MANUEL DE RÉFÉRENCE DES POINTS D'ACCÈS/BRIDGES 802.11 a/b/g

ACKSYS
COMMUNICATIONS & SYSTEMS

SOMMAIRE

I INTRODUCTION

Ce manuel de référence est commun à l'ensemble de la gamme des points d'accès Wi-Fi suivants :

- WLg-LINK
- WLg-LINK-OEM-RJ
- WLg-LINK-OEM-TTL
- WLg-LINK-OEM-EVAL
- WLg-ABOARD/N
- WLg-ABOARD/NP
- WLg-ACCESS-ATEX
- WLg-IDA/N
- WLg-SWITCH
- WLg-XROAD/N
- WLg-XROAD/NP

Il apporte une aide à l'installation de votre produit en complément de l'aide en ligne (Menu HELP de l'administration WEB) et du guide d'installation rapide fourni avec votre produit.

Ce manuel documente la dernière version du firmware équipant les points d'accès ACKSYS précédemment cités. Si le firmware installé dans votre produit n'est pas à jour, veuillez vous reporter au changelog disponible sur le site web d'ACKSYS (http://www.acksys.fr/) afin de déterminer les fonctionnalités dont vous disposez.

Toutes les recommandations d'installation liées au matériel, telles que les alimentations, les antennes, les branchements des câbles sont documentés dans le manuel hardware.

Recommandations importantes

Attention, l'exploitation d'un matériel Wi-Fi est soumise à la législation du pays où il est installé, législation que vous devez connaître et respecter. En quelques mots, cette législation spécifie les fréquences d'émission radio ainsi que les puissances d'émission radio qui sont autorisées suivant le milieu intérieur ou extérieur.

Dans tous les cas où cette législation ne serait pas respectée et ceci pour n'importe quelle raison, ACKSYS se désengage de toute responsabilité.

Attention, les informations liées à la législation écrites dans ce document ne sont données qu'à titre indicatif et ne sauraient engager ACKSYS si elles devenaient incomplètes ou même fausses suite à des évolutions.

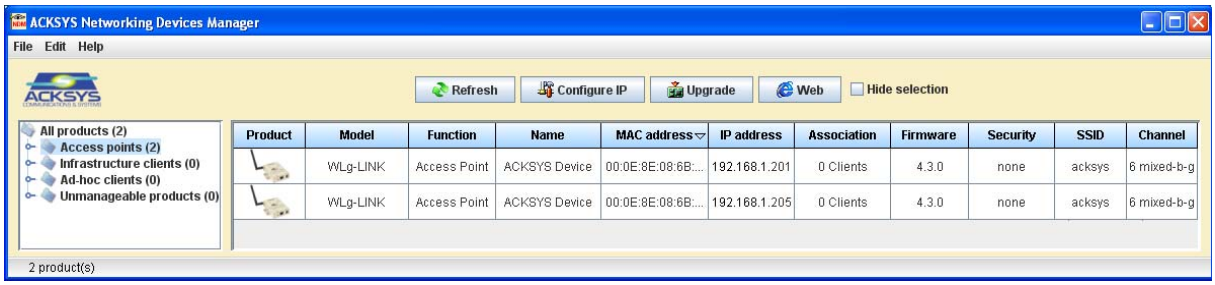
II L'INSTALLATION DU PRODUIT SUR LE RÉSEAU

Cette première partie est traitée dans le manuel hardware spécifique à chaque produit. Nous vous invitons donc à commencer la lecture de ce manuel en suivant méthodiquement toutes les recommandations qui y sont données.

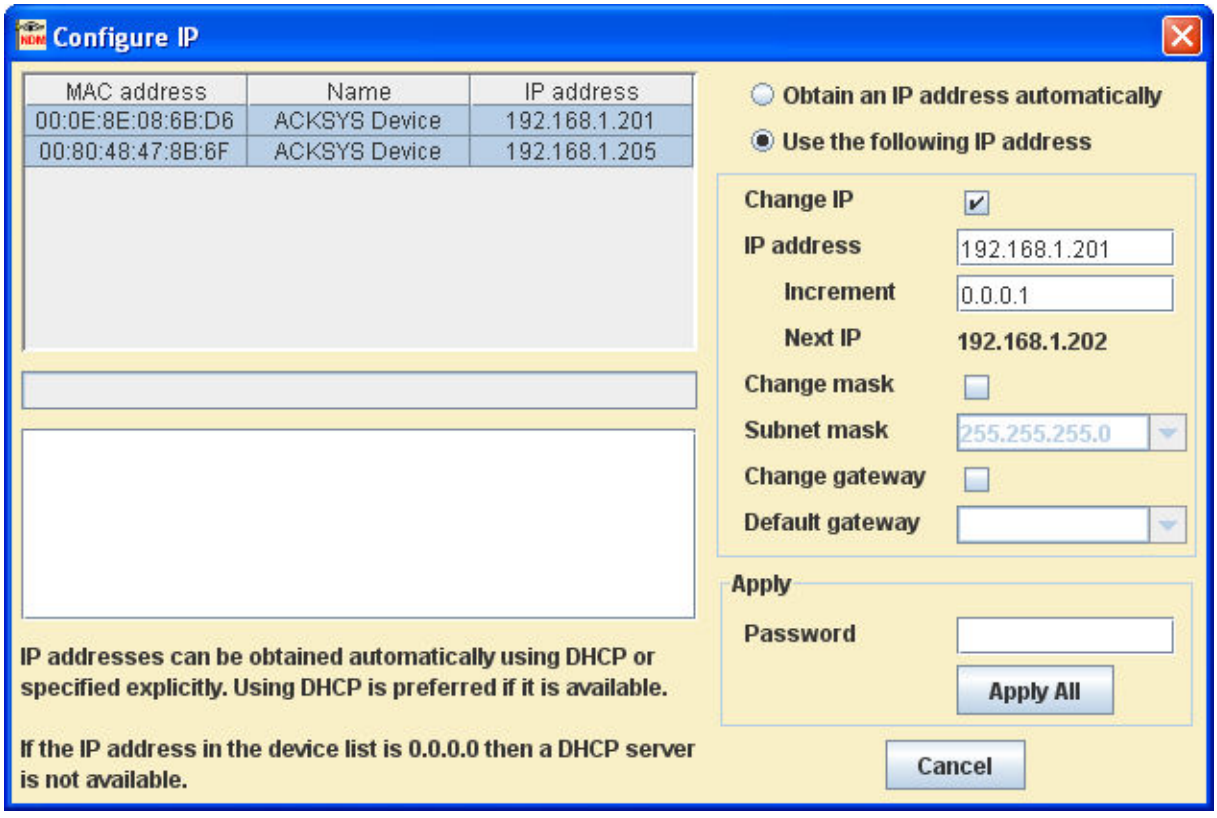
III CONFIGURATION D'UNE NOUVELLE ADRESSE IP

Une fois le produit raccordé physiquement à votre réseau local, il convient de lui affecter une adresse IP compatible avec ce réseau sauf si l'adresse IP par défaut (voir paragraphe « Les paramètres par défaut ») l'est déjà.

Pour modifier l'adresse IP de votre produit, vous devez utiliser l'application ACKSYS NDM que vous trouverez sur le CD-ROM livré avec le produit.
Depuis un P.C du réseau, exécutez cette application. La liste des produits détectés doit apparaître.



L'application détecte tous les produits ACKSYS de type points d'accès/bridge présents sur le réseau local, sélectionnez le ou les produits à configurer et cliquez sur le bouton « Configure IP».



Si vous n'avez sélectionné qu'un seul produit avant de cliquer sur le bouton « Configure IP », Il ne vous reste plus qu'à attribuer les paramètres IP (adresse IP, masque de sous réseau et adresse IP de la passerelle) de ce produit, soit de façon manuelle ou automatique (Les paramètres IP seront alors affectés au produit selon le protocole DHCP). Cliquez ensuite sur le bouton « Apply ».

Si vous avez sélectionné plusieurs produits avant de cliquer sur le bouton « Configure IP », alors ils doivent apparaître dans la fenêtre de configuration.

- Si vous souhaitez attribuer manuellement à chaque équipement ses paramètres IP (adresse IP, masque de sous réseau et adresse IP de la passerelle), cliquez sur le produit à configurer et cliquez ensuite sur le bouton « Apply ».
- Si vous souhaitez configurer plusieurs produits en même temps, alors sélectionnez l'ensemble des produits à configurer puis choisissez votre configuration en vous servant de l'incrément, ou en utilisant la configuration automatique par DHCP et cliquez ensuite sur le bouton « Apply All ». Les paramètres IP de tous les produits seront alors mis à jour.

Une fois que le produit à une adresse IP compatible avec votre réseau, vous pouvez accéder au serveur Web embarqué dans le produit pour commencer sa configuration.

Note : l'utilisation de la configuration automatique par DHCP, nécessite la présence d'un serveur DHCP sur votre réseau local.

IV L'ADMINISTRATION PAR HTTP

Une fois votre produit configuré avec une adresse IP compatible avec votre réseau local, vous pouvez accéder au serveur web du produit en cliquant simplement sur le bouton « Web » ou encore en lançant directement votre naviguateur Internet. Une page d'accueil d'authentification vous demande le « username » et le mot de passe. Le username par défaut est « admin » et il n'y a pas de mot de passe.

Pour aller plus loin et commencer le paramétrage du produit, vous devez maintenant déterminer :

- Le mode de fonctionnement du réseau Wi-Fi :
  - Le mode infrastructure
  - Le mode ad-hoc
- Le type de réseau Wi-Fi : 802.11a, 802.11b, 802.11g, 802.11b/g
- Le SSID du réseau Wi-Fi
- Le canal (ou fréquence) du réseau Wi-Fi
- La sécurité à mettre en œuvre (WEP, WPA, WPA2, 802.1x, filtrage MAC)
- Le mode de fonctionnement du produit, selon les 3 possibilités suivantes :
  - **bridge infra** ou **point d'accès** pour un réseau en mode infrastructure
  - **bridge ad-hoc** pour un réseau en mode ad-hoc

IV.1 Les menus de paramétrage

Une fois ces paramètres connus, vous pouvez alors naviguer dans les 5 menus suivants et commencer le paramétrage :

- Le menu *BASIC* :
  - Sous-menu *WIZARD*[1] : assistant de configuration
  - Sous-menu *LAN* : configuration paramètres LAN
  - Sous-menu *DHCP*[1] : configuration du serveur DHCP
  - Sous-menu *WIRELESS* : configuration des paramètres Wi-Fi
  - Sous-menu *NAT*[2] : configuration du mode NAT
  - Sous-menu *SNMP* : configuration de l'agent SNMP
  - Sous-menu *TFTP* : configuration du serveur TFTP
  - Sous-menu *ALARM*[3] : configuration des alarmes

- Le menu *ADVANCED* :
  - Sous-menu *MAC ADDRESS FILTER* : configuration du filtre MAC pour le mode point d'accès
  - Sous-menu *ADVANCED ETHERNET* : configuration du lien Ethernet
  - Sous-menu *ADVANCED WIRELESS* : paramètres avancés du Wi-Fi
  - Sous-menu *C-KEY*[3]: gestion du C-KEY

- Le menu TOOLS :
  - Sous-menu *ADMIN* : configuration des mots de passe utilisateur et administrateur, sauvegarde et restauration de tous les paramètres de configuration dans un fichier
  - Sous-menu *TIME* : gestion de l'heure
  - Sous-menu *SYSTEM* : restauration des paramètres usine et redémarrage du produit
  - Sous-menu *FIRMWARE* : téléchargement d'une nouvelle version du firmware, lecture de la version courante

- Le menu STATUS :
  - Sous-menu *DEVICE INFO* : informations sur le produit : adresse IP, canal radio, mode, SSID
  - Sous-menu *WIRELESS* : liste des clients Wi-Fi connectés, des points d'accès détectés…
  - Sous-menu ETHERNET : état des liens Ethernet
  - Sous-menu *LOGS* : liste des évènements survenus
  - Sous-menu *STATISTICS* : compteurs des trames transférés
  - Sous-menu ALARM[3] : état des alarmes configurées

- Le menu HELP :
  - Sous-menu MENU : description de tous les menus
  - Sous-menu BASIC, ADVANCED, TOOLS, STATUS : aide du menu correspondant
  - Sous-menu GLOSSARY : glossaire des termes utilisés

[1] Menu disponible uniquement en mode Access Point
[2] Menu disponible uniquement en mode Bridge
[3] Menu disponible uniquement sur : WLg-SWITCH, WLg-IDA/N, WLg-IDA/NP

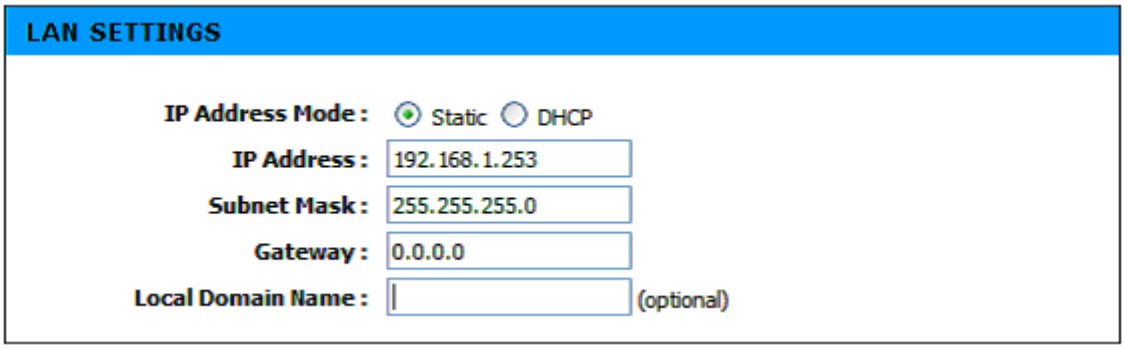
Attention, certaines fonctionnalités sont spécifiques au mode Bridge ou ACCESS POINT, dès lors les menus correspondants apparaîtront ou pas suivant le mode.
Par exemple, les menus « BASIC→DHCP ».

IV.2 Le menu HELP

Ce menu fournit une explication sur l'ensemble des paramètres de chacun des menus plus un glossaire détaillé.

IV.3 Le menu LAN

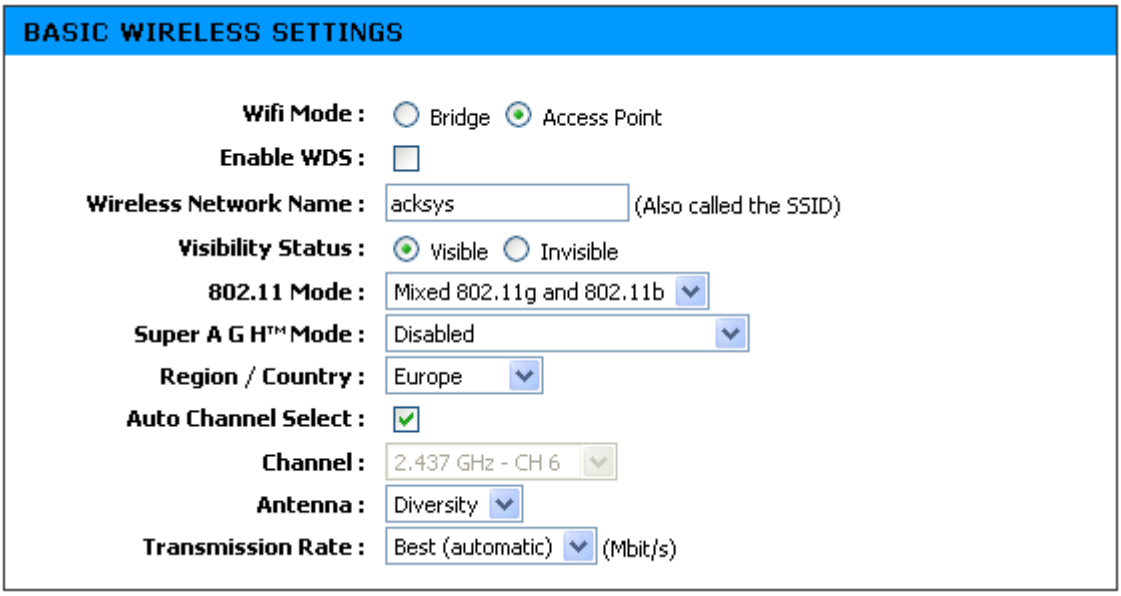
Ce menu permet de définir les paramètres du produit côté réseau filaire.



Le mode d'adressage IP peut être statique (L'adresse IP est alors fournie explicitement par l'utilisateur) ou dynamique (L'adresse IP est alors négociée entre le module DHCP client du produit et un serveur DHCP du réseau).

Tous les champs de ce menu sont clairement documentés dans le menu HELP.

IV.4 Le menu WIRELESS

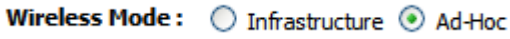


IV.4.1 Le mode bridge ou Access Point

Le mode par défaut du produit est le mode « ACCESS POINT ». Si vous souhaitez basculer en mode « BRIDGE », il convient d'activer le mode « BRIDGE » à l'aide du radio bouton Wi-Fi mode.

Le produit va alors immédiatement se réinitialiser et lors du prochain accès au serveur web de configuration, nous noterez que la bannière en haut de page a été changée et que le mot BRIDGE apparaît en lieu et place du mot « ACCESS POINT ». Les autres paramètres peuvent alors être modifiés.

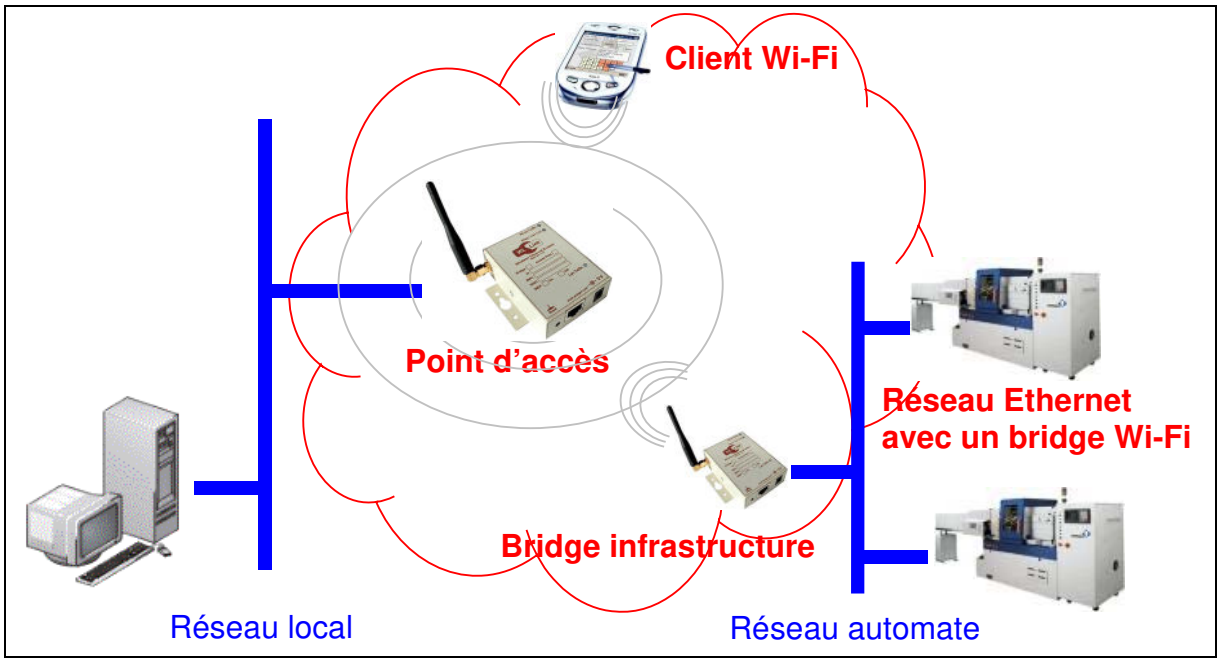
Une fois en mode bridge, le nouveau paramètre « Wireless Mode » est affiché.



IV.4.1.1 Le mode infrastructure

Dans un tel réseau, nous retrouvons 2 types d'équipements :

- Le point d'accès
- Les clients Wi-Fi qui viennent se connecter au point d'accès (Jusqu'à 20 avec le point d'accès ACKSYS). Il peut s'agir de clients Wi-Fi avec interface Wi-Fi intégrée ou encore tout autre dispositif utilisant une interface Wi-Fi en mode bridge.



Le point d'accès crée une cellule Wi-Fi (définie par un nom de réseau et une fréquence/canal radio) à laquelle tous les clients configurés en mode infrastructure viendront se connecter.

Le produit ACKSYS remplir les fonctions de :

- **Point d'accès, le bouton radio « Wi-Fi mode » doit être sur ACCESS POINT.**
- **Bridge, le bouton radio « Wi-Fi mode » doit être sur BRIDGE et le bouton « Wireless mode » doit etre sur infrastructure.**

Le mode Infrastructure est un mode de fonctionnement qui permet de connecter les équipements dotés d'une interface Wi-Fi entre eux via un ou plusieurs points d'accès (AP) qui agissent comme des concentrateurs (exemple : Hub/Switch en réseau filaire). Ce mode est essentiellement utilisé en entreprise. La mise en place d'un tel réseau oblige de poser à intervalle régulier des bornes (AP) dans la zone qui doit être couverte par le réseau. Les bornes, ainsi que les machines, doivent être configurées avec le même SSID (voir paragraphe « Le SSID ») afin de pouvoir communiquer. L'avantage de ce mode est de garantir un passage obligé par l'AP. Il est donc possible de vérifier qui entre sur le réseau. En revanche, le réseau ne peut pas s'agrandir, hormis en posant de nouvelles bornes.
Au travers de la fonction WDS (voir paragraphe « Le mode WDS »), Il est possible d'augmenter la zone de couverture d'un réseau Wi-Fi au chaînant plusieurs points d'accès.

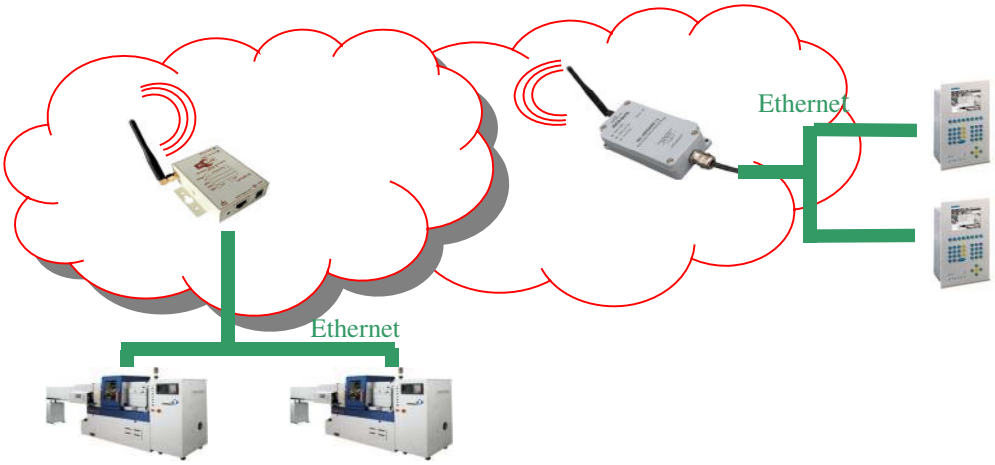
IV.4.1.2 Le mode ad-hoc

Dans un tel réseau, et contrairement au mode infrastructure, nous retrouvons un seul type d'équipement. Autrement dit, il n'y a pas de points d'accès. Evidemment ce mode n'a de sens que si le produit est paramétré en mode bridge.

Le mode « Ad-Hoc » est un mode de fonctionnement qui permet de connecter directement les ordinateurs équipés d'une carte réseau Wi-Fi, sans utiliser un matériel tiers tel qu'un Point d'accès (Access Point [AP]). Ce mode est idéal pour interconnecter rapidement des machines entre elles sans matériel supplémentaire. La mise en place d'un tel réseau se borne à configurer les machines en mode Ad-Hoc, la sélection d'un canal (fréquence radio) et d'un SSID (nom de réseau) communs à tous. L'avantage de ce mode est qu'il est plus facile à mettre en œuvre.
Chaque équipement configuré en mode ad-hoc va créer sa propre cellule Wi-Fi. Pour que la communication puisse avoir lieu entre 2 équipements ou plus, il faut obligatoirement que les cellules des équipements voulant communiquer **se superposent**.
Si deux équipements du réseau sont hors de portée l'un de l'autre, ils ne pourront pas communiquer, même s'ils "voient" d'autres équipements. En effet, contrairement au mode infrastructure, le mode ad-hoc ne propose pas de système de distribution capable de transmettre les trames d'une station à une autre.

Pour que votre réseau ad-hoc fonctionne correctement, tous les équipements Wi-Fi configurés en mode ad-hoc doivent utiliser le même SSID et le même canal.
Le mode ad-hoc ne fonctionne qu'en 802.11b, avec ou sans clé WEP (comprenez sans WPA ni WPA2)

Toutes les cellules partagent le même canal et le même SSID. Elles doivent toutes se superposer. Aucun des équipements ne peut jouer le rôle de « routeur » pour aider un équipement à dialoguer avec un autre.

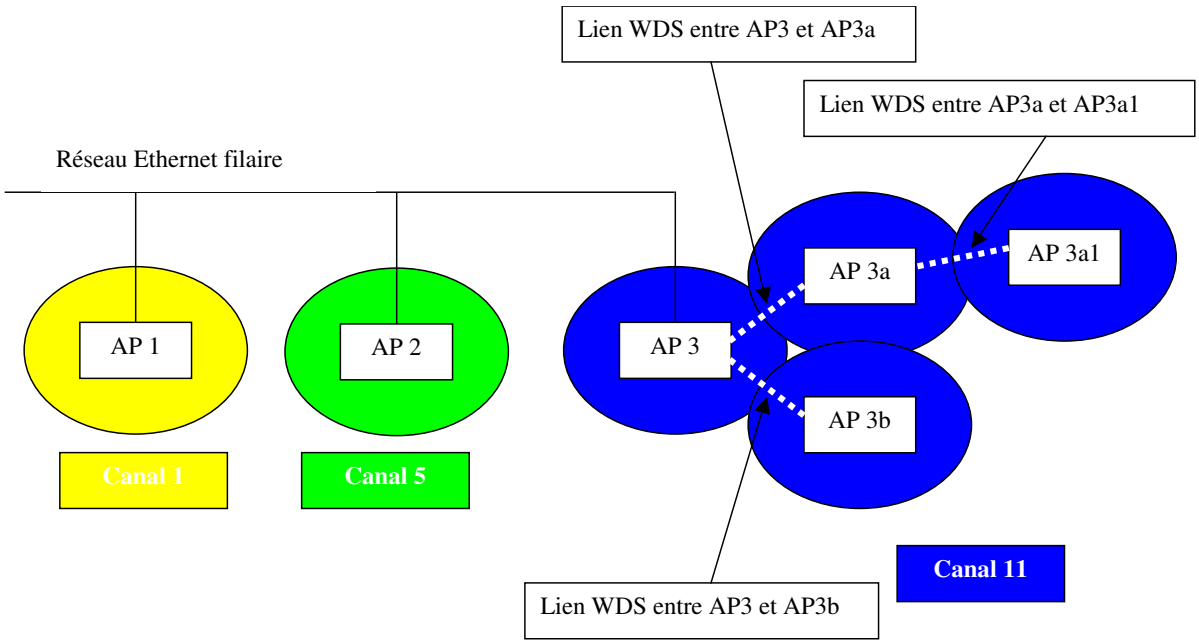


IV.4.2 Le mode WDS

Dans le cas où certaines stations seraient trop éloignées d'un point d'accès, et que le réseau filaire n'est plus accessible, il devient nécessaire d'augmenter la portée de la cellule Wi-Fi de ce point d'accès. Dans ce cas, on peut ajouter au réseau Wi-Fi un ou plusieurs répéteurs chargés d'amplifier le signal Wi-Fi, ces répéteurs étant interconnectés entre eux sans aucun câble. Cette fonctionnalité est intégrée dans notre produit au travers du mode WDS de la norme 802.11. Les répéteurs peuvent être chaînés les uns aux autres (on parle alors de topologie « chaînée ») ou ils peuvent être raccordés à un point d'accès central (on parle alors de topologie en étoile)

Le synoptique ci-dessous illustre un mixte des 2 topologies avec 3 répéteurs ajoutés pour augmenter la portée de la cellule du point d'accès AP3.

Tous les répéteurs doivent être sur le même canal radio (11 par exemple).
Chacun de ces répéteurs réalise aussi la fonction de base de point d'accès.

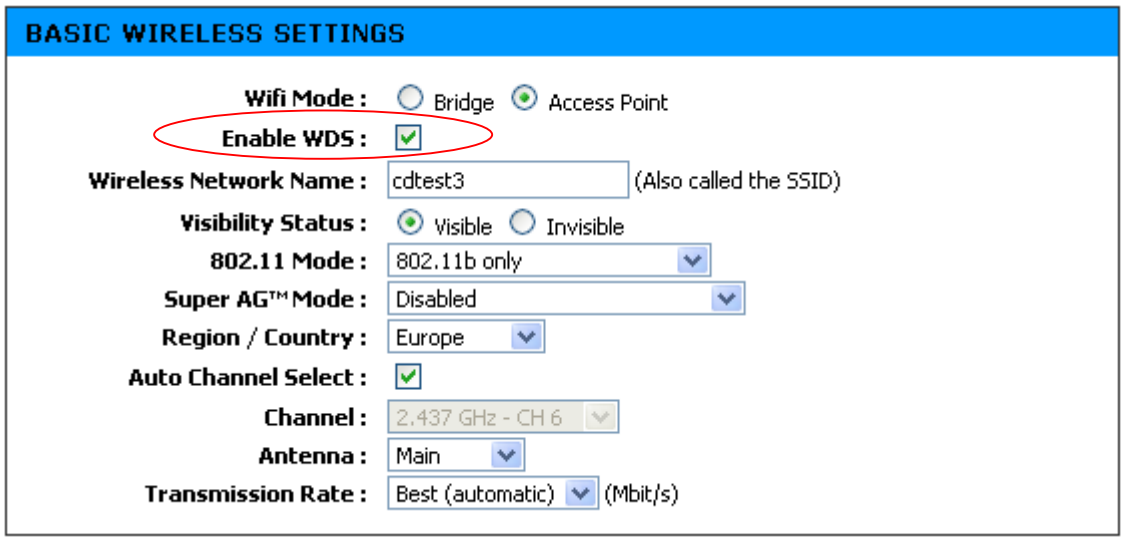


Cette illustration montre la création de 3 liens WDS dont 2 uniquement avec l'AP3. L'AP3 doit donc connaître l'adresse MAC des points d'accès AP3a et AP3b et réciproquement.
L'AP3a doit connaître l'adresse MAC de l'AP3a1 et réciproquement.

