Notes de version pour les points d'accès Cisco Small Business AP541N versions 1.7.2 à 2.0.4

Septembre 2012

78-19182-09

Mise à niveau du micrologiciel

Nous vous recommandons d'effectuer une sauvegarde du périphérique dans un fichier enregistré sur un autre périphérique avant de mettre à niveau le micrologiciel.

Si vous avez effectué la mise à niveau du micrologiciel de la version 1.7.2 vers la version 1.8.0, 1.9.0, 1.9.1, 1.9.2, 2.0.0, 2.0.1 ou 2.0.2, vous *devez* restaurer les paramètres par défaut du périphérique en maintenant enfoncé le bouton de **réinitialisation** pendant au moins 10 secondes. Vous devez reconfigurer *manuellement* le périphérique pour votre réseau. Si vous rechargez le fichier de configuration créé avec la version 1.7.2 du micrologiciel et tentez de l'exécuter sur la version 1.8.x, 1.9.x ou 2.0.x du micrologiciel, les résultats sont imprévisibles.

La version 2.0.3 n'a pas été publiée.

Mises en garde pour la version 2.0.4

Mises en garde résolues

CSP #535465 : une station de client sans fil demandait continuellement une adresse DHCP. Le serveur envoyait des réponses, mais celles-ci ne s'affichaient pas sur l'interface sans fil.

Dans la version 2.0.1, le système TX FIFO qui gère le trafic de multidiffusion lorsque le point d'accès change de canal afin de rechercher d'autres points d'accès a été désactivé. Cependant, vous devez désactiver tous les systèmes TX FIFO lorsque le point d'accès change de canal afin de rechercher d'autres points d'accès. Si le point d'accès envoie des paquets aux systèmes TX FIFO alors qu'il est passé à un autre canal pour rechercher des balises, le microcode de la puce sans fil peut arrêter les paquets sortants.

Le point d'accès recherche régulièrement des points d'accès lorsque la mise en grappe ou la détection de points d'accès pirates sont activées. Lorsque la mise en grappe ou la détection de points d'accès pirates ne sont pas utilisées, le point d'accès ne change pas de canal pour détecter d'autres points d'accès. L'AP541N n'effectue pas d'analyse de canal agressive dans les deux premières minutes après le démarrage du point d'accès pour générer rapidement une table des éventuels points d'accès pirates ; il effectue cette opération uniquement au démarrage, puis ne l'effectue plus sauf si la fonctionnalité de détection des points d'accès pirates ou de mise en grappe est activée.

CSCub73520 : le problème du traitement DHCP entre le point d'accès et le serveur DHCP lorsque la mise en grappe ou la détection de points d'accès pirates est activée a été résolu.

Mises en garde pour la version 2.0.2

Mises en garde ouvertes

CSCty56257 : le basculement d'une version du micrologiciel à une autre peut prendre du temps et, une fois terminé, la page de connexion peut ne pas s'afficher automatiquement dans certains navigateurs, tels qu'Internet Explorer 8.

Solution de contournement : patientez deux minutes et actualisez l'écran. L'écran de connexion devrait s'afficher. Si ce n'est pas le cas, lancez un cycle d'alimentation du périphérique. Si vous utilisez Internet Explorer 8, vous pouvez également accéder à **Outils > Options Internet > Sécurité > Personnaliser le niveau** et activer **Demander le nom d'utilisateur et le mot de passe**. Ce paramètre peut aider à éviter le problème.

CSCtg90061 : l'ID d'objet (OID) sysUpTime ne correspond pas au temps de disponibilité réel du système. L'OID sysUpTime est actuellement lié à l'activation de SNMP. Par conséquent, à chaque fois que SNMP est activé, l'OID sysUpTime est initialisé à 0.

