avec l'exemple ci-dessus de règle d'application activée, le routeur ouvrira une plage de ports (de 6000 à 6200) pour le trafic entrant chaque fois qu'un ordinateur du réseau interne ouvrira une application qui envoie des données sur Internet via un port compris dans la plage 6500 à 6700.

Règles d'applications

Liste de règles d'application définies. Cochez la case à gauche «Activer» pour activer ou désactiver directement la valeur saisie. Il est possible de changer une entrée en cliquant sur l'icône Modifier, ou de l'éliminer en cliquant sur l'icône Supprimer. Si vous cliquez sur l'icône Modifier, l'élément est mis en surbrillance et la section de modification de la règle d'application est activée pour modification.

MISE EN FORME DE TRAFIC

La fonctionnalité de gestion de trafic améliore le rendement de votre réseau en priorisant les applications.

Configuration Traffic Shaping

Activer Traffic Shaping

Lorsque cette option est activée, le routeur limite le flux du trafic sortant de manière à ne pas dépasser le débit de liaison montante du grand réseau.

Classification automatique

Cette option est activée par défaut pour que votre routeur détermine automatiquement les programmes prioritaires pour le réseau. Pour obtenir des performances optimales, utilisez l'option Classification automatique pour définir automatiquement la priorité de vos applications.

Fragmentation dynamique

Cette option devrait être activée lorsque la liaison montante à Internet est lente. Il peut être utile de limiter l'impact des paquets volumineux à faible priorité sur les paquets plus urgents en les fragmentant en paquets plus courts.

Vitesse automatisée de la liaison montante/descendante

Lorsque cette option est activée, le routeur mesure automatiquement la bande passante utile des liens en amont et en aval à chaque rétablissement de la communication avec l'interface WAN (après un redémarrage, par exemple).

Débit de liaison montante mesuré

Il s'agit du débit de liaison montante mesuré lors du dernier rétablissement de l'interface de grand réseau. La valeur pourrait être inférieure à celle indiquée par votre FSI car cette dernière ne comprend pas tous les surdébits de protocole réseau associés au réseau de votre FSI. En général, cette valeur ne représente que 87 % à 91 % du débit de liaison montante indiqué pour les connexions xDSL et présente environ 5 kbps de moins pour les connexions réseau par câble.

Vitesse de liaison montante manuelle

Si l'option Vitesse automatisée de la liaison montante est désactivée, cette option vous permet de définir la vitesse de la liaison montant de façon manuelle. La vitesse de la liaison montante est la vitesse à laquelle les données peuvent être transférées du routeur vers le FAI. Cette vitesse est déterminée par votre FAI. Les FAI présentent fréquemment le facteur de vitesse en paire liaison montante/descendante, par exemple 1,5 Mbit/s-284 Kbit/s. Dans ce cas, vous devriez entrer la valeur 284. Vous pouvez également vérifier la vitesse de la liaison montante par l'entremise d'un service tel que www.dsreports.com. Il est à noter toutefois que les sites tels que DSL Reports ne tiennent pas compte de tout le trafic de données imposé par les protocoles réseau. Par conséquent, ils indiquent des vitesses légèrement inférieures au débit de liaison montante mesuré ou au débit évalué du FAI.

Type de connexion

Par défaut, le routeur détermine automatiquement si la connexion sous-jacente est un réseau xDSL/à relais de trame ou un autre type de connexion (comme un modem câble ou un réseau Ethernet); il affiche le résultat sous la forme **Réseau xDSL ou à relais de trame détecté**. Si vous avez une connexion réseau non courante par laquelle vous êtes actuellement connecté via xDSL mais pour laquelle vous avez réglé les paramètres WAN à «Statique» ou «DHCP», régler cette option à **réseau xDSL ou autre à relais de trame** permet de s'assurer que le routeur reconnaîtra qu'il doit contrôler le trafic de manière un peu différente en vue d'assurer des performances optimales. Si vous choisissez l'option **Réseau xDSL ou autre à relais de trame**, la vitesse en amont mesurée s'affiche comme étant un peu plus lente qu'habituellement sur ces connexions, mais elle permet d'obtenir de bien meilleurs résultats.

Ligne d'abonné numérique ou réseau à délais de trames détecté

Lorsque l'option **Type de connexion** est réglée à **Détection automatique**, le type de connexion détecté automatiquement est affiché ici.

Ajouter/Modifier les règles de Traffic Shaping

Une règle de Traffic Shaping identifie un flux de messages particulier et lui assigne une priorité. Pour la plupart des applications, le classement automatique conviendra et aucune règle de mise en forme du trafic spécifique ne sera nécessaire.

La gestion de trafic accepte les chevauchements entre les règles, où plusieurs règles peuvent correspondre à un flux de messages donné. Si plus d'une règle correspond à un flux de messages particulier, la règle ayant la plus haute priorité s'appliquera.

Activer

Indique si l'entrée sera active ou inactive.

Nom

Créez un nom significatif pour cette règle.

Priorité

La priorité du flux de messages est définie ici : la valeur 0 correspond à la priorité la plus haute (plus urgent) et la valeur 255 à la priorité la plus faible (moins urgent).

Protocole

Protocole utilisé par les messages.

Plage IP locale

La règle s'applique au flux de messages dont l'adresse IP côté réseau local est comprise dans la plage configurée ici.

Plage de ports locaux

La règle s'applique au flux des messages dont le numéro de port côté réseau local est compris dans la plage indiquée ici.

Plage d'adresses IP à distance

La règle s'applique à un flux de messages dont l'adresse IP du côté WAN est dans la plage définie ici.

Plage de ports à distance

La règle s'applique à un flux de messages dont le numéro de port côté WAN est compris dans la plage configurée ici.

Enregistrer/Mettre à jour

Enregistrez les modifications apportées dans la liste suivante.

Effacer

Réinitialisez cette zone de l'écran en annulant toute modification que vous avez apportée.

Règles de Traffic Shaping

Cette section dresse la liste de toutes les règles de gestion de trafic définies. Cochez la case à gauche «Activer» pour activer ou désactiver directement la valeur saisie. Il est possible de changer une entrée en cliquant sur l'icône Modifier, ou de l'éliminer en cliquant sur l'icône Supprimer. Si vous cliquez sur l'icône Modifier, l'élément est mis en surbrillance et la section de modification de la règle de mise en forme du trafic est activée pour modification.

ROUTAGE

Ajouter/Modifier la route

Ajoute une nouvelle route à la table de routage IP ou modifie une route existante.

Activer

Indique si l'entrée sera activée ou désactivée.

IP de destination

Adresse IP des paquets qui empruntent cette route.

Masque de réseau

Un segment du masque indique les bits de l'adresse IP qui doivent correspondre.

Passerelle

Indique la prochaine étape si cette route est utilisée. Une passerelle 0.0.0.0 indique qu'il n'y a pas de prochaine étape; l'adresse IP correspondante est directement connectée au routeur de l'interface visée : Réseau local ou grand réseau.

Métrique

La valeur métrique de la route est une valeur comprise entre 1 et 16; cette valeur indique le coût d'utilisation de la route. Une valeur de 1 correspond au coût le plus bas, et 15, au coût le plus élevé. Une valeur de 16 indique que la route n'est pas accessible à partir de ce routeur. Lorsqu'ils tentent d'atteindre une destination particulière, les ordinateurs de votre réseau sélectionnent la route la plus appropriée en ignorant les routes inaccessibles.

Interface

Indique quelle interface -- LAN ou WAN -- le paquet IP doit utiliser pour transiter hors du routeur, lorsque cette route est utilisée.

Enregistrer/Mettre à jour

Enregistrez les modifications apportées dans la liste suivante.

Effacer

Réinitialisez cette zone de l'écran en annulant toute modification que vous avez apportée.

Liste de routes

La section présente les entrées de la table de routage courante. Certaines routes obligatoires sont prédéfinies et ne peuvent être modifiées. Pour modifier les routes que vous ajoutez, cliquez sur l'icône Modifier; pour les supprimer, cliquez sur l'icône Supprimer. Lorsque vous cliquez sur l'icône Modifier, l'article visé est mis en évidence et la section «Modifier la route» est activée pour permettre d'entrer les modifications. Cochez la case à gauche «Activer» pour activer ou désactiver directement la valeur saisie.

CONTROLE DES ACCES

La section Contrôle des accès vous permet de contrôler l'accès aux données entrantes et sortantes des périphériques de votre réseau. Utilisez cette fonction aux fins de contrôle parental pour ne permettre l'accès qu'à des sites approuvés, pour limiter l'accès au Web en fonction de l'heure ou des jours, et pour bloquer l'accès à des applications comme des utilitaires ou des jeux sur liaison d'égal à égal.

Activer

Par défaut, la fonction de contrôle des accès est désactivée. Cochez cette option pour activer le contrôle des accès.

Remarque: Lorsque la fonction Contrôle d'accès est désactivée, chaque périphérique du réseau dispose d'un libre accès à Internet. Si cette fonction est activée, l'accès à Internet est limité pour les périphériques couverts par une stratégie de contrôle des accès. Tous les autres périphériques auront un libre accès à Internet.

Assistant Stratégie

L'assistant de politique vous guide à travers les étapes permettant de définir chaque politique de contrôle des accès. Une politique définit le «Qui, Quel, Quand et Comment» du contrôle des accès -- les ordinateurs de qui seront affectés par le contrôle, quelles adresses Internet seront contrôlées, quand le contrôle sera-t-il en vigueur et comment le contrôle est-il installé. Vous pouvez définir de nombreuses politiques. L'assistant apparaît lorsque vous cliquez sur le bouton ci-dessous et également lorsque vous modifiez une politique existante.

Ajouter une politique

Cliquez sur ce bouton pour commencer à créer une nouvelle politique de contrôle des accès.

Table des politiques

Cette section présente les politiques de contrôle d'accès actuellement définies. Il est possible de changer une politique en cliquant sur l'icône Modifier, ou de l'éliminer en cliquant sur l'icône Supprimer. Lorsque vous cliquez sur l'icône Modifier, l'assistant de gestion des politiques démarre et vous guide durant le processus de modification de la politique. Pour activer ou désactiver des politiques individuelles de la liste, il suffit de cliquer dans la case à cocher Activer.

FILTRE DE SITE WEB

Les sites Web énumérés ici sont utilisés lorsque l'option Filtre Web est activée à la page Avancé
→ Contrôle des accès.

Ajouter une règle de filtrage Web

Cette section permet d'ajouter des sites Web à utiliser pour l'option de contrôle des accès.

URL/Domaine de site Web

Entrez l'URL (adresse) du site Web à autoriser, par exemple : **google.com**. N'entrez pas le préfixe **http://** de cette adresse. Entrez le domaine le plus inclusif; par exemple, entrez **kyocera.com** pour obtenir l'accès à la fois à **www.kyocera.com** et à **support.kyocera.com**.

Enregistrer

Enregistrez les modifications apportées dans la liste suivante.

Remarque: De nombreux sites Web créent des pages à l'aide d'images et de contenu provenant d'autres sites. Si vous n'autorisez pas tous les sites Web utilisés pour créer une page vous ne pourrez accéder aux sites. Par exemple, pour accéder au site **my.yahoo.com**, vous devez permettre l'accès aux sites **yahoo.com**, **yimg.com** et **doubleclick.net**.

Règles de filtrage de site Web

La section contient la liste des sites Web actuellement autorisés.

FILTRE D'ADRESSE MAC (FILTRE RESEAU)

La section du filtre d'adresse MAC peut être utilisée pour filtrer l'accès au réseau par des appareils en fonction des adresses MAC uniques de leur carte réseau. Cette option est très utile pour empêcher les périphériques sans fil non autorisés de se connecter à votre réseau. Une adresse MAC est un numéro d'identification unique attribué par le fabricant de l'adaptateur réseau.

Configuration du filtrage MAC

Choisissez le type de filtre MAC nécessaire.

Désactiver l'option de filtrage MAC: Quand Arrêt est sélectionné, les adresses MAC ne sont pas utilisées pour contrôler l'accès au réseau.

Activez l'option de filtrage MAC ainsi que l'option AUTORISÉ pour les ordinateurs de la liste d'accès au réseau : Lorsque l'option «AUTORISÉ» est cochée, seuls les ordinateurs dont l'adresse MAC figure dans la liste des règles de filtrage MAC peuvent accéder au réseau.