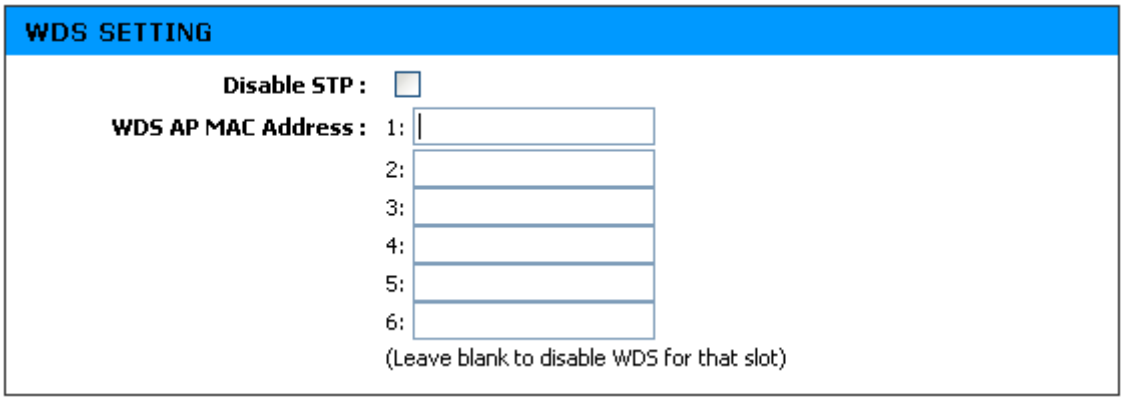
Il faut aussi noter que la liaison entre AP3a et AP3b ne doit pas être établie car une boucle sur le réseau serait créée. Par défaut, le produit intègre une implémentation du protocole STP qui évite les boucles réseau en supprimant les liaisons qui posent problème.

Le point d'accès ACKSYS est capable de gérer jusqu'à 6 liens WDS, autrement dit-il peut mémoriser 6 adresses MAC différentes.

IV.4.2.1 Le menu WDS



La figure ci-dessus présente la case à cocher « Enable WDS » qui permet d'activer la fonctionnalité WDS du produit. Le fait de cocher cette case fait apparaître le menu suivant :



Champ « Disable STP » : Cette option, si elle est cochée, permet de ne pas mettre en œuvre le protocole STP.

ATTENTION : si cette option est cochée, il est impératif de créer des liaisons entre les différents points d'accès de manière à ne pas créer de boucles sur le réseau.

Champs « WDS AP MAC Address » : Les six paramètres suivants permettent de définir quels seront les points d'accès « visibles » par le produit. Il suffit de rentrer les adresses MAC des points d'accès avec lesquels nous devons être en contact. Pour reprendre le schéma de la page précédente, AP3 devra entrer les adresses MAC de AP3a et de AP3b.

IV.4.3 Le SSID

Un SSID (Service Set Identifier) est un nom composé de chiffres et/ou de lettres uniques qui permet d'identifier un WLAN, garantissant ainsi que les périphériques sans fil se connectent au WLAN approprié lorsque plusieurs WLAN fonctionnent les uns près des autres. Le même SSID, est configuré sur tous les équipements sans fil et les points d'accès du réseau. Il définit un réseau logique (le réseau physique étant défini par le canal).

Diffusion du SSID

Par défaut, ce nom de réseau est émis en clair sur le réseau dans des trames dites « de balise » de façon à aider la configuration des clients sans fil qui souhaiteraient s'y raccorder.

Il est en revanche possible de désactiver cette fonction (bouton radio « visibility status » sur « Invisible »). Ne pensez pas pour autant que ce SSID soit définitivement caché et que votre réseau est donc protégé !

Remarque : Si vous paramétrez votre SSID sur le point d'accès en « invisible », alors le client qui ne connaît pas le SSID ne pourra se connecter au point d'accès.

De notre point de vue le SSID est un élément de sécurité mais pas suffisant pour sécuriser votre réseau. C'est pourquoi il est conseillé d'utiliser la sécurité par clé WEP ou WPA/WPA2.

IV.4.4 Le mode 802.11

Le produit peut être installé dans l'un des 3 types de réseaux sans fil suivants :

- 802.11b :

Bande de Fréquence	Bande passante (Typique)	Vitesse de transmission (max)	Portée (intérieur)	Portée (extérieur)
2.4 GHz	4.5 Mbit/s	11 Mbit/s	~35 m	~100 m

Réseau intérieur/extérieur dans la bande 2.4 GHz fonctionnant à 11 Mbits/s théorique (6 Mbits/s réel). Le débit maximum peut être obtenu jusqu'à une distance de 50 m en intérieur et 200 m en extérieur.

- 802.11g :

Bande de Fréquence	Bande passante (Typique)	Vitesse de transmission (max)	Portée (intérieur)	Portée (extérieur)
2.4 GHz	25 Mbit/s	54 Mbit/s	~25 m	~75 m

Réseau intérieur/extérieur dans la bande 2.4 GHz fonctionnant à 54 Mbits/s théorique (26 Mbits/s réel). Le débit maximum peut être obtenu jusqu'à une distance de 27 m en intérieur et 75 en extérieur. Le succès du 802.11g (transfert haut débit et compatible avec le 802.11b) a favorisé l'apparition de protocoles spécifiques comme le Super G autorisant des

débits encore plus élevés jusqu'à 108 Mbps. Votre produit supporte à ce titre le mode Super G d'ATHEROS.

- 802.11a/h :

Bande de Fréquence	Bande passante (Typique)	Vitesse de transmission (max)	Portée (intérieur)	Portée (extérieur)
5 GHz	25 Mbit/s	54 Mbit/s	~25 m	~75 m

Réseau intérieur/extérieur utilisant la bande 5GHz et fonctionnant à 54Mbits/s. La bande 5GHz est plus sensible aux obstacles que celle des 2,4 GHz, mais est moins utilisée et donc moins perturbée. Elle permet d'obtenir un haut débit (dans un rayon de 10 mètres : 54 Mbits/s théoriques, 30 Mbits/s réels). Le débit maximum peut être obtenu jusqu'à une distance de 10 m en intérieur. Il peut encore être augmenté jusqu'à 108 Mbps en exploitant le mode Super AG spécifique à ATHEROS.

Les canaux utilisables dans la bande ainsi que les puissances d'émission sont spécifiées par les législations de votre pays. Attention, seules les normes 802.11b et 802.11g sont compatibles. Ainsi un équipement 802.11g peut communiquer avec un équipement 802.11b à la vitesse de 11Mbits/s.

IV.4.5 Les modes Super G et Super AG

Les modes Super G (pour la bande 2.4 GHz) ou Super AG (Pour la bande 5 GHz) ne peuvent être exploités que si tout le réseau Wi-Fi utilise des chipsets ATHEROS ou compatibles.

Ces modes s'appuient sur un ensemble de caractéristiques étudiées pour augmenter le débit d'un réseau 802.11a ou 802.11g, jusqu'à 60 Mbps utile/108 Mbps théorique contre 18 à 22 Mbps utile/54 Mbps théorique en mode normal :

- Bursting (Caractéristique standard)
- Fast frames (Caractéristique propriétaire)
- Compression (Caractéristique standard, la compression/décompression est faite directement par le chipset ATHEROS)
- Turbo mode (Caractéristique propriétaire)

Il n'est pas possible de programmer indépendamment toutes ces caractéristiques.

Le mode Super G (ou Super AG) peut être complètement désactivé ou encore activé selon l'un des 3 modes suivants :

- Sans turbo
- Avec turbo en mode dynamique : C'est le réseau qui décide tout seul s'il peut exploiter le mode turbo. Chaque fois que du trafic est détecté sur des

canaux adjacents au canal utilisé (qui seraient utilisées en mode turbo), le mode turbo n'est plus utilisé jusqu'à ce que la situation change.

- Avec turbo en mode statique : Le mode turbo est forcé.

Attention, le mode Turbo est un mode propriétaire, qui ne peut fonctionner que si toutes les stations du réseau le supporte.

Les débits possibles dans ces modes sont : 108 Mbps, 96 Mbps, 72 Mbps, 54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps et 6 Mbps.

IV.4.6 Le canal radio et la région

Le canal radio définit le réseau physique (le réseau logique étant défini par le SSID).

L'exploitation des canaux est soumise à la réglementation de la zone où appartient le pays ou encore du pays lui-même.

Le monde est découpé en 3 zones :

- les pays de la zone Europe, régit par l'ETSI (European Telecommunications Standards Institute)
- Les pays de la zone US, régit par FCC (Federal Communications Commission)
- Les pays de la zone asie, régit par MKK/TELEC

Les canaux qu'il est possible d'utiliser sont automatiquement mis à jour lorsque vous sélectionnez votre pays ou votre région dans le menu « region/country ».

La puissance émise maximale (appelée PIRE) pour un canal dépend de la législation du pays (voir www.arcep.fr pour la France) et du milieu "intérieur/extérieur".

IV.4.7 Les réseaux 802.11b/g

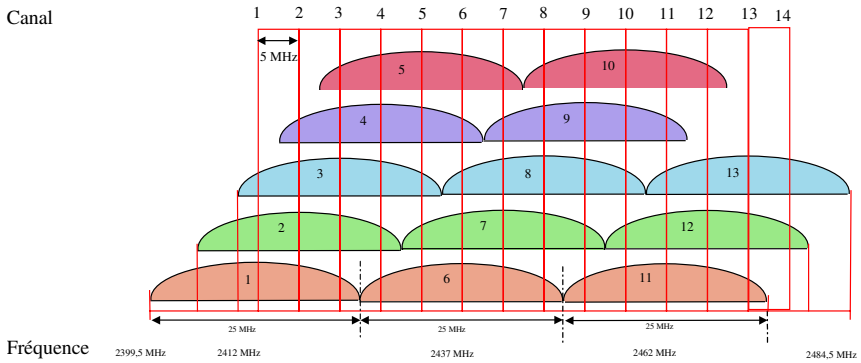
Ces réseaux utilisent la bande de 2.4 GHz, appelée bande ISM (Industrial Scientific and Medical), qui s'étend sur le spectre [2.3995-2.4965].

Canal (25 MHz)	Fréquence centrale en GHz	Autorisée par
1	2,412	Asia MKK, Europe ETSI, US FCC
2	2,417	Asia MKK, Europe ETSI, US FCC
3	2,422	Asia MKK, Europe ETSI, US FCC
4	2,427	Asia MKK, Europe ETSI, US FCC
5	2,432	Asia MKK, Europe ETSI, US FCC
6	2,437	Asia MKK, Europe ETSI, US FCC
7	2,442	Asia MKK, Europe ETSI, US FCC
8	2,447	Asia MKK, Europe ETSI, US FCC
9	2,452	Asia MKK, Europe ETSI, US FCC
10	2,457	Asia MKK, Europe ETSI, US FCC
11	2,462	Asia MKK, Europe ETSI, US FCC
12	2,467	Asia MKK, Europe ETSI
13	2,472	Asia MKK, Europe ETSI
14	2,484	Asia MKK

Tous les canaux d'une largeur de 25 MHz (12.5 MHz de part et d'autre de la fréquence centrale) sont espacés de 5 MHz sauf le canal 14 qui est espacé de 12 MHz avec le canal 13.

Attention, il est extrêmement important de comprendre que les 14 canaux ne sont pas disjoints. En effet le canal 1 interfère le canal 2, le canal 3, le canal 4 et le canal 5. Ce qui signifie qu'un réseau Wi-Fi sur le canal 1 va interférer avec un réseau Wi-Fi installé à proximité sur le canal 5 et donc dégradé ses performances. Et paradoxalement, 2 réseaux Wi-Fi proches situés sur le même canal ne créent pas d'interférences l'un sur l'autre. Dans ce cas, les mécanismes de détection de collision fonctionnent, et les réseaux se partagent simplement la bande passante.

L'illustration ci-dessous montre ce phénomène de recouvrement des canaux. Nous verrons plus loin que ce phénomène de recouvrement n'existe pas avec les canaux de la bande 802.11a, ce qui permet l'installation d'un nombre de réseaux plus important dans une même zone.



Pour éviter les interférences sur le réseau Wi-Fi, vous devez choisir des canaux qui ne se chevauchent pas. Par exemple vous pourrez utiliser les canaux 1, 6, 11. Ils sont suffisants pour couvrir une zone tout entière.

Le 2,4 GHz en France

La France n'autorise que les canaux de 1 à 13, tous libres d'emploi en intérieur et extérieur, avec cependant une limitation de la puissance émise (appelée PIRE) à respecter.

La PIRE maximale pour un canal est dépendante de la législation du pays (voir www.arcep.fr pour la France) et du milieu "intérieur/extérieur".

En intérieur :

100mW de PIRE (i.e. 20 dBm) sur tous les 13 canaux

En extérieur :

100mW de PIRE (i.e. 20 dBm) sur les canaux 1 à 9
10mW de PIRE (i.e. 2 dBm) sur les canaux 10 à 13

IV.4.8 Les réseaux 802.11a/h

Ces réseaux utilisent la bande 5 GHz appelée UN-II (Unlicensed-National Information Infrastructure).

Canal	Fréquence centrale en GHz	Puissance	Autorisée par
34	5,170		Japan TELEC
36	5,180	40 mW (FCC), 200 mW (ETSI)	Europe ETSI, US FCC
38	5,190		Japan TELEC
40	5,200	40 mW (FCC), 200 mW (ETSI)	Europe ETSI, US FCC
42	5,210		Japan TELEC
44	5,220	40 mW (FCC), 200 mW (ETSI)	Europe ETSI, US FCC
46	5,230		Japan TELEC
48	5,240	40 mW (FCC), 200 mW (ETSI)	Europe ETSI, US FCC
52	5,260	250 mW (FCC), 200 mW (ETSI)	Europe ETSI, US FCC
56	5,280	250 mW (FCC), 200 mW (ETSI)	Europe ETSI, US FCC
60	5,300	250 mW (FCC), 200 mW (ETSI)	Europe ETSI, US FCC
64	5,320	250 mW (FCC), 200 mW (ETSI)	Europe ETSI, US FCC
100	5,500	1 W	Europe ETSI
104	5,520	1 W	Europe ETSI
108	5,540	1 W	Europe ETSI
112	5,560	1 W	Europe ETSI
116	5,580	1 W	Europe ETSI
120	5,600	1 W	Europe ETSI
124	5,620	1 W	Europe ETSI
128	5,640	1 W	Europe ETSI
132	5,660	1 W	Europe ETSI
136	5,680	1 W	Europe ETSI
140	5,700	1 W	Europe ETSI
149	5,745	1 W	US FCC
153	5,765	1 W	US FCC
157	5,785	1 W	US FCC
161	5,805	1 W	US FCC
165	5,825	1 W	US FCC

En résumé :
US et Canada (FCC) : 13 canaux répartis sur les fréquences

- [5.150 à 5.250 GHz] (Appelée U-NII I)
- [5.250 à 5.350 GHz] (Appelée U-NII II)
- [5.725 à 5,825] (Appelée U-NII III)

Europe (ETSI) : 19 canaux répartis sur les fréquences

- [5.150 à 5.350 GHz],

- [5.5 à 5,725]

Japan (TELEC) : 4 canaux répartis sur les fréquences
- [5.150 à 5,250]

Le 5 GHz en France
Le Wi-Fi sur la bande du 5GHz est libre d'emploi en intérieur et en partie à l'extérieur, une limitation de la puissance émise (appelée PIRE), ainsi que quelques contraintes techniques particulières :

En intérieur :
200mW de PIRE (i.e. 23 dBm) sur les canaux 36 à 64
1000mW de PIRE (i.e. 30 dBm) sur les canaux 100 à 140
Interdit sur les canaux 149 à 165.

En extérieur :
Interdit sur les canaux 36 à 64.
1000mW de PIRE (i.e. 30 dBm) sur les canaux 100 à 140
Interdit sur les canaux 149 à 165.

Contraintes particulières :
Pour les canaux 36 à 64 et les canaux 100 à 140, à l'intérieur comme à l'extérieur, un mécanisme de Sélection Dynamique de Fréquences (DFS) est obligatoire. Les produits compatibles 802.11h le mettent en oeuvre. Un mécanisme de Contrôle de Puissance de l'Emetteur (non, ce n'est pas le CPE, mais bien le Transmiter Power Control, ou TPC) permettant de réduire la puissance de l'émetteur de 3 dB est recommandé. S'il n'est pas présent, alors la PIRE max autorisée est diminuée de 3 dB (par exemple, 27 dBm au lieu de 30 dBm, soit 500 mW au lieu de 1000 mW). Les produits compatibles 802.11h mettent ce mécanisme en oeuvre.

Le tableau qui suit est cité en exemple et est valable pour la France (voir http://www.arcep.fr)

Bandes de fréquences	Utilisation	Limite de PIRE moyenne maximale autorisée	Densité de PIRE moyenne maximale autorisée	Techniques d'atténuation
Bande 5150-5250 MHz (canaux 30 à 50)	intérieur	200 mW	0,25 mW dans toute bande de 25 kHz	pas d'obligation
Bande 5250-5350 MHz (canaux 50 à 70)	intérieur	200 mW avec une régulation de la puissance de l'émetteur* 100 mW sans régulation de la puissance de l'émetteur*	10 mW/MHz pour toute bande de 1 MHz avec une régulation de la puissance de l'émetteur 5 mW/MHz pour toute bande de 1 MHz sans régulation de la puissance de l'émetteur	Obligation de mettre en place les techniques d'atténuation
Bande 5470-5725 MHz (canaux 94 à 145)	intérieur/extérieur	1 W avec une régulation de la puissance de l'émetteur* 0,5 W sans régulation de la puissance de l'émetteur*	50 mW/MHz dans toute bande de 1 MHz avec une régulation de la puissance de l'émetteur 25 mW/MHz dans toute bande de 1 MHz sans régulation de la puissance de l'émetteur	Obligation de mettre en place les techniques d'atténuation

IV.5 Les différents modes de sécurité

Tout réseau, câblé ou sans fil, doit être sécurisé. La problématique pour les réseaux sans fils est plus compliquée puisqu'il est impossible de protéger l'infrastructure physique.

Il existe donc un grand nombre de mesures de sécurité spécifiques, dont les suivantes :

- Désactivation de la diffusion du SSID. Ce sujet a déjà été traité au paragraphe « **Diffusion du SSID** », page 16.
- Filtrage par adresse MAC
- WEP
- WPA avec authentification 802.1x ou en mode PSK
- WPA2 avec authentification 802.1x ou en mode PSK

IV.5.1 Le filtrage d'adresses MAC en mode point d'accès

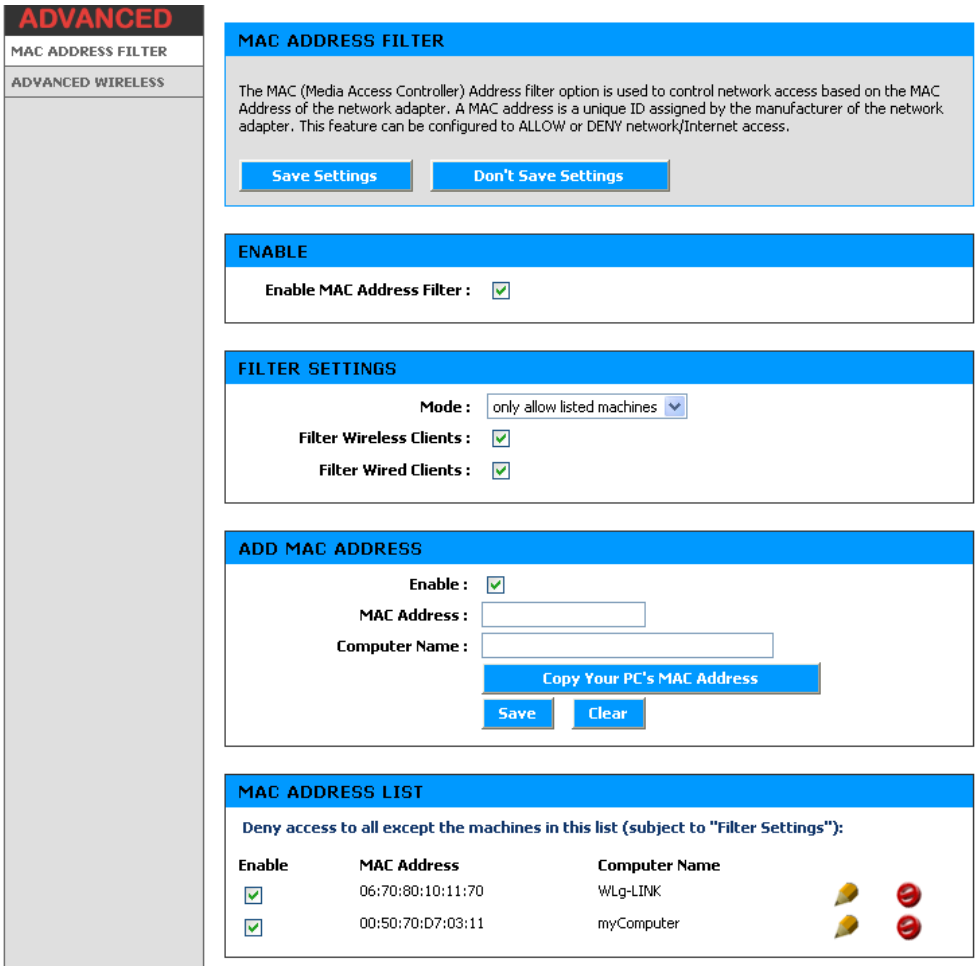
Les points d'accès ACKSYS offrent la possibilité de spécifier les adresses MAC qui peuvent être utilisées ou interdites sur le point d'accès qu'elles viennent du WLAN « Filter Wireless Clients » et/ou encore du LAN « Filter Wired Clients ». Nous rappelons que l'adresse MAC est une adresse matérielle unique spécifique à chaque équipement du réseau.

Le point d'accès ACKSYS gère donc une base d'adresses MAC fonctionnant suivant deux modes :

- Un mode où la liste contient des adresses MAC autorisées « only allow listed machines ». Seules les stations possédant une adresse MAC dans cette liste pourront se connecter au point d'accès.
- Un autre mode où la liste contient des adresses MAC interdites « only deny listed machines ». Seules les stations possédant une adresse MAC dans cette liste ne pourront pas se connecter au point d'accès.

IV.5.1.1 Le menu MAC ADDRESS FILTER

Pour activer le filtre sur les adresses MAC, il faut se rendre dans le menu « ADVANCED\MAC ADDRESS FILTER » et activer la case à cocher « Enable MAC address filter ».



IV.5.2 Le filtrage d'adresses MAC en mode bridge

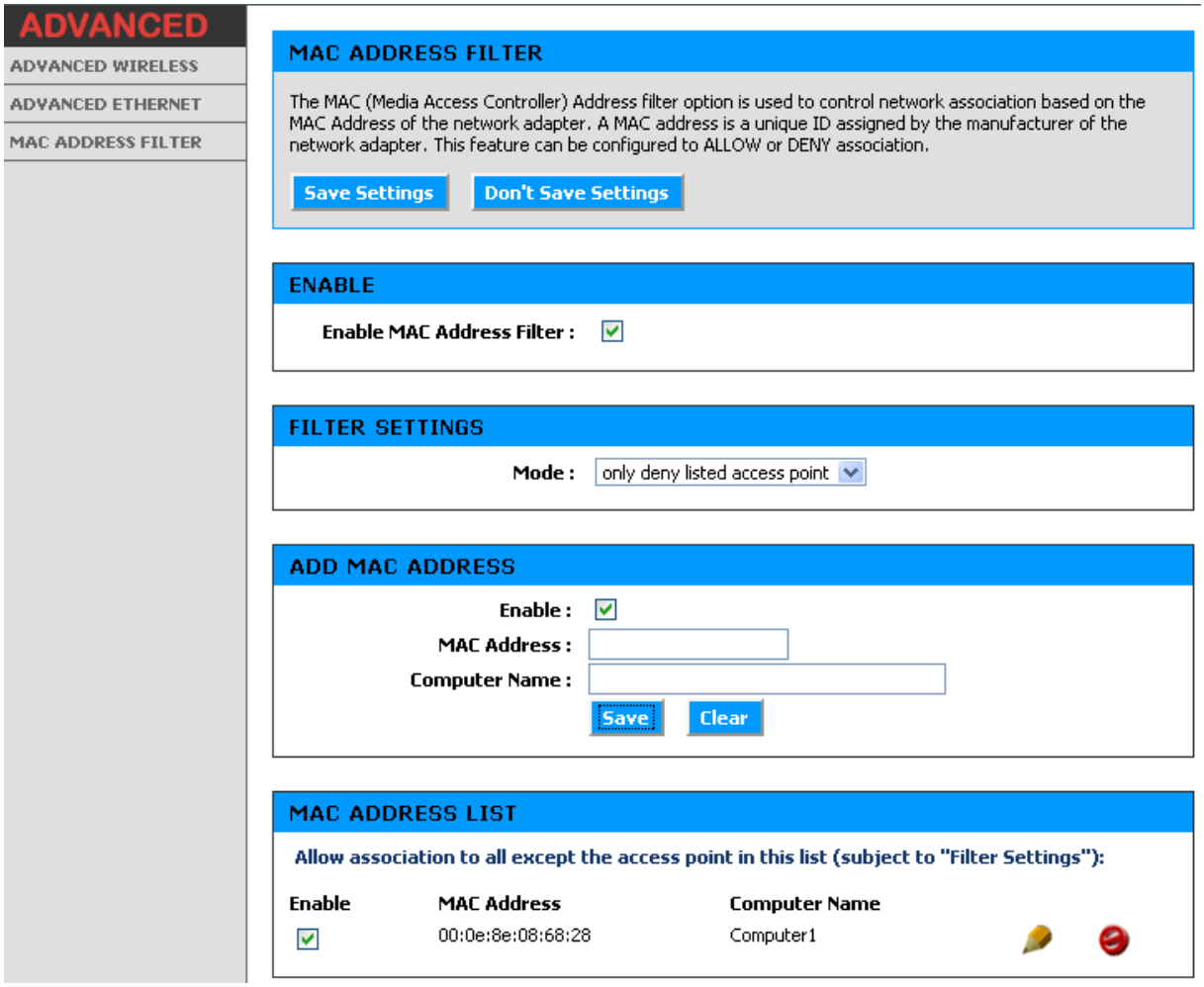
Les bridges ACKSYS offrent la possibilité de spécifier les adresses MAC des points d'accès qui peuvent être utilisés ou interdits. Nous rappelons que l'adresse MAC est une adresse matérielle unique spécifique à chaque équipement du réseau.

Le bridge ACKSYS gère donc une base d'adresses MAC fonctionnant suivant deux modes :

- Un mode où la liste contient des adresses MAC autorisées « only allow listed machined ». Le bridge se connectera uniquement aux points d'accès possédant une adresse MAC dans cette liste.
- Un autre mode où la liste contient des adresses MAC interdites « only deny listed machines ». Le bridge ne se connectera pas à tout point d'accès possédant une adresse MAC dans cette liste.

IV.5.2.1 Le menu MAC ADDRESS FILTER

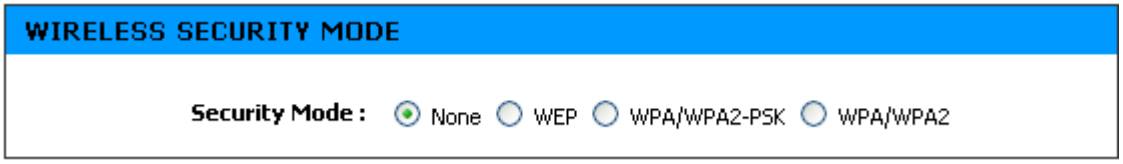
Pour activer le filtre sur les adresses MAC, il faut se rendre dans le menu « ADVANCED\MAC ADDRESS FILTER » et activer la case à cocher « Enable MAC address filter ».



Les niveaux de sécurité WEP & WPA & WPA2

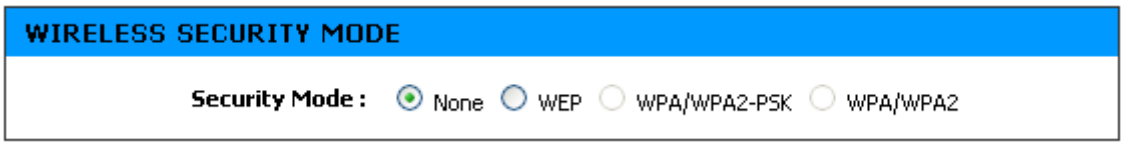
En plus des deux méthodes de sécurité (Filtrage MAC et non-diffusion du SSID), quatre autres choix sont possibles :

En mode infrastructure (point d'accès ou bridge), le produit supporte les quatre choix possibles :



- None : Aucune sécurité
- WEP : Sécurité par clé WEP
- WPA/WPA2-PSK : Sécurité en mode WPA ou WPA2 sans authentification 802.1x
- WPA / WPA2 : Sécurité en mode WPA ou WPA2 avec authentification 802.1x

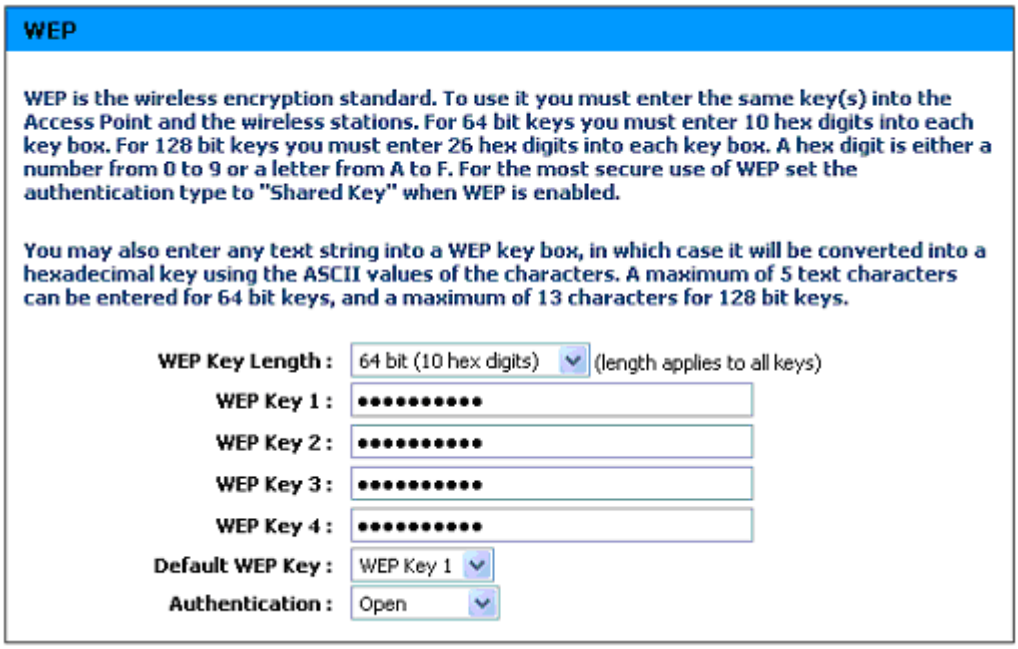
En mode **Bridge Ad-Hoc**, le produit supporte uniquement la sécurité par clé WEP :



- None : Aucune sécurité
- WEP : Sécurité par clé WEP

Les paramètres de sécurité décrits dans ce document sont paramétrables dans le menu BASIC \ WIRELESS.

