

9160 G2

Passerelle sans fil (Wireless Gateway)

Manuel d'utilisation

2 novembre 2009

P/N 8000347.A



Certifié conforme ISO 9001
Système de gestion de la qualité



© Copyright 2009 par Psion Teklogix Inc.

2100 Meadowvale Boulevard, Mississauga, Ontario, Canada L5N 7J9

<http://www.psionteklogix.com>

Ce document, et les informations qu'il contient, est la propriété de Psion Teklogix Inc., est émis en stricte confidentialité et ne doit pas être reproduit ou copié, en tout ou partie, sauf dans le seul but de promouvoir la vente de biens et services fabriqués par Psion Teklogix. En outre, ce document ne peut pas servir de base à une conception, une fabrication, un sous-contrat, ou de quelque manière qui pourrait être préjudiciable aux intérêts de Psion Teklogix Inc.

Non responsabilité

Tout a été mis en œuvre pour assurer que cette documentation soit complète, précise et à jour. En outre, des modifications sont régulièrement ajoutées aux informations contenues dans ce document ; ces modifications seront intégrées aux nouvelles éditions de cette publication.

Psion Teklogix Inc. se réserve le droit d'apporter des améliorations et/ou des modifications au(x) produit(s) et/ou au(x) programme(s) décrit(s) dans ce document sans préavis et ne pourra être tenu pour responsable des dommages, notamment, mais sans s'y limiter, les dommages accessoires consécutifs à une utilisation des informations présentées, notamment, mais sans s'y limiter, les erreurs typographiques.

Windows® et le logo Windows sont des marques commerciales ou déposées de Microsoft Corporation aux États-Unis et/ou dans d'autres pays.

Toutes les marques et noms commerciaux sont la propriété de leurs détenteurs respectifs.

Garantie de retour à l'usine

Psion Teklogix Inc. fournit une garantie de retour à l'usine de ce produit pendant une durée de douze (12) mois conformément à la Déclaration de garantie limitée et de limitation de responsabilité prévue à l'adresse suivante :

www.psionteklogix.com/warranty

La garantie des équipements fabriqués par Psion Teklogix ne s'applique pas aux produits qui ont été altérés, modifiés ou réparés par toute autre personne qu'un employé d'une entreprise de services agréée par Psion Teklogix. Reportez-vous aux termes et conditions de vente de Psion Teklogix pour plus de détails.



Important : Les garanties de Psion Teklogix prennent effet à la date d'expédition.

Services et informations

Psion Teklogix fournit une gamme complète de services d'assistance produit et d'informations à ses clients dans le monde entier. Ces services incluent l'assistance technique et les réparations produits. Pour localiser votre service d'assistance local, rendez-vous sur

www.psionteklogix.com/service-and-support.htm

Pour accéder à plus d'informations sur les produits courants et n'étant plus disponibles à la vente, rendez-vous sur <https://teknet.psionteklogix.com> et connectez-vous ou appuyez sur « Not Registered? » (Vous n'êtes pas enregistré ?), selon que vous êtes déjà inscrit ou non à Teknet. Une section d'informations produit archivées est disponible en ligne.



Directive 2002/96/CE relative aux déchets d'équipements électriques et électroniques (DEEE)

Ce produit et ses accessoires répondent aux exigences de la directive 2002/96/CE relative aux déchets d'équipements électriques et électroniques (DEEE). Si votre produit ou accessoire Psion Teklogix en fin de cycle de vie porte une étiquette comme illustré ici, contactez votre représentant pour obtenir des détails sur l'organisation du recyclage.

Pour obtenir la liste des filiales internationales, rendez-vous à l'adresse suivante :

www.psionteklogix.com/EnvironmentalCompliance

Directive 2002/95/CE relative à la limitation de l'utilisation de certaines substances dangereuses (RoHS)

Qu'est-ce que la directive RoHS ?

L'Union Européenne a décidé de la mise en place de normes environnementales dans la conception et la fabrication de produits électriques et électroniques vendus en Europe, afin de réduire la pénétration de substances dangereuses dans l'environnement. La « directive relative à la limitation de l'utilisation de certaines substances dangereuses (RoHS) » impose des niveaux de trace maximum de plomb, cadmium, mercure, chrome hexavalent, PBB et PBDE ignifuges pouvant être contenus dans un produit. Seuls les produits répondant à ces normes environnementales élevées peuvent être « mis sur le marché » dans les états membres depuis le 1er juillet 2006.



Logo RoHS

Bien qu'il n'y ait aucune obligation légale de marquage des produits conformes à la directive RoHS, Psion Teklogix Inc. indique sa conformité avec la directive comme suit :

Le logo RoHS situé à l'arrière du produit ou sous la batterie dans le compartiment de la batterie (ou sur un accessoire comme le chargeur ou une station d'accueil) signifie que le produit est conforme à RoHS, comme le demande la directive européenne. Sauf indication ci-dessous, un produit Psion Teklogix produit qui n'est pas doté d'un logo RoHS signifie qu'il a été mis sur le marché de l'UE avant le 1er juillet 2006, et qu'il est donc exclus du champ d'application de cette directive.