ACTIVEZ l'option de filtrage MAC ainsi que l'option REFUSÉ pour les ordinateurs de la liste d'accès au réseau : Lorsque l'option «REFUSER» est sélectionnée, l'accès au réseau sera refusé à tous les ordinateurs dont l'adresse MAC figure dans la liste de règles de filtrage MAC.

Ajouter un règle de filtrage MAC

Utilisez cette section pour ajouter des adresses MAC à la liste ci-dessous.

Adresse MAC

Entrez l'adresse MAC d'un ordinateur que vous souhaitez contrôler par filtrage MAC. Les ordinateurs ayant obtenu une adresse IP du serveur DHCP du routeur figureront dans la liste de clients DHCP. Sélectionnez un périphérique dans le menu déroulant.

Enregistrer

Enregistrez les modifications apportées dans la liste suivante.

Règles de filtrage MAC

Cette section dresse la liste des périphériques réseau contrôlés par le filtrage MAC.

PARAMETRES DU PARE-FEU

Le routeur fournit un pare-feu sécuritaire de par la nature même de la fonction NAT (traduction d'adresses réseau). En effet, cette fonction ne répond à aucune requête entrante non sollicitée sur aucun port, ce qui rend votre réseau local invisible et le protège contre les attaques informatiques, à moins que vous ne configuriez votre routeur autrement. Cependant, certaines applications réseau ne peuvent pas fonctionner si le pare-feu est trop sécurisé. Ces applications doivent ouvrir des ports spécifiques du pare-feu pour fonctionner correctement. Les options de cette page définissent plusieurs façons d'ouvrir le pare-feu pour répondre aux besoins de certaines applications. Voir aussi [Avancé → Serveur virtuel](#), [Avancé → Routage de port](#), [Avancé → Règles d'application](#) et [Avancé → Réseau \(UPnP\)](#) pour des options connexes.

Paramètres du pare-feu

Activer SPI

La fonction SPI («stateful packet inspection» (inspection de l'état des paquets), appelé aussi «dynamic packet filtering» (filtrage dynamique des paquets) aide à empêcher les cyberattaques en faisant un suivi plus approfondi de l'état par session. Elle valide les paquets conformes au protocole acheminés pendant la session. Lorsque le protocole est TCP, SPI vérifie que les numéros séquentiels des paquets restent dans la plage valide pour la session, rejetant les paquets dont les numéros séquentiels sont invalides.

Que SPI soit activé ou non, le routeur surveille toujours l'état des connexions TCP et s'assure que chaque indicateur de paquet TCP est valide pour l'état en cours.

Filtrage de point d'extrémité NAT

Les options de filtrage de point d'extrémité NAT contrôlent la façon dont le NAT du routeur gère les demandes de connexion entrante sur les ports déjà utilisés.

Indépendant du point d'extrémité

Une fois qu'une application côté LAN a créé une connexion à travers un port particulier, la fonction NAT transfère toutes les requêtes de connexion entrantes avec le même port vers l'application LAN, peu importe leur source. C'est l'option la moins restrictive, qui offre la meilleure connectivité et qui permet à certaines applications (en particulier aux applications P2P) de se comporter presque comme si elles étaient connectées directement à Internet.

Adresse restreinte

La fonction NAT (traduction d'adresses de réseau) achemine les requêtes de connexion entrantes vers un hôte du réseau local que si elles proviennent de la même adresse IP que celle avec laquelle une connexion a été établie. Ceci permet à l'application à distance de renvoyer des données par le biais d'un port autre que celui utilisé par la session sortante créée.

Port et adresse restreints

La NAT ne transmet aucune requête entrante avec la même adresse de port qu'une connexion déjà établie.

Il est à noter que certaines de ces options peuvent interagir avec d'autres restrictions de port. La méthode de filtrage indépendant de point d'extrémité a la priorité sur les filtres de données entrantes ou les horaires. Par conséquent, il se peut qu'une requête de session entrante associée à une session sortante pénètre par un port malgré la présence d'un filtre de port actif. Toutefois, les paquets seront rejetés tel que prévu lorsqu'ils seront envoyés aux ports bloqués (par horaire ou par filtre des données entrantes) pour lesquels on ne retrouve aucune session active. Le filtrage limité de port et d'adresse permet d'assurer que les horaires et les filtres de données entrantes fonctionnent correctement, bien qu'il limite le niveau de connectivité. Par conséquent, il est parfois nécessaire de recourir aux ports de déclenchement, aux serveurs virtuels ou aux serveurs de jeux pour ouvrir les ports requis par une application. Le filtrage limité d'adresse offre un compromis qui permet d'éviter des problèmes de communication avec certains types de routeurs NAT (en particulier les routeurs NAT symétriques) tout en laissant les filtres de données entrantes et les accès programmés fonctionner normalement.

Filtrage de point d'extrémité UDP

Contrôle le filtrage de point d'extrémité pour les paquets UDP.

Filtrage de point d'extrémité TCP

Contrôle le filtrage des ports de fin des paquets du protocole TCP.

Anciennement, les termes « à cône plein » (Full Cone), « à cône restrictif » (Restricted Cone), « à cône restrictif sur les ports » (Port Restricted Cone) et « symétrique » étaient utilisés pour désigner différentes variations du NAT. Ces termes ne sont pas employés ici car ils ne décrivent pas complètement le comportement de la technique NAT du routeur. Bien que le mappage ne soit pas parfait, les correspondances perdues suivantes entres les modes de classification « conique » et de filtrage de point d'extrémité peuvent être extraites : Si ce routeur est configuré pour un filtrage indépendant de point d'extrémité, il applique une méthode « à cône plein »; le filtrage limité d'adresse applique une méthode « à cône restrictif »; le filtrage limité de port et d'adresse applique une méthode « à cône restrictif sur les ports ».

Préservation port NAT

L'option de préservation de port NAT (activée par défaut) vise à assurer que le port utilisé par l'hôte du réseau local lors d'une connexion à Internet est également utilisé comme port Internet visible. Cette méthode garantit la meilleure compatibilité pour les communications Internet.

Dans certaines circonstances il est conseillé de désactiver cette fonction.

Vérification anti-usurpation

L'activation de cette option peut vous protéger contre certains types d'attaques d'usurpation. Il est recommandé d'utiliser cette option avec discernement puisqu'elle peut entraîner la perte de la connexion au grand réseau avec certains modems. Le cas échéant, il peut être nécessaire de changer l'adresse 192.168.0.x du sous-réseau local (par 192.168.2.x, par exemple), pour rétablir la connexion au grand réseau.

Hôte DMZ

DMZ signifie «zone démilitarisée». Si une application ne fonctionne pas bien derrière le routeur, vous pouvez exposer un ordinateur directement à Internet et faire tourner l'application sur cette machine.

Lorsqu'un hôte de réseau local est configuré en tant qu'hôte DMZ, il devient la destination pour tous les paquets entrants qui ne correspondent pas aux autres sessions ou règles de données entrantes. Si une autre règle d'entrée est en vigueur, elle sera utilisée plutôt que d'envoyer des paquets à l'hôte DMZ. Ainsi, une session active, un serveur virtuel, un déclencheur de port actif ou une règle de jeu aura la priorité sur l'envoi d'un paquet à l'hôte DMZ host. (La politique DMZ ressemble à une règle de jeu par défaut qui effectue le routage de tous les ports qui ne sont pas autrement attribués spécifiquement.)

Le routeur n'offre qu'une protection pare-feu limitée pour l'hôte en DMZ. Le routeur ne transmet pas de paquet TCP qui ne concorde pas avec une session DMZ active, sauf s'il s'agit d'un paquet d'établissement de connexion (SYN). Excepté pour cette protection limitée, l'hôte DMZ est effectivement «en dehors du pare-feu». Tout utilisateur qui envisage d'utiliser un hôte DMZ doit aussi penser à faire tourner un pare-feu sur ce système hôte DMZ pour obtenir une protection additionnelle.

Les adresses IP du côté grand réseau des paquets reçus par l'hôte ZDM sont traduites en adresses IP de côté réseau local. Cependant, les numéros de port ne sont pas traduits. Par conséquent, les applications de l'hôte ZDM peuvent dépendre d'un ou de plusieurs numéros de port précis.

La fonctionnalité ZDM (zone démilitarisée, ou publique) ne constitue que l'un des moyens permettant d'autoriser les requêtes entrantes qui peuvent sembler non sollicitées à la fonction NAT. En règle générale, l'hôte ZDM ne devrait être utilisé qu'en dernier ressort, puisqu'il est beaucoup plus exposé aux attaques informatiques que tout autre système du réseau local. Il est recommandé d'explorer d'autres types de configuration, notamment un serveur virtuel, une règle de jeu ou un port de déclenchement. Les serveurs virtuels ouvrent un port pour les sessions entrantes destinées à une application donnée (en plus d'autoriser le routage de port et l'utilisation de passerelles ALG).

Une règle de jeu fonctionne à l'instar d'une ZDM sélective, où le trafic entrant associé à un ou plusieurs ports est acheminé à un hôte donné du réseau local, ce qui limite l'exposition des ports par rapport à un hôte ZDM. Un port de déclenchement est une fonction de jeu activée par le trafic sortant. Elle permet de router les ports uniquement lorsque le déclencheur est actif.

Peu d'applications nécessitent vraiment l'utilisation de l'hôte ZDM. Un hôte ZDM peut être requis dans les cas suivants :

- Un système hôte doit pouvoir prendre en charge plusieurs applications susceptibles d'utiliser des ports d'entrée qui se chevauchent de manière à ce que deux règles de jeux ne puissent être utilisées et entrer potentiellement en conflit.
- Permet de traiter les connexions entrantes qui font appel à un protocole autre que ICMP, TCP, UDP et IGMP (de même que les protocoles GRE et ESP, s'ils sont activés par les ALG PPTP et IPSec).

Activer DMZ

Remarque : Mettre un ordinateur en DMZ peut l'exposer à divers risques pour la sécurité. Utiliser cette option n'est recommandé qu'en dernier ressort.

Adresse IP DMZ

Indique l'adresse IP locale de l'ordinateur du réseau auquel vous désirez accorder un accès sans restriction à Internet. Si cet ordinateur obtient son adresse de façon automatique par DHCP, vous pourriez définir une réservation statique à la page Paramètres de base → Paramètres réseau de façon à empêcher l'adresse IP de l'ordinateur ZDM d'être modifiée.

Session de réseau local non-UDP/TCP/ICMP

Lorsqu'une application de réseau local qui utilise un protocole autre que UDP, TCP ou ICMP ouvre une session sur Internet, la fonction NAT du routeur peut suivre une telle session même si elle ne reconnaît pas le protocole. Cette fonction permet d'activer certaines applications (ou, ce qui est encore plus important, une connexion RPV unique à un hôte distant) sans qu'il soit nécessaire d'utiliser une passerelle ALG.

Il est à noter que cette fonctionnalité ne s'applique pas à l'hôte ZDM (le cas échéant). L'hôte ZDM traite toujours ces types de session.

Activer

Activer cette option (la valeur par défaut) permet des connexions RPV à un hôte éloigné. (Mais, dans le cas de multiples connexions RPV, il faut utiliser ALG RPV.) Toutefois, désactiver cette option ne désactive que le réseau privé virtuel si ALG RPV est également désactivé.

Configuration de la passerelle d'application (ALG)

Vous pouvez ici activer ou de désactiver les algorithmes (ALG). Certains protocoles et applications nécessitent un traitement spécial du payload (champ libre) IP pour leur permettre de fonctionner avec la fonction NAT (traduction d'adresses réseau). Chaque ALG assure un traitement spécial pour un protocole ou une application spécifique. Plusieurs ALG pour les applications courantes sont activés par défaut.

PPTP

Permet à plusieurs machines raccordées au réseau local de se connecter à leurs réseaux d'entreprise à l'aide du protocole PPTP. Lorsque l'option ALG PPTP est activée, les ordinateurs du réseau local peuvent établir des connexions RPV PPTP avec le même serveur ou d'autres serveurs virtuels différents. Lorsque l'option ALG PPTP est désactivée, le routeur autorise l'exploitation RPV de manière restrictive -- Les ordinateurs du réseau local peuvent créer des tunnels RPV vers d'autres serveurs Internet RPV mais pas vers le même serveur.