IV.5.2.2 Le menu WEP



Pour remédier aux problèmes de confidentialité des échanges sur les réseaux sans fils, le standard 802.11 intègre un mécanisme simple de chiffrement des données, il s'agit du WEP, Wired Equivalent Privacy.

Le WEP (Wired Equivalent Privacy) tient son nom du fait qu'il devait fournir aux réseaux sans-fil une confidentialité comparable à celle d'un réseau local classique.

Le WEP est un protocole chargé du chiffrement des trames 802.11 utilisant l'algorithme symétrique RC4 avec des clés d'une longueur de 64 bits ou 128 bits. Le principe du WEP consiste à définir dans un premier temps une clé secrète de 64 ou 128 bits. Cette clé secrète doit être déclarée au niveau du point d'accès et des clients. La clé sert à créer un nombre pseudo-aléatoire d'une longueur égale à la longueur de la trame.
La clé partagée par toutes les stations est statique, c'est-à-dire que pour déployer un grand nombre de stations Wi-Fi il est nécessaire de les configurer en utilisant la même clé de session. Ainsi la connaissance de la clé est suffisante pour déchiffrer les communications.
De plus, 24 bits de la clé servent uniquement pour l'initialisation, ce qui signifie que seuls 40 bits de la clé de 64 bits servent réellement à chiffrer et 104 bits pour la clé de 128 bits.

Dans le cas de la clé de 64 bits, une attaque par force brute (c'est-à-dire en essayant toutes les possibilités de clés) peut très vite amener le pirate à trouver la clé de session.

Le WEP n'est donc pas suffisant pour garantir une réelle confidentialité des données. Pour autant, il est vivement conseillé de mettre au moins en oeuvre une protection WEP 128 bits afin d'assurer un niveau de confidentialité minimum et d'éviter de cette façon 90% des risques d'intrusion.

Attention, le WEP a été identifié par les cryptologues comme contenant des faiblesses importantes. Pour avoir un bon niveau de confidentialité il est conseillé d'utiliser dès que possible le cryptage WPA ou WPA2/802.11i à la place du WEP.

Si jamais le WEP doit être conservé pour une raison ou pour une autre, les clés doivent être choisies aléatoirement et changées fréquemment. Il faut également éviter les clés avec une valeur qui se répète (1111111111111111) ou avec une suite numérique (0123456789ABCDEF)

Vous pouvez configurer jusqu'à 4 clés WEP dans un équipement Wi-Fi.

Authentification par clé WEP :

Authentification : Le mécanisme d'authentification utilise la clé partagée pour l'envoi des données chiffrées. Il existe deux mécanismes d'authentification :

- « Open » System Authentication : mécanisme par défaut, il n'y a pas d'authentification véritable, toute station désirant se connecter est automatiquement authentifiée par son adresse MAC.

- « Shared Key » Authentification : ce mécanisme se déroule en quatre étapes :

    - La station envoie une requête d'authentification au point d'accès.

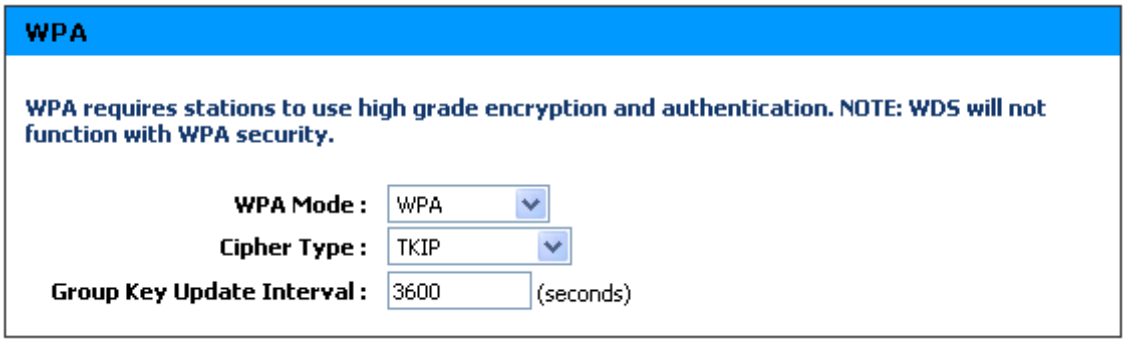
    - Le point d'accès envoie un texte en clair de 128 bits générés par l'algorithme WEP.

    - La station chiffre ce texte avec la clé WEP et l'envoie dans une trame d'authentification.

    - Le point d'accès déchiffre le texte reçu avec la clé WEP et le compare avec le texte envoyé, s'il y a égalité il confirme à la station son authentification et la station peut alors s'associer. Sinon le point d'accès envoie une trame d'authentification négative.

Le mode Shared Key Authentification qui semble être plus sécurisé est en réalité à éviter car il introduit une faille de sécurité. En effet comme les données passent en claires puis ensuite cryptées, il est plus facile pour un pirate de trouver la clé WEP utilisée. Le mode Open est considéré par les spécialistes de la sécurité comme plus sécurisé que le mode « shared » (partagé).

IV.5.2.3 Le menu WPA/WPA2



WPA (Wi-Fi Protected Access) doit être considéré comme une évolution du cryptage WEP. Le WPA a été élaboré par la Wi-Fi Alliance et l'IEEE dans l'attente de la nouvelle norme WPA2 (encore appelée 802.11i).

Précédemment les réseaux Wi-Fi disposaient de clés WEP fixes, décidées sur les points d'accès.

Comme vu précédemment l'utilisation des clés WEP a révélé deux faiblesses :

- L'utilisation d'algorithmes cryptographiques peu développés l'a rendu très vulnérable. Il suffit de quelques heures à un éventuel pirate pour casser les clés utilisées.
- Seconde faiblesse, l'impossibilité d'authentifier un ordinateur ou un utilisateur qui se connecterait au réseau.

Afin de pallier le problème de cryptographie, WPA a définit une nouvelle méthode de chiffrement et de contrôle d'intégrité :

- TKIP (*Temporal Key Integrity Protocol*) : ce protocole a été conçu afin de s'adapter au mieux au matériel existant. Il utilise RC4 comme algorithme de chiffrement, ajoute un contrôle d'intégrité MIC et introduit un mécanisme de gestion des clés (création de clés dynamiques à un intervalle de temps prédéfini)

WPA2 a à son tour définit une dernière méthode de chiffrement et de contrôle d'intégrité :

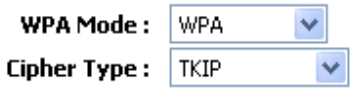
- CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*) : plus puissant que TKIP, il utilise AES (Advanced Encryption Standrad) comme algorithme de chiffrement. C'est la solution qui semble se distinguer à long terme.

WPA et WPA2 (802. 11i) sont identiques dans leur mode de fonctionnement, si ce n'est pour ce qui touche à l'algorithme de chiffrement mis en oeuvre : TKIP (Temporal Key Integrity Protocol) basé sur RC4 dans le premier cas et, dans le second, AES-CCMP (Counter Mode with CBC-MAC) nettement plus sûr, car basé sur AES (Advanced Encryption Standard) et offrant une rétro-compatibilité avec TKIP

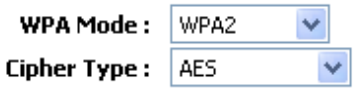
Le produit permet d'avoir quatre niveaux de sécurité différents pour la sécurité WPA et WPA2.
Vous pouvez choisir entre les quatre niveaux de sécurité suivants :

WPA Mode	**Cipher Type**	**Solution de sécurité**
WPA	TKIP	RC4-TKIP
WPA	AES	RC4-CCMP
WPA2	TKIP	AES-TKIP
WPA2	AES	AES-CCMP

Si vous sélectionnez WPA dans le champ « WPA Mode », le « Cipher Type » sélectionné par défaut est *TKIP*.



Si vous sélectionnez WPA2 dans le champ « WPA Mode », le « Cipher Type » sélectionné par défaut est *AES*.



Lorsque le produit est en mode Point d'Accès, vous avez la possibilité de paramétrer l'intervalle de temps qui gère la gestion dynamique des clés « Group Key Update Interval ». Cet intervalle de temps définit le temps de rotation des clés.

Le WPA et WPA2 peuvent fonctionner en deux modes : « WPA/WPA2-PSK » et « WPA-WPA2 ». Le mode WPA /WPA2-PSK (Pre-Shared Key) appelé aussi WPA-Personal est un mode dans lequel les utilisateurs partagent une même phrase secrète. Le mode WPA-WPA2 appelé aussi WPA/WPA2-Enterprise inclut une authentification basée sur 802.1x/EAP. En résumé, on peut considérer le mode PSK comme un mode dégradé, où il n'y a que le chiffrement des données et pas d'authentification.

IV.5.2.3.1 Le mode PSK

Le WPA/WPA2-PSK (encore appelé WPA-PERSONNAL) profite de la sécurité (WPA/WPA2) sans disposer de serveur d'authentification. La configuration du WPA/WPA2-PSK (WPA-Personal) commence par la détermination d'une "passphrase" permettent de générer une clé de 256 bits, en utilisant TKIP pour le WPA et CCMP pour le WPA2. WPA/WPA2-PSK change automatiquement les clés à un intervalle de temps prédéfini. La longueur de la Pre-Shared Key doit être comprise entre 8 et 63 caractères.

Remarque : Tous les composants au sein de votre réseau doivent utiliser la même Pre-Shared Key (PSK) afin de pouvoir communiquer les uns avec les autres.

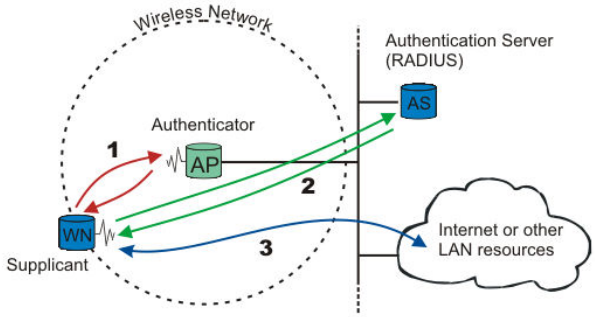
IV.5.2.3.2 Le mode Enterprise

Le WPA/WPA2 (encore appelé WPA/WPA2-Enterprise) impose l'utilisation du protocole 802.1x. Ce dernier protocole est une réponse au besoin d'authentifier les machines ou les utilisateurs connectés sur un réseau local. Il permet donc de transférer les paquets d'authentification vers divers éléments d'un réseau mais offre aussi un mécanisme pour échanger des clés qui vont être utilisées pour chiffrer les communications et en contrôler l'intégrité.

L'authentification 802.1x est un mécanisme permettant l'authentification des clients. (Un peu comme le filtrage par adresse MAC).. Cette authentification fait aujourd'hui partie de la nouvelle norme 802.11i (la dernière édition est encore appelée WPA2).

Une authentification met en œuvre plusieurs acteurs :

- Le client, encore appelé supplicant ou Wireless Node (WN), il s'agit de l'entité qui souhaite être authentifiée de façon à avoir accès aux ressources du réseau
- Le point d'accès sans fil Wi-Fi encore appelé authenticator
- Le serveur d'authentification, en général un serveur RADIUS (Remote Authentication Dial-In User Service). Pour information, le serveur RADIUS est supporté par les versions server de Windows (à partir de Windows Server 2003) et Linux.
- La méthode d'authentification. Il en existe plusieurs qui, suivant les mécanismes d'authentification (login/mot de passe ou certificat) mis en place côté serveur et client, apportent des niveaux de sécurité différents.



La première étape est l'association physique du client avec le point d'accès (chemin 1 sur l'illustration). Cette étape est bien sûr préalable à la phase d'authentification 802.1x.

Tant qu'il n'est pas authentifié, le client ne peut pas avoir accès au réseau, seuls les échanges liés au processus d'authentification sont relayés vers le serveur d'authentification par le point d'accès (chemin 2 sur l'illustration).

Une fois authentifié, le point d'accès laisse passer le trafic lié au client (chemin 3 sur l'illustration) et ce dernier peut avoir accès aux ressources du réseau.

Il est important de rappeler que 802.1x offre aussi un mécanisme pour échanger des clés qui vont être utilisées pour chiffrer les communications et en contrôler l'intégrité.

IV.5.2.3.2.1 Les méthodes d'authentification

Toutes les méthodes s'appuient sur un même protocole appelé EAP (Extensible Authentication Protocol)

Les 4 méthodes les plus utilisées sont les suivantes.

- EAP-MD5 : pas d'authentification mutuelle entre le client et le serveur RADIUS, le client s'authentifie par mot de passe ;

- EAP-TLS : authentification mutuelle entre le client et le serveur RADIUS par le biais de certificats (côté client et côté serveur) ;

- EAP-TTLS et EAP-PEAP : authentification mutuelle du client et du serveur RADIUS par le biais d'un certificat côté serveur, le client peut utiliser un couple login/mot de passe ;

Attention, la méthode utilisée est transparente pour le point d'accès, seuls le supplicant et le serveur d'authentification l'utilisent. Le choix d'une méthode plutôt qu'une autre dépend d'une part, des méthodes supportées par le supplicant et le serveur d'authentification et d'autre part, du niveau de sécurité exigé.

Par exemple, un supplicant Windows XP SP2 supporte en standard :

- PEAP avec l'authentification par login mot de passe (appelée MSCHAP Version 2) ou encore l'authentification avec l'utilisation de certificat.

Les points d'accès ACKSYS supportent toutes ces méthodes d'authentification. Dans l'illustration ci-après, est documenté le menu « EAP (802.1x) » qui contient tous les paramètres nécessaires à la mise en œuvre du 802.1x lorsque le produit ACKSYS est paramétré en point d'accès et qu'il réalise la fonction AUTHENTICATOR.

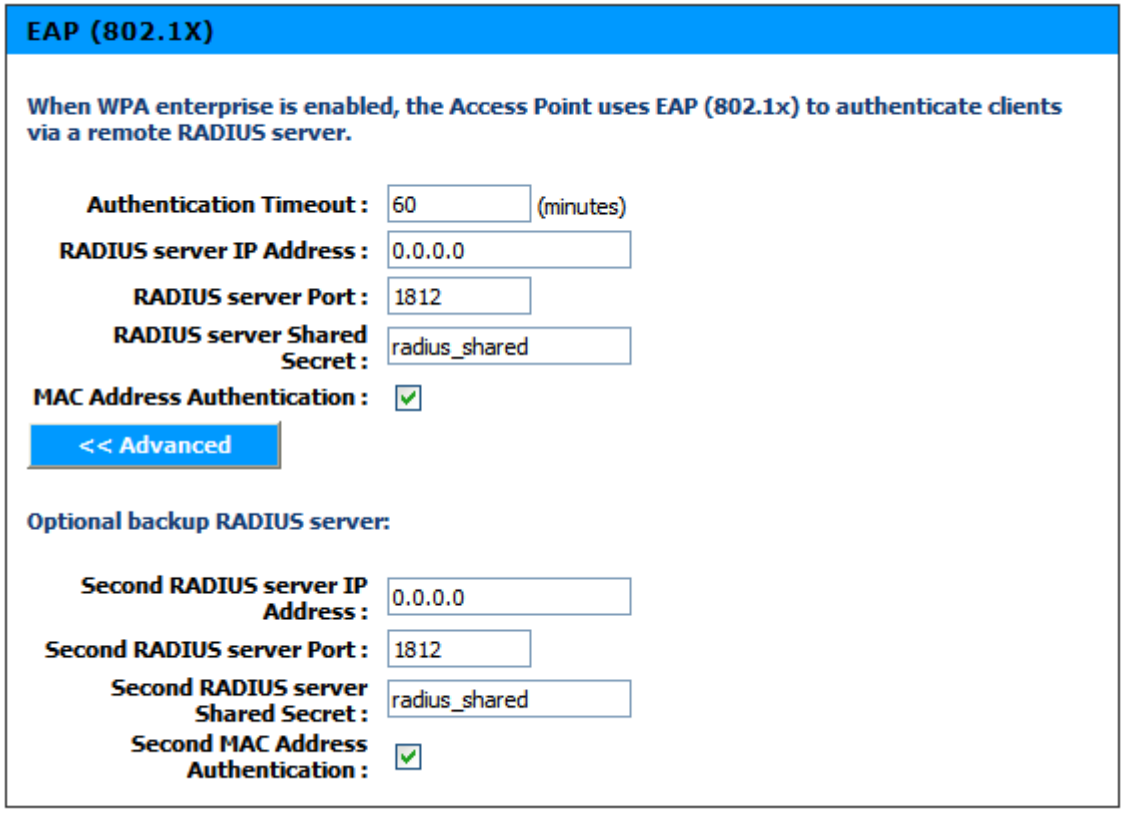
En mode bridge, les produits ACKSYS permettent d'utiliser la méthode d'authentification MSCHAP Version 2 lorsque le produit réalise la fonction SUPPLICANT. La description des menus relatifs à cette fonctionnalité est détaillée au paragraphe :

IV.5.2.3.2.2 Le menu EAP (802.1x) en mode point d'accès

Ce menu permet le paramétrage de l'AP de façon à permettre à un supplicant de s'authentifier auprès d'un serveur RADIUS.

Un bouton 

permet le paramétrage d'un second serveur RADIUS avec les mêmes paramètres que le premier à l'exception du timeout d'authentification.



Le champ « authentication timeout »

Dès que le timeout renseigné dans ce champ expire (il est exprimé en minutes), le client doit alors se ré-authentifier.

Le champ « RADIUS SERVER IP ADDRESS »

Ce champ doit contenir l'adresse IP du serveur RADIUS. Sur le serveur RADIUS doit être installé de la même façon l'adresse du client RADIUS, il conviendra d'y mettre l'adresse IP du point d'accès.

Le champ « RADIUS SERVER SHARED SECRET »

Ce champ est une chaîne de texte servant de mot de passe entre le point d'accès (le client RADIUS) et le serveur RADIUS.

Les secrets partagés sont utilisés pour vérifier que les messages RADIUS, à l'exception du message de requête d'accès, sont envoyés par un périphérique compatible RADIUS configuré avec le même secret partagé. Les secrets partagés vérifient aussi que le message RADIUS n'a pas été modifié en transit (intégrité du message). Le secret partagé est également utilisé pour crypter certains attributs RADIUS, tels que User-Password et Tunnel-Password.

Lors de la création et de l'utilisation d'un secret partagé :

- vous devez utiliser le même secret partagé sensible à la casse sur les deux périphériques RADIUS ;
- vous devez utiliser un secret partagé différent pour chaque paire serveur RADIUS – client RADIUS ;
- vous pouvez utiliser un secret partagé comportant jusqu'à 64 caractères. Pour protéger votre serveur IAS et vos clients RADIUS contre les attaques de force brute, utilisez de secrets partagés longs (plus de 22 caractères) ;
- le secret partagé doit être constitué d'une séquence aléatoire de lettres, de chiffres et de caractères de ponctuation, et il doit être souvent modifié afin de protéger votre serveur IAS et vos clients RADIUS contre les attaques de dictionnaire.

Le champ « RADIUS SERVER PORT »

Il s'agit du port utilisé lors d'une demande d'authentification d'un client RADIUS vers un serveur RADIUS.
La valeur 1812 pour l'authentification est le port RADIUS standard défini dans le RFC 2865. Toutefois, de nombreux serveurs d'accès utilisent par défaut le port 1645 pour les demandes d'authentification. Quel que soit le numéro de port que vous choisissez d'utiliser, vérifiez que le service IAS et votre point d'accès sont configurés pour utiliser le même.

La case à cocher « MAC ADDRESS AUTHENTIFICATION »

Si cette case est activée, le contrôle de l'adresse MAC du supplicant est ajouté à l'authentification. Autrement dit le supplicant doit toujours se connecter à la même station.

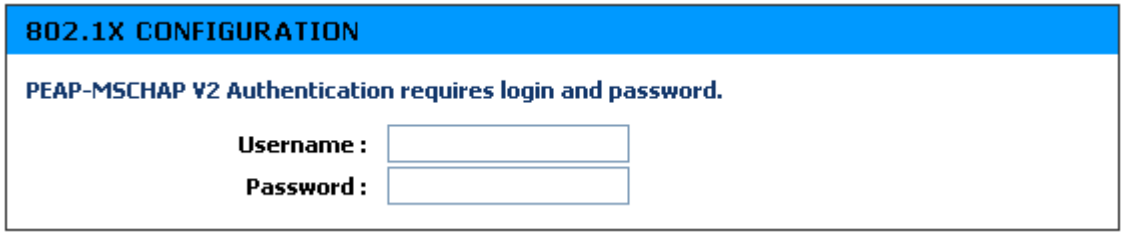
IV.5.2.3.2.3 Le menu 802.1x en mode bridge

Attention cette fonctionnalité n'est disponible que sur les deuxièmes versions des produits (notée V2), elle nécessite en effet une évolution des produits.

Pour accéder à la fenêtre de configuration « 802.1x Configuration » il est nécessaire de sélectionner « WPA/WPA2 » dans le menu « Wireless security mode ».

Ce menu permet le paramétrage du bridge supplicant afin qu'il puisse s'authentifier auprès d'un serveur RADIUS.

Attention, parmi les quatre méthodes EAP décrites en IV.5.2.3.2.1, seule la méthode EAP-PEAP avec authentification par login et mot de passe (MS-CHAPV2) est ici supportée.



Champ « Username » : Ce champ contient le nom d'un utilisateur valide sur votre serveur radius.

Champ « Password » : Ce champ contient le password associé au nom d'utilisateur entré ci-dessus.

IV.6 Le roaming

IV.6.1 Généralités

Le « roaming » traduit la capacité d'un client Wi-Fi mobile (fonction bridge infrastructure dans le produit ACKSYS) à changer de point d'accès sans pour autant perdre la connexion réseau.

Sans la fonction de roaming, un client Wi-Fi va attendre de perdre la communication avec le point d'accès pour :

- Chercher un nouveau point d'accès (recherche sur tous les canaux).
- Faire une demande d'association avec le meilleur point d'accès trouvé.

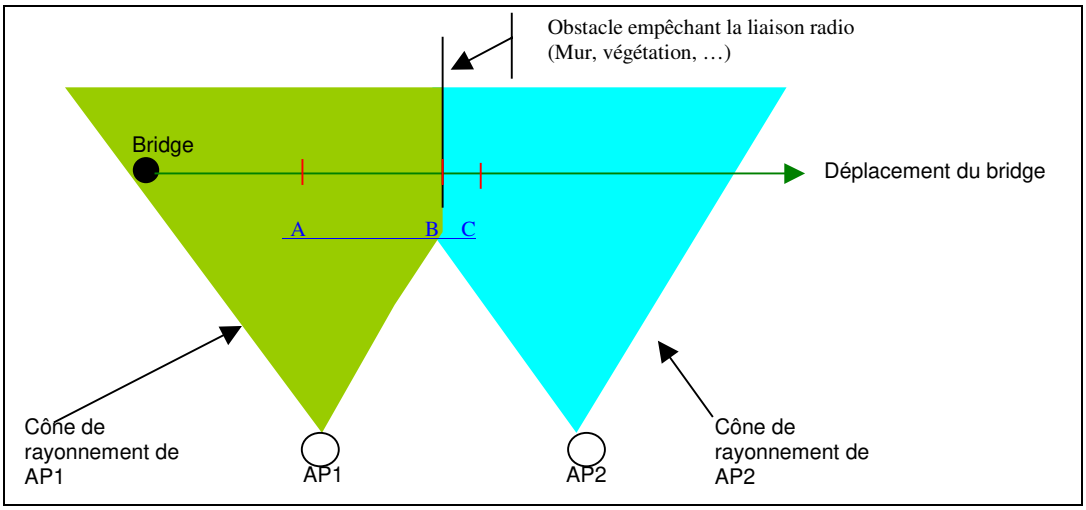
Ce processus peut être long (plusieurs secondes), et pendant cette période les informations provenant du client Wi-Fi à destination de l'infrastructure réseau se trouvant derrière le point d'accès ne sont pas transmises.

Le **temps de roaming**, c'est à dire le temps nécessaire au bridge pour passer d'un point d'accès à un autre, va dépendre de plusieurs paramètres que l'on se doit de maîtriser afin que ce temps soit le plus petit et le plus constant possible.
Un paramètre important est la qualité de la liaison radio entre la station et le point d'accès qui est mesurée par le RSSI.

IV.6.2 Comprendre le roaming

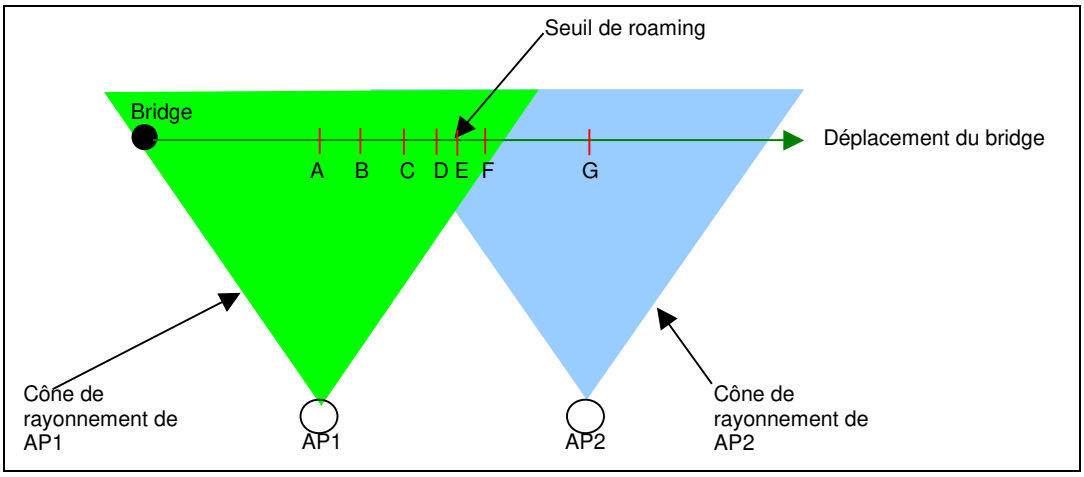
En Wi-Fi on peut distinguer deux cas où l'on a besoin de roaming :

- Perte du point d'accès : Dans ce cas la rupture est brutale et sans diminution préalable du RSSI. Cela peut se produire si dans la couverture radio de votre point d'accès il y a des zones d'ombre.



Position A : la communication est excellente avec AP1
Position B : La communication avec l'AP1 s'interrompt brutalement lors du passage de l'obstacle, on doit passer sur l'AP2.
Position C : Le bridge s'est associé avec l'AP2, la communication reprend.

- Meilleur point d'accès : Ce cas est le plus fréquent. Cela peut se produire si dans votre couverture radio il existe des zones de recouvrement entre plusieurs point d'accès.



Le tableau ci-dessous présente les différents niveaux de RSSI (exprimé en %) entre le bridge et AP1 d'une part, entre le bridge et AP2 d'autre part, en fonction du de l'endroit où se trouve le bridge.

	A	**B**	**C**	**D**	**E**	**F**	**G**
RSSI avec AP1	100%	50%	40%	30%	20%	10%	0%
RSSI avec AP2	0%	0%	10%	20%	30%	40%	100%

Dans l'illustration ci-dessus :

Seuil de scan : 50 % du RSSI MAX
Seuil de roaming : 45 % du RSSI MAX

Position A : la communication est excellente avec AP1. Aucun scan n'est effectué car le RSSI (100%) est supérieur au seuil de scan (50%).

Position B : la station passe en dessous de 50% de RSSI avec AP1 et se met à la recherche d'un nouveau point d'accès → Le processus de scan démarre.

Position C : la station arrive dans la zone de couverture de AP2.

Position D : la station atteint le seuil de changement de point d'accès (45%) mais n'a pas trouvé de meilleur point d'accès.

Position E : AP2 est trouvé avec un meilleur RSSI que le RSSI courant avec AP1. La station décide donc de basculer sur AP2 et se déconnecte de AP1.

Position F : le processus de scan reste actif car le nouveau RSSI courant (avec AP2) est en dessous du seuil de scan.

Position G : la station stoppe le processus de scan car le RSSI courant (avec AP2) devient supérieur au seuil de scan.

Afin de permettre dans les deux cas de toujours trouver un point d'accès le plus rapidement possible, nous devons :

- Scruter les canaux afin de maintenir une liste des points d'accès avec lesquels nous pourrions nous associer si un des deux cas se présentait.
- Vérifier que le dialogue avec le point d'accès courant est toujours correct.
- Surveiller le RSSI du point d'accès avec lequel nous sommes associés afin de détecter le moment où nous avons un meilleur point d'accès

Problèmes liés à la liaison radio :

- Il est impossible de scruter tous les canaux sans induire une baisse des performances du système. En effet lorsque le client mobile écoute un canal différent de celui du point d'accès, il lui est impossible de communiquer avec le point d'accès.
- La détection de la perte de point d'accès est longue car le client mobile attend de ne plus recevoir un certain nombre de trame de management provenant du point d'accès. Pendant ce temps les trames sont toujours envoyées au point d'accès. Comme il ne répond pas, elles seront retransmises puis perdues.
- Une trame émise doit être acquittée par le point d'accès pour être considérée comme correctement transmise. Si le point d'accès n'acquitte pas la trame elle sera retransmise plusieurs fois à la vitesse actuelle, puis plusieurs fois à la vitesse inférieure, etc. Cela jusqu'a ce que le point d'accès acquitte la trame ou que la transmission échoue sur la plus petite vitesse. Plus la vitesse est faible, plus le temps pour transmettre la trame est long.

IV.6.3 Configuration du Roaming

Acksys a mis en place une solution permettant de configurer les différents aspects énumérés ci-dessus.