Solution de contournement : vérifiez **GUI Status (État de l'interface) > Informations concernant l'appareil > Temps d'activité du système**. Sinon, si une requête SNMP doit être envoyée, à condition que SNMP soit activé manuellement une fois le périphérique redémarré ET qu'il ne soit pas désactivé, sysUpTime sera proche du temps de disponibilité réel.

Mises en garde résolues

CSCtn81839 : le périphérique n'envoie qu'un paquet ARP gratuit pour une adresse au lieu de deux ou trois lors de la désactivation ou de l'activation de DHCP.

CSCts45126 : dans Google Chrome 13, la page À propos de ne s'affiche pas correctement.

CSCtn81981 : le périphérique ne diffuse pas de message Goodbye et envoie un seul paquet ARP gratuit pour une adresse IP au lieu de deux ou trois.

CSCtn82389 : la vérification des erreurs pour les SSID désactivés n'est pas cohérente.

CSCtn82420 : une adresse MAC en double ne devrait pas être autorisée dans le filtrage MAC.

CSCtn82500 : le contrôle d'accès d'administration ne devrait pas accepter d'adresses IP sources non valides.

Mises en garde pour la version 2.0.1

Mises en garde ouvertes

CSCts45075 : lors de l'utilisation avec Google Chrome, si l'utilisateur définit une adresse de redirection HTTP dans l'onglet **Sans fil** et qu'il enregistre les paramètres, un espace est ajouté avec le préfixe « http:// », ce qui entraîne l'échec de la fonctionnalité.

Solution de contournement : Firefox et Internet Explorer sont les seuls navigateurs pris en charge. Chrome n'est pas complètement pris en charge. Si vous souhaitez tout de même utiliser Chrome, supprimez l'espace à gauche dans la barre d'adresse, puis enregistrez les paramètres.

CSCts45092 : Firefox 4, 5 et Google Chrome rencontrent parfois des problèmes lors de l'ouverture des pages de l'interface graphique (session suspendue). Ce problème apparaît uniquement si plusieurs périphériques WAP sont connectés au même routeur comme périphérique WAP autonome ou dans une configuration de cluster.

Solution de contournement : Google Chrome n'est pas complètement pris en charge. Les versions ultérieures de Firefox telles que 4.x et 5.x ne sont pas entièrement prises en charge. Utilisez Internet Explorer ou effacez les cookies, l'historique et la mémoire cache du navigateur.

Mises en garde résolues

CSCti77839 : l'analyse RF fonctionne correctement et affiche tous les points d'accès.

CSCts51824 : impossible de voir tous les points d'accès voisins dans la liste UI Neighbor (Voisin d'interface utilisateur) (**État >Détection de point d'accès non autorisé**).

CSCts51821 : impossible de recevoir une adresse DHCP.

Mises en garde pour la version 2.0.0

Mises en garde ouvertes

CSCtn81665 : Bonjour ne démarre pas pour les modules enfichables dynamiques.

Solution de contournement : retirez puis reconnectez le câble Ethernet (non PoE). Effectuez un redémarrage.

CSCtn82461 : les noms d'hôtes qui commencent par un chiffre devraient être acceptés.

Les noms d'hôtes ne contenant que des chiffres ne sont pas autorisés. Cependant, un nom d'hôte qui commence par un chiffre et qui se termine par un chiffre ou un caractère non numérique devrait être accepté mais est actuellement rejeté.

Solution de contournement : n'utilisez pas de chiffre comme premier caractère.

CSCtn84775 : IPv6 n'est pas pris en charge avec Bonjour.

Solution de contournement : il n'y a aucune solution de contournement pour le moment.

Mises en garde résolues

CSCth14132 : l'isolation des stations est sporadique.

CSCth12675 : la configuration du filtrage MAC sur **Bloquer** ne bloque pas l'accès.