Désactiver ALG PPTP offre l'avantage d'accroître la performance du réseau privé virtuel. Activer ALG PPTP permet également les connexions RPV entrantes en provenance du serveur RPV du côté LAN (reportez-vous à la section *Avancé* → *Serveur virtuel*).

IPSec (RPV)

Permet à plusieurs clients RPV de se relier à leurs réseaux corporatifs à l'aide d'une connexion IPSec. Certains clients RPV permettent au protocole IPSec de traverser la fonction NAT (NAT Traversal). Cette option peut nuire au fonctionnement des clients RPV. Si vous éprouvez des difficultés à vous connecter à votre réseau corporatif, essayez de désactiver cette option.

Vérifiez auprès de l'administrateur système de votre réseau corporatif si votre client RPV prend en charge NAT Traversal.

Notez que les connexions RPV L2TP utilisent en général IPSec pour sécuriser la connexion. Pour configurer une connexion RPV directe dans ce cas, la fonction de passerelle d'application (ALG) IPSec doit être activée.

RTSP

Permet aux applications utilisant le protocole de diffusion RTSP (Real Time Streaming Protocol) de recevoir les flux de données audio-vidéo d'Internet. QuickTime et Real Player font partie des applications courantes qui exploitent ce protocole.

Windows/MSN Messenger

Prise en charge de Microsoft Windows Messenger (client de messagerie Internet fourni dans Microsoft Windows) et de MSN Messenger sur des ordinateurs de réseau local. L'ALG SIP doit aussi être activée lorsque l'ALG Windows Messenger est activée.

FTP

Permet aux clients et serveurs FTP de transférer les données à travers NAT. Reportez-vous à la page *Avancé* → *Serveur virtuel* si vous souhaitez héberger un serveur FTP.

H.323 (NetMeeting)

Permet aux clients H.323 (particulièrement pour Netmeeting) de communiquer par le biais de NAT. Veuillez noter que si vous désirez que vos amis vous appellent, vous devrez également configurer un serveur virtuel pour NetMeeting. Reportez-vous à la page *Avancé* → *Serveur virtuel* pour savoir comment configurer un serveur virtuel.

SIP

Permet aux périphériques et aux applications qui utilisent VoIP (voix sur IP) de communiquer au moyen de la technique NAT. Certains périphériques et applications VoIP ont la capacité de détecter les périphériques NAT et de fonctionner en périphérie de ceux-ci. Cette passerelle ALG pourrait interférer avec le fonctionnement de tels périphériques. Si vous éprouvez des difficultés à effectuer des appels VoIP, essayez de désactiver cette passerelle ALG.

Wake-On-LAN (réveil par le réseau)

Cette fonction permet l'acheminement des «paquets magiques» (autrement dit, des paquets de réveil) entre le réseau étendu et un ordinateur du réseau local ou un autre périphérique à fonction Wake on LAN (WOL). Le périphérique WOL doit être défini comme tel à la page *Avancé* → *Serveur virtuel*. L'adresse IP LAN du serveur virtuel est généralement réglée à l'adresse broadcast 192.168.0.255. L'ordinateur connecté au réseau local et dont l'adresse réside dans le paquet magique sera réveillé.

MMS

Permet au lecteur Windows Media, grâce au protocole MMS, de recevoir du contenu multimédia diffusé en continu en provenance d'Internet.

FILTRE ENTRANT

Lorsque vous utilisez les fonctions de serveur virtuel, serveur de jeux ou d'administration à distance pour ouvrir des ports particuliers pour le trafic Internet, vous augmentez l'exposition de votre réseau local aux cyberattaques lancées sur Internet. Dans ces situations, vous pouvez utiliser des filtres de données entrantes pour limiter cette exposition en spécifiant les adresses IP des hôtes Internet auxquels vous faites confiance et qui pourront accéder à votre réseau local via les ports que vous avez ouverts. Vous pourriez, par exemple, accorder un accès au serveur de jeux sur votre réseau local domestique à certains de vos amis que vous invitez à jouer à un jeu.

Les filtres entrants peuvent servir à limiter l'accès à un serveur de votre réseau à un système ou groupe de systèmes. Les règles de filtre s'appliquent aux fonctions Serveur virtuel, Serveur de jeux ou Administration à distance. Chaque filtre peut servir pour plusieurs fonctions; par exemple, un filtre «Clan du jeu» peut autoriser tous les membres d'un groupe de jeu particulier à jouer à plusieurs jeux différents pour lesquels des entrées ont été créées. En même temps un filtre «Admin» pourrait n'autoriser que les systèmes connectés à votre réseau d'entreprise à accéder aux pages admin et au serveur FTP que vous utilisez à la maison. Si vous ajoutez une adresse IP au filtre, cette modification se répercutera partout où le filtre est utilisé.

Ajouter/Modifier la règle de filtre entrant

Cette section vous permet d'ajouter ou de modifier des entrées dans la liste des règles de filtrage des données entrantes ci-dessous.

Nom

Entrez un nom significatif pour la règle.

Action

La règle peut autoriser ou interdire les messages.

Plage d'adresses IP à distance

Définissez les plages d'adresses Internet auxquelles la règle s'applique. Pour une adresse IP unique, entrez la même adresse dans les deux champs **Début** et **Fin**. Vous pouvez saisir jusqu'à huit plages d'adresses. La case **Activer** vous permet d'activer ou de désactiver des entrées particulières de la liste de plages.

Enregistrer/Mettre à jour

Enregistrez les modifications apportées dans la liste suivante.

Effacer

Réinitialisez cette zone de l'écran en annulant toute modification que vous avez apportée.

Liste de règles de filtre entrant

La section présente la liste des règles de filtre de données entrantes actuelles. Il est possible de changer une entrée en cliquant sur l'icône Modifier, ou de l'éliminer en cliquant sur l'icône Supprimer. Lorsque vous cliquez sur l'icône Modifier, l'article visé est mis en évidence et la section «Modifier la règle de filtre entrant» est activée pour permettre la modification.

En plus des filtres énumérés ici, il existe deux filtres prédéfinis disponibles dans les cas où des filtres de données entrantes peuvent être appliqués :

Autoriser tous

Autoriser tout utilisateur WAN à accéder à la fonction connexe.

Refuser tous

Empêche tous les utilisateurs du réseau étendu d'accéder à la fonction connexe. (Les règles de filtrage entrant ne s'appliquent pas aux utilisateurs du réseau local.)

SANS-FIL AVANCE

Puissance de transmission

En temps normal, l'émetteur sans fil fonctionne à puissance maximale. Dans certains cas toutefois, il peut être nécessaire de restreindre une fréquence spécifique à une zone plus petite. En réduisant la puissance de l'émetteur radio, vous pouvez empêcher que les transmissions dépassent les limites physiques de votre espace de travail, de votre bureau à la maison ou de votre réseau sans fil.

Période de la balise

Les balises sont des paquets envoyés par un routeur sans fil pour synchronisation avec les périphériques sans fil. Indiquez une valeur comprise entre 20 et 1000 dans le champ Période de balise. La valeur par défaut est réglée à 100 millisecondes.

Seuil RTS

Lorsqu'un nombre excessif de collisions de paquets sur liaison sans fil se produit, il est possible d'améliorer les performances en utilisant le protocole de transmission RTS/CTS (Request to Send/Clear to Send). Le transmetteur sans fil commencera à envoyer des trames RTS (et attendra les paquets CTS) lorsque la taille du bloc de données en octets sera supérieure au seuil RTS. Vous devriez laisser ce paramètre à sa valeur par défaut, soit 2 346 octets.

Seuil de fragmentation

Les trames de l'environnement sans-fil peuvent être divisées en plus petites unités (fragments) pour améliorer les performances en présence d'interférences FR et dans les zones limites de la couverture FR. La fragmentation se produit lorsque la taille de paquet en octets est supérieure au seuil de fragmentation. Ce paramètre doit garder sa valeur par défaut de 2 346 octets. Une valeur de fragmentation trop basse peut entraîner une dégradation des performances du réseau.

Intervalle DTIM

Un DTIM est un mécanisme de comptage à rebours informant les clients de la prochaine fenêtre pour l'écoute des messages broadcast (diffusion générale) et multicast (multidiffusion). Lorsque le routeur sans fil a mis en mémoire tampon des messages broadcast ou multicast pour les clients associés, il envoie le DTIM suivant associé à une valeur d'intervalle DTIM. Les clients sans fil détectent les balises et se réveillent pour recevoir les messages broadcast et multicast. La valeur par défaut est 1. Les valeurs valides sont comprises dans la fourchette de 1 à 255.

Compatible 802.11d

Active le fonctionnement de 802.11d. La spécification de réseau sans fil 802.11d est destinée à des domaines de réglementation supplémentaires. Ce supplément à la spécification 802.11 définit les exigences de la couche physique (mise en canal, modèles de saut de fréquence, nouvelles valeurs des attributs MIB actuels), ainsi que d'autres exigences qui étendent l'utilisation des réseaux sans fil 802.11 à d'autres pays. La spécification 802.11 actuelle définit le fonctionnement dans un nombre limité de pays. Ce supplément ajoute les exigences et les définitions nécessaires pour que les périphériques 802.11 fonctionnent dans des marchés non couverts par la spécification actuelle. Sélectionnez cette option si vous vous trouvez dans l'un de ces domaines de réglementation supplémentaires.

Isolation Sans-fil

Activer l'option Isolation Sans fil empêche les clients sans fil de communiquer ensemble.

Activer WMM

Activer l'option WMM peut aider à contrôler le temps d'attente et les gigue pendant l'acheminement de contenu multimédia sur une connexion sans fil.

Activation du WDS

Lorsque l'option WDS est activée, ce point d'accès fonctionne comme répéteur sans fil et peut communiquer avec d'autres PA par le biais de liaisons WDS. Notez que WDS est incompatible WPA -- ces deux fonctions ne peuvent être utilisées en même temps. Une liaison WDS est bidirectionnelle; c'est pourquoi ce point d'accès doit connaître l'adresse MAC (créée le lien WDS) de l'autre PA, et l'autre PA doit avoir un lien WDS de retour vers ce PA. Vérifiez que les points d'accès sont configurés avec le même numéro de canal.

Adresse MAC du PA WDS

Indique la première moitié du lien WDS. L'autre point d'accès doit également avoir l'adresse MAC de ce PA d'origine pour permettre le retour. Entrez une adresse MAC pour chacun des autres points d'accès que vous désirez connecter au système de distribution sans fil (WDS).

WISH

L'acronyme WISH (Wireless Intelligent Stream Handling) désigne une technologie conçue pour optimiser votre expérience d'utilisateur de réseau sans fil en priorisant la circulation des données de diverses applications.

WISH

Activer WISH

Sélectionnez cette option pour permettre à WISH de prioriser le trafic.

Classificateurs de priorité

HTTP

Permet au routeur de reconnaître les transferts HTTP de nombreux flux («streams») de données audio et vidéo et de leur donner une priorité par rapport aux autres données. Les lecteurs de contenu numérique utilisent couramment de tels flux.

Windows Media Center

Permet au routeur de reconnaître certains flux audio et vidéo générés par un PC Windows Media Center et de leur donner priorité dans le trafic. Ces flux sont utilisés par des systèmes appelés Windows Media Extenders, tel que la console Xbox 360.

Automatique

Lorsque cette option est activée, le routeur tente automatiquement de donner priorité aux flux de données que, normalement, il ne distingue pas, en se basant sur le comportement qu'affichent ces flux. Ceci entraîne la dé-prioritisation de flux qui affichent des caractéristiques de transfert en bloc, tels que les transferts de fichier; le trafic interactif, tel que les données de jeux ou de VoIP, conserve toutefois sa priorité normale.

Ajouter/Modifier règle WISH

Une règle WISH identifie un flux de messages spécifique et lui attribue une priorité. Pour la plupart des applications, les classificateurs par priorité garantissent l'application des priorités et des règles WISH spécifiques ne sont pas nécessaires.

WISH accepte les chevauchements entre les règles. Si plus d'une règle correspond à un flux de messages particulier, la règle ayant la plus haute priorité s'appliquera.

Activer

Indique si l'entrée sera active ou inactive.