Les paramètres de configuration du roaming se trouvent dans plusieurs menus :

- Basic Wireless : Dans ce menu vous trouverez les paramètres pour activer ou désactiver le roaming ainsi que les paramètres de base. Après ce paramétrage, le roaming fonctionnera pour les cas les plus courants.
- Advanced Wireless : Dans ce menu vous trouverez les paramètres permettant de régler plus finement le roaming afin d'atteindre les performances nécessaires au fonctionnement de votre système.

Il est possible d'agir sur d'autres paramètres qui ne sont pas spécifiques au roaming :

Le nombre de retransmissions selon la vitesse de communication (voir la section « Gestion des retransmissions »)

- Le nombre de canaux utilisables dans la cellule (voir la configuration de votre point d'accès).
- La fréquence d'émission des « beacons » par votre point d'accès.

IV.6.3.1 Le menu Basic wireless

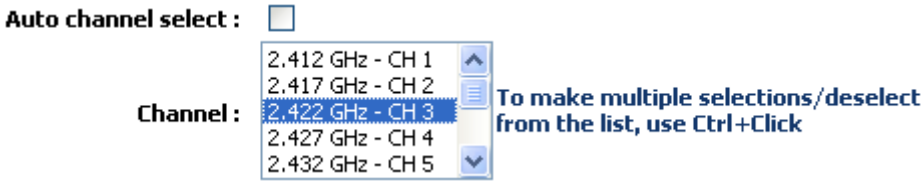
Le roaming s'active grâce à l'option suivante :

Sélectionner « Enable » ouvre la fenêtre de paramètres du roaming (Basic Roaming settings). Une fenêtre de paramétrage avancé (Advanced roaming settings) devient également accessible. Néanmoins, pour pouvoir activer le roaming, il faut décocher la case « Auto channel select » dans le cadre « Basic wireless settings », puis sélectionner un ou plusieurs canaux dans la liste des canaux disponibles.

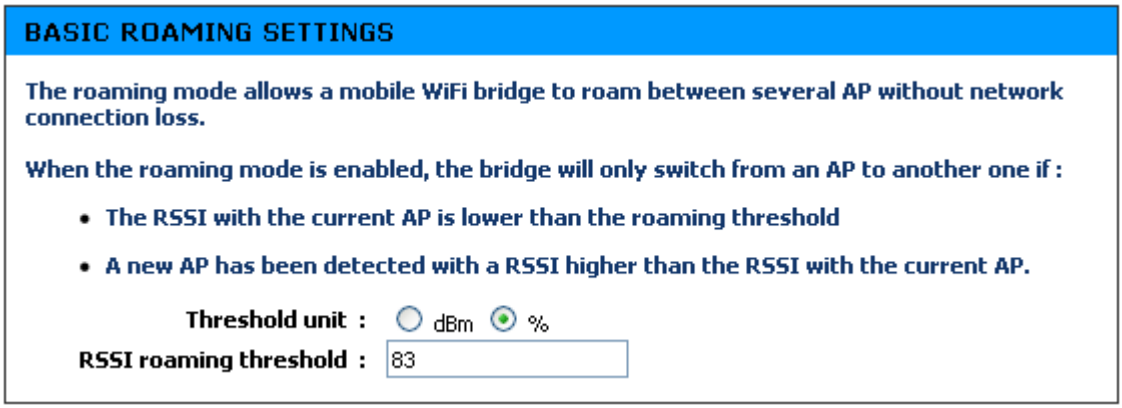
Si cette fonction est inhibée, alors le bridge attendra de perdre la connexion avec le point d'accès en cours avant de se connecter sur un autre point d'accès.

Une fois le ou les canaux sélectionnés, seuls les points d'accès utilisant ces mêmes canaux seront visibles par le bridge.

Pour des performances élevées il est déconseillé de sélectionner plusieurs canaux.



La fenêtre de paramétrage du roaming est donnée ci-dessous :



Elle permet de régler le seuil de basculement entre deux points d'accès. Il peut être exprimé en pourcentage ou en dBm.

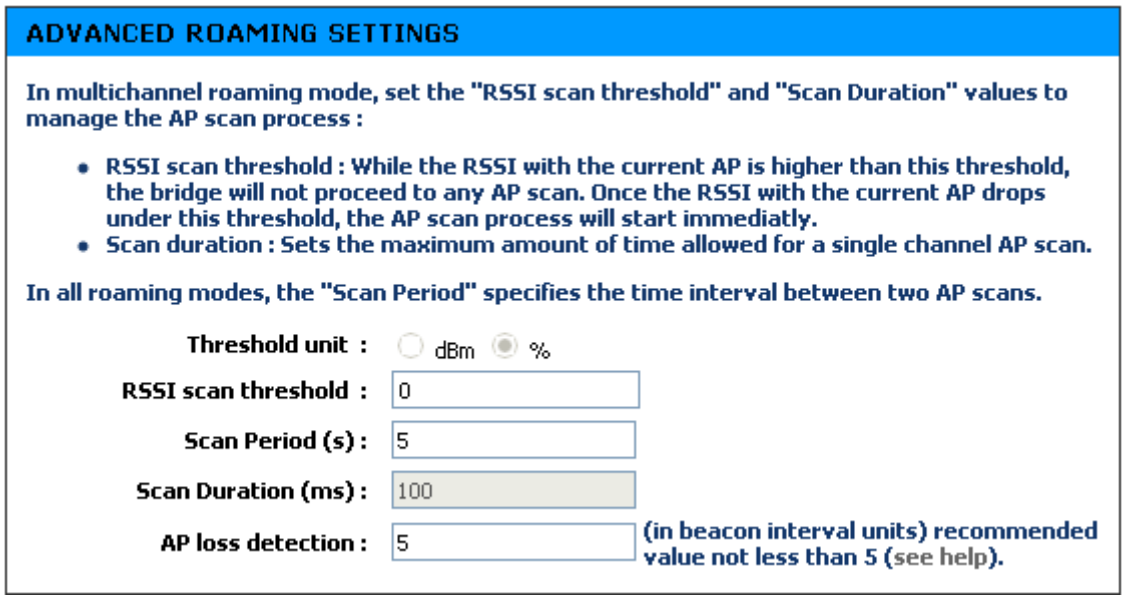
Le bridge passera de AP1 à AP2 si :

$$(RSSI_{(AP1)} < RSSI_{(AP2)}) \text{ ET } (RSSI_{(AP1)} < \text{seuil})$$

Ainsi, il est impossible de basculer sur un point d'accès qui offrirait une moins bonne qualité de signal (moins bon débit).

IV.6.3.2 Le menu Advanced Wireless

Une seconde fenêtre « Advanced roaming settings » permet le paramétrage du processus de scan. Attention, ces paramètres sont à manipuler avec beaucoup de prudence et des valeurs erronées peuvent conduire à une perte de bande passante, voire à des déconnections.



Champ « Threshold unit » : Ce champ définit l'unité dans laquelle le « RSSI scan threshold » est exprimé (dBm ou pourcentage). Ce champ n'est accessible qu'en mode multichannel.

Champ « RSSI scan threshold » : Ce champ définit le seuil au-dessous duquel le processus de scan de nouveaux points d'accès peut démarrer. Ce champ n'est accessible qu'en mode multichannel.

Valeur par défaut : 0% ou –95dBm.

Champ « Scan Period » : Ce champ définit la période du processus de scan. Cette valeur doit être ajustée en fonction de la vitesse à laquelle se déplace la station. Ce champ est toujours accessible quel que soit le nombre de canaux radio sélectionnés.

- En mode multichannel, le processus de scan réalise un scan actif et passif.
- En mode monochannel, le processus de scan réalise un scan actif (Le scan passif est fait continuellement).

Valeur par défaut : 5s.

Champ « Scan duration » : Ce champ définit la durée du processus de scan, autrement dit le temps d'écoute d'un canal radio. S'il est trop court, il est possible de ne pas détecter de point d'accès. Ce champ n'est accessible qu'en mode multichannel.

Valeur par défaut : 100 ms.

Champ « AP loss detection » : Ce champ permet de définir combien il faut de beacons successifs perdus pour supposer que le point d'accès est devenu inaccessible. Les beacons sont des trames émises périodiquement par le point d'accès pour signaler sa présence. Il s'agit donc d'un time-out exprimé en nombre d'intervalles de beacons.

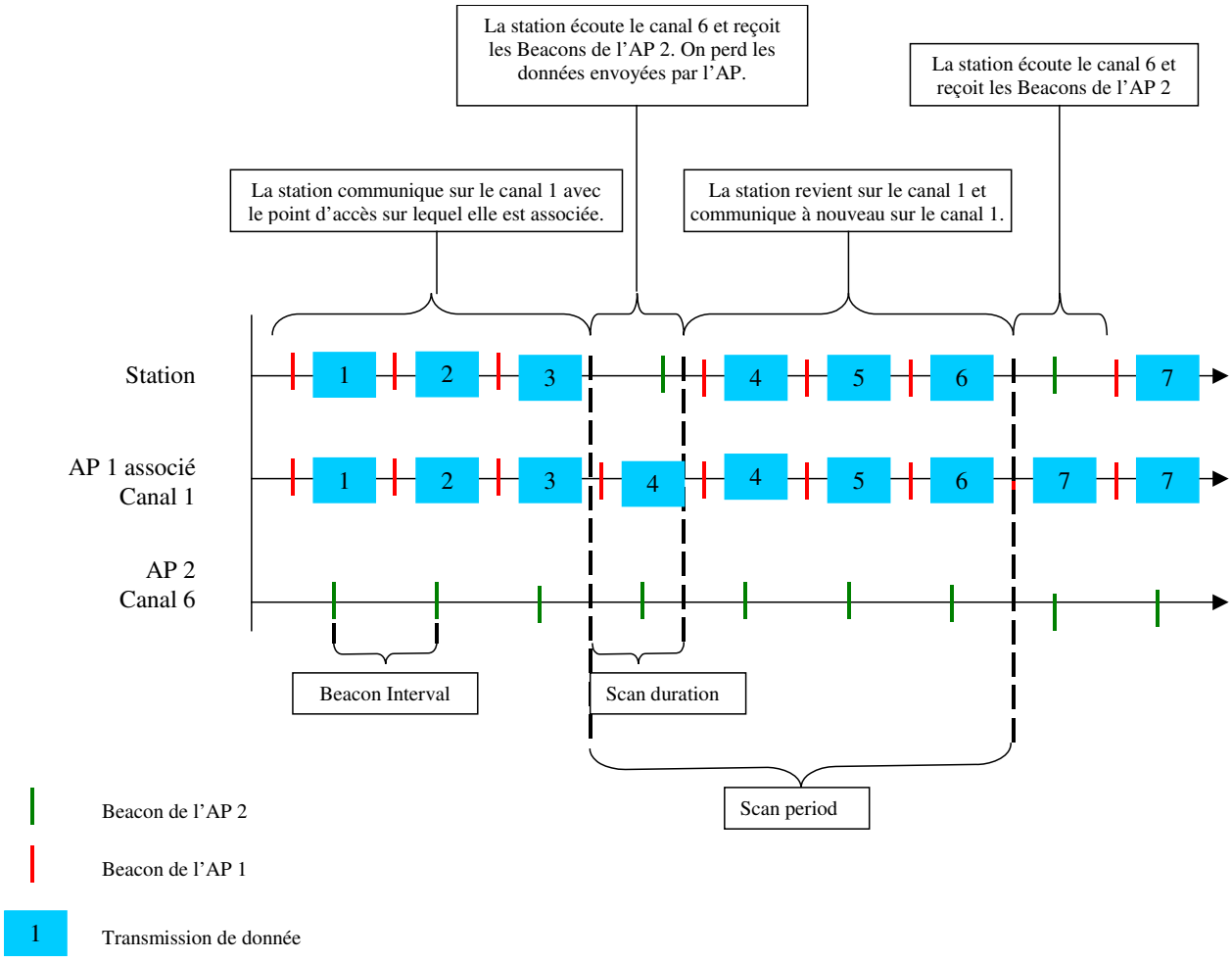
Pour réduire ce time out, vous pouvez :

Réduire la valeur de ce champ

Réduire l'intervalle de temps entre deux beacons sur votre point d'accès.

Valeur par défaut : 5

Schéma explicatif du scan multi-canal



ATTENTION :

Dans la mesure où le « scan » de canaux radio perturbe la connexion en cours (une connexion en cours sur le canal radio X est temporairement interrompue lorsque le bridge scrute le canal radio Y), il est conseillé de n'utiliser la fonction de roaming que sur un seul canal (on parle de mode monochannel). Dans ce

dernier cas, le produit est continuellement à la recherche de meilleurs points d'accès en écoutant les trames de beacon émises par les points d'accès environnants (on parle alors de scan passif). De plus, à un rythme paramétrable appelé **période de scan**, le produit envoie des « probe requests » (on parle de scan actif) de façon à détecter aussi les points d'accès qui n'auraient pas été découverts dans le scan passif.

En revanche, lorsque 2 canaux radio ou plus doivent être utilisés (ce mode est appelé multichannel), il est évidemment inconcevable de scanner continuellement tous les canaux. C'est pourquoi le produit offre des fonctions de paramétrage :

- **Seuil de RSSI (RSSI scan threshold)** en dessous duquel le « scan » doit démarrer (il ne sert à rien de scruter d'autres canaux si la connexion avec le point d'accès en cours est excellente). Évidemment, ce seuil devra être supérieur au seuil de roaming.

- **Durée d'un scan (Scan duration)**. Pendant toute la durée d'un scan, le scan du canal radio est fait suivant les 2 modes (actifs et passifs).

Dans ce mode multichannel, un canal radio différent est scanné à chaque période de scan.

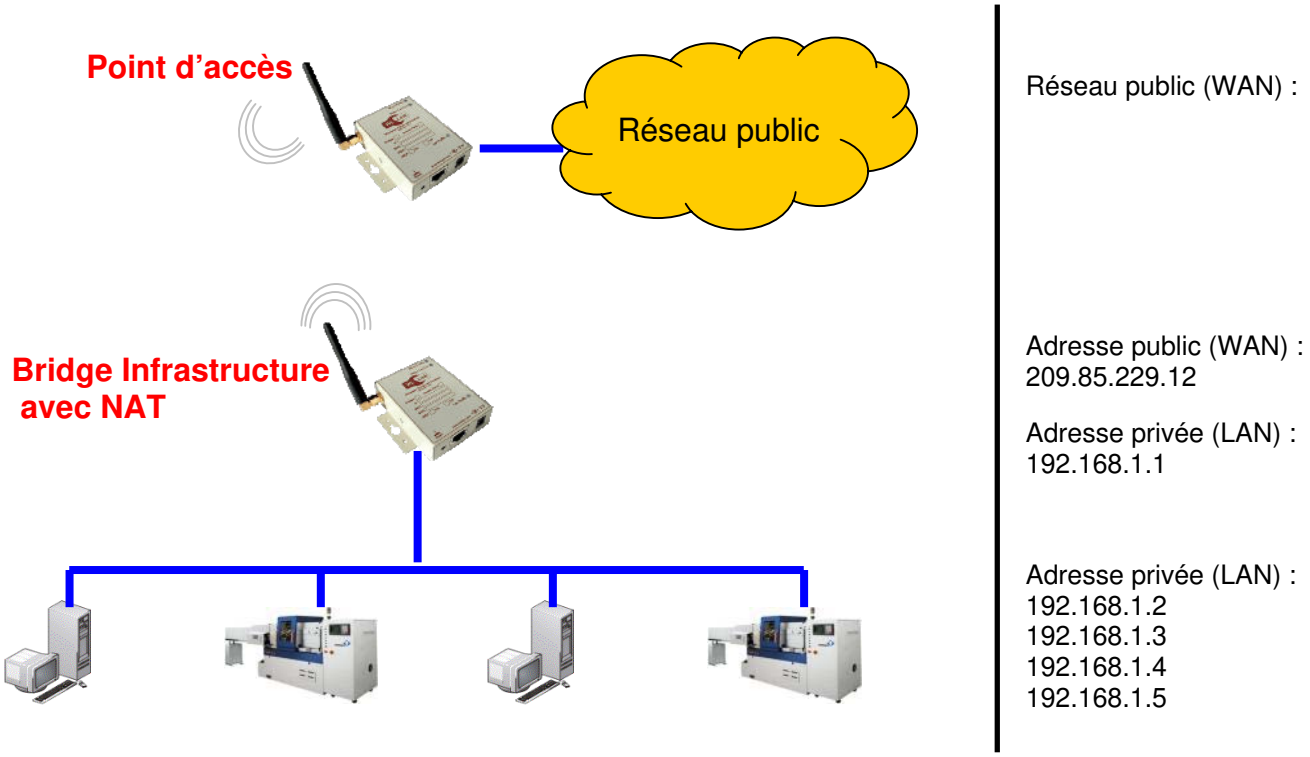
La bande passante de la connexion en cours est d'autant plus altérée que la période de scan est courte ou la durée de scan est longue.
Le temps de découverte de nouveaux points d'accès est d'autant plus long qu'il y a de canaux à scanner.

IV.7 Le NAT

Le NAT (Network Translation Address) permet de faire correspondre un ensemble d'adresses d'un intranet privé (LAN) avec une seule adresse IP externe publique (WAN).

Cette technique permet d'économiser des adresses Ipv4 sur le réseau public. Son fonctionnement implique :

- le trafic du réseau privé n'est pas accessible par le réseau public
- seule l'interface WAN du bridge sera accessible à partir du réseau public
- le trafic en provenance du réseau privé et à destination du réseau public est, lui, autorisé en utilisant le bridge comme passerelle



Une analogie peut-être faite avec un multiplexeur qui aguillerait une ou plusieurs adresses du réseau privé vers une unique adresse publique.

Attention, si NDM est placé sur le réseau public, il sera incapable de trouver le bridge.

IV.7.1 Le menu NAT

La fonctionnalité NAT n'est disponible que dans le mode bride infrastructure et ce, depuis la version 4.4.0.

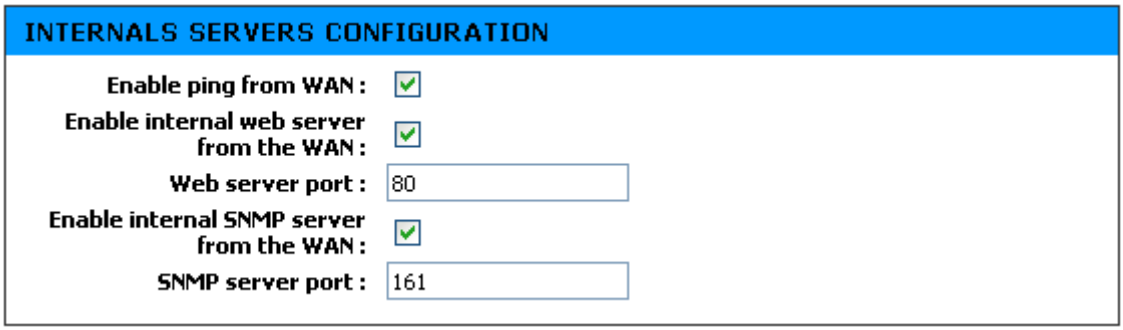
Le menu de configuration du NAT se trouve dans la section Basic du bridge. Par défaut, le NAT n'est pas activé. Pour l'activer, cochez la case à cocher suivante :

Une fois cette case cochée, les détails de la configuration du NAT sont disponibles. Ces options permettent de configurer les éléments suivants :

- les serveurs internes au produit (adminweb, snmp)
- la configuration de l'interface WAN
- établir des règles de Port forwarding
- établir des règles de Port triggering

Lorsque le NAT est activé, l'adresse IP du LAN doit être statique afin de pouvoir utiliser la fonction de « port forwarding ».

Les serveurs internes :



Champ « Enable ping from WAN » : Cette option, si elle est cochée, permet d'autoriser le produit à répondre au requêtre ICMP ping arrivant sur son port WAN.

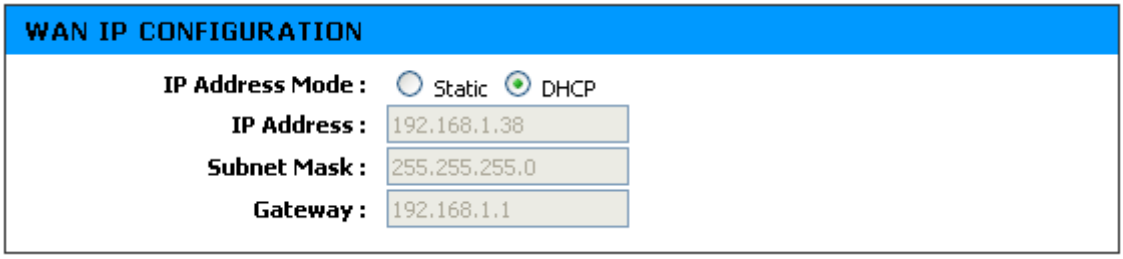
Champ « Enable internal web server from the WAN » : Cette option, si elle est cochée, permet d'autoriser le server web interne au produit à répondre aux requêtes en provenance du WAN sur le port TCP spécifié par le champ « **Web server port** ».

Champ « Web server port » : Permet de configurer le port TCP utilisé pour accéder au serveur web interne au produit.

Champ « Enable internal SNMP server from the WAN » : Cette option, si elle est cochée, permet d'autoriser l'agent SNMP interne au produit à répondre aux requêtes en provenance du WAN sur le port TCP spécifié par le champ « **SNMP server port** ».

Champ « SNMP server port » : Permet de configurer le port TCP utilisé pour accéder à l'agent SNMP interne au produit.

Configuration IP du Port WAN :



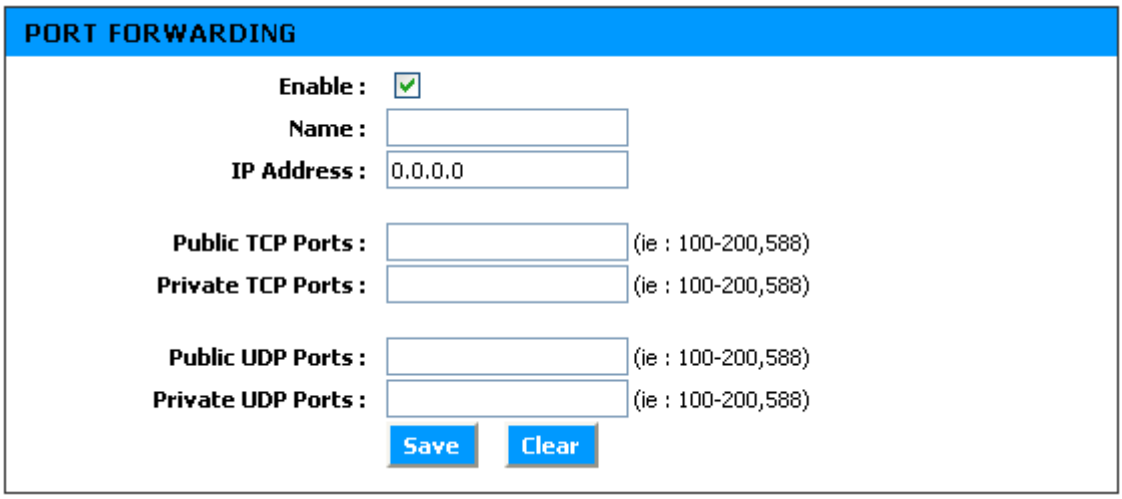
Champ « IP Address Mode » : Permet de choisir de quelle manière les paramètres IP du WAN seront configurés. Par défaut, la configuration automatique par **DHCP** est activée. Vous pouvez choisir une configuration manuelle de l'interface WAN en sélectionnant **Static**.

Champ « IP Address » : Si le mode de configuration **Static** est utilisé, ce champ contient l'adresse IP de l'interface WAN.

Champ « Subnet Mask » : Si le mode de configuration **Static** est utilisé, ce champ contient le masque de sous réseau de l'interface WAN.

Champ « Gateway » : Si le mode de configuration **Static** est utilisé, ce champ contient l'adresse IP de la passerelle de l'interface WAN.

Redirection de port (Port Forwarding) :



Ces options de configurations permettent d'établir des règles de redirection de port. En effet, un serveur se trouvant du côté privé d'un NAT ne peut pas être contacté directement par des machines du WAN.

La redirection de port permet de palier à ce défaut en redirigent les requêtes arrivant de l'interface WAN par un port spécifié vers une IP fixe appartenant au réseau privé.

Note : de par le fonctionnement de cette option, chaque port n'autorise qu'une seule règle de redirection.

Champ « Enable » : Cette option active les règles de redirection de port. Sinon aucune des règles établies ne sera prise en compte.

Champ « Name » : Contient le nom de règle. Ce nom nous permettra de retrouver facilement la règle dans la liste des règles de redirection de port.

Champ « IP Address » : Contient l'adresse IP vers laquelle rediriger la requête en provenance du WAN.

Champ « Public TCP ports » : Contient le port ou la plage de ports TCP qui devront être redirigés du public vers le privé. Il est possible de spécifier plusieurs ports ou plages de ports en les séparant par des virgules. Il est possible de laisser ce champ vide dans le cas où seuls des ports UDP seraient utilisés.

Champ « Private TCP ports » : Contient le port ou la plage de ports TCP vers lesquels les ports de « Public TCP Port » devront être redirigés. La syntaxe de ce champ doit être la même que celle du « Public TCP Ports ».

Exemples :

Public TCP Ports	Private TCP Port	Comportement du NAT
4000	22	Le port TCP public 4000 est redirigé sur le port TCP privé 22.
1000-1002	10-12	Les ports TCP publics 1000, 1001, 1002 sont redirigés respectivement sur les ports TCP privés 10, 11, 12.
68,18-20	100,200-202	Le port TCP public 68 est redirigé sur le port TCP privé 100. Et les ports TCP publics 18, 19, 20 sont redirigés respectivement sur les ports TCP privés 200, 201, 202.

Champ « Public UDP ports » : Contient le port ou la plage de ports UDP qui devront être redirigés du public vers le privé. Il est possible de spécifier plusieurs ports ou plages de ports en les séparant par des virgules. Il est possible de laisser ce champ vide dans le cas où seuls des ports TCP seraient utilisés.

Champ « Private UDP ports » : Contient le port ou la plage de ports UDP vers lesquels les ports de « Public UDP Port » devront être redirigés. La syntaxe de ce champ doit être la même que celle du « Public UDP Ports ».

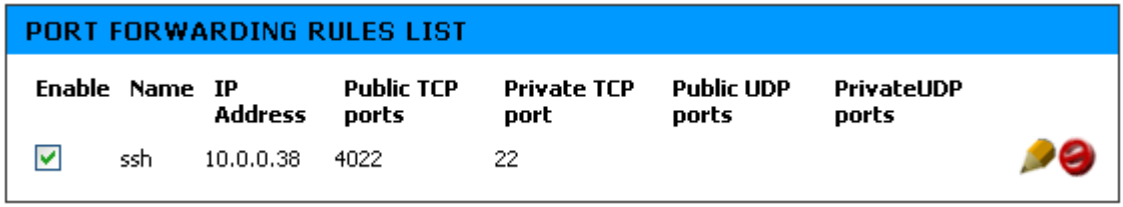
Exemples :

Public UDP Ports	Private UDP Port	Comportement du NAT
4000	22	Le port UDP public 4000 est redirigé sur le port UDP privé 22.
1000-1002	10-12	Les ports UDP publics 1000, 1001, 1002 sont redirigés respectivement sur les ports UDP privés 10, 11, 12.
68,18-20	100,200-202	Le port UDP public 68 est redirigé sur le port UDP privé 100. Et les ports UDP publics 18, 19, 20 sont redirigés respectivement sur les ports UDP privés 200, 201, 202.

Le bouton « Save » permet de valider l'ensemble des champs précédents. Une fois ce bouton appuyé, la règle s'ajoutera automatiquement à la liste des règles de redirection de port.

Le bouton « Cancel » permet de remettre les champs précédents à leur état par défaut. Cela permet aussi d'annuler la modification d'une règle.

La liste des règles de redirection de port :



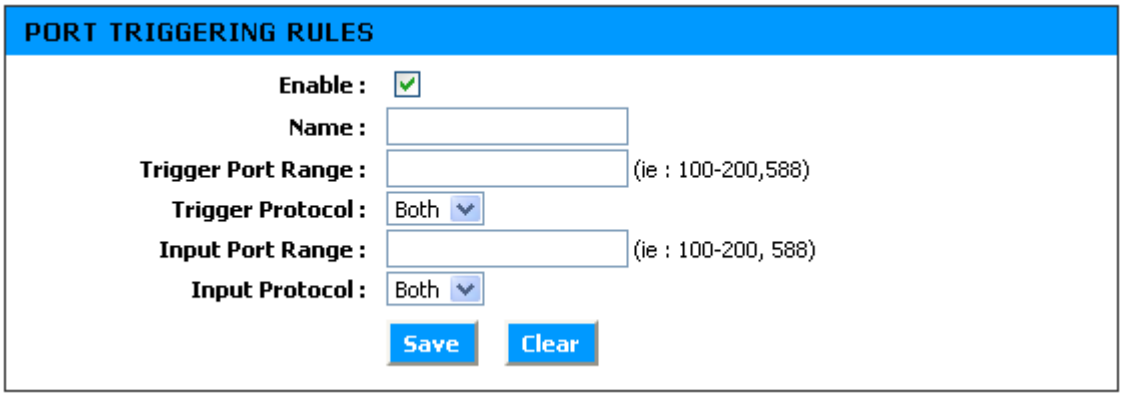
Cette liste permet de récapituler l'ensemble des règles de redirection de port. Les informations qui y sont présentées reprennent les paramètres entrés lors de l'édition de la règle.

Champ « Enable » : Si cette option est utilisée, elle permet d'activer la règle de redirection de port se trouvant sur cette ligne. Sinon cette règle ne sera prise en compte.

Déclenchement de port (Port Triggering) :

Cette fonctionnalité permet de faire une redirection de port dynamique et automatique. Le déclenchement est réalisé par une requête sur un port côté privé spécifique (Trigger Port Range) et va engendrer l'ouverture côté public (input port) d'un ou plusieurs ports.

Lorsque le port déclencheur est refermé, les ports ouverts du côté public seront fermés à la fin de leur communication.



Champ « Enable » : Si cette option est utilisée, elle permet d'activer les règles de déclenchement de port. Sinon aucune des règles établies ne sera prise en compte.

Champ « Name » : Contient le nom de règle. Ce nom nous permettra de retrouver facilement la règle dans la liste des règles de déclenchement de port.

Champ « Trigger port Range » : Contient le ou les ports privés qui déclencheront l'ouverture des ports publics. Il est possible de spécifier plusieurs ports ou plage de port en les séparant par des virgules.

Champ « Trigger Protocol » : Permet de choisir si le port défini par **« Trigger port Range »** est un port UDP, TCP ou bien les deux.