Mises en garde pour la version 1.9.2

ATTENTION Les mises à jour non valides du fichier de configuration XML peuvent entraîner un échec irrécupérable du périphérique. Lorsque vous apportez des mises à jour directement dans le fichier de configuration (par exemple, à l'aide d'un éditeur de texte), utilisez les valeurs de chaîne décrites dans le guide d'administration du point d'accès bibande à fréquence unique Cisco Small Business AP541N. Tout écart par rapport aux valeurs autorisées ou erreurs typographiques peut entraîner un dysfonctionnement du point d'accès. Dans certains cas, la récupération d'un tel échec par restauration des paramètres d'usine du périphérique est impossible.

À la date de rédaction de ces notes, tous les périphériques sont fournis avec l'ID de version de matériel (VID) V01 ; à l'avenir, en raison de l'éventuelle fin de vie d'un composant Flash, il est possible que nous fournissions la nouvelle version de matériel (VID) V02 à des fins de compatibilité avec le nouveau composant Flash. Dans ce cas, les périphériques dotés de l'ID de version de matériel (VID) V02 doivent s'exécuter sur la version 1.9.2 du micrologiciel ou version ultérieure, c'est-à-dire qu'ils ne doivent pas revenir à une version antérieure du micrologiciel.

Mises en garde pour la version 1.9.1

Mises en garde ouvertes

CSCth14132 : l'isolation des stations est sporadique.

Parfois, lorsque l'isolation des stations (communications LAN locales) est définie sur **Disabled auto** (Désactivée automatiquement), le périphérique revient à l'état **Blocking** (Bloquer). La configuration continue à indiquer que la fonctionnalité est **Désactivée**. Par conséquent, les ordinateurs ne peuvent pas accéder aux périphériques locaux, tels que les imprimantes. L'accès aux périphériques distants (en dehors du LAN du point d'accès local) est disponible (par exemple, l'accès à un site Web externe).
Solution de contournement : redémarrez le périphérique.

CSCth12675 : la configuration du filtrage MAC sur **Bloquer** ne bloque pas l'accès.

Si vous définissez le filtrage MAC de sorte à bloquer des adresses spécifiques, le périphérique ne parvient pas à empêcher l'association et l'authentification.
Solution de contournement : aucune.

Mises en garde résolues

CSCth09954 : CCA échoue en raison d'un nom de périphérique mal propagé.

Le nom de périphérique **AP 541NA-K9** a été propagé par les annonces CDP reçues de périphériques UC520. Le nom devrait être **AP541N-A-K9** (sans espace). L'espace entre **AP** et **541NA-K9** a empêché Cisco Configuration Assistant (CCA) d'accéder au point d'accès AP 541N à des fins de configuration.

Mises en garde pour la version 1.9.0

Mises en garde ouvertes

CSCtg53062 : l'interface de configuration autorise plus de 10 membres de cluster.

L'interface de configuration autorise plus de 10 membres de cluster. Cependant, l'ajout de plus de 10 membres de cluster dégrade les performances du périphérique, le voisinage réseau qui parfois affiche une force de signal NULL. Solution de contournement : nous recommandons qu'un cluster ne regroupe pas plus de 10 membres.

Mises en garde résolues

Les mises en garde suivantes ont été résolues dans la version 1.9.0 :

CSCtg28316 : la file d'attente multidiffusion du pilote WL se bloque.

Après une certaine période, le point d'accès arrête de transférer les trames de multidiffusion ou de diffusion. De plus, la dernière trame de la file d'attente de multidiffusion est toujours effacée.

CSCtg28338 : l'actualisation de la clé WPA se bloque.

Si au cours de la dissociation, le point d'accès actualise une clé de diffusion client, ce client n'est pas pris en compte et la machine d'état de la clé WPA se bloque.

CSCtg28357 : message d'erreur avec MIB Walk : Vous devez définir l'instance apRadioStationIsolation dans CISCO-WLAN-ACCESS-POINT-MIB.