Nom

Créez un nom significatif pour cette règle.

Priorité

Vous indiquez ici la priorité de flux de messages. Quatre priorités sont définies :

- BK: Arrière-plan (moins urgent).
- BE: Meilleur effort.
- VI: Vidéo.
- VO: Voix (le plus urgent).

Protocole

Protocole utilisé par les messages.

Plage IP de l'hôte 1

La règle s'applique à un flux de messages pour lequel l'adresse IP d'un ordinateur se retrouve dans la plage définie ici.

Plage de ports de l'hôte 1

La règle s'applique au flux des messages dont le numéro de port de l'hôte 1 est compris dans la plage indiquée ici.

Plage IP hôte 2

La règle s'applique au flux de messages pour lequel l'adresse IP de l'autre ordinateur fait partie de la plage de valeurs entrée ici.

Plage de ports de l'hôte 2

La règle s'applique à un flux de messages pour lequel le numéro de port de l'hôte 2 est compris dans la plage définie ici.

Enregistrer/Mettre à jour

Enregistrez les modifications apportées dans la liste suivante.

Effacer

Réinitialisez cette zone de l'écran en annulant toute modification que vous avez apportée.

Règles WISH

Cette section présente la liste des règles WISH définies. Cochez la case à gauche «Activer» pour activer ou désactiver directement la valeur saisie. Il est possible de changer une entrée en cliquant sur l'icône Modifier, ou de l'éliminer en cliquant sur l'icône Supprimer. Si vous cliquez sur l'icône Modifier, l'élément est mis en surbrillance et la section de modification de la règle WISH est activée pour modification.

WI-FI PROTECTED SETUP (WEP)**Wi-Fi Protected Setup (WEP)****Activer**

Activez la fonction de configuration de l'accès Wi-Fi protégé.

Verrouiller les paramètres de sécurité sans fil

Verrouiller les paramètres de sécurité sans fil permet d'empêcher un nouveau registraire externe utilisant son NIP de les modifier. Des périphériques peuvent toutefois être encore ajoutés au moyen de la fonction Wi-Fi Protected Setup (configuration protégée Wi-Fi). On peut également modifier les paramètres du réseau sans fil à l'aide des options Configuration manuelle du réseau sans fil, Assistant de configuration du réseau sans fil, ou un registraire de gestion WLAN externe existant.

Paramètres NIP

Un NIP est un nombre unique utilisable pour ajouter le routeur à un réseau existant ou créer un nouveau réseau. Il est possible que le NIP par défaut soit indiqué sur le dessous du routeur. Pour plus de sécurité, il est conseillé de faire générer un nouveau NIP. Vous pouvez en tout temps restaurer le NIP d'origine. Mais seul l'administrateur (compte «admin») peut modifier ou remettre à zéro ce numéro.

NIP actuel

Affiche la valeur actuelle du NIP du routeur.

Rétablir le NIP par défaut

Rétablit le NIP par défaut du routeur.

Générer un nouveau NIP

Créez un nombre aléatoire représentant un NIP valide. Celui-ci devient le NIP du routeur. Vous pouvez ensuite copier ce NIP dans l'interface utilisateur du registraire.

Ajouter station sans fil

Cet assistant vous aide à ajouter des périphériques sans fil au réseau à l'aide du protocole Wi-Fi Protected Setup.

L'assistant vous demandera d'entrer le NIP de l'appareil, ou d'appuyer sur le bouton de configuration de cet appareil. Si l'appareil prend en charge la fonction Wi-Fi Protected Setup et qu'il possède un bouton de configuration, vous pouvez ajouter cet appareil au réseau en appuyant sur son bouton puis sur celui du routeur dans les 60 secondes qui suivent. Le voyant d'état du routeur clignotera trois fois si l'appareil a été ajouté avec succès au réseau.

Il existe plusieurs façons d'ajouter un dispositif sans fil à votre réseau. L'accès au réseau sans fil est géré par un registraire. Le registraire n'autorise l'accès d'un dispositif au réseau sans fil que si vous avez entré le NIP ou appuyé sur le bouton Configuration de l'accès Wi-Fi protégé du dispositif. Le routeur agit à titre de registraire pour le réseau, bien que d'autres dispositifs puissent également jouer ce rôle.

Assistant Ajouter un périphérique sans fil

Démarrez l'assistant.

RESEAU AVANCE

UPnP

UPnP (Universal Plug and Play) est une architecture de réseautage qui assure la compatibilité entre le matériel, les logiciels et les périphériques d'un réseau. Ce routeur peut prendre en charge la fonction UPnP et peut être utilisé conjointement avec d'autres dispositifs et logiciels UPnP.

Activer UPnP

Si vous avez besoin du service UPnP, vous pouvez l'activer ici.

Permettre aux utilisateurs de désactiver l'accès Internet.

Désactivez cette option pour empêcher les clients UPnP de mettre fin à la connexion au grand réseau.

Autoriser les utilisateurs à modifier le mappage du serveur virtuel

Désactiver cette option empêche les clients UPnP d'ajouter, de modifier, de supprimer ou de désactiver des entrées de serveur virtuel.

Ping WAN

Effectuer un test ping sur les adresses IP du réseau étendu public est une méthode courante qu'utilisent les pirates informatiques pour vérifier si votre adresse IP WAN est valide.

Activer la réponse du Ping de grand réseau

Si vous laissez cette option désactivée, le routeur ignorera les commandes **ping** pour l'adresse IP WAN publique du routeur.

Filtre entrant de test Ping du grand réseau

Sélectionnez un filtre qui contrôle les ordinateurs de grand réseau autorisés à utiliser la fonctionnalité Ping. Si le filtre dont vous avez besoin ne figure pas dans la liste de filtres, accédez à l'écran *Avancé* → *Filtre de données entrantes* et créez un nouveau filtre.

Vitesse du port WAN

Ce champ est habituellement réglé à Auto. Si vous éprouvez des difficultés à vous connecter au grand réseau, essayez les autres paramètres.

Flux Multicast (multidiffusion)

Le routeur utilise le protocole IGMP pour assurer une multidiffusion efficace -- transmission de contenu identique (p. ex. multimédia) d'une source à plusieurs destinataires.

Activer les flux de multidiffusion

Cette option doit être activée si une application sur le réseau local participe à un groupe multidiffusion. Si vous disposez d'une application de réseau local multimédia qui ne reçoit pas le contenu attendu, essayez d'activer cette option.

Connexion PPPoE

Cette option définit si les ordinateurs reliés au réseau local peuvent agir comme clients PPPoE et négocier les sessions PPP par le biais du routeur sur le lien Ethernet du réseau étendu.

Activer émulation PPPoE

L'activation de cette option permet aux ordinateurs du réseau local d'agir comme des clients PPPoE. La désactivation de cette option empêche les ordinateurs du réseau local d'établir des connexions directes PPPoE.

REPRISE

Le routeur peut établir une liaison ascendante au moyen du port Ethernet WAN ou de tout autre modem connecté aux ports USB, ExpressCard ou CardBus. Même si tous ces périphériques sont connectés, un seul à la fois peut établir une liaison. Si la connexion WAN échoue, le routeur tente automatiquement d'établir une nouvelle liaison avec un autre périphérique. Cette fonction est appelée reprise automatique.

Détection d'échec WAN

La détection d'échec de liaison WAN recherche la présence de trafic sur la liaison Ethernet WAN (s'applique uniquement aux liaisons Ethernet WAN, et non aux modems). Si cette liaison est inactive pendant trop longtemps, le routeur effectue un test ping sur une adresse IP cible. S'il n'y a aucune réponse, le routeur assume qu'il n'y a plus de liaison et tente de la rétablir avec un modem.

Activer

Cette fonction permet d'activer la détection d'échec de liaison Ethernet. Même si elle est désactivée, si vous débranchez le câble Ethernet du port WAN, le routeur tentera une reprise de liaison sur un modem.

Temporisation

Si la liaison Ethernet est inactive pendant cette période de temps, le routeur envoie un ping ou tente une reprise sur un modem.

Activation du ping en mode inactif

Lorsque cette fonction est sélectionnée, le routeur envoie un ping à la fin de la temporisation de liaison. Si le ping obtient une réponse, le routeur remet à zéro le compteur de temporisation, sinon, il tente une reprise sur un modem.

Cible ping

La cible ping par défaut est la passerelle du routeur. Vous pouvez spécifier une autre adresse IP cible ici.

Interfaces WAN

Cette section permet de changer l'ordre de reprise des périphériques (ou interfaces), de contrôler leur état, de fermer la liaison active ou de transférer la liaison sur un autre périphérique. Le périphérique en haut de la liste a la priorité. Il s'agit du périphérique que le routeur tente de lancer lorsqu'il démarre. Si la liaison ne peut être établie sur ce périphérique ou est coupée ultérieurement, le routeur tentera de la rétablir sur le prochain périphérique disponible dans la liste. Lorsqu'une liaison échoue sur un périphérique, le routeur passe toujours au périphérique suivant dans la liste jusqu'au dernier, puis reprend la liste depuis le début.

Connecteur

Le connecteur est le port physique dans lequel le modem ou le câble Ethernet est branché.

Périphérique

La description du périphérique apparaît ici.

État

État de la liaison d'un périphérique, qui peut être l'un des suivants.

Prêt

Le périphérique est branché et disponible, mais pas actif.

Établissement

Le routeur tente de transférer la liaison sur le périphérique.

Établie

La liaison est active sur le périphérique.

Suspendue

Le routeur n'essaiera pas de transférer la liaison sur un autre périphérique avant l'expiration d'une temporisation. Cela s'applique uniquement aux modems, qui doivent se conformer aux spécifications du fournisseur quant au nombre de tentatives de connexion au réseau. La temporisation dépend du nombre de tentatives de connexion successives.

Contrôle

Le périphérique ayant une liaison active affichera une icône en forme de cercle et de barre oblique. Si vous cliquez sur cette icône, le routeur coupera la liaison. Dans ce cas, il n'y a pas de reprise automatique.

Une icône en forme d'ampoule s'affiche pour tous les autres périphériques disponibles. Si vous cliquez sur cette icône, le routeur tentera d'établir la liaison avec ce périphérique. Si nécessaire, il fermera d'abord la liaison active. La reprise passera au périphérique suivant de la liste.

Priorité

Cliquez sur les flèches montantes ou descendantes pour changer la priorité du périphérique.

AIDE SUR LES OUTILS

- Paramètres d'administrateur
- Heure
- Syslog
- Paramètres de courriel
- Système
- Microprogramme
- DNS dynamique
- Vérification de système
- Horaires

PARAMETRES D'ADMINISTRATEUR

La section Paramètres d'administrateur permet de configurer l'accès sécurisé à la gestion Web. Par défaut, aucun mot de passe n'est configuré. Il est fortement recommandé de créer un mot de passe afin de sécuriser votre nouveau routeur.

Langue du système

La langue d'affichage des pages Web du routeur peut être modifiée ici.

Mot de passe Admin

Entrez un mot de passe pour l'utilisateur «admin», qui aura un accès complet à l'interface de gestion Web.

Mot de passe d'accès à Internet

Entrez un mot de passe pour l'utilisateur «utilisateur» qui n'aura qu'un accès lecture à l'interface de gestion Web.

Nom de la passerelle

Le nom du routeur peut être changé ici.

Délai d'inactivité

Si le routeur ne détecte pas d'activité d'administration (sur le réseau étendu ou le réseau local) durant ce nombre de minutes, il mettra fin à la session de l'administrateur.

Activer le serveur HTTPS

L'activation de cette option rend possible la gestion à distance avec le protocole sécurisé HTTP (HTTPS).

Activer la gestion à distance

L'activation de la gestion à distance vous permet de gérer le routeur à partir de n'importe quel endroit sur Internet. La désactivation de la gestion à distance vous permet de gérer le routeur uniquement à partir des ordinateurs de votre réseau local.

Port admin à distance

Port que vous utiliserez pour accéder à l'interface de gestion sur Internet. Par exemple, si vous indiquez ici «1080» comme valeur de port pour accéder au routeur à partir d'Internet, vous utiliserez une adresse URL au format suivant :
<http://mon.domaine.com:1080/>.