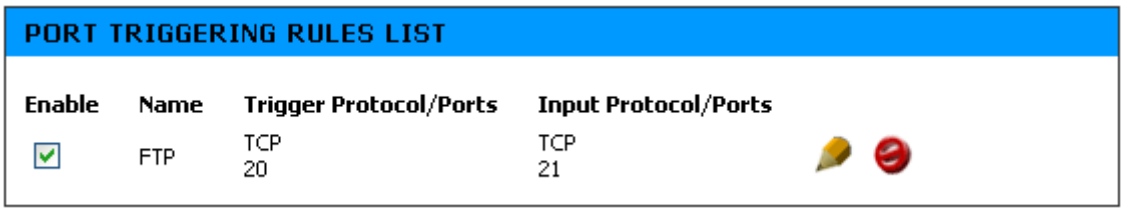
Champ « Input port Range » : Contient le ou les ports publics qui seront ouverts. Il est possible de spécifier plusieurs ports ou plage de ports en les séparant par des virgules.

Champ « Input Protocol » : Permet de choisir si le port défini par **« Input port Range »** est un port UDP, TCP ou bien les deux.

Le bouton « Save » permet valider l'ensemble des champs précédents. Une fois ce bouton appuyé, la règle s'ajoutera automatiquement à la liste des règles de déclenchement de port.

Le bouton « Cancel » permet de remettre les champs précédents à leur état par défaut. Cela permet aussi d'annuler la modification d'une règle.

La liste des règles de déclenchement de port :



Cette liste permet de récapituler l'ensemble des règles de déclenchement de port. Les informations qui y sont présentées reprennent les paramètres entrés lors de l'édition de la règle.

Champ « Enable » : Si cette option est utilisée, elle permet d'activer la règle de déclenchement de port se trouvant sur cette ligne. Sinon cette règle ne sera pas prise en compte.

IV.8 Utilisation de la C-KEY

Pour savoir si votre produit peut être équipé d'une C-KEY reportez-vous à la documentation fournie avec votre produit.

La C-KEY est une unité optionnelle de sauvegarde de la configuration du produit. Elle ne doit être ôtée ou insérée que lorsque le produit est hors tension.

IV.8.1 Installation de votre C-KEY

Pour ôter la C-KEY, dévissez les deux vis latérales puis tirez verticalement la C-KEY pour l'extraire du boîtier. Vous pouvez, au besoin, vous aider d'un tournevis en faisant doucement levier dans les encoches prévues à cet effet à la base des colonnettes de fixation.

Pour monter une nouvelle C-Key, assurez-vous que le méplat est bien orienté vers l'arrière du boîtier, puis insérez-la verticalement dans l'ouverture, sans forcer, et vissez.

NOTE : Les produits sont livrés sans C-KEY (sauf si vous commandez un produit avec l'option). Vous trouverez un cache que vous devez ôter de la même manière qu'une C-KEY.

IV.8.2 Utilisation de votre C-KEY

Écriture de la configuration dans la C-KEY

La configuration est écrite automatiquement dans la C-KEY lors de la sauvegarde des paramètres par SNMP ou HTTP.

La configuration est écrite automatiquement dans la C-KEY uniquement si la configuration contenue dans la C-KEY est compatible avec votre produit et que l'intégrité des données est correcte. Dans les autres cas il est nécessaire de passer par l'interface de gestion pour forcer l'écriture dans la C-KEY.

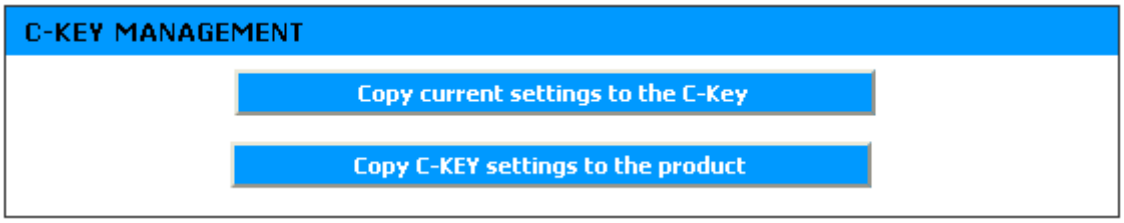
Utilisation de la configuration stockée :

Au démarrage, lorsque la C-KEY est détectée, si la configuration contenue est intègre et compatible avec votre produit, le produit démarrera automatiquement avec la configuration de la C-KEY sans effacer la configuration interne du produit.

Si la configuration ne concerne pas un produit compatible avec le vôtre ou que l'intégrité des données n'est pas correcte, le produit ignorera le contenu de la C-KEY et démarrera sur la configuration interne du produit.

Interface de gestion

L'interface de gestion contient une page permettant de gérer la configuration contenue dans la C-KEY.
Cette page est accessible via le menu « Advanced C-KEY ».



Copy C-KEY settings to the product

Ce bouton permet de copier la configuration de la C-KEY dans votre produit.

Copy current settings to the C-KEY

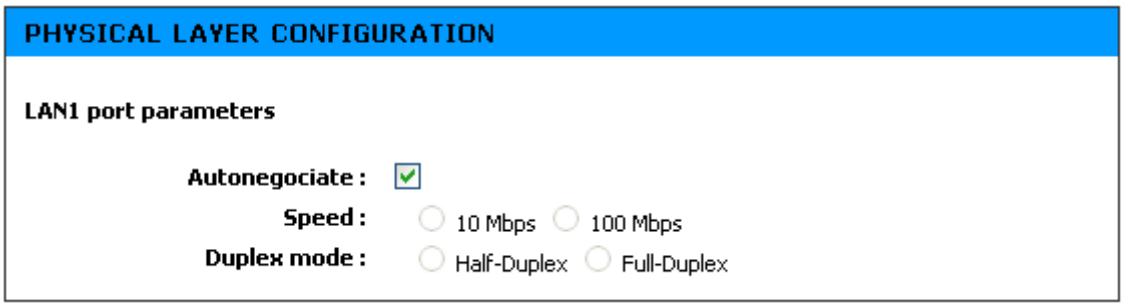
Cette opération permet de remplacer le contenu de la C-KEY par la configuration interne du produit.

IV.9 Configuration avancée des interfaces Ethernet

Depuis la version 4.2.0 il est possible d'accéder à un paramétrage avancé de l'interface LAN du produit. Ces paramètres sont accessibles dans l'onglet « Advanced Ethernet » du menu « Advanced »

Suivant la gamme de votre produit, deux pages sont disponibles.

Pour un produit de la gamme WLg-LINK :

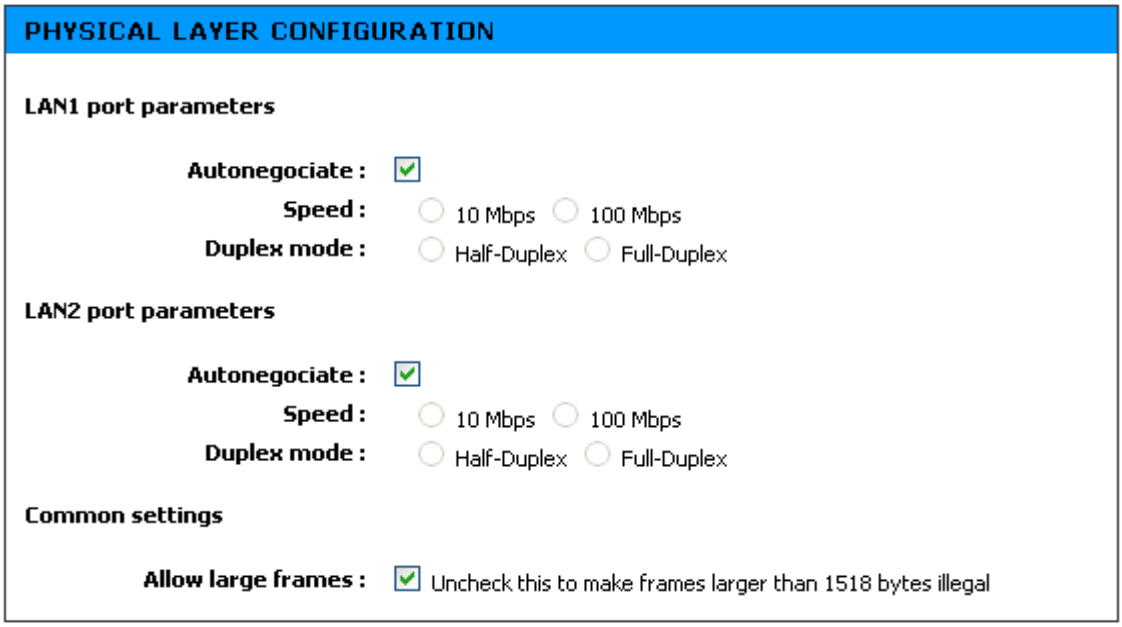


Champ « Autonegociate » : Par défaut cette option est activée et permet de détecter automatiquement la vitesse de la communication ainsi que le mode duplex.

Champ « Speed » : permet de choisir la vitesse de l'interface ethernet (10Mbps ou 100Mbps).

Champ « Duplex mode » : permet de choisir le mode half-duplex ou full-duplex pour l'interface ethernet.

Pour un produit de la gamme WLg-ABOARD :



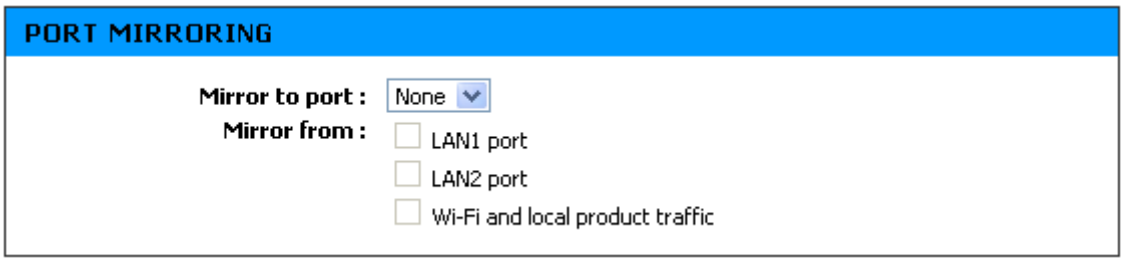
Champ « Autonegociate » : Par défaut cette option est activée et permet de détecter automatiquement la vitesse de la communication ainsi que le mode duplex.

Champ « Speed » : permet de choisir la vitesse de l'interface ethernet (10Mbps ou 100Mbps).

Champ « Duplex mode » : permet de choisir le mode half-duplex ou full-duplex pour l'interface ethernet.

Champ « Allow large frames » : permet (si coché) d'autoriser les trames de plus de 1518 octets. La taille maximum des trames sera alors de 1540 octets. Si cette option est désactivée, les trames de plus de 1518 octets seront considérées comme invalides.

Les produits équipés de deux ports LAN (ou plus) sont équipés de la technologie « Port mirroring » qui permet de dupliquer le trafic d'une interface ethernet vers une autre. La configuration du port mirroring est paramétrable à partir du menu « Advanced ethernet » :



Champ « Mirror to port » : ce champ détermine l'interface ethernet vers laquelle le flux ethernet dupliqué sera envoyé.

Champ « Mirror from » : ce champ détermine l'interface ethernet source.

IV.10 Établir une liaison Wi-Fi sur une distance supérieure à 1 km

Il est tout à fait possible d'établir des liaisons Wi-Fi sur plusieurs kilomètres en prenant certaines précautions :

- Les antennes doivent être placées en vue l'une de l'autre et face à face. Cela veut dire qu'aucun obstacle ne doit se trouver entre les deux antennes (Un arbre, une butte, un bâtiment, etc.) voir ci-dessous.

  « En vue » signifie réellement visible pour un humain. Les ondes Wi-Fi se propagent comme la lumière visible (en ligne droite), et même **moins bien** quand elles traversent des matériaux transparents.

- Vous devez augmenter la PIRE de votre produit (Attention à respecter la réglementation en vigueur dans votre région).
- Placez les antennes au-dessus de tout obstacle.
- Le RSSI de la liaison ne doit pas être trop bas, sinon vous pourriez perdre le lien lors de mauvaises conditions climatiques (Pluie, vent…)

Note :

Pour augmenter la PIRE de votre produit vous pouvez :

Utiliser une antenne avec un plus fort gain,

et / ou

Utiliser un produit avec une puissance radio plus importante.

Exemple d'installation

Produit à vue (On voit le haut du mât sur lequel est installé le produit)

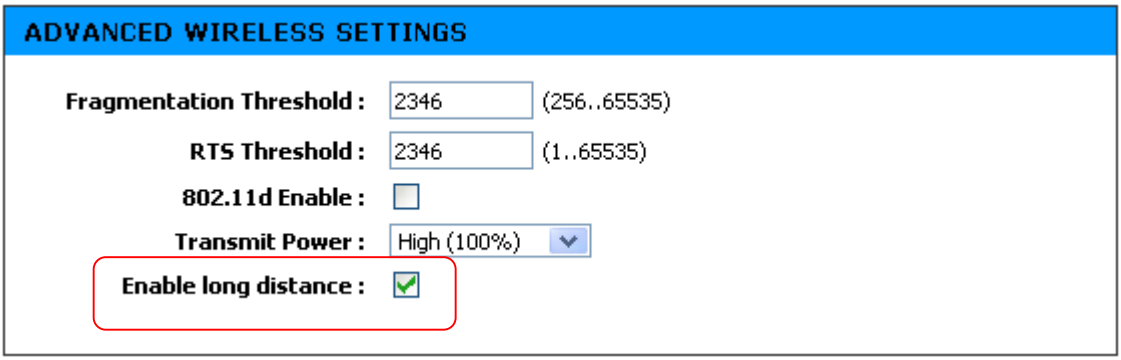
Produit pas à vue (on ne voit pas l'autre produit)

IV.11 Configuration de la distance

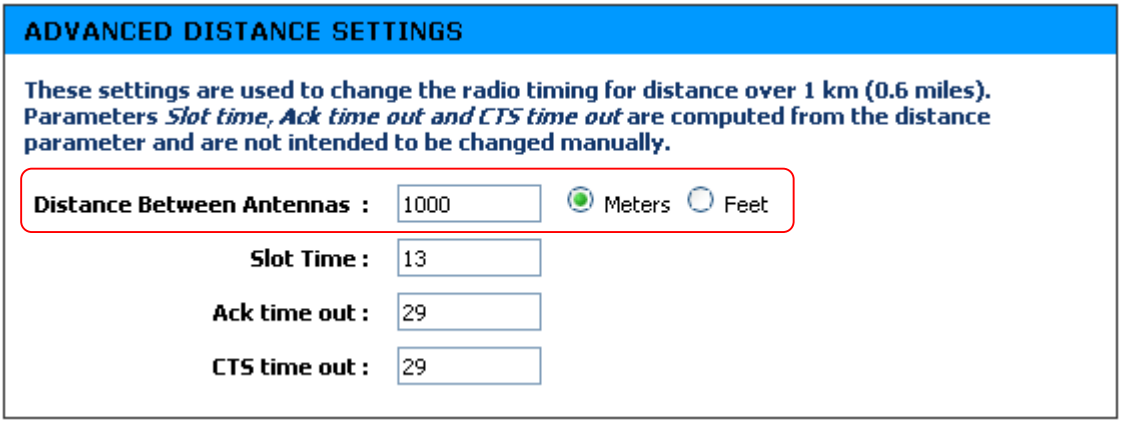
Les valeurs standard utilisées par le Wi-Fi permettent une communication jusqu'à une distance de 1 km. Passée cette distance, le délai de propagation entre les deux points (Le point d'accès et le bridge par exemple) ne permet plus de tenir une bande passante optimale.

Il est possible d'utiliser nos produits au-delà de 1 km et jusqu'à 5 km en configurant le paramètre distance dans l'interface WEB.

Dans la page « Advanced Wireless »



Cochez le paramètre « Enable long distance » pour faire apparaître les paramètres de configuration.



Utilisez le paramètre « Distance between Antennas » pour configurer la distance qui se trouve entre vos produits.
Ne touchez pas aux autres paramètres (Slot Time, Ack Time out, CTS time) sans avoir bien compris les conséquences que cela aura sur le protocole Wi-Fi. Ils sont calculés automatiquement par le paramètre distance.

La modification du paramètre distance ne change pas la puissance de sortie du produit. Seuls les paramètres temporels du Wi-Fi sont changés.

IV.12 Configuration du 802.11d

Le 802.11d permet à une station de paramétrer automatiquement les canaux utilisables et la puissance maximum autorisée dans la région du point d'accès.

Pour cela, cette fonction doit être activée dans le point d'accès et dans la station.

IV.12.1 Paramétrage dans la station

Dans la section « *advanced wireless settings* » de la page Advanced wireless cocher la case « 802.11d Enable »

IV.12.2 Paramétrage dans le point d'accès

Dans la section « *advanced wireless settings* » de la page Advanced wireless cocher la case « 802.11d Enable »

IV.13 Configuration du Lan Time-out

Cette fonction n'est disponible que dans le mode point d'accès.

Elle permet de désactiver le point d'accès Wi-Fi si on détecte que le lien LAN ne fonctionne plus.

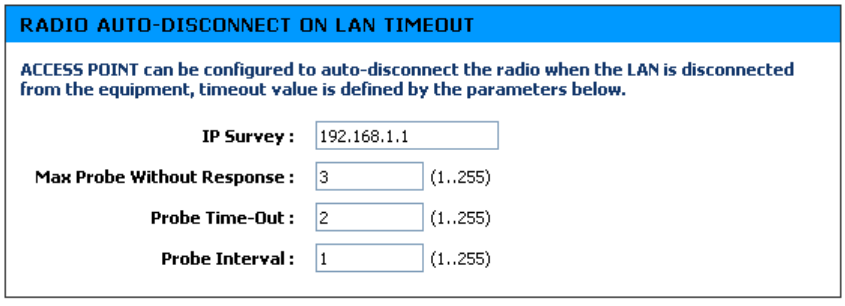
Pour cela on envoie des pings à intervalle régulier vers une machine.
Tant qu'elle répond l'interface Wi-Fi de votre point d'accès est active. Si elle ne répond plus, l'interface Wi-Fi est désactivée.

Cela permet de gérer la redondance des points d'accès Wi-Fi dans une cellule.

IV.13.1 Configuration du Lan time-out

Pour activer cette fonction dans la section « *advanced wireless settings* » de la page Advanced wireless cocher la case « Enable LAN Time-Out »

Une fois la fonction activée, le cadre « *RADIO AUTO-DISCONNECT ON LAN TIMEOUT* » s'affiche dans la même page.



IP Survey : Ce champ permet de configurer l'adresse IP à scruter sur le LAN.

Max probe Without response : Ce champ indique le nombre de pings consécutifs sans réponse qui provoqueront la désactivation de l'interface Wi-Fi.
Valeur par défaut : 3

Probe Time-Out : Ce champ permet de configurer le temps en secondes pendant lequel on attend la réponse au ping envoyé.
Valeur par défaut : 2

Probe Interval : Ce champ permet de configurer l'intervalle de temps entre deux émissions de ping.
Valeur par défaut 1

Le time-out sur l'interface LAN est donnée par :
Max Probe * (Probe Time-Out + Probe Interval)

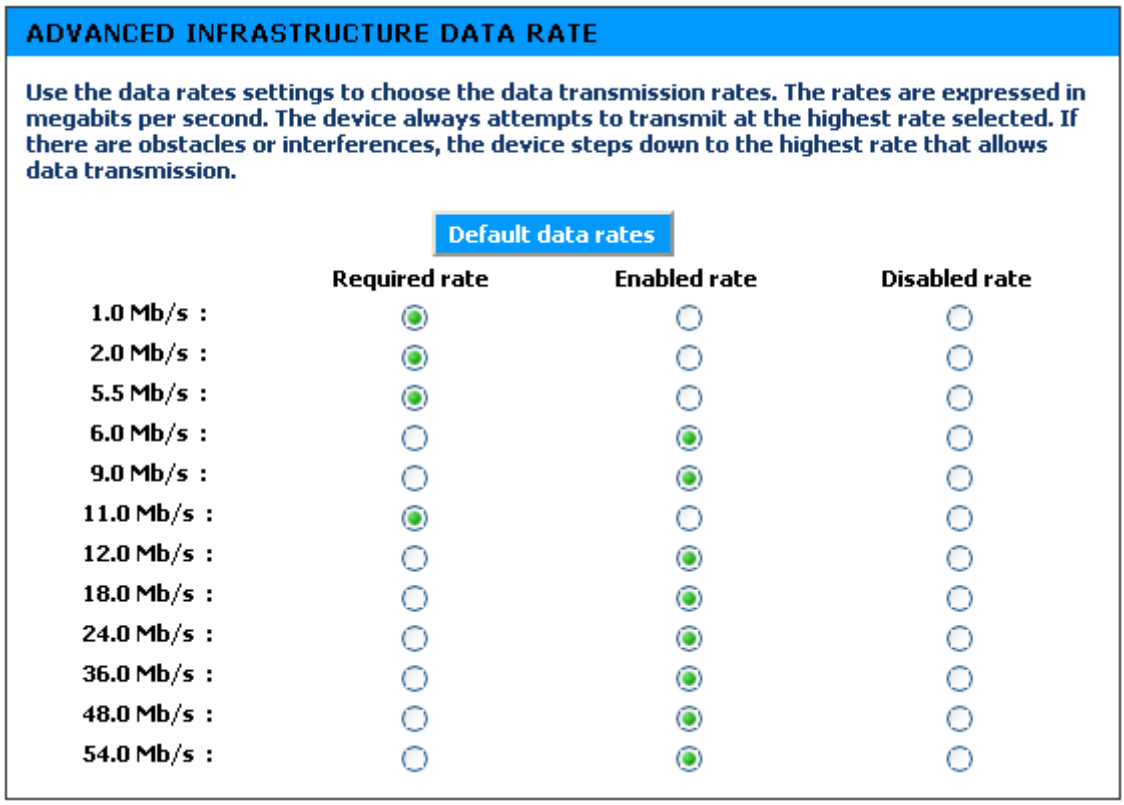
Ce qui donne une valeur par défaut de 6 secondes.

IV.14 Gestion des vitesses de transmission

Cette fonction n'est disponible que dans le mode point d'accès.

Il est possible de sélectionner les vitesses utilisables dans la cellule radio. Toutes les stations associées avec votre point d'accès, utiliseront ces vitesses.

Le menu « *Advanced Wireless* » permet de configurer les vitesses de transmission.



Required rate : Les vitesses sélectionnées dans cette colonne, doivent être supportées par les stations. Si ce n'est pas le cas, elles ne pourront pas s'associer avec votre point d'accès.
Vous devez sélectionner au moins une vitesse dans cette colonne.
La vitesse la plus faible sélectionnée servira à transmettre les trames du protocole Wi-Fi ainsi que les trames multicast et broadcast.

Enable rate : Les vitesses sélectionnées dans cette colonne sont utilisables par les stations si elles les supportent.

Disabled rate : Les vitesses sélectionnées dans cette colonne, ne seront pas utilisées par les stations.

Default data rates : Configure les valeurs par défaut correspondant à votre mode 802.11.

Si dans la liste « *Required rate* » vous ne sélectionnez pas les vitesses les plus faibles, vous réduisez la portée de votre point d'accès.

Les vitesses 11, 5.5, 2 et 1 Mb/s ne sont pas disponible dans les modes 802.11a.

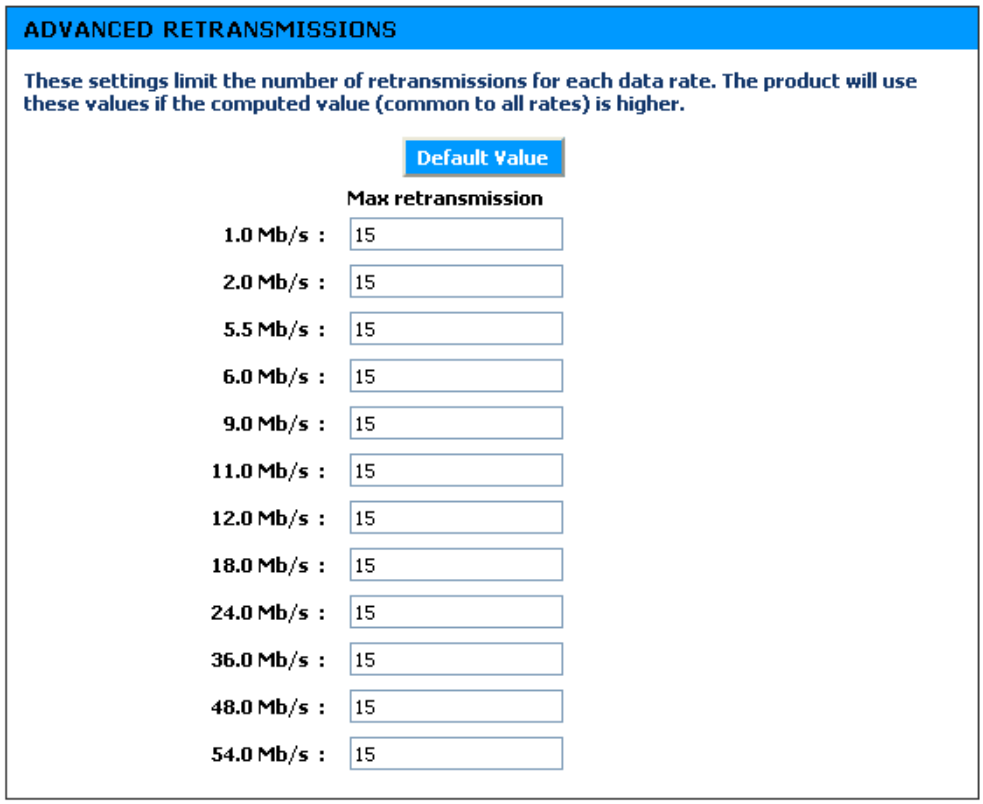
IV.15 Gestion des retransmissions

Cette fonction n'est disponible que dans le mode bridge.

Dans le protocole Wi-Fi, toute trame de données émise doit être acquittée par le destinataire. A défaut, l'expéditeur va la retransmettre plusieurs fois à la vitesse actuellement utilisée.
Après plusieurs tentatives infructueuses à la vitesses maximale permise, l'expéditeur va retransmettre en utilisant des vitesses de plus en plus faibles.
Ce mécanisme permet la communication même en cas de conditions radio fluctuantes, mais il peut engendrer des retards non déterministes dans la transmission des données, qui peuvent être néfastes dans le cas du roaming.

Par défaut votre produit va tester jusqu'à 4 vitesses différentes et fera au maximum 15 retransmissions par vitesse. Le nombre de retransmissions par vitesse sera automatiquement diminué si vous avez un bon niveau de signal.

Ce mécanisme garantit un faible taux d'échec de transmission, mais peut induire de la latence dans la communication.
Si vous réduisez le nombre maximum de retransmissions vous risquez de réduire la fiabilité de la transmission.



Pour chaque vitesse vous pouvez saisir la valeur maximum du nombre de retransmissions que vous souhaitez avoir.

Le bouton « *Default value* » remet les valeurs d'usine pour toutes les vitesses.

IV.16 Gestion des alarmes

Cette fonction n'est disponible que sur les produits disposant d'un contact d'alarme.

Plusieurs sources d'alarme sont disponibles dans votre produit :

- Perte de l'une des deux alimentations (si vous utilisez deux sources d'alimentation électrique).
- Perte de l'un des liens Ethernet (Le nombre de sources disponibles dépend du nombre de ports Ethernet sur votre produit).

Chaque source peut être gérée dans deux modes :

- ✓ **Reset automatique** : La source d'alarme est valide uniquement pendant le défaut.
- ✓ **Reset manuel** : La source d'alarme reste valide après la disparition du défaut. Une intervention manuelle sur la page « Status → Alarm » est nécessaire pour dévalider la source d'alarme.

Chaque source d'alarme peut être

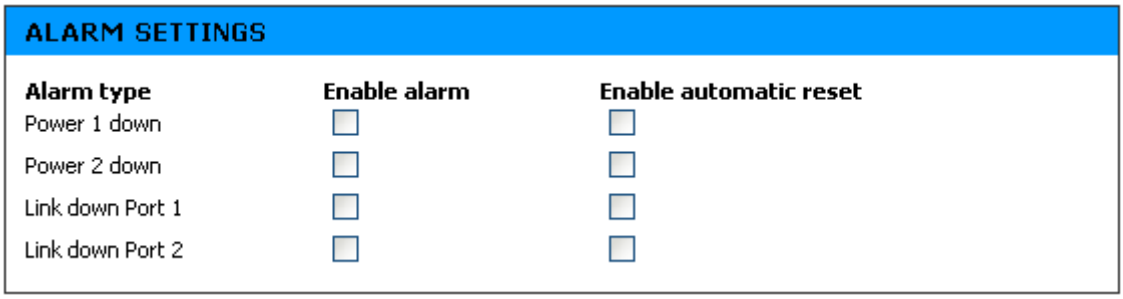
- ✓ Activée ou inhibée individuellement.
- ✓ Configurée en mode reset automatique ou en mode reset manuel.

Le contact d'alarme est fermé dans chacune des conditions suivantes :

- ✓ Produit en cours de démarrage
- ✓ Produit hors service
- ✓ Au moins une source d'alarme valide

Le contact d'alarme est ouvert quand les conditions suivantes sont réunies :

- ✓ Produit opérationnel
- ✓ Aucune source d'alarme valide



Enable alarm : Active ou désactive la source d'alarme.

Enable automatic reset : si vous cochez la case correspondante à une source, elle sera gérée en mode reset automatique. Sinon la source d'alarme sera gérée en mode reset manuel.

IV.17 Gestion des VLAN

Cette fonction n'est disponible que sur le produit disposant d'un switch manageable.