Les bases MIB sont ajoutées dans le répertoire MIB net-SNMP, (C:\usr\share\snmp\mibs) :

```
CISCO-WLAN-ACCESS-POINT-MIB.txt
CISCO-WLAN-ACCESS-POINT-REF-MIB-A-SKU.txt
CISCO-WLAN-ACCESS-POINT-REF-MIB-E-SKU.txt
CISCO-WLAN-ACCESS-POINT-REF-MIB-N-SKU.txt
```

Les noms de bases MIB sont C:\usr\etc\snmp (snmp.conf). Exemple :

```
mibdirs C:/usr/share/snmp/mibs
persistentDir C:/usr/snmp/persist
tempFilePattern C:/usr/temp/snmpdXXXXXX
mibs +OLD-CISCO-CHASSIS-MIB
mibs +CISCO-WLAN-ACCESS-POINT-REF-MIB
mibs +CISCO-WLAN-ACCESS-POINT-REF-MIB
mibs +CISCO-WLAN-ACCESS-POINT-REF-MIB
mibs +CISCO-WLAN-ACCESS-POINT-MIB
```

En cas de problème avec les bases MIB ajoutées, l'exécution d'une commande **MIB walk** à l'invite de commande génère un message d'erreur. Exemple :

```
C:\Documents and Settings\tdobrovo\Desktop>snmpwalk -v 2c -c public 172.25.144.155
sysObjectID

Undefined OBJECT (apRadioStationIsolation): À la ligne 3670 dans C:/usr/
share/snmp/mibs/CISCO-WLAN-ACCESS-POINT-MIB.txt
SNMPv2-MIB::sysObjectID.0 = OID: CISCO-SMI::ciscoProducts.1135.1.28
```

Pour éviter cette erreur, définissez **apRadioStationIsolation** dans **CISCO-WLAN-ACCESS-POINT-MIB**.

CSCtg28364 : point d'accès EDCA autonome : valeurs incorrectes signalées pour les attributs de file d'attente de rafale TxOP.

Le paramètre **EDCA Max Burst** doit être en unité de périodes de **32us**, mais n'est pas converti correctement par le point d'accès.

CSCtg28367 : Cisco AP541N MIB sysObjectId ne retourne pas le bon numéro.

L'OID retourné par l'objet dans le code du point d'accès est incorrect.

CSCtg28374 : la commande cdp show neighbor n'affiche que quatre entrées CDP.

Lorsque la commande **`cdh show neighbor`** est exécutée sur la console, seulement quatre entrées de voisins s'affichent.

Mises en garde pour la version 1.8.0

Mises en garde ouvertes

Il n'existe aucune mise en garde ouverte pour la version 1.8.0 :

Mises en garde résolues

Les mises en garde suivantes ont été résolues dans la version 1.8.0 :

CSCtd63549 : le paramètre de temps ne permet pas de définir le fuseau horaire.

CSCtd63503 : les téléphones IP sans fil sont souvent désenregistrés.

CSCtd63487 : certaines pages s'affichent très lentement.

CSCtd62176 : les paquets vocaux sont abandonnés à la réception sur les clients 7921.

CSCtd62146 : l'image principale est endommagée après 10 jours.

CSCtd62123 : l'heure système ne peut pas être définie à l'aide de l'interface graphique utilisateur.

CSCtd62096 : supprimez les références IPV6, car elles ne sont pas prises en charge.

CSCtd62087 : WPA-PSK-AES échoue si deux SSID ouverts à différents niveaux de sécurité portent le même nom.

CSCtd62084 : les paramètres d'isolation des stations ne se propagent pas lorsque la mise en grappe est activée.

CSCtd62071 : les valeurs de champs de gestion et de VLAN non balisés ne peuvent pas être modifiées.

Mises en garde pour la version 1.7.2

Mises en garde ouvertes

Les mises en garde suivantes sont ouvertes dans la version 1.7.2 :

CSCtd63549 : le paramètre de temps ne permet pas de définir le fuseau horaire.

La configuration NTP dans la fenêtre Configuration ne permet pas de configurer le fuseau horaire.