Utiliser HTTPS

Activer cette option nécessite que toute administration à distance utilise le protocole HTTP Sécurisé (HTTPS). Par exemple, si vous indiquez «1080» comme valeur du port ci-dessus, pour accéder au routeur à partir d'Internet vous utiliserez une adresse URL au format suivant : <https://mon.domaine.com:1080/>.

Filtre entrant Admin à distance

Sélectionnez un filtre qui contrôle l'accès tel que requis pour ce port admin. Si le filtre dont vous avez besoin ne figure pas dans la liste de filtres, accédez à l'écran Avancé → Filtre de données entrantes et créez un nouveau filtre.

HEURE

L'option de configuration des heures permet de définir, mettre à jour et gérer l'heure de l'horloge interne du routeur. À partir de cette section, vous pouvez définir le fuseau horaire dans lequel vous vous trouvez ainsi que le serveur de temps. Vous pouvez aussi configurer l'option d'heure avancée pour ajuster automatiquement l'horloge aux dates prévues.

Configuration de l'heure

Heure courante du routeur

Affiche l'heure mise à jour actuellement par le routeur. Si cette heure est incorrecte, utilisez les options ci-dessous pour la configurer correctement.

Fuseau horaire

Sélectionnez votre fuseau horaire dans le menu déroulant.

Activer l'option Heure avancée

Cochez cette option si l'heure avancée (DST) s'applique à votre emplacement.

Décalage de l'heure avancée

Sélectionnez le décalage horaire si votre région observe l'heure avancée.

Début DST et Fin DST

Sélectionnez l'heure de début et de fin des modifications liées à l'heure avancée (DST). Par exemple, supposons que pour Début DST vous sélectionnez Mois=Oct, Sem=3e, Jour=Dim et Heure=2 h. Ceci équivaut à dire : «L'heure avancée commence le troisième dimanche d'octobre à 2 □h».

Configuration automatique de l'heure

Activer le serveur NTP

Sélectionnez cette option pour synchroniser l'horloge du routeur avec un serveur de temps NTP sur Internet. Si vous utilisez des horaires ou des journaux, cette option constitue la meilleure façon d'assurer la précision de ces éléments.

Veillez noter que, même lorsque le serveur NTP est activé, vous devez encore choisir un fuseau horaire et régler les paramètres d'heure avancée.

Serveur NTP utilisé

Sélectionnez un serveur de temps réseau pour la fonction de synchronisation. Saisissez l'adresse d'un serveur de temps ou sélectionnez-en un dans la liste. Si vous ne parvenez pas à utiliser un serveur, choisissez-en un autre.

Définir manuellement la date et l'heure

Si l'option Serveur NTP n'est pas activée, vous pouvez régler manuellement l'heure de votre routeur ici, ou cliquez sur le bouton **Copier les paramètres d'heure de l'ordinateur** pour copier l'heure de l'ordinateur que vous utilisez. (Vérifiez que l'heure de l'ordinateur est réglée correctement).

Remarque: Si le routeur cesse d'être alimenté en courant pour une quelconque raison, il ne peut continuer de faire fonctionner l'horloge et lorsque l'alimentation sera rétablie, l'heure sera inexacte. Afin de maintenir l'heure exacte pour les programmes et les journaux, vous devez soit changer l'heure après avoir redémarré le routeur, soit activer l'option de serveur de temps NTP.

SYSLOG

Cette section vous permet d'archiver vos fichiers journaux dans un serveur Syslog .

Activer la journalisation au serveur Syslog

Activez cette option si votre réseau utilise un serveur Syslog auquel vous désirez transmettre des messages de journalisation.

Adresse IP du serveur Syslog

Entrez l'adresse IP LAN du serveur Syslog.

PARAMETRES DE COURRIEL

La fonction de courriel ne peut être utilisée pour l'envoi des fichiers de journaux du système, des messages d'alerte du routeur et de l'avis de mise à jour du progiciel à votre adresse de courriel.

Activer

Activer l'envoi d'avis par courriel

Lorsque cette option est activée, les journaux d'activité du routeur ou les avis de mise à niveau du microprogramme peuvent être envoyés par courriel à l'adresse courriel désignée, et les paramètres suivants sont affichés.

Paramètres de courriel

De l'adresse courriel

Cette adresse de courriel s'affichera comme celle de l'expéditeur lorsque vous recevrez un fichier de journal ou une mise à niveau du progiciel par courriel.

Adresse de courriel du destinataire

Entrez l'adresse de courriel du destinataire.

Adresse du serveur SMTP

Entrez l'adresse du serveur SMTP pour l'envoi des courriels.

Activer l'authentification

Si votre serveur SMTP exige une authentification, sélectionnez cette option.

Nom du compte

Entrez votre nom de compte pour l'envoi de courriel.

Mot de passe

Entrez le mot de passe associé au compte.

Vérifiez le mot de passe

Tapez de nouveau le mot de passe associé au compte.

Envoyer journal par courriel lorsque plein ou programmation

Lorsque le journal est plein

Sélectionnez cette option si vous désirez que les journaux soient envoyés par courriel lorsqu'un journal est plein.

Programmé

Sélectionnez cette option si vous voulez que les journaux soient envoyés par courriel selon un horaire programmé.

Programmation

Si vous avez sélectionné l'option Selon la programmation, sélectionnez l'une des règles de programmation définies. Si vous ne voyez pas la programmation pertinente dans la liste des plages horaires, allez à l'écran Outils → Horaires et créez une nouvelle programmation.

Remarque: En règle général, les courriels sont envoyés à l'heure de début définie pour un horaire. L'heure de fin est rarement utilisée. Cependant, le redémarrage du routeur pendant la période d'heure entraînera l'envoi de courriels supplémentaires.

SYSTEME

Cette section permet de gérer les paramètres de configuration du routeur, de le redémarrer et de restaurer ses paramètres par défaut. La restauration des paramètres par défaut supprime tous les paramètres actuels, y compris les règles que vous avez créées.

Enregistrer sur le disque dur local

Cette option vous permet d'enregistrer la configuration du routeur dans un fichier de votre ordinateur. N'oubliez pas d'effectuer cette sauvegarde avant de procéder à une mise à niveau du progiciel.

Charger à partir du disque dur local

Utilisez cette option pour restaurer les paramètres de configuration du routeur enregistrés précédemment.

Restaurer aux valeurs par défaut d'origine

Cette option restaure tous les paramètres de configuration aux valeurs en vigueur dans le routeur à sa sortie de l'usine. Tous les paramètres non sauvegardés seront perdus. Si vous voulez enregistrer les paramètres de configuration de votre routeur, utilisez l'option ci-dessus, Enregistrer les paramètres.

Réinitialiser le routeur

Permet de redémarrer le routeur. Cette option est pratique lorsque vous devez redémarrer le routeur mais que vous ne vous trouvez pas à proximité.

MICROPROGRAMME

Utiliser la section Progiciel pour installer la version la plus récente pour une optimisation des fonctions et des performances. Si vous souhaitez recevoir un avis lorsqu'une nouvelle version du progiciel est publiée, cochez la case en regard de l'option **Avis par courriel d'une nouvelle version du progiciel**.

Pour mettre à niveau le progiciel, suivez les étapes ci-dessous :

1. Cliquez sur le bouton **Naviguer** pour repérer le fichier de mise à niveau sur votre ordinateur.
2. Après avoir trouvé le fichier à utiliser, cliquez sur le bouton **Charger** ci-dessous pour lancer le processus de mise à niveau du progiciel. Cette opération peut prendre quelques minutes.
3. Attendez que le routeur ait redémarré. Ce processus peut prendre encore une minute ou plus.
4. Confirmez dans la page d'état la révision du progiciel mis à jour.

Information sur le microcode

Cette zone affiche les numéros de version du progiciel actuellement installé sur votre routeur et la mise à niveau la plus récente disponible.

Mise à niveau progiciel

Remarque: Certaines mises à niveau du progiciel ont restauré les options de configuration aux valeurs par défaut d'origine. Avant d'exécuter une mise à niveau, n'oubliez pas d'enregistrer la configuration actuelle à l'écran Outils → Système.

Transférer

Après avoir enregistré le fichier de mise à niveau du microprogramme sur l'ordinateur, utilisez cette option pour rechercher le fichier puis télécharger les données vers le routeur.

Options d'avis de mise à niveau du progiciel

Vérifier automatiquement en ligne la dernière version du microcode

Lorsque cette option est activée, votre routeur consulte le site Web de façon périodique afin de vérifier si vous possédez la version la plus récente du microcode.

Courriel d'avis concernant une version de microprogramme plus récente

Lorsque cette option est activée, dès qu'un nouveau progiciel est disponible un courriel est envoyé à l'adresse indiquée à la section Courriel. Vous devez avoir activé l'option Avis par courriel à la page Outils → Paramètres Courriel.

DNS DYNAMIQUE

La fonctionnalité DNS dynamique vous permet d'héberger un serveur (Web, FTP, jeu, etc.) à l'aide d'un nom de domaine que vous vous êtes procuré (www.lenomdevotrechoix.com) avec votre adresse IP attribuée de façon dynamique. La plupart des FAI à large bande attribuent des adresses IP dynamiques (variables). Lorsque vous utilisez un fournisseur de service DNS dynamique, vos amis peuvent entrer votre nom d'hôte pour se connecter à votre serveur, peu importe votre adresse IP.

Activer DNS dynamique

Activez cette option si vous avez acheté votre propre nom de domaine et si vous vous êtes enregistré auprès d'un fournisseur de services DNS dynamique. Les paramètres suivants sont affichés lorsque l'option est activée.

Adresse du serveur

Sélectionnez un fournisseur de services DNS dynamique dans la liste déroulante.

Nom d'hôte

Entrez votre nom d'hôte complet, par exemple : **monhôte.mondomaine.net**.

Nom d'utilisateur ou clé

Entrez le nom d'utilisateur ou la clé que votre fournisseur de services Internet vous a transmis. Si le fournisseur de services DNS dynamique ne fournit qu'une clé, entrez cette clé dans les trois champs.

Mot de passe ou clé

Entrez le mot de passe ou la clé fourni(e) par votre FAI. Si le fournisseur de DNS dynamique n'attribue qu'une clé, entrez-la dans les trois champs.

Vérifiez le mot de passe ou la clé.

Saisissez de nouveau le mot de passe ou la clé fournie par votre FAI. Si le fournisseur de services DNS dynamique ne fournit qu'une clé, entrez sa valeur dans les trois champs

Temporisation

Période entre les mises à jour régulières au DNS dynamique, si votre adresse IP dynamique n'a pas changée. La période de temporisation est indiquée en heures.

Remarque: Si une mise à niveau de DNS dynamique échoue (par exemple, lors de la saisie de paramètres inexacts), le routeur désactive automatiquement la fonction DNS dynamique et enregistre l'échec dans le journal.

Remarque: Après avoir configuré le routeur pour le DNS dynamique, vous pouvez utiliser un navigateur pour accéder à l'URL de votre domaine (par exemple <http://www.mondomaine.info>); le routeur tentera d'acheminer la requête au port 80 de votre réseau local. Si vous effectuez cette opération depuis un ordinateur du côté réseau et qu'aucun serveur virtuel n'est défini pour le port 80, le routeur renverra la page d'accueil de configuration du routeur. Reportez-vous à la page de configuration Avancé → Serveur virtuel pour définir un serveur virtuel.

VERIFICATION DE SYSTEME

Test Ping

La fonction «Ping» est un utilitaire Internet qui envoie une série de messages brefs vers l'ordinateur visé et génère un rapport sur les résultats. Vous pouvez l'utiliser pour tester le fonctionnement d'un ordinateur et pour connaître la qualité de la connexion à cette machine en se basant sur la vitesse des réponses.

Nom d'hôte ou adresse IP

Entrez l'adresse IP de l'ordinateur cible ou son nom de domaine complet.

Ping

Lancer un test ping sur l'hôte indiqué.

Stop

L'hôte reçoit des messages Ping continuellement, jusqu'à ce que vous cliquiez sur ce bouton.

Exemple :

Nom d'hôte ou adresse IP

www.whitehouse.gov

Résultat ping

Please wait, resolving www.whitehouse.gov....
Resolved to 205.161.7.102.
Response from 205.161.7.102 received in 7 milliseconds.
Response from 205.161.7.102 received in 6 milliseconds.
Response from 205.161.7.102 received in 7 milliseconds.
User stopped ping.