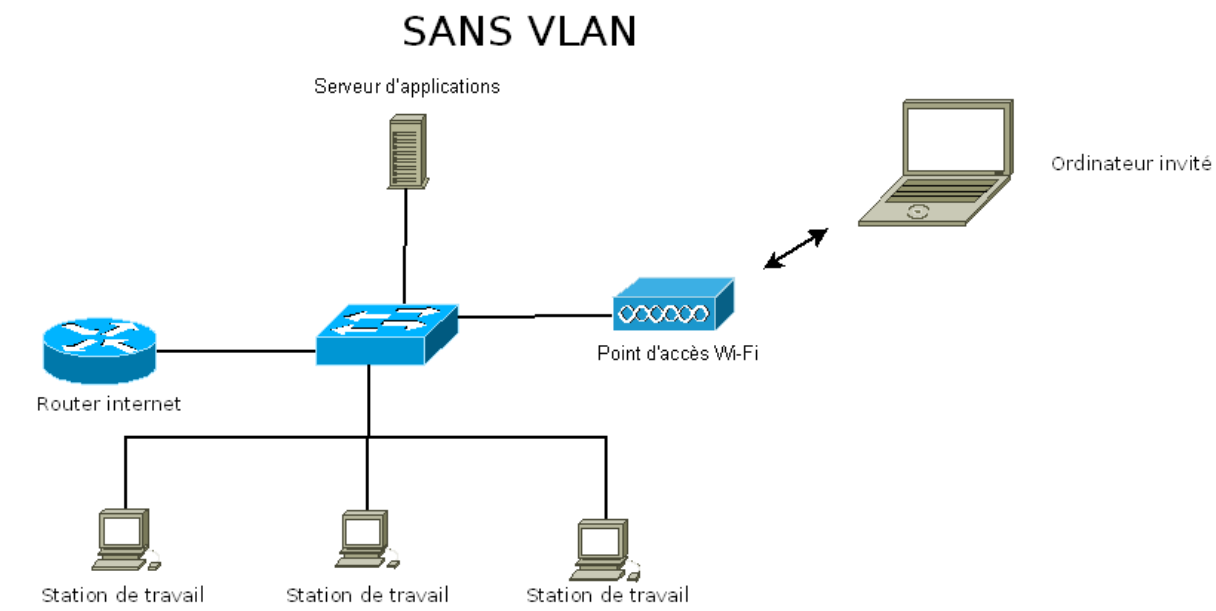
IV.17.1 Introduction aux VLAN

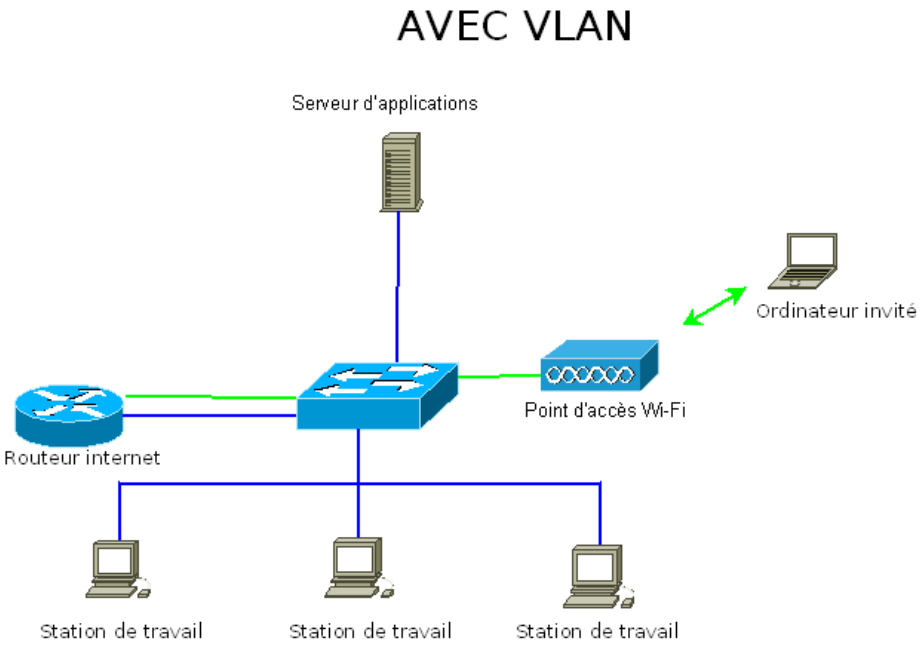
Un **VLAN** (*Virtual Local Area Network* ou *Virtual LAN*, en français *Réseau Local Virtuel*) est un réseau local regroupant un ensemble de machines de façon logique et non physique.
En effet dans un réseau local, la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels (VLANs) il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage...) en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc.).

Les VLAN compatibles avec le standard 802.1q fonctionnent grâce à l'insertion d'un tag de 4 octets entre l'adresse MAC source et le type de trame. Ce tag permet de stocker l'identifiant du VLAN sur 12 bits (soit 4096 VLAN possibles).

Dans la figure ci-dessous :

- **Sans VLAN** : Tous les ordinateurs peuvent avoir accès à toutes les ressources du réseau (Serveur d'applications, routeur internet, stations de travail…).
- **Avec VLAN** : Les ordinateurs de chaque VLAN peuvent uniquement accéder aux ressources appartenant à leur VLAN.
    - **VLAN Vert** : L'ordinateur invité n'a pas accès au serveur d'applications, ni aux stations de travail, mais uniquement au routeur Internet.
    - **VLAN Bleu** : Les stations de travail ont accès au serveur d'applications et au routeur Internet, mais ne peuvent pas accéder à l'ordinateur invité.





IV.17.2 Typologie des VLAN

Plusieurs types de VLAN sont définis, selon le critère de commutation et le niveau auquel il s'effectue :

- **VLAN de niveau 1** : Définit un réseau virtuel en fonction des ports de raccordement sur le switch ;
- **VLAN de niveau 2** : Définit un réseau virtuel en fonction des adresses MAC des stations. Ce type de VLAN est beaucoup plus souple que le VLAN par port car le réseau est indépendant de la localisation de la station ;
- **VLAN de niveau 3** : On distingue plusieurs types de VLAN de niveau 3 :

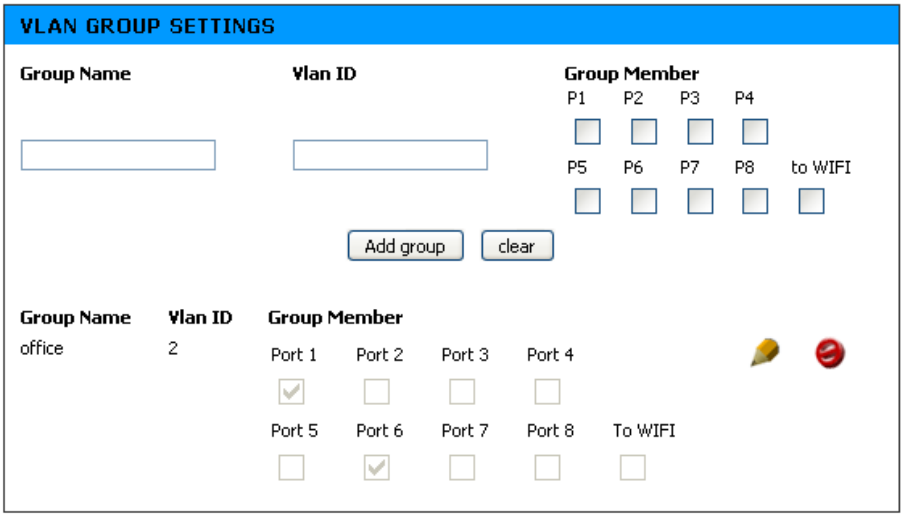
- **Le VLAN par sous-réseau** : Associe des sous-réseaux selon l'adresse IP source des datagrammes. Ce type de solution apporte une grande souplesse dans la mesure où la configuration des commutateurs se modifie automatiquement en cas de déplacement d'une station. En contrepartie une légère dégradation de performances peut se faire sentir dans la mesure où les informations contenues dans les paquets doivent être analysées plus finement.
- **Le VLAN par protocole** : Regroupe toutes les machines utilisant le même protocole au sein d'un même réseau.

IV.17.3 Configuration des VLAN

Votre produit supporte les VLAN 802.1q de niveau 1.
L'affectation des VLAN sera faite en fonction des ports Ethernet.

Le menu Basic → VLAN vous permet de configurer jusqu'à 64 VLAN.

IV.17.4 Configuration des groupes de VLAN

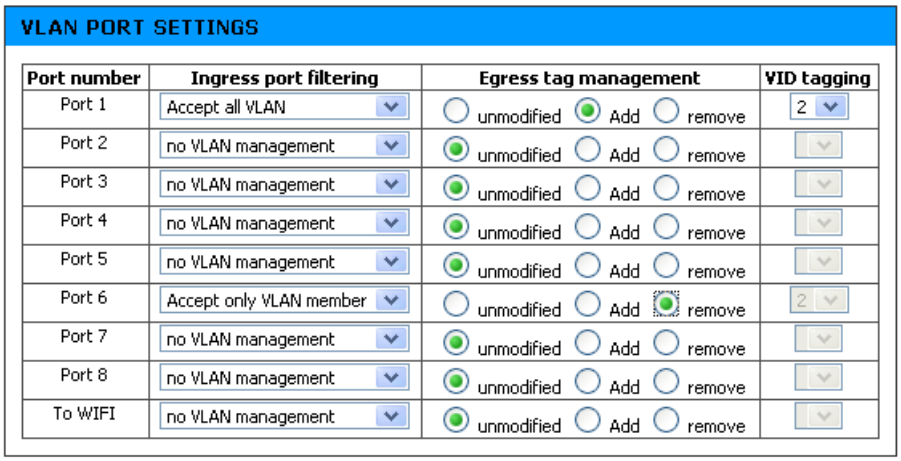


Chaque VLAN doit faire partie d'un groupe. Pour chaque groupe vous devez spécifier :

Group Name : Le nom du groupe.
Vlan ID : La liste des numéros de VLAN composant le groupe. Par exemple :
2 ;3 ;4 : Ce groupe va gérer les VLAN numéro 2,3 et 4
2-5 : Ce groupe va gérer les VLAN numéro 2,3,4, et 5.
Il est possible de mixer les deux notations.
2 ;3 ;4 ;6-10 : Ce groupe va gérer les VLAN numéro 2,3,4,6,7,8,9 et 10.
Group Member : Les ports faisant partie du groupe. Seul les ports faisant partie de ce groupe pourront transmettre des trames de ce VLAN.

Cliquez sur le bouton « Add group » pour ajouter votre groupe à la liste.
Cliquez sur pour éditer le groupe correspondant.
Cliquez sur pour effacer le groupe correspondant.

IV.17.5 Configuration des VLAN par port



Après avoir saisi des groupes de ports, vous pouvez gérer la configuration des VLAN par port.
Pour chaque port vous devez configurer :

Ingress port filtering : Permet de filtrer les trames reçues sur ce port.
- No VLAN management : Les VLAN ne sont pas gérés, les trames contenant un tag seront détruites
- Accept all VLAN : Ce port acceptera tous les VLAN ID.
- Accept only VLAN members : Ce port acceptera seulement les VLAN ID faisant partie des groupes configuré pour ce port.

Egress tag management : Permet de gérer le tag pour les trames émises.
- Unmodified : Les trames ne sont pas modifiées.
- Add : Si la trame ne contient pas déjà un tag VLAN, on en ajoute un avec un VLAN ID égal au champ « VID tagging ».
- Remove : Si la trame contient un tag il sera supprimé.

VID tagging : Le VLAN ID à utiliser lors de l'ajout du tag dans la trame.

IV.18 Configuration du QOS

Cette fonction n'est disponible que sur le produit disposant d'un switch manageable.

IV.18.1 Introduction au QOS

Le QOS (Quality of Service) permet de hiérarchiser les données sur un réseau Ethernet. Par défaut, sur un réseau Ethernet tous les paquets on le même niveau de priorité, et ils seront traités dans l'ordre d'arrivée.
Avec les mécanismes de QOS les flux entrants vont être classés dans des files d'attente différentes en fonction de la priorité de chaque trame. Les files d'attente vont être organisées afin de permettre aux paquets les plus prioritaires d'être traités avant les moins prioritaires.

Deux méthodes sont couramment utilisées pour gérer le QOS.

- Par le tag 802.1q : Dans ce tag ajouté à la trame Ethernet, un champ est réservé pour stocker la priorité de la trame. La norme 802.1p définit 7 niveaux de priorité utilisables dans le tag. L'avantage de cette méthode est qu'elle n'est pas liée au protocole de niveau 3.
- Par le TOS / DSCP : Il s'agit d'un champ se trouvant dans l'entête de la trame IP. Ce champ permet de stocker la priorité de la trame. Avec cette méthode on peut définir 64 niveaux de priorité.

IV.18.2 Typologie du QOS

Plusieurs types de QOS sont définis, selon le niveau auquel il s'effectue :

- **QOS de niveau 2** : La priorité de la trame est définie par le port sur lequel la trame est reçue. La priorité est stockée dans le tag 802.1q. La norme 802.1p définit 7 niveaux de priorité.
- **QOS de niveau 3** : La priorité de la trame est définie en fonction du service utilisé (port, UDP, TCP). Elle est stockée dans le champ DSCP / TOS de la trame IP. Le nombre de bits réservés dans la trame IP permet la gestion de 64 niveaux de priorité.

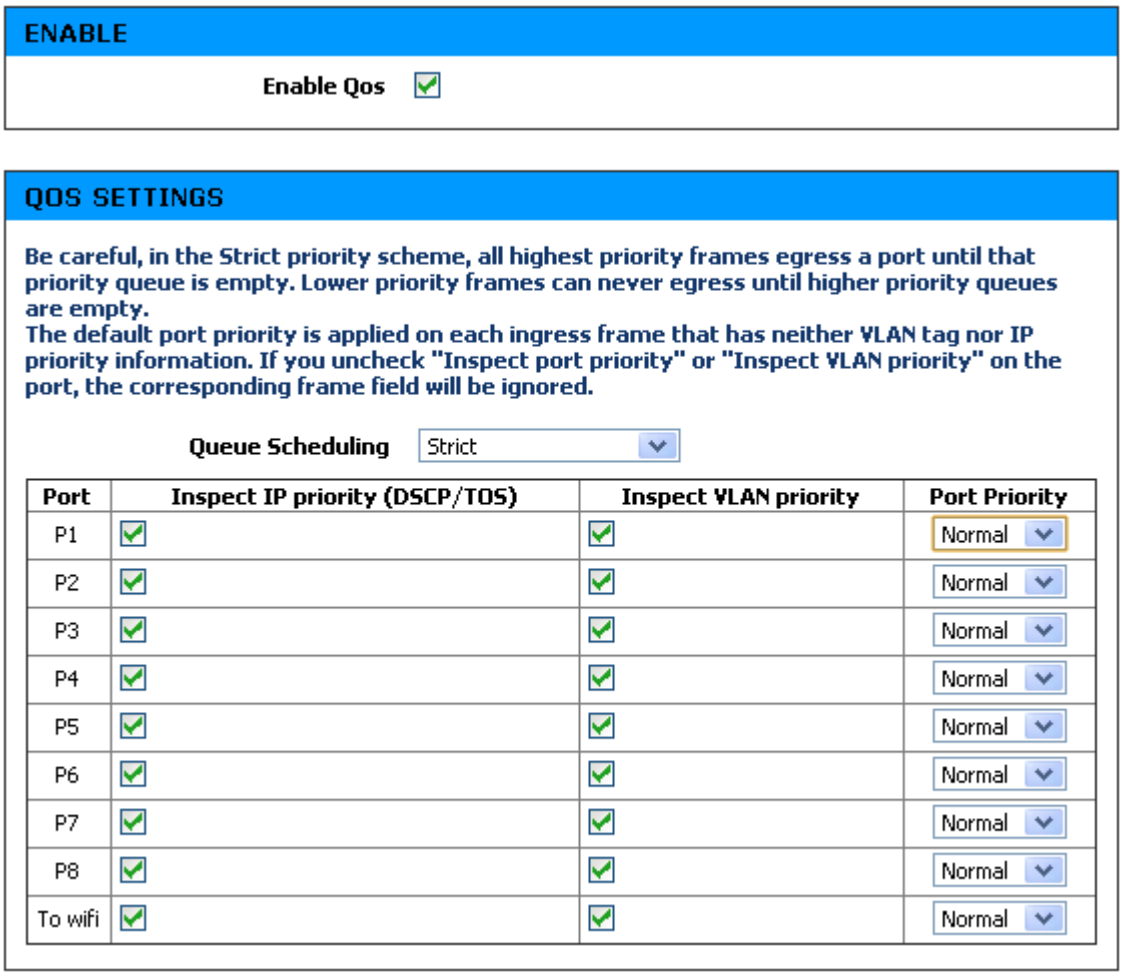
IV.18.3 Configuration du QOS

Votre produit supporte le QOS de niveau 2 et 3 pour les trames dont le niveau de priorité est déjà défini.
Si aucun niveau de priorité n'est défini dans la trame, vous pouvez lui en associer un par défaut en fonction du port sur lequel la trame sera reçue.

Votre produit supporte 4 files d'attentes par port Ethernet. Il est possible dans le menu Advanced → QOS, de gérer la relation entre :

- Les 7 niveaux définis dans la norme 802.1p et les 4 files d'attente.
- Les 64 niveaux définis dans le champ DSCP / TOS et les 4 files d'attente

La configuration du QOS se trouve dans le menu Basic → QOS.



Enable Qos : Active ou désactive la fonction QOS.

Queue scheduling : Permet de choisir la façon dont les files d'attente vont être régies :

Strict : Ce mode traite toujours la trame de plus forte priorité en premier. Ceci assure que le trafic de forte priorité est bien servi, par contre le trafic de plus faible priorité peut ne jamais être traité.

Weight fair : Dans ce mode la priorité des files d'attente sera flottante. Ceci garantit que tous les niveaux de priorité seront traités, mais on augmentera la latence du trafic prioritaire.

Les autres paramètres définissent port par port le mode de gestion du QOS.

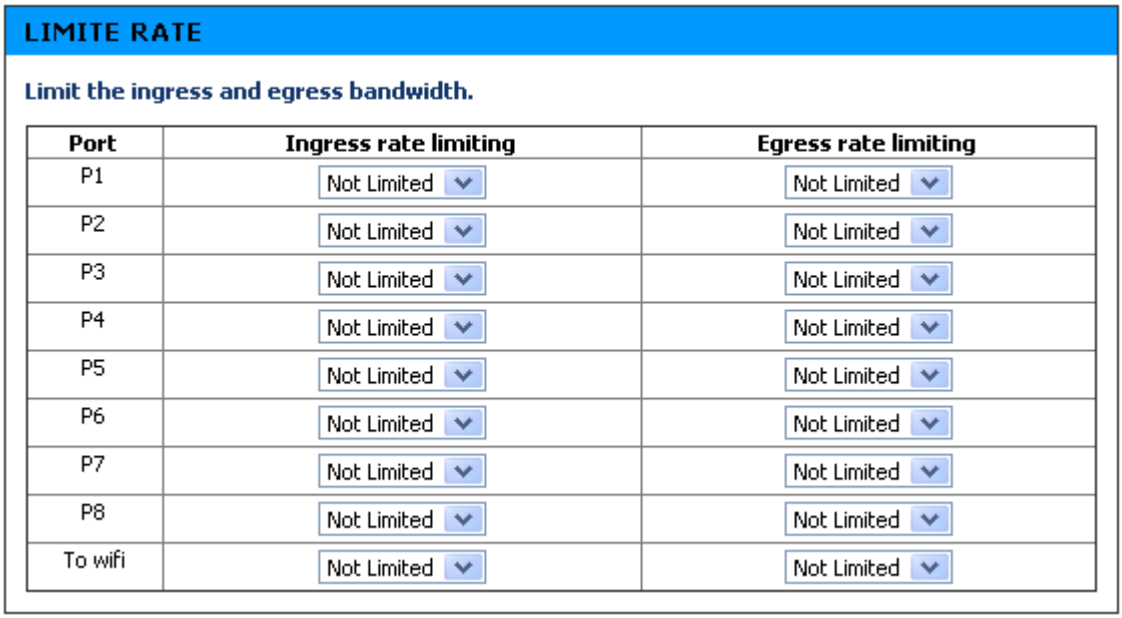
Inspect IP priority (DSCP / TOS) : Si cette option est cochée, la valeur du champ DSCP / TOS de la trame sera prise en compte.
Inspect VLAN priority : Si cette option est cochée, la valeur du champ QOS contenu dans le tag 802.1q sera prise en compte.
Port Priority : Permet de définir la priorité d'un port. Cette priorité sera appliquée aux trames ne contenant pas d'informations de priorité. L'information de priorité ne sera pas écrite dans la trame. Pour écrire l'information de priorité dans le tag 802.1q il faut administrer le VLAN QOS qui à été créé automatiquement dans le menu Basic / VLAN.

IV.19 Configuration de la limitation de bande passante

Cette fonction n'est disponible que sur le produit disposant d'un switch manageable.

Il est possible de limiter la bande passante entrante et sortante des ports Ethernet.

La configuration de la limitation de bande passante se trouve dans le menu Basic / QOS.



Pour chaque port vous pouvez limiter la bande passante entrante et sortante.

Ingress rate limiting : Permet de limiter la bande passante entrante d'un port.
Egress rate limiting : Permet de limiter la bande passante sortant d'un port.

Pour la bande passante entrante ou sortante vous pouvez choisir entre :

Not limited : La bande passante n'est pas limitée
128 Kbps : La bande passante est limitée à 128 Kbit/s
256 Kbps : La bande passante est limitée à 256 Kbit/s
512 Kbps : La bande passante est limitée à 512 Kbit/s
1 Mbps : La bande passante est limitée à 1 Mbit/s
2 Mbps : La bande passante est limitée à 2 Mbit/s
4 Mbps : La bande passante est limitée à 4 Mbit/s
8 Mbps : La bande passante est limitée à 8 Mbit/s

V L'ADMINISTRATION PAR SNMP

Le protocole SNMP définit le dialogue entre une station de management et un agent SNMP pour :

- Connaître l'état du produit
- Configurer le produit
- Gérer les événements exceptionnels

Votre produit intègre un agent SNMP V2c à partir de la version 4.2.0. Cet agent est néanmoins capable de gérer les requêtes des clients SNMP V1. Le choix de la version du protocole est réalisé de manière automatique par le produit.

En effet, si une requête SNMP V2c valide est reçue par le produit, la trame de réponse sera une trame SNMP V2c.

De la même manière, si une requête SNMP V1 valide est reçue par le produit, la trame de réponse sera une trame SNMP V1.

Il vous est aussi donné la possibilité de générer des traps SNMP V2c ou SNMP V1.

V.1 La MIB SNMP

D'une façon générale, un agent intègre une ou plusieurs MIB.
La MIB est une arborescence dans laquelle on va pouvoir lire ou écrire des informations afin de pouvoir surveiller ou configurer l'agent. Le chemin dans l'arborescence conduisant à chaque valeur est codé sous une forme numérique qui est appelée OID.

Il existe deux MIB standardisées. La MIB II est la plus répandue.

Votre produit supporte les groupes suivants dans la MIB II :

- System, OID .1.3.6.1.2.1.1, permet d'avoir des informations sur le produit.
- IP, OID .1.3.6.1.2.1.4.20.1.4.2, permet d'avoir des informations sur les interfaces IP du produit.

Un agent SNMP peut également supporter une MIB spécifique nommée « MIB entreprise ».

L'OID de la « MIB entreprise » ACKSYS est : « **.1.3.6.1.4.1.28097** ». Vous trouverez le détail de cette MIB dans ce document.

Le fichier de MIB est joint sur le CDROM fourni avec votre produit. Il est également téléchargeable depuis notre site Internet.

V.2 Les communautés SNMP

La communauté SNMP est une chaîne de caractères fonctionnant comme un nom d'utilisateur / mot de passe. La communauté permet de limiter l'accès aux données pouvant être lues ou écrites par SNMP.

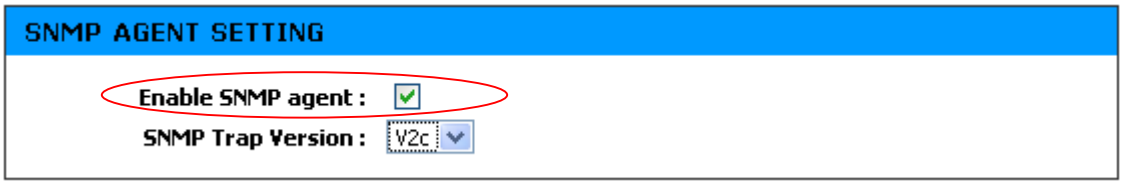
V.3 Les Traps SNMP

Les « traps » SNMP sont des messages émis par l'agent lors d'événements exceptionnels.
Les produits ACKSYS supportent les traps suivants :

- ColdStart : Permet de signaler le démarrage du produit.
- Linkdown : Permet de signaler une rupture du lien Wi-Fi avec le point d'accès (uniquement en mode bridge infrastructure).
- LinkUp : Permet de signaler un établissement du lien Wi-Fi avec le point d'accès (uniquement en mode bridge infrastructure).
- Power1 On : Permet de signaler la montée de l'alimentation (uniquement sur le WLg-ABOARD/N).
- Power1 Off : Permet de signaler la perte de l'alimentation (uniquement sur le WLg-ABOARD/N).
- Power2 On : Permet de signaler la montée de l'alimentation (uniquement sur le WLg-ABOARD/N).
- Power2 Off : Permet de signaler la perte de l'alimentation (uniquement sur le WLg-ABOARD/N).

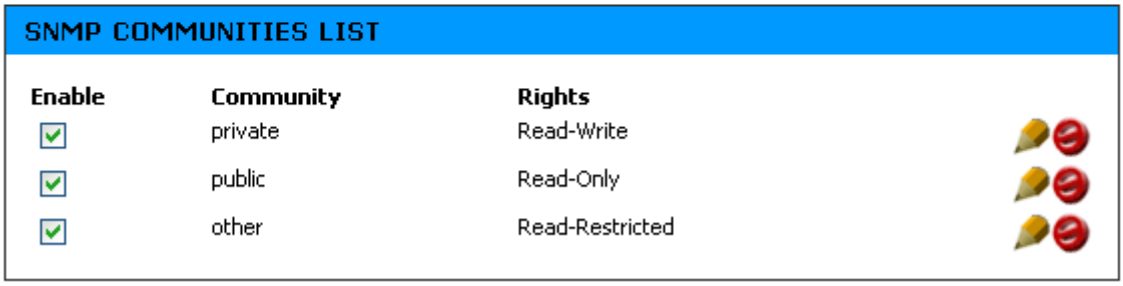
V.4 Le menu SNMP

Depuis la version 3.8.0 du firmware, l'agent SNMP est activé par défaut sur votre produit. Si la version de votre produit est inférieure à 2.2.0, vous pouvez activer l'agent SNMP en allant dans le menu « Basic » puis « SNMP », puis en cochant la case « Enable SNMP agent ».



V.5 Filtrage SNMP

Depuis la version 4.2.0 du firmware, il est possible de créer des communautés et d'y associer des droits. Pour cela il suffit d'utiliser le formulaire intitulé « SNMP communities setting ».



Ajouter une communauté :

Il suffit d'inscrire le nom de la communauté souhaité dans le champ « **Community Name** », de sélectionner le type de droit qui y sera associé. Et ensuite de cliquer sur le bouton save. Cette communauté sera alors directement ajoutée à la liste des communautés.

Il existe trois types de droits applicables à une communauté :

- Read Only : les membres de cette communauté ne seront pas autorisés à modifier les valeurs des OIDs de la MIB.
- Read Write : les membres de cette communauté pourront lire et modifier à leur guise les valeurs des OIDs de la MIB
- Read-Restricted : les membres de cette communauté ne seront pas autorisés à modifier les valeurs des OIDs de la MIB. Mais ne

pourront pas non plus lire les OIDs dit « sensibles » tel que les clés WEP ou WPA.

Pour chaque communauté, il est possible de spécifier une plage d'adresse IP autorisé. Le formulaire « **SNMP IP Filtering Rules** » permet de configurer cette fonctionnalité :

Pour associer une plage d'adresses IP, il faut :

- Choisir une communauté dans la liste déroulante « Community »
- Entrer le début de la plage d'adresses IP autorisée
- Entrer la fin de la plage d'adresses IP autorisée
- Cliquer sur save pour valider

Une fois le bouton save cliqué, la règle vient s'ajouter au à la liste disponible dans le cadre « SNMP IP filtering rules list ». Il est alors possible de supprimer la règle en cliquant sur l'icône « ». Il est aussi possible de l'éditer en cliquant sur l'icône « ».

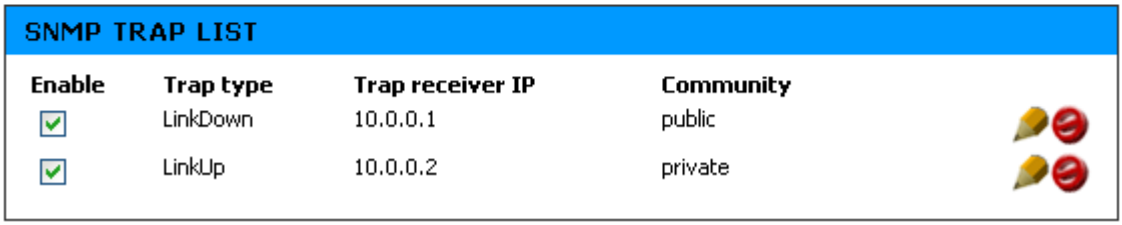
Si une requête SNMP arrive en provenance d'un appareil dont l'adresse IP ne figure dans aucune des règles, elle sera ignorée.

V.6 Gestion des traps

Pour configurer les traps, il faut aller dans le menu « Basic » puis « SNMP ».
Attention, l'agent SNMP doit avoir été activé au préalable.

Dans un premier temps, il est nécessaire de définir avec quelle version du protocole SNMP seront envoyés les traps. Pour cela il suffit de positionner la combo box « SNMP Trap Version » avec la valeur souhaitée :

Vous pouvez maintenant ajouter, supprimer et éditer des traps SNMP en utilisant le formulaire suivant :



Ajouter un trap

Renseigner ces paramètres dans la section « SNMP TRAP SETTING » de la page SNMP :

- Enable : décochez cette case si vous souhaitez désactiver ce trap
- Trap type : Le type de trap souhaité (ColdStart, Linkdown, LinkUp)
- Trap receiver IP : L'adresse IP de l'équipement qui doit recevoir le trap
- Community : La communauté de destination du trap

Une fois ces informations renseignées, cliquez sur le bouton save. Le nouveau trap est ajouté dans la section « SNMP TRAP LIST ».