CSCtd63503 : les téléphones IP sans fil sont souvent désenregistrés.

Les téléphones IP peuvent s'enregistrer correctement auprès du gestionnaire d'appels et passer des appels. Cependant, les téléphones sont désenregistrés après 5 minutes, parfois en cours d'appel. L'association sans fil est préservée. Il est possible que les messages d'entretien (messages de bon fonctionnement) envoyés par le téléphone n'atteignent pas CME, et par conséquent CME désenregistre les téléphones.

CSCtd63487 : certaines pages s'affichent très lentement.

Certaines pages de l'interface de configuration s'affichent lentement dans l'image AP541N-1.2(1) lorsque l'onglet Advanced (Avancé) est sélectionné.

CSCtd62176 : les paquets vocaux sont abandonnés à la réception sur les clients 7921.

Les paquets vocaux sont abandonnés à la réception sur les clients 7921. Le gestionnaire d'appels utilise le codec G.711 par défaut. La transmission et la réception aux deux extrémités devraient être de 50 pps (paquets par seconde). La transmission sur le 7960 est de 50 pps (égale à la réception sur le 7921) mais la réception sur le 7960 est uniquement de 40 à 43 pps, soit environ 14 % de paquets abandonnés sur le flux RTP entre le 7921 et le 7960.

CSCtd62146 : l'image principale est endommagée après 10 jours.

L'image principale est endommagée après 10 jours d'utilisation. Après plusieurs redémarrages d'une image 1.4(0), elle est soudainement signalée comme étant endommagée et le périphérique est renvoyé vers l'image secondaire.

CSCtd62123 : l'heure système ne peut pas être définie à l'aide de l'interface graphique utilisateur.

Le paramètre d'heure système ne peut pas être défini manuellement à l'aide de l'interface graphique utilisateur.

CSCtd62096 : supprimez les références à IPV6, car elles ne sont pas prises en charge.

Des références à IPV6 sont présentes, mais ne sont pas prises en charge.

CSCtd62087 : WPA-PSK-AES échoue si deux SSID ouverts à différents niveaux de sécurité portent le même nom.

Le périphérique Cisco autorise deux SSID à porter le même nom, s'ils ont des niveaux de sécurité différents. Cependant, la plupart des périphériques client ne voient pas la différence et les considèrent comme un même BSSID. Si deux SSID portent le même nom, un avec WPA-PSK-AES et un sans, le réseau ne parvient pas à transmettre le trafic.

CSCtd62084 : les paramètres d'isolation des stations ne se propagent pas lorsque la mise en grappe est activée.

Les paramètres d'isolation des stations pour les VAP ne se propagent pas lorsque la mise en grappe est activée.

CSCtd62071 : les valeurs de champs de gestion et de VLAN non balisés ne peuvent pas être modifiées.

Les champs Management VLANid (Gestion de l'ID de VLAN) et Untagged VLANid (ID de VLAN non balisé) dans l'interface acceptent la saisie utilisateur. Cependant, les modifications ne sont pas acceptées et les valeurs de la configuration du périphérique conservent la valeur par défaut, de 1.

Informations connexes

Assistance	
Communauté d'assistance Cisco Small Business	www.myciscocommunity.com/community/smallbizsupport
Assistance technique et documentation en ligne (identification obligatoire)	www.cisco.com/support
Coordonnées de l'assistance téléphonique	www.cisco.com/en/US/support/tsd_cisco_small_ business_support_ center_contacts.html
Téléchargements de logiciel (Identification obligatoire)	Rendez-vous sur le site tools.cisco.com/support/downloads, puis saisissez le numéro du modèle dans la zone de recherche de logiciels Software Download Search.
Cisco Small Business	
Site Cisco Partner Central pour les petites entreprises (connexion partenaire requise)	www.cisco.com/web/partners/sell/smb
Accueil Cisco Small Business	www.Cisco.com/smb
Marketplace	www.cisco.com/go/marketplace

78-21009-01