HORAIRES

Des programmations peuvent être créées et être utilisées avec des règles de mise en application. Par exemple, si vous désirez restreindre l'accès à Internet du lundi au vendredi de 15 h à 20 h, vous pourriez créer une programmation en sélectionnant les valeurs Lun, Mar, Mer, Jeu et Ven, puis entrer 15 h comme heure de début et 20 h comme heure de fin.

Ajouter/modifier une règle d'horaire

Cette section vous permet d'ajouter ou de modifier des entrées dans la liste de règles de programmation ci-dessous.

Nom

Attribuez un nom significatif à l'horaire, par exemple « Règle de semaine ».

Jour(s)

Cochez les cases des jours désirés ou cliquez sur le bouton radio Toute la semaine pour sélectionner les sept jours de la semaine.

1 jour - 24 heures

Sélectionnez cette option si vous désirez que cette programmation soit en vigueur au cours du ou des jours sélectionnés.

Heure de début

Si vous n'utilisez pas l'option 1 jour, entrez l'heure ici. L'heure de début doit être entrée dans deux champs. Le premier champ permet de saisir l'heure et le second, les minutes. Les événements de messagerie ne sont normalement déclenchés que par l'heure de début.

Temps de fin

L'heure de fin est saisie dans le même format que l'heure de début. L'heure est indiquée dans la première case et les minutes, dans la seconde. L'heure de fin est utilisée pour la plupart des autres règles mais, habituellement, pas pour les événements de courriel.

Enregistrer/Mettre à jour

Enregistrez les modifications apportées dans la liste suivante.

Effacer

Réinitialisez cette zone de l'écran en annulant toute modification que vous avez apportée.

Liste de règles de programmation

Cette section montre les règles de programmation actuellement définies. Il est possible de changer une entrée en cliquant sur l'icône Modifier, ou de l'éliminer en cliquant sur l'icône Supprimer. Si vous cliquez sur l'icône Modifier, l'élément est mis en surbrillance et la section de modification de la règle de programmation est activée pour modification.

AIDE SUR L'ETAT

- Info routeur
- Sans fil (Wi-Fi)
- Routage
- Journaux
- Statistiques
- Sessions actives
- Sessions WISH

INFO ROUTEUR

Tous les détails de vos connexions au réseau et à Internet sont affichés sur la page Info routeur. La version du progiciel figure aussi sur cette page.

Remarque : Certains navigateurs interdisent l'actualisation de l'affichage d'état du grand réseau lors d'une modification d'état. Certains navigateurs requièrent l'actualisation de l'affichage pour pouvoir obtenir la mise à jour de l'état. Certains navigateurs signalent une condition d'erreur lors d'une tentative d'affichage de l'état du grand réseau.

WAN

L'information affichée portera sur la connexion au grand réseau présentement active. Pour modifier les priorités de reprise des diverses connexions au grand réseau ou pour effectuer une connexion/déconnexion manuelle, allez à la page *Avancé* → *Reprise*. Si la connexion est de type DHCP, cliquer sur le bouton **Libérer DHCP** retire l'adresse IP attribuée au routeur. Le routeur ne répondra pas aux messages IP en provenance du réseau étendu tant que vous n'aurez pas cliqué sur le bouton **Renouveler DHCP** ou remis de nouveau le routeur sous tension. Lorsque vous cliquez sur **Renouveler DHCP**, le routeur envoie une requête au serveur du FAI pour obtenir une nouvelle adresse IP.

Réseau local

Cette section de l'écran affiche les paramètres de configuration figurant à la page *Config de base* → *Réseau*. L'**adresse MAC** est l'identificateur, attribué en usine, des ports du réseau local.

Réseau sans fil (Wi-Fi)

Cette zone de l'écran présente les paramètres de configuration des pages *Standard* → *Sans fil* page, *Avancé* → *WISH* et *Avancé* → *WPS* page. L'option **Adresse MAC** correspond à l'identificateur attribué par le fabricant de la carte réseau sans fil.

Ordinateurs du réseau local

Cette zone de l'écran se régénère sans cesse pour afficher tous les ordinateurs et dispositifs DHCP connectés côté LAN de votre routeur. La «plage» de détection est limitée à la plage d'adresses configurée dans le serveur DHCP. Les PC dont l'adresse n'est pas comprise dans cette plage n'apparaîtront pas dans la liste. Si le client DHCP (c.-à-d. un ordinateur configuré à «Obtenir automatiquement une adresse») fournit un nom d'hôte, cette information sera également affichée.

Tout PC ou dispositif doté d'une adresse IP statique comprise dans la plage de détection figurera dans la liste, mais pas son nom d'hôte.

Membres Multicast IGMP

Si le protocole IGMP est activé, cette zone de l'écran présente tous les groupes multidiffusion dont font partie les périphériques de réseau local.

SANS FIL (WI-FI)

La section Sans fil vous permet d'afficher les clients sans fil connectés à votre routeur.

Adresse MAC

Identificateur Ethernet (adresse MAC) du client sans fil.

Adresse IP

Adresse IP côté réseau du client.

Mode

Norme de transmission utilisée par le client. Les valeurs sont 11a, 11b, 11g ou 11n pour les normes 802.11a, 802.11b, 802.11g ou 802.11n, respectivement.

Débit

Débit réel de transmission du client, en mégabits par seconde.

Signal

C'est la mesure relative de la qualité du signal. La valeur est indiquée sous forme de pourcentage de la meilleure qualité théorique. La qualité du signal est affectée par la distance, l'interférence des autres sources de fréquences radio (comme les téléphones sans fil ou les réseaux sans fil avoisinants), et par les obstacles situés entre le routeur et l'appareil sans fil.

Si l'option **Exiger une ouverture de session** est activée, vous pouvez également contrôler les privilèges d'accès Internet pour les clients sans fil reliés.

ROUTAGE

La section sur le routage affiche toutes les informations de routage configurées pour votre routeur.

Une valeur de 0.0.0.0 pour la passerelle signifie qu'il n'y a pas de prochain saut et que l'adresse IP est directement connectée au routeur sur l'interface indiquée : LAN ou WAN. Une valeur de 0.0.0.0 pour l'IP de destination et le masque de sous-réseau signifie qu'il s'agit de la route par défaut.

JOURNAUX

Le routeur enregistre automatiquement dans sa mémoire interne (sous forme de journaux) les événements présentant un intérêt potentiel. Si la mémoire ne permet pas d'enregistrer tous les événements, les journaux des événements plus anciens sont effacés, et seuls les plus récents sont conservés. L'option Journaux vous permet de visualiser les journaux du routeur. Vous pouvez définir quels types d'événements vous souhaitez consulter et le niveau à afficher. Ce routeur prend également en charge un serveur Syslog (journal de système) vous permettant d'envoyer les fichiers de journaux à un ordinateur de votre réseau exploitant un utilitaire Syslog.

Quoi afficher

Sélectionnez les types d'événements que vous souhaitez afficher.

- Pare-feu et sécurité
- Système
- État du routeur

Afficher niveaux

Sélectionnez le niveau d'événements que vous souhaitez visualiser.

- Critique
- Attention
- Informationnel

Appliquer les paramètres journal maintenant

Cliquez sur ce bouton après avoir entré les modifications dans la section Options journal pour les mettre en vigueur et les rendre permanentes.

Actualiser

Ce bouton permet d'actualiser l'affichage des entrées de journal. De nouveaux événements peuvent être survenus depuis votre dernier accès au journal.

Effacer

Ce bouton permet d'effacer toutes les entrées de journal.

Envoyer courriel maintenant?

Si vous avez indiqué une adresse courriel à l'écran Outils → Paramètres de courriel et que vous cliquez sur le bouton **Courriel maintenant**, le journal du routeur sera envoyé à l'adresse courriel spécifiée.

Enregistrer le journal

Sélectionnez cette option pour enregistrer le journal du routeur dans un fichier de votre ordinateur.

STATISTIQUES

La page Statistiques affiche toutes les données statistiques de transmission et réception des paquets sur réseaux local, WAN et sans fil.

K-octets envoyés

Nombre de paquets envoyés par le routeur.

K-octets reçus

Nombre de paquets reçus par le routeur.

Paquets abandonnés en transmission

Nombre de paquets abandonnés à l'envoi à cause d'erreurs, de collisions ou d'un manque de ressources du routeur.

Perte de paquets RX

Nombre de packets perdus pendant leur réception, en raison d'erreurs, de collisions, ou de limites de ressources du routeur.

Collisions

Nombre de paquets perdus à cause de collisions Ethernet (au moins deux périphériques tentant d'utiliser un circuit Ethernet en même temps).

Erreurs

Nombre d'échecs de transmission entraînant la perte d'un paquet. Un environnement RF bruyant peut causer un taux d'erreur élevé sur le réseau sans fil.

SESSIONS ACTIVES

La page Sessions actives affiche tous les détails des sessions Internet actives utilisant votre routeur. Une session Internet est une conversation entre un programme ou une application sur un ordinateur LAN et un programme ou une application sur un ordinateur WAN.

Local

L'adresse IP et, si approprié, le numéro de port de l'application locale.

NAT

Numéro de port de l'application du côté LAN tel que perçu par l'application du côté WAN.

Internet

Adresse IP et, s'il y a lieu, numéro de port de l'application sur Internet.

Protocole

Protocole de communication utilisé pour la conversation.

Province

État des sessions qui utilisent le protocole TCP.

- NO: Aucun(e) -- Cette entrée sert de marque de réservation pour une connexion future éventuelle.
- SS: Envoi de SYN -- Un des systèmes tente de démarrer une connexion.
- EST: Connexion établie -- transmission de données en cours.
- FW: FIN Wait -- Le système client a envoyé une requête d'arrêt de la connexion.
- CW: Close Wait -- (connexion en attente): le système client a envoyé une requête de déconnexion.
- TW: Time Wait -- Attente pendant une courte durée qu'une connexion à l'état FIN Wait soit entièrement fermée.
- LA: Last ACK -- Courte attente jusqu'à ce qu'une connexion en mode Close Wait soit totalement terminée.
- CL: Fermé -- La connexion n'est plus active mais la session reste en mode suivi au cas où des paquets retransmis sont encore en attente.

Dir

Sens d'ouverture de la conversation :

Vers l'extérieur

Initialisé de LAN à WAN.

Vers l'intérieur

Initialisé de WAN à LAN.

Priorité

Préférence attribuée aux paquets sortants de cette conversation par la logique du moteur QoS. Plus le nombre est petit, plus la priorité est élevée.

Temporisation

Nombre de secondes de temps d'inactivité avant que le routeur considère que la session est terminée. La valeur initiale du délai d'attente est fonction du type et de l'état de la connexion.

300 secondes

Connexionsx UDP.

240 secondes

Connexions TCP réinitialisées ou fermées. La connexion ne s'interrompt pas instantanément, de façon à permettre le passage des paquets tardifs ou le rétablissement de la connexion.

7800 secondes

Établissement ou fermeture des connexions TCP.

SESSIONS WISH

Lorsque l'option WISH a été activée, la page Sessions WISH affiche tous les détails des sessions sans fil locales actives passant par le routeur. Une session WISH est une conversation entre un programme ou une application sur un ordinateur connecté sans fil du côté réseau local et un autre ordinateur, sans égards au mode de connexion de ce dernier.

Expéditeur

Adresse IP et, s'il y a lieu, numéro de port de l'ordinateur qui a établi une connexion réseau.

Cible

Adresse IP et, s'il y a lieu, numéro de port de l'ordinateur avec lequel la connexion réseau a été établie.

Protocole

Protocole de communication utilisé pour la conversation.

Province

État des sessions qui utilisent le protocole TCP.

- NO: Aucun(e) -- Cette entrée sert de marque de réservation pour une connexion future éventuelle.
- SS: Envoi de SYN -- Un des systèmes tente de démarrer une connexion.
- EST: Connexion établie -- transmission de données en cours.
- FW: FIN Wait -- Le système client a envoyé une requête d'arrêt de la connexion.
- CW: Close Wait -- (connexion en attente): le système client a envoyé une requête de déconnexion.
- TW: Time Wait -- Attente pendant une courte durée qu'une connexion à l'état FIN Wait soit entièrement fermée.