Remarques :

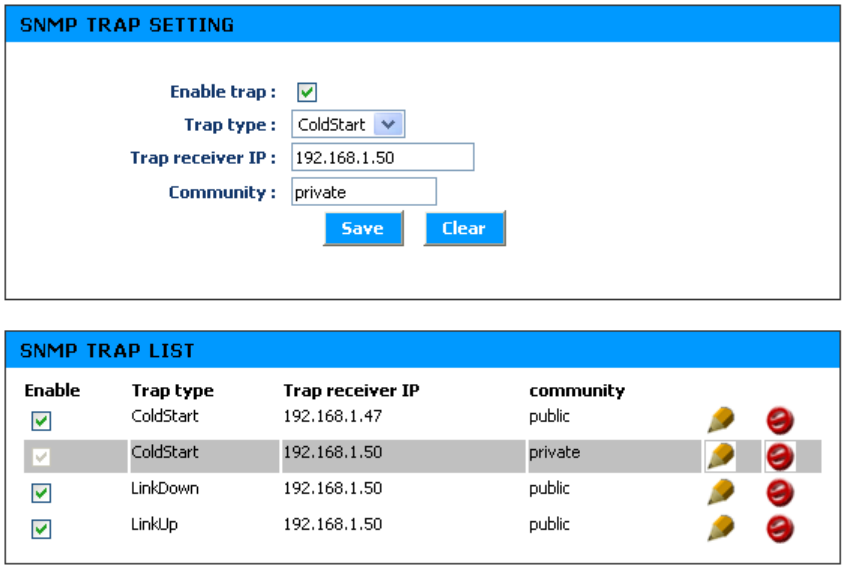
- Vous pouvez configurer un maximum de 5 traps.
- Vous pouvez configurer plusieurs fois le même trap.
- Tous les traps n'ont pas forcément la même adresse IP de destination.
- Tous les traps n'ont pas forcément la même communauté de destination.
- La communauté de destination peut être différente de la communauté de l'agent.

Supprimer un trap

Si vous souhaitez supprimer un trap dans la liste, cliquez sur l'icône « » du trap que vous souhaitez supprimer puis confirmez votre choix.

Modifier un trap

Si vous souhaitez modifier la configuration d'un trap, cliquez sur l'icône « » du trap que vous souhaitez modifier.



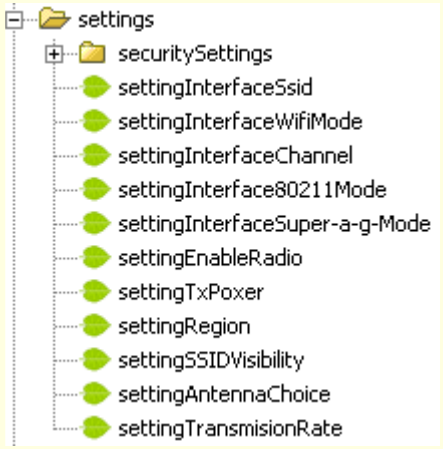
Le trap qui va être modifié apparaît sélectionné dans la liste. Vous pouvez modifier la configuration du trap dans la section « SNMP TRAP SETTING ». Une fois le trap modifié, cliquez sur save afin de sauvegarder vos modifications. La liste est ensuite mise à jour.

V.7 La MIB entreprise ACKSYS

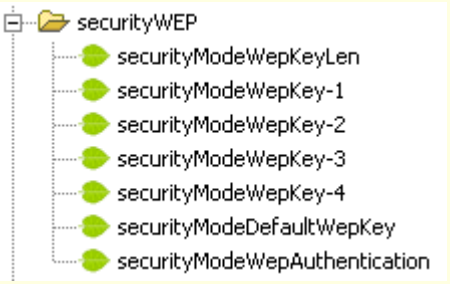
Remarques :

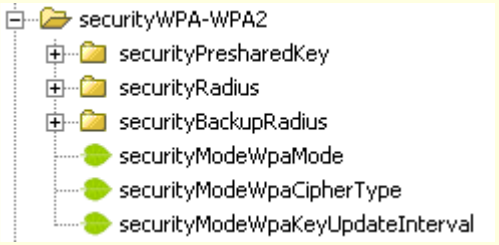
- Selon le mode de fonctionnement courant (Bridge ou Point d'Accès), n'est accessible qu'un seul des deux groupes de paramètres « bridge-mode » ou « access-point-mode ».
- Tout changement dans la configuration par SNMP, sera prise en compte uniquement au prochain redémarrage.
- Il est possible de redémarrer le produit par SNMP, en écrivant un 1 dans l'OID .1.3.6.1.4.1.28097.1.2.1.0.

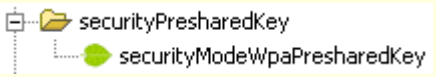
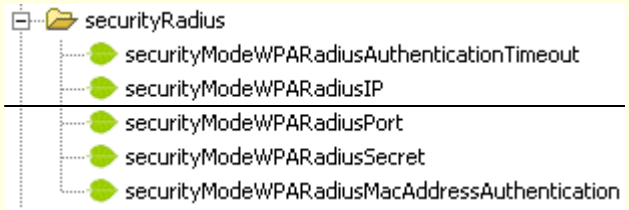
OID	Accès	Nom	Description	Valeurs
.1.3.6.1.4.1.28097.1		ACKSYS-WLG-MIB	La MIB pour les produits point d'accès et bridge Wi-Fi 802.11 a/b/g/h.	
.1.3.6.1.4.1.28097.3.0	Lecture	acksysProductID	Code d'identification du produit	1 : WLg-LINK 2 : WLg-ABOARD/N 3 : WLg-LINK-V2 4 : WLg-ABOARD/N-V2 5 : WLg-SWITCH 6 : WLg-DONGLE-OEM 7 : WLg-DONGLE 9 : WLg-XROAD/N 10 : WLg-XROAD/S 11 : WLg-IDA/N 12 : WLg-IDA/S 13 : WLg-XROAD/NP 14 : WLg-IDA/NP
.1.3.6.1.4.1.28097.2.0		acksysMIB		
.1.3.6.1.4.1.28097.1.1		WifiInterface	Partie de la MIB permettant d'accéder aux données liées à l'interface Wi-Fi.	

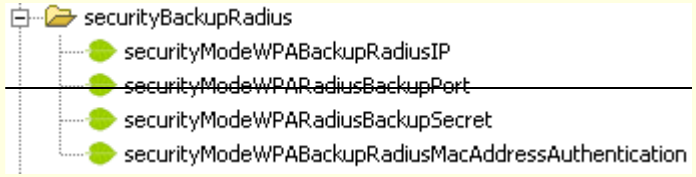
OID	Accès	Nom	Description	Valeurs
.1.3.6.1.4.1.28097.1.1.1 		**setting**	**Partie de la MIB permettant de configurer l'interface Wi-Fi.**	
~~.1.3.6.1.4.1.28097.1.1.1.1.0~~ **Obsolète**	~~Lecture Ecriture~~	~~settingInterfaceSsid~~	~~SSID de l'interface Wi-Fi.~~	~~Chaîne de caractères avec une longueur maximale de 33 caractères.~~
.1.3.6.1.4.1.28097.1.1.1.2.0	Lecture Ecriture	settingInterfaceWifiMode	Sélectionne le mode de fonctionnement du produit.	1 : Bridge 2 : Point d'Accès
.1.3.6.1.4.1.28097.1.1.1.3.0	Lecture Ecriture	settingInterfaceChannel	Sélectionne le canal radio à utiliser.	Le numéro du canal radio. Les numéros utilisables dépendent de la bande radio utilisée : A, H ou B/G (utilisé seulement pour les modes Access Point et Bridge ad-hoc)
.1.3.6.1.4.1.28097.1.1.1.4.0	Lecture Ecriture	settingInterface80211Mode	Sélectionne le mode de compatibilité 802.11x.	1 : 802.11b uniquement 2 : 802.11g uniquement 3 : 802.11 b/g 4 : 802.11 a/h

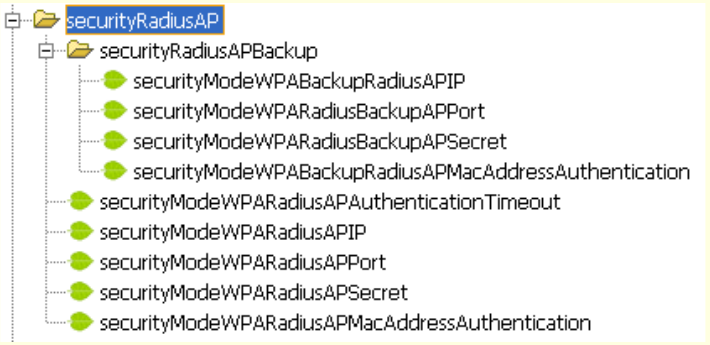
OID	Accès	Nom	Description	Valeurs
.1.3.6.1.4.1.28097.1.1.1.5.0	Lecture Ecriture	settingInterfaceSuper-a-g-Mode	Sélectionne le mode super a/g à utiliser.	1 : mode super a/g désactivé 2 : super a/g sans turbo 3 : super a/g avec turbo statique 4 : super a/g avec turbo dynamique
.1.3.6.1.4.1.28097.1.1.1.6.0	Lecture Ecriture	SettingEnableRadio	Active / Désactive la carte radio	1 : Désactive la carte radio 2 : Active la carte radio
.1.3.6.1.4.1.28097.1.1.1.7.0	Lecture Ecriture	SettingTxPower	Fixe le niveau de puissance en sortie de la carte radio	1 : Fort (100 %) 2 : Moyen (50 %) 3 : Bas (25%)
.1.3.6.1.4.1.28097.1.1.1.8.0	Lecture Ecriture	SettingRegion	Fixe le domaine de régulation de la carte	2 = Israel 4 = USA 5 = Hong Kong 6 = Canada 7 = Australie 10 = France oudoor 14 = Europe 17 = Japon 18 = Singapore 20 = Corée
.1.3.6.1.4.1.28097.1.1.1.9.0	Lecture Ecriture	SettingSSIDVisibility	Permet de cacher le SSID aux autres équipements Wi-Fi	1 : SSID non visible 2 : SSID visible
.1.3.6.1.4.1.28097.1.1.1.10.0	Lecture Ecriture	SettingAntennaChoice	Permet de spécifier le port utilisé pour l'antenne	1 : diversité 2 : main 3 : auxiliaire

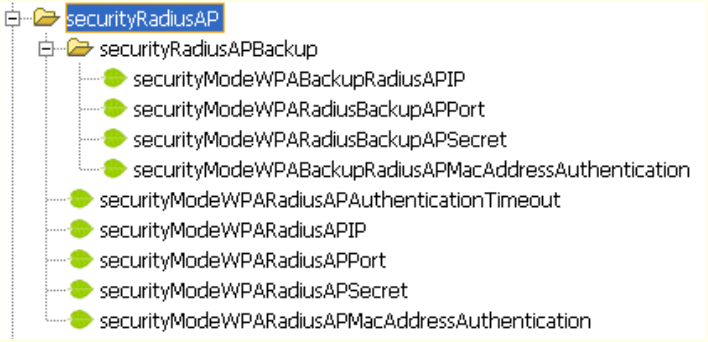
OID	Accès	Nom	Description	Valeurs
.1.3.6.1.4.1.28097.1.1.1.11.0	Lecture Ecriture	SettingTransmission Rate	Permet de spécifier le débit de la liaison Wi-Fi en Mbps	0 : automatique Avec Super AG : 108,96,72,54,48,36,24,18,12 Sans super AG : 54,48,36,24,18,12,9,6 Mode 802.11b : 11,5.5,2,1
.1.3.6.1.4.1.28097.1.1.1.9 		**securitySettings**	**Partie de la MIB permettant de configurer les différents modes de sécurité.**	
.1.3.6.1.4.1.28097.1.1.1.9.1.0	Lecture Ecriture	SecurityMode	Permet de configurer le type de sécurité utilisé	1 : aucune 2 : WEP 3 : WPA-WPA2-PSK 4 : WPA-WPA2
.1.3.6.1.4.1.28097.1.1.1.9.2 		**securityWEP**	**Partie de la MIB permettant de configurer la sécurité WEP**	

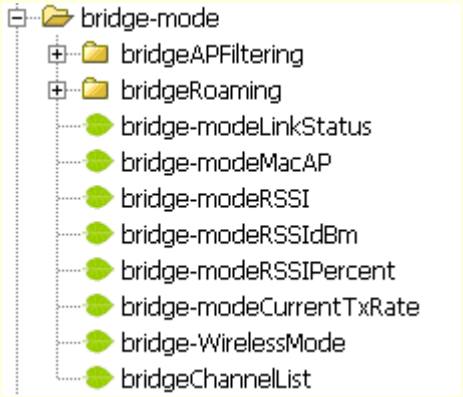
OID	Accès	Nom	Description	Valeurs
.1.3.6.1.4.1.28097.1.1.1.9.2.1.0	Lecture Ecriture	securityModeWepKeyLen	Longueur de la clé WEP	64 ou 128
.1.3.6.1.4.1.28097.1.1.1.9.2.2.0	Lecture Ecriture	SecurityModeWepKey-1	Clef WEP numéro 1	Clef WEP en hexadecimal
.1.3.6.1.4.1.28097.1.1.1.9.2.3.0	Lecture Ecriture	SecurityModeWepKey-2	Clef WEP numéro 2	Clef WEP en hexadecimal
.1.3.6.1.4.1.28097.1.1.1.9.2.4.0	Lecture Ecriture	SecurityModeWepKey-3	Clef WEP numéro 3	Clef WEP en hexadecimal
.1.3.6.1.4.1.28097.1.1.1.9.2.5.0	Lecture Ecriture	SecurityModeWepKey-4	Clef WEP numéro 4	Clef WEP en hexadecimal
.1.3.6.1.4.1.28097.1.1.1.9.2.6.0	Lecture Ecriture	SecurityModeDefaultWepKey	Numéro de la clé WEP selectionnée	1,2,3,4
.1.3.6.1.4.1.28097.1.1.1.9.2.7.0	Lecture Ecriture	SecurityModeWepAuthentication	Sélectionne le mode d'authentification	1 : open 2 : shared
.1.3.6.1.4.1.28097.1.1.1.9.3 		**SecurityWPA-WPA2**	**Partie de la MIB qui permet de configurer le mode WPA et WPA2**	
.1.3.6.1.4.1.28097.1.1.1.9.3.4.0	Lecture Ecriture	SecurityModeWpaMode	Permet de choisir la version de WPA utilisé	1 : WPA 2 : WPA2
.1.3.6.1.4.1.28097.1.1.1.9.3.5.0	Lecture Ecriture	SecurityModeWpaCipherType	Permet de choisir le mode de cryptage des données	1 : TKIP 2 : AES
.1.3.6.1.4.1.28097.1.1.1.9.3.6.0	Lecture Ecriture	SecurityModeWpaKeyUpdateInterval	Permet de choisir la durée entre deux changement de Group Key	Durée en seconde (entre 1 et 65535)

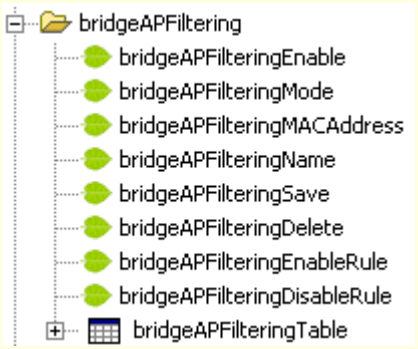
OID	Accès	Nom	Description	Valeurs
.1.3.6.1.4.1.28097.1.1.1.9.3.1 		**SecurityPresharedKey**	**Partie de la MIB qui permet de configurer la PresharedKey du mode WPA**	
.1.3.6.1.4.1.28097.1.1.1.9.3.1.1.0	Lecture Ecriture	SecurityModeWpaPresharedKey	Contient la PresharedKey du mode WPA	Chaîne de caractères avec une longueur comprise entre 8 et 63 caractères
~~**.1.3.6.1.4.1.28097.1.1.1.9.3.2**~~ **Obsolète** 		~~**SecurityRadius**~~	~~**Partie de la MIB permettant de configurer la sécurité en mode WPA Radius**~~	
~~.1.3.6.1.4.1.28097.1.1.1.9.3.2.1.0~~ **Obsolète**	~~Lecture Ecriture~~	~~SecurityModeWpaRadiusAuthenticationTimeout~~	~~Contient la durée maximum d'authentification~~	~~Exprimée en minutes~~
~~.1.3.6.1.4.1.28097.1.1.1.9.3.2.2.0~~ **Obsolète**	~~Lecture Ecriture~~	~~SecurityModeWpaRadiusIP~~	~~Contient l'adresse IP du server Radius~~	~~Adresse IP~~
~~.1.3.6.1.4.1.28097.1.1.1.9.3.2.3.0~~ **Obsolète**	~~Lecture Ecriture~~	~~SecurityModeWpaRadiusPort~~	~~Contient le numério de port utilisé par le server Radius~~	~~1 à 65535~~
~~.1.3.6.1.4.1.28097.1.1.1.9.3.2.4.0~~ **Obsolète**	~~Lecture Ecriture~~	~~SecurityModeWpaRadiusSecret~~	~~Contient le mot de passe utilsé dans les communication entre le server radius et le pointd'accès~~	~~Chaîne de caractères de longueur comprise entre 1 et 64 caractères~~

OID	Accès	Nom	Description	Valeurs
.1.3.6.1.4.1.28097.1.1.1.9.3.2.5.0 **Obsolète**	Lecture Ecriture	SecurityModeWpaRadiusMacAdressAuthentication	Permet de d'utiliser l'adresse MAC du supplicant pour l'authentification avec le serveur Radius	1 : désactivé 2 : activé
.1.3.6.1.4.1.28097.1.1.1.9.3.3 Obsolète 		**SecurityBackupRadius**	**Partie de la MIB permettant de configurer la sécurité en mode WPA Radius d'un second serveur radius**	
.1.3.6.1.4.1.28097.1.1.1.9.3.3.1.0 **Obsolète**	Lecture Ecriture	SecurityModeWpaBackupRadiusIP	Contient l'adresse IP du second server Radius	Adresse IP
.1.3.6.1.4.1.28097.1.1.1.9.3.3.2.0 **Obsolète**	Lecture Ecriture	SecurityModeWpaRadiusPort	Contient le numério de port utilisé par le second server Radius	1 à 65535
.1.3.6.1.4.1.28097.1.1.1.9.3.3.3.0 **Obsolète**	Lecture Ecriture	SecurityModeWpaBackupRadiusSecret	Contient le mot de passe utilsé dans les communication entre le second server radius et le pointd'accès	Chaîne de caractères de longueur comprise entre 1 et 64 caractères
.1.3.6.1.4.1.28097.1.1.1.9.3.3.4.0 **Obsolète**	Lecture Ecriture	SecurityModeWpaBackupRadiusMacAdressAuthentication	Permet de d'utiliser l'adresse MAC du supplicant pour l'authentification avec le second server radius	1 : désactivé 2 : activé

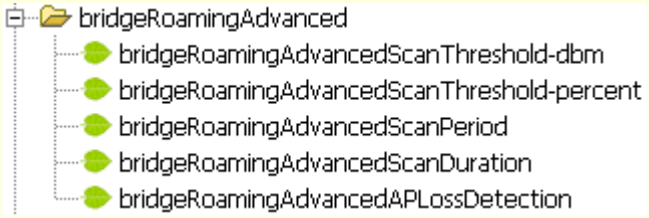
OID	Accès	Nom	Description	Valeurs
.1.3.6.1.4.1.28097.1.1.1.9.3.2.6 		**securityRadiusAP**	**Partie de la MIB permettant de configurer le serveur RADIUS pour le WPA/WPA2-enterprise**	
.1.3.6.1.4.1.28097.1.1.1.9.3.2.6.1.0	Lecture Ecriture	securityModeWPARadiusAuthenticationTimout	Contient la durée maximum d'authentification	Exprimée en minutes
.1.3.6.1.4.1.28097.1.1.1.9.3.2.6.2.0	Lecture Ecriture	securityModeWPARadiusAPIP	Contient l'adresse IP du serveur RADIUS	Adresse IP
.1.3.6.1.4.1.28097.1.1.1.9.3.2.6.3.0	Lecture Ecriture	securityModeWPARadiusAPPort	Contient le numéro de port utilisé par le serveur RADIUS	1 à 65535
.1.3.6.1.4.1.28097.1.1.1.9.3.2.6.4.0	Lecture Ecriture	SecurityModeWPARadiusAPSecret	Contient le mot de passe utilisé dans les communications entre le serveur RADIUS et le point d'accès	Chaîne de caractères de longueur comprise entre 1 et 64 caractères
.1.3.6.1.4.1.28097.1.1.1.9.3.2.6.5.0	Lecture Ecriture	SecurityModeWPARadiusAPAuthenticationTimeout	Permet d'utiliser l'adresse MAC du demandeur pour l'authentification auprès du serveur RADIUS	1 : désactivé 2 : activé

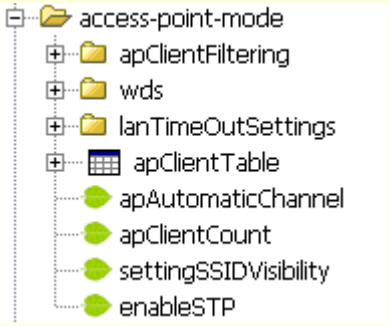
OID	Accès	Nom	Description	Valeurs
.1.3.6.1.4.1.28097.1.1.1.9.3.2.6.6 		**SecurityRadiusAPBackup**	**Partie de la MIB permettant de configurer un second serveur RADIUS**	
.1.3.6.1.4.1.28097.1.1.1.9.3.2.6.6.1.0	Lecture Ecriture	SecurityModeWPABackupRadiusAPIP	Contient l'adresse IP du second serveur RADIUS	Adresse IP
.1.3.6.1.4.1.28097.1.1.1.9.3.2.6.6.2.0	Lecture Ecriture	SecurityModeWPARadiusBackupPort	Contient le numéro de port utilisé par le second serveur RADIUS	1 à 65535
.1.3.6.1.4.1.28097.1.1.1.9.3.2.6.6.3.0	Lecture Ecriture	SecurityModeWPARadiusBackupSecret	Contient le mot de passe utilisé dans les communications entre le second serveur RADIUS et le point d'accès	Chaîne de caractères de longueur comprise entre 1 et 64 caractères
.1.3.6.1.4.1.28097.1.1.1.9.3.2.6.6.4.0	Lecture Ecriture	SecurityModeWPABackupRadiusMacAddressAuthentication	Permet d'utiliser l'adresse MAC du supplicant pour l'authentification avec le second serveur RADIUS	1 : désactivé 2 : activé

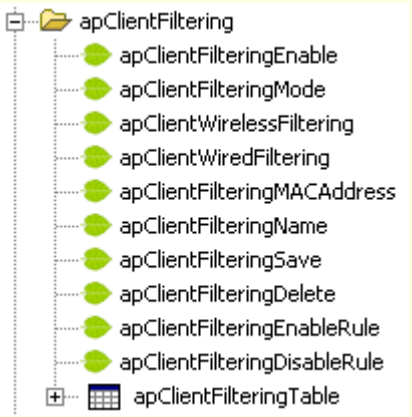
OID	Accès	Nom	Description	Valeurs
.1.3.6.1.4.1.28097.1.1.2 		**bridge-mode**	**Partie de la MIB donnant des informations sur le fonctionnement en mode bridge.** NOTE: Ces informations ne s'appliquent qu'aux bridges en mode **infrastructure**.	
.1.3.6.1.4.1.28097.1.1.2.1.0	Lecture	bridge-modeLinkStatus	Etat de la connexion au point d'accès.	1 : « up », liaison Wi-Fi établie 2 : « down », liaison Wi-Fi rompue
.1.3.6.1.4.1.28097.1.1.2.2.0	Lecture	bridge-modeMacAP	Adresse MAC du point d'accès auquel le bridge est connecté.	
.1.3.6.1.4.1.28097.1.1.2.3.0	Lecture	bridge-modeRSSI	Valeur du RSSI de la connexion (selon format ATHEROS).	
.1.3.6.1.4.1.28097.1.1.2.4.0	Lecture	bridge-modeRSSIdBm	Valeur du RSSI en dBm.	
.1.3.6.1.4.1.28097.1.1.2.5.0	Lecture	bridge-modeRSSIPercent	Valeur du RSSI en pourcentage.	
.1.3.6.1.4.1.28097.1.1.2.6.0	Lecture	bridge-modeCurrentTxRate	Vitesse de transmission actuelle en bits par seconde.	
.1.3.6.1.4.1.28097.1.1.2.7.0	Lecture Ecriture	bridge-WirelessMode	Permet de choisir entre le mode infrastructure et le mode ad-hoc	1 : infrastructure 2 : ad-hoc

OID	Accès	Nom	Description	Valeurs
.1.3.6.1.4.1.28097.1.2.8 		**bridgeAPFiltering**	**Partie de la MIB qui permet de configurer le filtrage de point d'accès**	
.1.3.6.1.4.1.28097.1.1.2.8.1.0	Lecture Ecriture	bridgeAPFilteringEnable	Permet d'activer ou de désactiver le filtrage d'adresse MAC.	1 : activé 2 : désactivé
.1.3.6.1.4.1.28097.1.1.2.8.2.0	Lecture Ecriture	bridgeAPFilteringMode	Permet de faire un filtre qui rejette ou accepte la liste d'adresse MAC	1 : allow 2 : deny
.1.3.6.1.4.1.28097.1.1.2.8.3.0	Lecture Ecriture	bridgeAPFilteringMACAddress	Adresse MAC de l'AP	Adresse MAC
.1.3.6.1.4.1.28097.1.1.2.8.4.0	Lecture Ecriture	bridgeAPFilteringName	Nom de l'AP	Chaine de caractères de longueur 1 à 63 caractères
.1.3.6.1.4.1.28097.1.1.2.8.5.0	Ecriture	bridgeAPFilteringSave	Ecrire 1 à cette adresse va créer une règles avec **bridgeAPFilteringMACAddress** et **bridgeAPFilteringComputerName**	1
.1.3.6.1.4.1.28097.1.1.2.8.6.0	Ecriture	bridgeAPFilteringDelete	Efface la règle spécifiée	Index de la règle à effacer

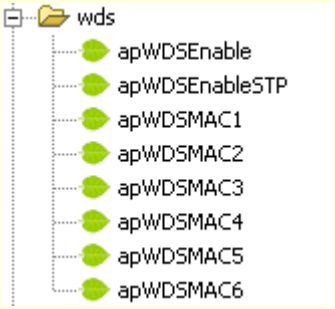
OID	Accès	Nom	Description	Valeurs
.1.3.6.1.4.1.28097.1.1.2.8.7.0	Ecriture	bridgeAPFilteringEnableRule	Active la règle spécifiée	Index de la règle à activer
.1.3.6.1.4.1.28097.1.1.2.8.8.0	Ecriture	bridgeAPFilteringDisableRule	Désactive la règle spécifiée	Index de la règle à désactiver
.1.3.6.1.4.1.28097.1.1.2.8.9		bridgeAPFilteringList	Table des règles de filtrage des points d'accès	
.1.3.6.1.4.1.28097.1.1.2.8.9.1		bridgeAPFilteringListEntry	Description d'une règle de filtrage	
.1.3.6.1.4.1.28097.1.1.2.8.9.1.1	Lecture	bridgeAPFilteringListId	Index de la règle	
.1.3.6.1.4.1.28097.1.1.2.8.9.1.2	Lecture	bridgeAPFilteringListName	Nom de la règle.	
.1.3.6.1.4.1.28097.1.1.2.8.9.1.3	Lecture	bridgeAPFilteringListMAC	Adresse MAC du point d'accès	
.1.3.6.1.4.1.28097.1.1.2.8.9.1.4	Lecture	bridgeAPFilteringListEnable	Indique si la règle est activée	1 : activée 2 : désactivée
.1.3.6.1.4.1.28097.1.1.2.9 		**bridgeRoaming**	**Partie de la MIB qui permet de configurer le roaming rapide**	
1.3.6.1.4.1.28097.1.1.2.9.2.0	Lecture Ecriture	BridgeRoamingEnable	Active / désactive la fonction de roaming	1 : activée 2 : désactivée
1.3.6.1.4.1.28097.1.1.2.9.3.0	Lecture Ecriture	BridgeRoamingRSSIThreshold -dBm	Configure le seuil de roaming en dBm	-20 dBm- -90 dBm
1.3.6.1.4.1.28097.1.1.2.9.4.0	Lecture Ecriture	BridgeRoamingRSSIThreshold-percent	Configure le seuil de roaming en pourcentage	1-100

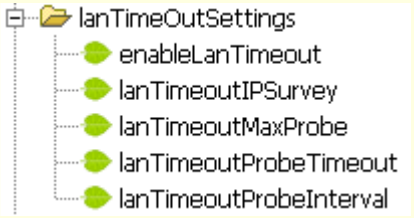
OID	Accès	Nom	Description	Valeurs
.1.3.6.1.4.1.28097.1.1.2.9.1 		**BridgeRoaming Advanced**	**Partie de la MIB qui permet de configurer les paramètres avancés du roaming rapide**	
.1.3.6.1.4.1.28097.1.1.2.9.1.1.0	Lecture Ecriture	BridgeRoamingAdvancedScanThreshold-dbm	Seuil à partir duquel on va scanner en roaming multi-canal	-20 dBm- -90 dBm
1.3.6.1.4.1.28097.1.1.2.9.1.2.0	Lecture Ecriture	BridgeRoamingAdvancedScanThreshold-percent	Seuil à partir duquel on va scanner en roaming multi-canal	1 % - 100 %
1.3.6.1.4.1.28097.1.1.2.9.1.3.0	Lecture Ecriture	BridgeRoamingAdvancedScanPeriod	Configure l'intervalle entre deux scans, en secondes	1 – 255
1.3.6.1.4.1.28097.1.1.2.9.1.4.0	Lecture Ecriture	BridgeRoamingAdvancedScanDuration	Configure la durée d'attente d'une réponse au scan sur le canal en milli-seconde	1 - 255
1.3.6.1.4.1.28097.1.1.2.9.1.5.0	Lecture Ecriture	bridgeRoamingAdvancedAPLossDetection	Time out de détection de perte de l'AP en nombre d'intervalles de beacon	1 - 255

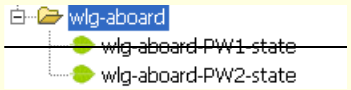
OID	Accès	Nom	Description	Valeurs
.1.3.6.1.4.1.28097.1.1.3 		**access-point-mode**	**Partie de la MIB donnant des informations sur le fonctionnement en mode point d'accès.**	
.1.3.6.1.4.1.28097.1.1.3.1		apClientTable	Table des clients connectés à ce point d'accès.	
.1.3.6.1.4.1.28097.1.1.3.1.1		apClientEntry	Description d'un client connecté.	
.1.3.6.1.4.1.28097.1.1.3.1.1.1	Lecture	clientMacAddr	Adresse MAC du client.	
.1.3.6.1.4.1.28097.1.1.3.1.1.2	Lecture	client80211Mode	Mode de fonctionnement de l'interface radio du client.	1 : 802.11b uniquement 2 : 802.11g uniquement 3 : 802.11 b/g 4 : 802.11 a/h
.1.3.6.1.4.1.28097.1.1.3.1.1.3	Lecture	clientTxRate	Vitesse de transmission du client en bits par seconde.	
.1.3.6.1.4.1.28097.1.1.3.1.1.4	Lecture	clientRssiPercent	Valeur du RSSI du client, en pourcentage.	
.1.3.6.1.4.1.28097.1.1.3.2.0	Lecture Ecriture	apAutomaticChannel	Active / désactive la sélection automatique des canaux	1 : La sélection automatique est désactivée 2 : La sélection automatique est activée
.1.3.6.1.4.1.28097.1.1.3.3.0	Lecture	apClientCount	Nombre de clients connectés au point d'accès	