- LA: Last ACK -- Courte attente jusqu'à ce qu'une connexion en mode Close Wait soit totalement terminée.
- CL: Fermé -- La connexion n'est plus active mais la session reste en mode suivi au cas où des paquets retransmis sont encore en attente.

Priorité

Priorité sur cette conversation attribuée aux paquets envoyés par liaison sans fil par la logique WISH. Les priorités sont :

- BK: Arrière-plan (moins urgent).
- BE: Meilleur effort.
- VI: Vidéo.
- VO: Voix (le plus urgent).

Temporisation

Nombre de secondes de temps d'inactivité avant que le routeur considère que la session est terminée. La valeur initiale du délai d'attente est fonction du type et de l'état de la connexion.

300 secondes

Connexionsx UDP.

240 secondes

Connexions TCP réinitialisées ou fermées. La connexion ne s'interrompt pas instantanément, de façon à permettre le passage des paquets tardifs ou le rétablissement de la connexion.

7800 secondes

Établissement ou fermeture des connexions TCP.

GLOSSAIRE DE L'AIDE

8

802.11

Famille de spécifications pour les réseaux locaux sans fil (WLAN), élaborée par un groupe de travail de l'IEEE (Institute of Electrical and Electronics Engineers).

A

Accès protégé Wi-Fi (WPA)

Version mise à jour de la norme de sécurité pour les réseaux sans fil, offrant des fonctions d'authentification et de chiffrage

ActiveX

Spécification de Microsoft pour l'interaction des composants logiciels.

Adressage IP privé automatique

Adressage APIPA. Adresse IP qu'un ordinateur sous Windows s'attribue à lui-même lorsqu'il est configuré pour obtenir une adresse IP automatiquement mais qu'aucun serveur DHCP n'est disponible sur le réseau.

Adresse IP

Numéro de 32 bits, en environnement Internet Protocol version 4, qui identifie chaque ordinateur transmettant des données sur Internet ou un intranet

Adresse MAC

Numéro d'identification (ID) unique du matériel que le fabricant attribue à chaque adaptateur Ethernet.

Adresse IP dynamique

Adresse IP attribuée par un serveur DHCP et pouvant être changée. Les fournisseurs d'accès à Internet par câble ont généralement recours à cette méthode pour attribuer des adresses IP à leurs clients.

ADSL

Asymmetric Digital Subscriber Line, ou liaison numérique asymétrique sur ligne d'abonné

Alphanumérique

Caractères A à Z et 0 à 9

Ancien

Technologie ou périphériques de versions antérieures

Antenne

Permet de transmettre et de recevoir des signaux RF.

Antenne Yagi

Antenne directionnelle servant à concentrer les signaux sans fil sur un emplacement particulier

AppleTalk

Ensemble de protocoles de réseau local développés par Apple pour ses systèmes informatiques

ASCII

American Standard Code for Information Interchange (ASCII). Ce système de caractères est la norme la plus couramment utilisée pour les fichiers texte.

Atténuation

Perte de puissance des signaux numériques et analogiques. La perte est plus importante lorsque le signal est transmis sur de longues distances.

B**Balise**

Cadre de données par lequel l'une des stations de travail d'un réseau Wi-Fi diffuse périodiquement des données de contrôle de réseau vers les autres stations sans fil.

Base de données

Organise l'information de façon à ce qu'elle puisse être gérée et mise à jour tout en étant facile à consulter par les utilisateurs ou les applications.

Bit/s

Bits par seconde

BOOTP

Protocole d'amorçage. Permet aux ordinateurs de s'initialiser et d'obtenir une adresse IP sans intervention de l'utilisateur.

Broadband

Large bande de fréquences disponible pour la transmission de données

C**Capacité de traitement**

Volume de données pouvant être transféré durant une période définie.

CardBus

Version plus récente de l'interface PCMCIA ou de la carte PC. Elle prend en charge les chemins de données 32 bits ainsi que l'accès direct à la mémoire (DMA) et consomme moins de courant.

Carte réseau

Carte insérée dans un ordinateur ou intégrée à la carte mère, qui permet au PC de se connecter à un réseau

CAT 5

Catégorie 5. Utilisé pour les connexions Ethernet 10/100 Mbps ou 1 Gbps

Certificats numériques:

Méthode électronique servant à fournir des attestations d'identité à un serveur afin d'obtenir l'accès à ce serveur ou à un réseau

Chiffrement

Conversion des données en texte chiffré afin qu'il ne puisse être facilement lu.

Chiffrement MPPE

Le chiffrement Microsoft Point-to-Point Encryption (MPPE) permet de sécuriser les transmissions de données sur connexions PPTP.

CIR

Carte réseau

Clé de la session

Clé de cryptage et de décryptage générée pour chaque session de communication entre deux ordinateurs

Client

Programme ou utilisateur qui demande des données au serveur

Collision

Lorsque deux périphériques sur le même réseau Ethernet tentent de transmettre des données exactement au même moment.

Concentrateur

Dispositif sans fil qui connecte ensemble plusieurs dispositifs

Cookie (témoin)

Information stockée sur le disque dur de votre ordinateur, contenant vos préférences pour le site qui a placé le témoin sur votre PC

Couche Data-Link

Deuxième couche du modèle OSI. Contrôle le flux des données sur le lien physique d'un réseau

Couche de la session

Cinquième couche du modèle OSI qui organise et synchronise la connexion et la communication entre les applications à chaque extrémité

Couche des applications

Septième couche du modèle OSI. Fournit des services aux applications pour assurer une communication appropriée avec les autres applications d'un réseau.

Couche physique

Première couche du modèle OSI. Permet au matériel de transmettre des signaux électriques sur une porteuse de données

Couche réseau

Troisième couche du modèle OSI qui s'occupe du routage du trafic sur un réseau

Courriel

On appelle courriel un message stocké sur l'ordinateur et transmis sur Internet

D**Data Encryption Standard (DES)**

Utilise une clé aléatoire de 56 bits que l'expéditeur et le destinataire doivent connaître lors de l'échange de données

DB-25

Connecteur mâle à 25 broches pour raccordement aux modems externes ou à des dispositifs à interface série RS-232

DB-9

Connecteur à 9 broches pour les connexions RS-232

dBd

Décibels associés à une antenne dipole

dB_i

Décibels relatifs à une antenne isotrope

dB_m

Décibels relatives à un milliwatt

Débit binaire

Nombre de bits transférés en un temps donné.

Débit en bauds

Vitesse de transmission des données

Déchiffrer

Permet de décoder et remettre en texte en clair un message chiffré

Détection d'intrusion

Fonction de sécurité qui analyse le réseau en vue de détecter les attaques provenant de l'intérieur et de l'extérieur du réseau

DHCP

Dynamic Host Configuration Protocol : Protocole utilisé pour attribuer automatiquement à chaque ordinateur ou périphérique requérant une adresse IP à partir d'une réserve d'adresses prédéfinie

Diffusion

Transfert des données simultanément dans toutes les directions

DMZ

« Zone démilitarisée » DMZ. Ordinateur qui se situe logiquement dans une zone tampon entre le réseau local et le grand réseau. L'ordinateur de la zone DMZ assouplit le niveau de protection de certains mécanismes de sécurité du routeur pour que ce dernier soit directement accessible par Internet.

DNS

DNS (système de nom de domaine) : Traduit les noms de domaine en adresses IP

Données

Information convertie au format binaire pour en permettre le traitement ou le transfert vers un autre périphérique

DSL

Ligne de l'abonné numérique. Connexion Internet à large bande par lignes téléphoniques

Duplex

Envoi et réception de données simultanément

Duplex intégral

Envoi et réception de données simultanément

E**EAP**

Extensible Authentication Protocol (EAP)

Ethernet

Technologie la plus utilisée pour les réseaux locaux.

É**Étalement du spectre en séquence directe**

DSSS : Technique de modulation utilisée par les dispositifs sans fil 802,11b

Étape

Action des paquets de données acheminés d'un routeur à un autre

F**FAI**

Fournisseur d'accès Internet (FAI)

FAI sans fil

Société qui fournit une connexion Internet large bande via une connexion sans fil

Fibre optique

Technique d'envoi de données au moyen de légères impulsions sur du fil ou de la fibre de verre ou de plastique

Fonction Wake on LAN

Permet de mettre un ordinateur sous tension au moyen de sa carte réseau

Fournisseur d'accès Internet (FAI)

Un FAI fournit l'accès à Internet aux utilisateurs et aux entreprises

Fragmentation

Division des données en segments plus petits pour faciliter le stockage

FTP

File Transfer Protocol, ou protocole de transfert de fichier. Façon la plus aisée de transférer des fichiers entre des ordinateurs sur Internet

G**Gain**

Capacité d'amplification du signal sans fil par un amplificateur

Gbps

Gigabits par seconde

Gigabit Ethernet

Technologie de transmission qui fournit un débit de 1 milliard de bits/seconde

Goulot d'étranglement

Moment dans les processus où quelque chose entraîne un ralentissement ou un arrêt total

Grand réseau

Réseau le plus vaste auquel votre réseau local est connecté. Il peut d'agir d'Internet ou d'un réseau régional ou d'entreprise.

H**H.323**

Norme qui assure la cohérence des transmissions voix et vidéo et la compatibilité des dispositifs de videoconference

Hachage

Transformation d'une chaîne de caractères en chaîne plus courte d'une longueur prédéfinie.

Hexadécimal

Caractères 0-9 et A-F

Hôte

Ordinateur sur un réseau

HTTP

Le protocole de transfert hypertexte est utilisé pour transférer des fichiers des serveurs HTTP (serveurs Web) aux clients HTTP (navigateurs Web)

HTTPS

Le protocole HTTP over SSL est utilisé pour chiffrer et déchiffrer les transmissions HTTP

I**ICMP**

ICMP (Internet Control Message Protocol)

IEEE

Institute of Electrical and Electronics Engineers

IIS

IIS (Internet Information Server) est un serveur Web et FTP fourni par Microsoft

IKE

Le protocole Internet Key Exchange sert à assurer la sécurité des connexions RPV.

Infrastructure

Dans un réseau sans fil, moment où les clients sans fil utilisent un point d'accès pour accéder au réseau.

Inspection dynamique

Fonction du pare-feu servant à surveiller le trafic entrant et sortant pour s'assurer que seules les réponses valides aux requêtes sortantes sont autorisées à traverser ce pare-feu

Interface graphique

Interface utilisateur graphique

Internet

Un système de réseaux à l'échelle de la planète qui utilise le protocole TCP/IP pour permettre aux ordinateurs du monde entier d'accéder aux ressources.

Internet Explorer

Navigateur World Wide Web créé et fourni par Microsoft

Internet Protocol (IP)

Méthode de transfert des données d'un ordinateur vers un autre sur Internet

Internet Protocol Security (IPSec)

Le protocole IPsec assure la sécurité au niveau de la couche de traitement des paquets de données de communication réseau

Intranet

Réseau privé

IP

Internet Protocol (IP)

IPsec

Internet Protocol Security (IPSec)

IPX

Internetwork Packet Exchange est un protocole de réseau développé par Novell pour permettre la communication entre leurs clients et serveurs Netware.

J**Java**

Langage de programmation servant à créer des programmes et des applets pour les pages Web

K**Kbit/s**

Kilo-bits par seconde

Kilo-octet

kilo-octet

L**L'authentification**

Permet de fournir des attestations d'identité, comme un mot de passe, en vue de vérifier l'authenticité de la personne ou du périphérique requérant.

Largeur de bande

Nombre maximum d'octets ou de bits par seconde pouvant être transmis vers un périphérique réseau et en sortir

Liste de contrôle des accès

ACL. Il s'agit d'une base de données des périphériques réseau autorisés à accéder aux ressources du réseau.

M**Masque de réseau**

Détermine la partie d'une adresse IP qui désigne le réseau et celle qui désigne l'hôte

Masque de sous-réseau

Détermine la partie d'une adresse IP qui désigne le réseau et celle qui désigne l'hôte

Mbps

Mégabits par seconde

MDI

MDI (Medium Dependent Interface, ou interface dépendante du médium), est un port Ethernet pour une connexion à un câble direct

MDIX

Un port MAU (Medium Dependent Interface Crossover) est un port Ethernet qui assure la connexion à un câble de liaison croisée.

MIB

Management Information Base (base d'information pour la gestion de réseau ou MIB) est un ensemble d'objets pouvant être géré par le biais de SNMP

Microprogramme

Programme informatique inséré dans un périphérique matériel pour lui indiquer comment fonctionner

Mise à niveau

Pour installer une version plus récente d'un logiciel ou d'un progiciel

Modem

Dispositif qui module les signaux numériques en provenance d'un ordinateur en signaux analogiques pouvant être transmis par les lignes téléphoniques. L'appareil démodule également les signaux analogiques des lignes téléphoniques en signaux numériques destinés à votre ordinateur.

Modem câble

Dispositif vous permettant de connecter un ordinateur à un câble coaxial et de recevoir un accès Internet de votre fournisseur de services câbles

Mot de passe

Séquence de caractères servant à authentifier les requêtes vers les ressources d'un réseau

MTU

L'unité de transmission maximale (MTU) est le paquet le plus volumineux pouvant être transmis sur un réseau à base de paquets tel qu'Internet

Multidiffusion

Envoi de données d'un périphérique vers plusieurs périphériques d'un réseau

N

NAT

La fonction Network Address Translation (NAT) permet la connexion de nombreuses adresses IP privées à Internet, ou à un autre réseau, par le biais d'une seule adresse IP.

Navigateur

Programme qui vous permet d'accéder à des ressources sur Internet et qui vous les fournit sous forme graphique

Navigateur Web

Utilitaire qui vous permet de visualiser le contenu et d'interagir avec toutes les informations du Web

NetBEUI

Le protocole NetBEUI est un protocole de communication de réseau local. Il s'agit d'une version améliorée du protocole NetBIOS.

NetBIOS

Système E/S de base du réseau

Network Time Protocol (protocole horaire de réseau)

Permet de synchroniser l'heure de tous les ordinateurs d'un réseau

Nom du domaine

Nom qui est associé à une adresse IP

Norme de chiffrement AES

AES. Norme de chiffrement gouvernementale

NTP

Network Time Protocol (protocole horaire de réseau)

O

OFDM

Le multiplexage par répartition orthogonale de la fréquence est une technique de modulation pour les normes 802.11a et 802.11g

OSI

Le modèle d'interconnexion de systèmes OSI est le modèle de référence qui définit la façon dont les données doivent transiter sur un réseau entre deux périphériques.

P

Par défaut

Valeur ou paramètre prédéterminé qui est utilisé par un programme lorsque aucune donnée n'a été entrée par l'utilisateur pour cette valeur ou ce paramètre

Pare-feu

Dispositif qui protège les ressources du réseau local de l'accès non autorisé des utilisateurs extérieurs au réseau

Partage de fichier

Permet aux ordinateurs d'un réseau d'accéder aux données résidant sur d'autres ordinateurs avec des niveaux de droits d'accès différents.

Passerelle

Dispositif qui connecte votre réseau à un autre, comme Internet

Personal Area Network (PAN)

Interconnexion des dispositifs de réseautage dans un rayon de 10 mètres

Ping

Utilitaire qui vérifie qu'une adresse Internet donnée existe et peut recevoir des messages. Ce programme envoie un paquet de contrôle à l'adresse visée et attend la réponse.

PoE

Power over Ethernet (PoE) est la norme utilisée pour transmettre le courant électrique sur les paires inutilisées d'un câble Ethernet catégorie 5

Point d'accès

AP. Dispositif qui permet aux clients sans fil de s'y connecter pour avoir accès au réseau.

POP3

Post Office Protocol version 3 est utilisé pour la réception des courriels

Port

Point d'extrémité de canal logique dans un réseau. Un ordinateur pourrait n'avoir qu'un seul canal physique (son canal Ethernet) mais disposer de plusieurs ports (canaux logiques) identifiés au moyen d'un numéro.

PPP

Le protocole Point à Point (PPP) permet à deux ordinateurs de communiquer entre eux par le biais d'une interface série, comme une ligne téléphonique

PPPoE

Le protocole PPPoE (Point-to-Point Protocol over Ethernet) est utilisé pour connecter plusieurs ordinateurs à un serveur distant via Ethernet.

PPTP

La fonction Point-to-Point Tunneling Protocol (PPTP) permet de créer des tunnels RPV sur Internet entre deux réseaux

Préambule

Permet de synchroniser les communications entre les périphériques d'un réseau

Protocole ARP (Address Resolution Protocol)

ARP. Utilisée pour mapper les adresses MAC aux adresses IP afin de permettre les conversions dans les deux sens.

Protocole de résolution d'adresses AppleTalk (AARP)

AARP. Utilisé pour mapper les adresses MAC des ordinateurs Apple à leurs adresses de réseau AppleTalk, afin de permettre les conversations bidirectionnelles.

Protocole IGMP

Le protocole Internet Group Management permet de s'assurer que les ordinateurs génèrent un rapport sur les membres du groupe multidiffusion pour les routeurs adjacents.

Protocole L2TP

Layer 2 Tunneling Protocol (protocole de tunnel de niveau 2)

Protocole OSPF

Le protocole OSPF (Open Shortest Path First) est un protocole d'acheminement des données qui est davantage utilisé que le protocole RIP dans les réseaux plus vastes, car seuls les changements de la table d'acheminement sont acheminés à l'ensemble des autres routeurs sur le réseau, tandis qu'avec le protocole RPI, toutes les données de la table d'acheminement sont envoyées à intervalles réguliers.

Protocole LPR/LPD

"Demandeur d'imprimante par ligne"/"Démon d'imprimante par ligne". Protocole TCP/IP de transmission de flux de données d'imprimante.

Q**QoS**

Qualité de Service

R

RADIUS

Le service RADIUS (Remote Authentication Dial-In User Service, ou service d'authentification d'utilisateur distant) permet aux utilisateurs distants de se connecter à un serveur central et d'être authentifiés afin de pouvoir accéder aux ressources d'un réseau.

Réinitialiser

Pour redémarrer un ordinateur et recharger son logiciel d'exploitation ou progiciel à partir d'une mémoire de stockage rémanente.

Rendez-vous

Version Apple du protocole UPnP, qui permet aux dispositifs d'un réseau de se découvrir les uns les autres et d'être connectés sans devoir configurer de paramètres.

Répétiteur

Retransmet le signal d'un point d'accès afin d'en étendre la couverture

Réseau ad-hoc

Réseau égal à égal entre clients sans fil

Réseau local

Réseau local

Réseau local

Groupe d'ordinateurs dans un édifice, qui ont accès aux fichiers par le biais d'un serveur

Réseau privé virtuel

RPV : Réseau privé virtuel. Un tunnel sécurisé sur Internet permettant de connecter des bureaux ou des utilisateurs éloignés au réseau de leur entreprise

Réseau sans fil

Réseau local sans fil (WLAN)

Réseau sans fil (Wi-Fi)

Connexion au réseau local par le biais de l'une des normes sans fil 802.11

Rétro-compatible

Possibilité pour les nouveaux périphériques de communiquer et d'interagir avec des périphériques moins récents afin de garantir l'interopérabilité

RIP

Le Routing Information Protocol (RIP) permet de synchroniser la table de routage de tous les routeurs d'un réseau.

RJ-11

Méthode de connexion la plus courante pour les téléphones

RJ-45

Méthode de connexion la plus couramment utilisée pour Ethernet.

RS-232C

Interface pour la communication série entre des ordinateurs et d'autres périphériques associés

RSA

Algorithme utilisé pour le chiffrement et l'authentification

S**Sans fil (Wi-Fi)**

Wireless Fidelity (Wi-Fi)

Semi-duplex

Des données ne peuvent pas être transmises et reçues simultanément

Serveur

Ordinateur connecté au réseau qui fournit des services et des ressources à d'autres ordinateurs également sur le réseau

Serveur de fichier

Ordinateur d'un réseau qui stocke des données pour que les autres ordinateurs du réseau puissent y accéder.

Service DNS dynamique

Le DNS dynamique est fourni par les entreprises pour permettre aux utilisateurs dont les adresses IP sont dynamiques d'obtenir un nom de domaine invariable. L'adresse IP est actualisée par un logiciel client sur un ordinateur ou par un routeur qui prend en charge le DNS dynamique dès le changement d'une adresse IP.

Simple Mail Transfer Protocol (protocole simple de transfert de courrier)

Permet d'envoyer et de recevoir du courriel

Simple Network Management Protocol (SNMP)

Assure la gestion et la surveillance des périphériques réseau

SIP

Protocole d'ouverture de session SIP. Protocole standard qui permet d'ouvrir des sessions avec du contenu multimédia, comme de la voix ou du clavardage.

SMTP

Simple Mail Transfer Protocol (protocole simple de transfert de courrier)

SNMP

Simple Network Management Protocol (SNMP)

SOHO

Petite entreprise/Bureau à domicile

SPI

Stateful Packet Inspection (SPI)

SSH

Secure Shell est une interface de ligne de commande qui permet de sécuriser les connexions à des ordinateurs distants

SSID

L'identificateur de jeu de services (SSID) est un nom de réseau sans fil

Syslog

System Logger (consigneur système) -- interface de consignation qui collecte dans un seul emplacement les journaux des différentes sources. À l'origine créé pour UNIX, il est maintenant disponible pour d'autres systèmes d'exploitation, y compris Windows.

Système de base Entrée/Sortie

BIOS. Programme utilisé par un ordinateur pour démarrer le système lors de sa mise sous tension

Système de distribution sans fil (WDS)

Système de distribution sans fil (WDS). Système qui permet l'interconnexion sans fil de points d'accès.

T**TCP**

Transmission Control Protocol (protocole de contrôle de transmission)

TCP brut

Un protocole TCP/IP pour la transmission des flux de données d'impression.

TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP)

Technologie UPnP (Universal Plug and Play)

Norme permettant à des périphériques de réseau de se découvrir mutuellement et de se configurer en vue de devenir un élément du réseau

Télécharger

Pour envoyer une demande d'un ordinateur vers un autre et pour que le fichier soit retransmis à l'ordinateur qui a envoyé la demande

Temps d'attente

Temps mis par un paquet pour transiter d'un point à un autre d'un réseau. Appelé également délai

TFTP

L'utilitaire de transfert de fichier TFTP (Trivial File Transfer Protocol) est plus simple à utiliser que FTP, bien qu'il offre moins de fonctionnalités.

Traceroute

Un utilitaire affiche les chemins entre votre ordinateur et une destination précise

Transférer

Pour envoyer une requête d'un ordinateur à un autre et avoir un fichier transmis de l'ordinateur requérant à l'autre

U**UDP**

User Datagram Protocol (UDP)

Unicast

Communication entre un expéditeur et un destinataire

UPnP

Technologie UPnP (Universal Plug and Play)

URL

L'Uniform Resource Locator (URL ou localisateur de ressources universel) est une adresse unique pour les fichiers accessibles sur le Net

USB

Bus série universel (USB)

UTP

Paire torsadée non blindée

V**VLAN**

Réseau local virtuel

VoIP

Voix sur IP

Voix sur IP

Envoi des données vocales sur Internet, et non sur le réseau PSTN

Voyant

Diode électroluminescente

W**WAN**

Grand réseau

WCN

Fonctionnalité Windows Connect Now. Technologie de Microsoft pour la configuration et l'amorçage de matériel réseau sans fil (points d'accès) et de client sans fil, y compris des ordinateurs et d'autres périphériques.

WEP

Le protocole Wired Equivalent Privacy (WEP) assure aux réseaux sans fil une sécurité supposément comparable à celle d'un réseau câblé.

WISP

Fournisseur de services Internet sans fil

WPA

Wi-Fi Protected Access (accès protégé Wi-Fi). Programme améliorant la sécurité Wi-Fi en fournissant un algorithme de chiffrement des données plus efficace comparativement au WEP.

X**xDSL**

Terme générique désignant un ensemble de technologies de ligne d'abonné numérique (DSL) telles que LNPA ou ADSL, HDSL, RADSL et SDSL.

Z**Zone démilitarisée**

DMZ : Ordinateur unique ou groupe d'ordinateurs auquel ont accès les utilisateurs sur Internet et les utilisateurs sur le réseau local, mais qui n'est pas protégé par le même protocole de sécurité que le réseau local.