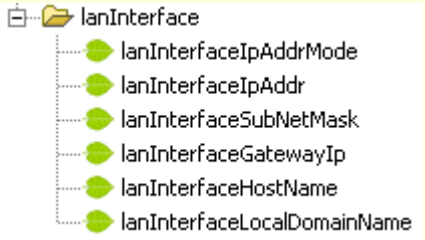
OID	Accès	Nom	Description	Valeurs
.1.3.6.1.4.1.28097.1.1.3.6.0	Lecture Ecriture	settingSSIDVisibility	Permet de spécifier si le SSID du point d'accès est visible ou non.	1 : désactivé 2 : activé
.1.3.6.1.4.1.28097.1.1.3.7.0	Lecture Ecriture	EnableSTP	Active / désactive le STP	1 : désactivé 2 : activé
.1.3.6.1.4.1.28097.1.1.3.4 		**apClientFiltering**	**Partie de la MIB qui permet de configurer le filtrage des clients**	
.1.3.6.1.4.1.28097.1.1.3.4.1.0	Lecture Ecriture	apClientFilteringEnable	Permet d'activer ou de désactiver le filtrage d'adresse MAC.	1 : désactivé 2 : activé
.1.3.6.1.4.1.28097.1.1.3.4.2.0	Lecture Ecriture	apClientFilteringMode	Permet de faire un filtre qui rejette ou accepte la liste d'adresse MAC	1 : désactivé 2 : activé
.1.3.6.1.4.1.28097.1.1.3.4.3.0	Lecture Ecriture	apClientWirelessFiltering	Filtre les clients présents du côté Wi-Fi	1 : désactivé 2 : activé
.1.3.6.1.4.1.28097.1.1.3.4.4.0	Lecture Ecriture	apClientWiredFiltering	Filtre les clients présents du côté LAN	1 : désactivé 2 : activé
.1.3.6.1.4.1.28097.1.1.3.4.5.0	Lecture Ecriture	apClientFilteringMACAddress	Adresse MAC du client	Adresse MAC

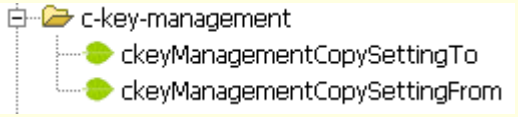
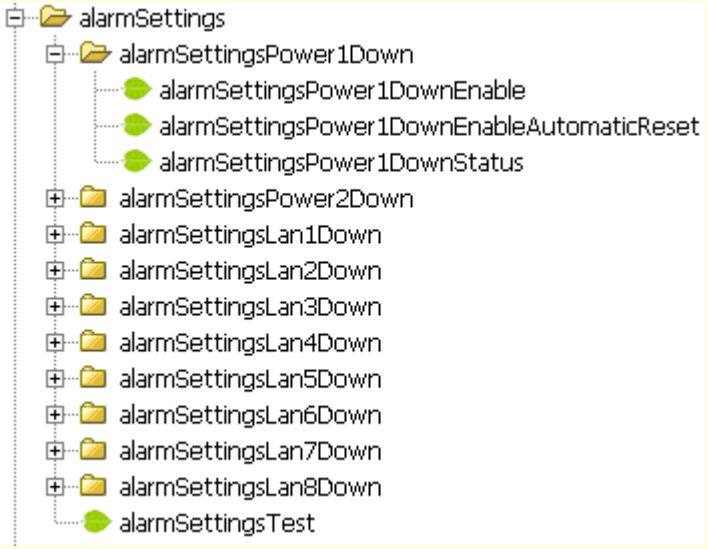
OID	Accès	Nom	Description	Valeurs
.1.3.6.1.4.1.28097.1.1.3.4.6.0	Lecture Ecriture	apClientFilteringName	Nom de la règle	Chaine de caractères de longueur 1 à 63 caractères
.1.3.6.1.4.1.28097.1.1.3.4.7.0	Ecriture	apClientFilteringSave	Ecrire 1 à cette adresse va créer une règle en utilisant **apClientFilteringMACAddress** et **apClientFilteringClientName**	1
.1.3.6.1.4.1.28097.1.1.3.4.8.0	Ecriture	apClientFilteringDelete	Efface la règle spécifiée	Index de la règle à effacer
.1.3.6.1.4.1.28097.1.1.3.4.9.0	Ecriture	apClientFilteringEnableRule	Active la règle spécifiée	Index de la règle à activer
.1.3.6.1.4.1.28097.1.1.3.4.10.0	Ecriture	apClientFilteringDisableRule	Désactive la règle spécifiée	Index de la règle à désactiver
.1.3.6.1.4.1.28097.1.1.3.4.11		apClientFilteringList	Table des règles de filtrage des clients	
.1.3.6.1.4.1.28097.1.1.3.4.11.1		apClientFilteringListEntry	Description d'une règle de filtrage	
.1.3.6.1.4.1.28097.1.1.3.4.11.1.1	Lecture	apClientFilteringListId	Index de la règle	
.1.3.6.1.4.1.28097.1.1.3.4.11.1.2	Lecture	apClientFilteringListName	Nom de la règle.	
.1.3.6.1.4.1.28097.1.1.3.4.11.1.3	Lecture	apClientFilteringListMAC	Adresse MAC du client	
.1.3.6.1.4.1.28097.1.1.3.4.11.1.4	Lecture	apClientFilteringListEnable	Indique si la règle est activée	1 : désactivé 2 : activé

OID	Accès	Nom	Description	Valeurs
.1.3.6.1.4.1.28097.1.1.3.5 		**WDSConfiguration**	**Partie de la MIB permettant de configurer le mode WDS**	
.1.3.6.1.4.1.28097.1.1.3.5.1.0	Lecture Ecriture	apWDSEnable	Permet d'activer ou de désactiver le WDS	1 : Désactivé 2 : Activé
.1.3.6.1.4.1.28097.1.1.3.5.2.0	Lecture Ecriture	apWDSEnableSTP	Permet d'activer ou de désactiver le STP	1 : Désactivé 2 : Activé
.1.3.6.1.4.1.28097.1.1.3.5.3.0	Lecture Ecriture	ApWDSMAC1	Adresse MAC numéro 1	Adresse IP
.1.3.6.1.4.1.28097.1.1.3.5.4.0	Lecture Ecriture	ApWDSMAC2	Adresse MAC numéro 2	Adresse IP
.1.3.6.1.4.1.28097.1.1.3.5.5.0	Lecture Ecriture	ApWDSMAC3	Adresse MAC numéro 3	Adresse IP
.1.3.6.1.4.1.28097.1.1.3.5.6.0	Lecture Ecriture	ApWDSMAC4	Adresse MAC numéro 4	Adresse IP
.1.3.6.1.4.1.28097.1.1.3.5.7.0	Lecture Ecriture	ApWDSMAC5	Adresse MAC numéro 5	Adresse IP
.1.3.6.1.4.1.28097.1.1.3.5.8.0	Lecture Ecriture	ApWDSMAC6	Adresse MAC numéro 6	Adresse IP

OID	Accès	Nom	Description	Valeurs
.1.3.6.1.4.1.28097.1.1.3.8 		**LanTimeOutSettings**	**Partie de la MIB permettant de configurer la surveillance du LAN**	
.1.3.6.1.4.1.28097.1.1.3.8.1.0	Lecture Ecriture	EnableLanTimeout	Active / désactive la fonction de surveillance du LAN	1 : Désactivé 2 : Activé
.1.3.6.1.4.1.28097.1.1.3.8.2.0	Lecture Ecriture	LanTimeoutIPSurvey	Adresse IP à surveiller sur le LAN	Adresse IP
.1.3.6.1.4.1.28097.1.1.3.8.3.0	Lecture Ecriture	LanTimeoutMacProbe	Nombre maximal de tests sans réponse avant l'extinction de l'interface Wi-Fi	1 - 255
.1.3.6.1.4.1.28097.1.1.3.8.4.0	Lecture Ecriture	LantimeoutProbeTimout	Combien de temps on attend chaque réponse en secondes.	1 – 255
.1.3.6.1.4.1.28097.1.1.3.8.1.0	Lecture Ecriture	LanTimeoutProbeInterval	Configure l'intervalle entre deux tests de l'interface LAN en secondes.	1 - 255
.1.3.6.1.4.1.28097.1.2 		**administration**	**Partie de la MIB permettant d'administrer le produit.**	
.1.3.6.1.4.1.28097.1.2.1.0	Lecture Ecriture	adminReset	Permet le redémarrage du produit par SNMP.	L'écriture de la valeur 1 déclenche le redémarrage.

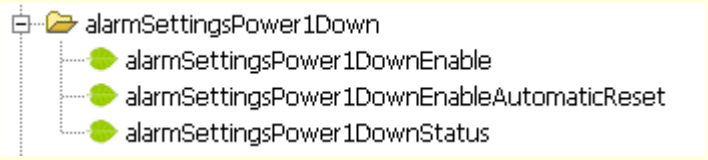
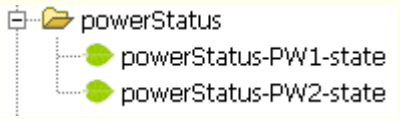
OID	Accès	Nom	Description	Valeurs
.1.3.6.1.4.1.28097.1.2.2.0	Lecture Ecriture	adminResetFactory	Remise du produit dans sa configuration d'usine. Une écriture dans ce champ provoque un redémarrage du produit. L'agent SNMP sera désactivé.	L'écriture de la valeur 1 déclenche le retour en configuration d'usine.
.1.3.6.1.4.1.28097.1.2.3.0	Lecture Ecriture	adminEnableWebServer	Permet d'activer ou de désactiver le server WEB interne au produit	1 : désactivé 2 : activé
.1.3.6.1.4.1.28097.1.2.4.0	Lecture Ecriture	AdminAutoSave	Permet d'activer ou de désactiver la sauvegarde automatique lors de la modification par SNMP	1 : désactivée 2 : activée
.1.3.6.1.4.1.28097.1.2.5.0	Lecture Ecriture	AdminSave	En écriture : permet de forcer la sauvegarde de la configuration. En lecture : Permet de savoir si la configuration a été changée depuis le démarrage du produit.	En écriture : 1 : force la sauvegarde. En lecture : 2 : sauvegarde requise 3 : sauvegarde non requise.
.1.3.6.1.4.1.28097.1.4		**ProductSpecific**	**Partie de la MIB permettant d'administrer des fonctions spécifique à certains produits**	
~~**.1.3.6.1.4.1.28097.1.4.1 Obsolète**~~ 		~~**Wlg-aboard**~~	~~**Fonction spècifique au WLg-ABOARD/N[P]**~~	
~~.1.3.6.1.4.1.28097.1.4.1.1.0~~ **Obsolète**	~~Lecture~~	~~wlg-aboard-PW1-state~~	~~Donne l'état de l'alimentation Power1 du produit.~~	~~1 : Alimentation présente 2 : Alimentation éteinte~~

OID	Accès	Nom	Description	Valeurs
~~.1.3.6.1.4.1.28097.1.4.1.2.0~~ **Obsolète**	~~Lecture~~	~~wlg-aboard-PW2-state~~	~~Donne l'état de l'alimentation Power2 du produit.~~	~~1 : Alimentation présente 2 : Alimentation éteinte~~
.1.3.6.1.4.1.28097.1.5 		**lanInterface**	**Partie de la MIB permettant d'administrer l'interface LAN**	
.1.3.6.1.4.1.28097.1.5.1.0	Lecture Ecriture	lanInterfaceIpAddrMode	Permet de choisir le mode de configuration de l'interface lan.	1 : static 2 : DHCP
.1.3.6.1.4.1.28097.1.5.2.0	Lecture Ecriture	lanInterfaceIpAddr	Permets de paramétrer l'adresse IP de l'interface LAN	Adresse IP
.1.3.6.1.4.1.28097.1.5.3.0	Lecture Ecriture	lanInterfaceSubNetMask	Permet de paramétrer le masque de sous réseau de l'interface LAN	Masque de sous réseau
.1.3.6.1.4.1.28097.1.5.4.0	Lecture Ecriture	lanInterfaceGatewayIP	Permet de paramétrer l'adresse IP de la Gateway associé à l'interface LAN	Adresse IP
.1.3.6.1.4.1.28097.1.5.5.0	Lecture Ecriture	lanInterfaceHostName	Permet de paramétrer le host name associé à l'interface LAN	Chaine de caractère de longueur comprise entre 1 et 64 carcartères
.1.3.6.1.4.1.28097.1.5.6.0	Lecture Ecriture	lanInterfaceLocalDomainName	Permet de paramétrer le nom de domaine local	Chaine de caractère de longueur comprise entre 1 et 64 carcartères

OID	Accès	Nom	Description	Valeurs
.1.3.6.1.4.1.28097.4 		**c-key-management**	**Gestion de la C-KEY**	
.1.3.6.1.4.1.28097.4.1.0	Ecriture	CkeyManagementCopySettingTo	Permet de copier la configuration du produit dans la C-KEY	1 : active l'écriture
.1.3.6.1.4.1.28097.4.2.0	Ecriture	CkeyManagementCopySettingFrom	Permet de copier la configuration de la C-KEY dans le produit, si la configuration de la C-KEY est valide	1 : active l'écriture
.1.3.6.1.4.1.28097.5 		**AlarmSettings**	**Gestion des alarmes**	

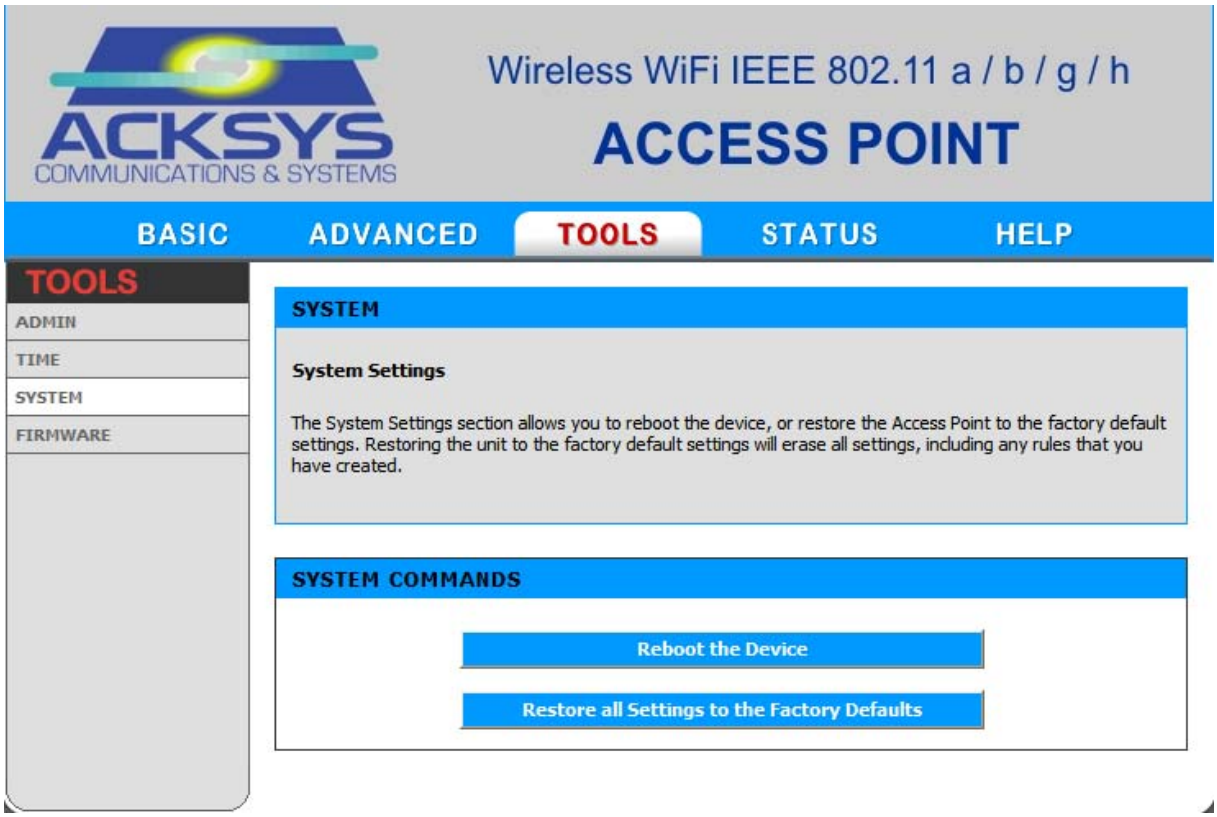
OID	Accès	Nom	Description	Valeurs
.1.3.6.1.4.1.28097.5.1.0	Write	AlarmSettingsTest	Permet de tester la sortie d'alarme.	1 : force la fermeture du contact d'alarme 2 : Force l'ouverture du contact d'alarme, si aucune autre source d'alarme n'est actuellement active.
La structure pour chaque source d'alarme est la même. Le nombre de sources est dépendant de votre produit. Nous allons donc documenter les OID des sources, puis les OID relatif à chaque source.				
.1.3.6.1.4.1.28097.5.2		**AlarmSettingsPower1Down**	**Configuration de la source d'alarme « perte de l'alimentation 1 »**	
.1.3.6.1.4.1.28097.5.3		**AlarmSettingsPower2Down**	**Configuration de la source d'alarme « perte de l'alimentation 2 »**	
.1.3.6.1.4.1.28097.5.4		**AlarmSettingsLan1down**	**Configuration de la source d'alarme « perte du lien Ethernet 1 »**	
.1.3.6.1.4.1.28097.5.5		**AlarmSettingsLan2down**	**Configuration de la source d'alarme « perte du lien Ethernet 2 »**	

OID	Accès	Nom	Description	Valeurs
.1.3.6.1.4.1.28097.5.6		**AlarmSettingsLan3down**	**Configuration de la source d'alarme « perte du lien Ethernet 3 »**	
.1.3.6.1.4.1.28097.5.7		**AlarmSettingsLan4down**	**Configuration de la source d'alarme « perte du lien Ethernet 4 »**	
.1.3.6.1.4.1.28097.5.8		**AlarmSettingsLan5down**	**Configuration de la source d'alarme « perte du lien Ethernet 5 »**	
.1.3.6.1.4.1.28097.5.9		**AlarmSettingsLan6down**	**Configuration de la source d'alarme « perte du lien Ethernet 6 »**	
.1.3.6.1.4.1.28097.5.10		**AlarmSettingsLan7down**	**Configuration de la source d'alarme « perte du lien Ethernet 7 »**	
.1.3.6.1.4.1.28097.5.11		**AlarmSettingsLan8down**	**Configuration de la source d'alarme « perte du lien Ethernet 8 »**	

OID	Accès	Nom	Description	Valeurs
			**Structure de chaque source**	
.1.0	Lecture Ecriture	Enable	Active ou désactive la source d'alarme. Une source désactivée ne peut plus générer une alarme	1 : désactivée 2 : activée
.2.0	Lecture Ecriture	AutomaticReset	Active ou désactive le reset automatique de la source d'alarme	1 : désactivé 2 : activé
.3.0	Lecture Ecriture	Status	Donne l'état de la source d'alarme	En lecture : 1 : Source non active 2 : Source active En écriture 3 : Acquitte la source d'alarme.
.1.3.6.1.4.1.28097.6 		**powerStatus**	**Partie de la MIB permettant de connaître l'état des alimentations**	
.1.3.6.1.4.1.28097.6.1.0	Lecture	PowerStatus-PW1-sate	Donne l'état de l'alimentation Power1 du produit.	1 : Alimentation présente 2 : Alimentation éteinte
.1.3.6.1.4.1.28097.6.2.0	Lecture	PowerStatus-PW2-sate	Donne l'état de l'alimentation Power2 du produit.	1 : Alimentation présente 2 : Alimentation éteinte

VI LES PARAMÈTRES PAR DÉFAUT

Les paramètres listés ci-après sont ceux fixés à la livraison du produit ou après un reset complet du produit (en général effectué avec un bouton poussoir dédié) ou encore depuis la rubrique « SYSTEM » du menu « TOOLS ».



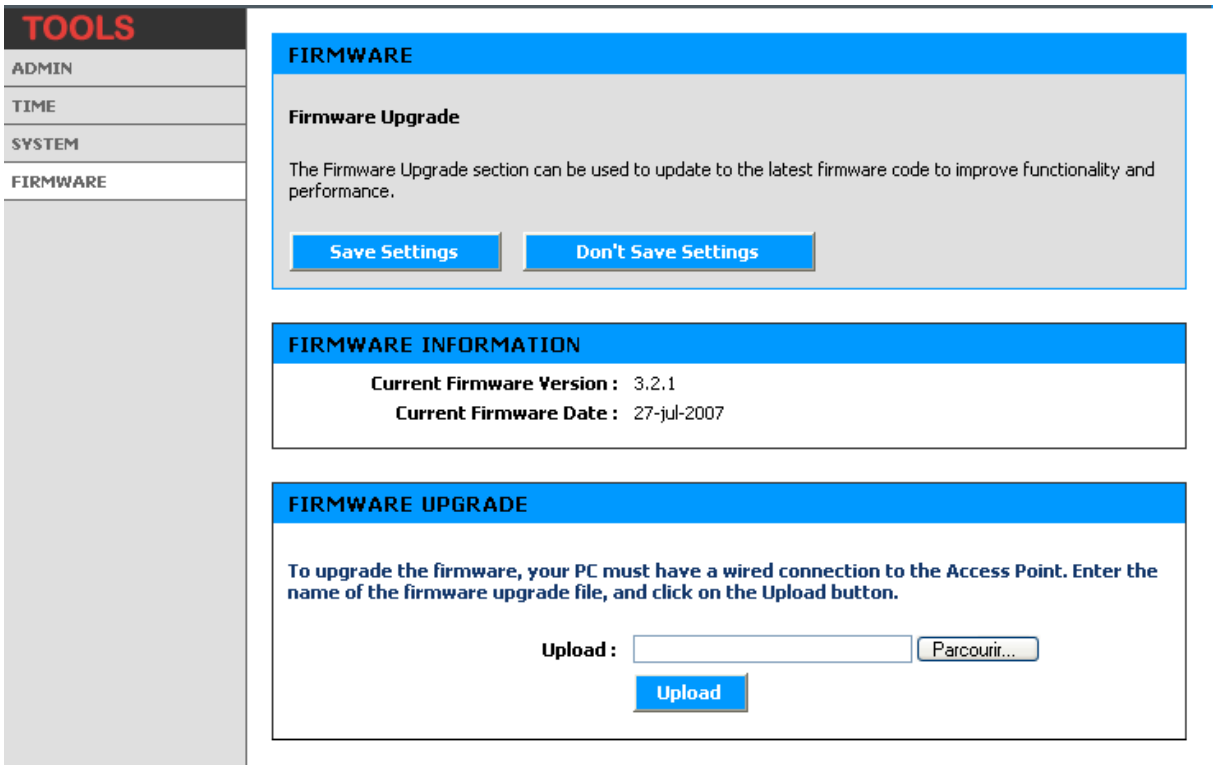
Username du login : « admin »
Mot de passe : Aucun

Mode « ACCESS POINT »
Adresse IP : 192.168.1.253, masque de sous réseau : 255.255.255.0
Canal radio : automatique
Mode b/g
ssid «acksys »
ssid diffusé
Aucune sécurité (ni wep, ni WPA, ni WPA2, ni filtrage MAC)
Gestion par SNMP désactivée
Serveur DHCP désactivé

VII MISE À JOUR DU PRODUIT

VII.1 Par l'interface WEB

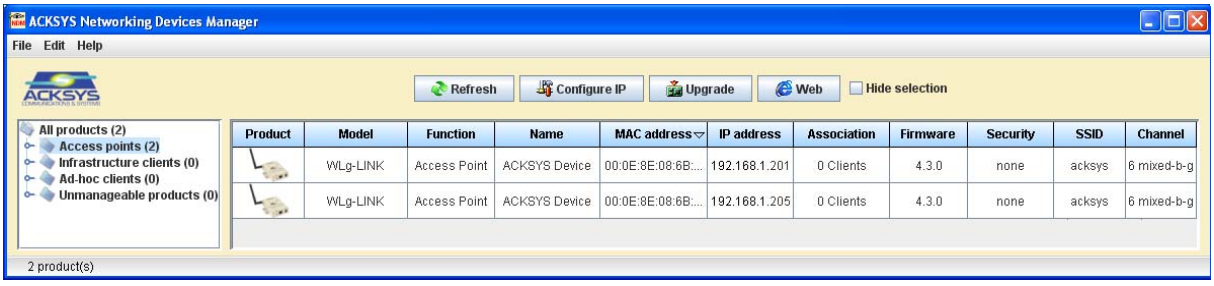
Télécharger une nouvelle version de firmware est une opération très simple qui peut être effectuée depuis le menu TOOLS/firmware.



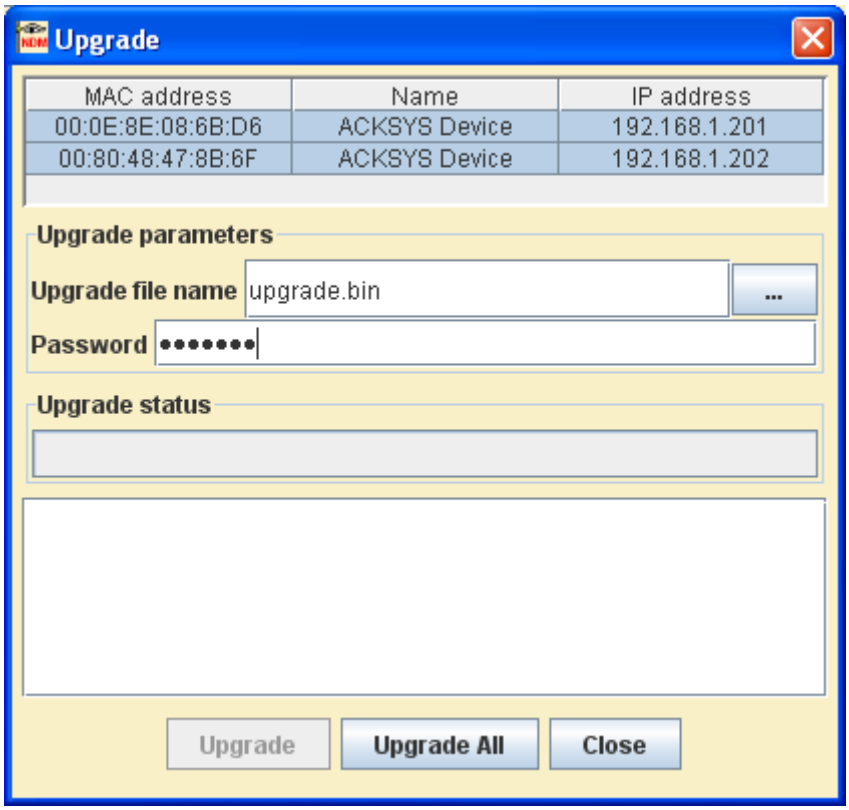
De plus, tous les paramètres de configuration restent conservés.

VII.2 Par l'application ACKSYS NDM

Le produit doit au préalable contenir un firmware version 3.6.0 ou plus.



Sélectionnez le ou les produits que vous souhaitez mettre à jour dans la liste.
Cliquez sur le bouton « Upgrade ».



Sélectionnez le fichier à charger, puis cliquez sur « Upgrade ».

Si vous souhaitez mettre à jour plusieurs produits en même temps, sélectionnez les dans la liste puis cliquez sur « Upgrade All ».

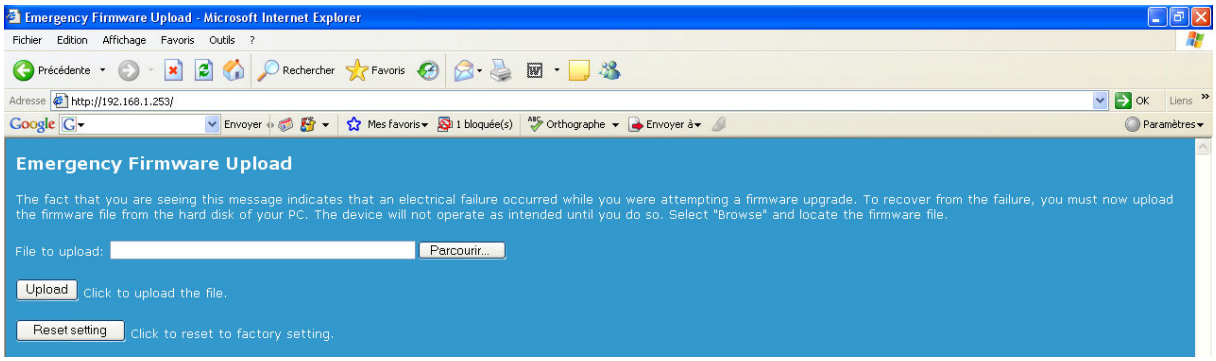
Remarque : La mise à jour de plusieurs produits en une fois avec le même fichier n'est possible uniquement que si le même mot de passe est configuré sur tous les produits.

Tous les paramètres de configuration restent conservés après l'opération de mise à jour.

VII.3 Récupération d'un produit après un problème de mise à jour

Si l'opération de mise à jour se passait mal suite à une mise hors tension inopinée du produit pendant la mise à jour de la flash eprom, un mode de fonctionnement de secours est automatiquement mis en place. Cette fonctionnalité a été intégrée à partir des firmwares revision 3.2.0.
Au 1er re-démarrage après la mise à jour, le produit constate alors de lui-même que la FLASH EPROM n'est plus intègre et exécute alors un serveur web restreint permettant uniquement de recharger à nouveau le firmware. Ce mode de fonctionnement est caractérisé par la led DIAG (led rouge) du produit qui clignote rapidement. Nous rappelons qu'elle est éteinte en mode de fonctionnement normal.

Pour accéder à ce mode, il suffit de taper l'adresse « 192.168.1.253 » dans la barre d'adresse de votre navigateur Web.



Il ne vous reste plus qu'à entrer à nouveau le nom du firmware dans le champ « file to upload » et de cliquez sur le bouton upload.

Une fois le firmware téléchargé correctement, la version peut être contrôlée depuis le menu TOOLS/firmware.

Tous les paramètres de configuration restent conservés sauf si la zone de mémoire flash contenant les paramètres de configuration a été corrompue. Dans ce dernier cas, les paramètres par défaut sont restaurés.

Depuis la révision 4.4.0 du firmware, cette page permet également de restaurer les paramètres par défaut du produit en cliquant sur le bouton « Reset setting ».