Remarque : Les accessoires ou périphériques n'ont pas tous un logo RoHS à cause de limitations d'espace physiques ou de leur statut d'exemption.

TABLE DES MATIÈRES

Synthèse de sécurité et des homologations.	xiii
---	------

Chapitre 1 : Introduction

1.1	À propos de ce manuel	3
1.2	Fonctionnalités d'aide en ligne, navigateurs pris en charge et limitations.	6
1.3	Conventions de texte.	7
1.4	Présentation de la passerelle sans fil 9160 G2 Wireless Gateway	7
1.4.1	Radios.	8
1.4.2	Fonctionnalités du point d'accès	9
1.4.3	Fonctionnalités de la station de base	9
1.4.4	Fonctionnalités du mini-contrôleur	9
1.5	Fonctionnalités et avantages	10
1.5.1	Conformité Wi-Fi et prise en charge des normes IEEE.	10
1.5.2	Fonctionnalités sans fil	10
1.5.2.1	Le protocole Psion Teklogix 802.IQ	11
1.5.3	Fonctionnalités de sécurité.	11
1.5.4	Interface Invité prête à l'emploi	12
1.5.5	Mise en cluster et gestion automatique.	12
1.5.6	Mise en réseau	13
1.5.7	Prise en charge SNMP.	13
1.5.8	Capacité de maintenance	14
1.6	Quelle est la prochaine étape ?	14

Chapitre 2 : Configuration d'installation requise

2.1	Choix de l'emplacement adéquat	17
2.1.1	Environnement	17
2.1.2	Maintenance	18
2.1.3	Radios.	18
2.1.4	Alimentation et câbles d'antenne.	18

2.1.4.1	Alimentation	18
2.1.4.2	Antennes	19
2.2	Connexion à des appareils externes	20
2.2.1	Ports	20
2.2.2	Installation du réseau local (LAN) : présentation	21
2.2.3	Installation d'un LAN : Ethernet	21
2.2.3.1	Câblage Ethernet	22
2.2.3.2	Port Ethernet à fibres optiques 100Base-FX	22
2.2.4	Indicateurs d'état (LED)	23
2.2.5	Connexion d'un terminal à affichage vidéo	23
2.3	Modification de la configuration avec un navigateur Web	24

Chapitre 3 : Liste de contrôle du pré-lancement

3.1	La passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway	27
3.1.1	Paramètres par défaut de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway	27
3.1.2	Ce que le point d'accès ne fournit pas	31
3.2	Ordinateur de l'administrateur	31
3.3	Ordinateurs client sans fil	32
3.4	Présentation de l'adressage IP statique et dynamique sur la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway	33
3.4.1	Comment le point d'accès obtient-il une adresse IP au démarrage ?	34
3.4.2	Adressage IP dynamique	34
3.4.3	Adressage IP statique	34
3.4.4	Restauration d'une adresse IP	35

Chapitre 4 : Étapes rapides de configuration et de lancement

4.1	Déballer la passerelle sans fil 9160 G2 Wireless Gateway	39
4.1.1	Matériel et ports de la passerelle sans fil 9160 G2 Wireless Gateway	39
4.1.2	Qu'y a-t-il dans la passerelle sans fil 9160 G2 Wireless Gateway ?	39
4.2	Connecter le point d'accès au réseau et à l'alimentation	40
4.2.1	Une remarque sur la configuration de connexions pour un réseau invité	42
4.2.1.1	Connexions matérielles pour un VLAN invité	42
4.3	Mise sous tension du point d'accès	42
4.4	Se connecter aux pages Web d'administration	42

4.4.1	Affichage des paramètres de base des points d'accès	43
4.5	Configurer les paramètres de base et démarrer le réseau sans fil	44
4.5.1	Configuration par défaut	44
4.6	Quelle est la prochaine étape ?	44
4.6.1	Vérifier que le point d'accès est connecté au réseau local	44
4.6.2	Tester la connectivité LAN avec les clients sans fil	45
4.6.3	Sécuriser et affiner le point d'accès avec des fonctions avancées	45

Chapitre 5 : Configuration des paramètres de base

5.1	Accès aux paramètres de base	49
5.2	Révision / Description du point d'accès	50
5.3	Fournir des paramètres réseau	51
5.4	Mise à jour des paramètres de base	52
5.5	Paramètres de base pour un point d'accès autonome	52
5.6	Votre réseau d'un coup d'œil : Présentation des icônes d'indicateur	52
5.7	Affichage de l'interface utilisateur avec des couleurs et styles différents	52

Chapitre 6 : Gestion des points d'accès et des clusters

6.1	Présentation	57
6.2	Accès à la gestion des points d'accès	57
6.3	Présentation de la mise en cluster	58
6.3.1	Qu'est-ce qu'un cluster ?	58
6.3.2	Combien de points d'accès un cluster peut-il prendre en charge ?	58
6.3.3	Quels types de points d'accès peuvent être mis en cluster ensemble ?	58
6.3.4	Quelle est la relation entre le point d'accès coordinateur et les autres membres du cluster ?	59
6.3.5	Quels paramètres sont/ne sont pas partagés dans le cadre de la configuration du cluster ?	59
6.3.5.1	Paramètres partagés dans la configuration du cluster	59
6.3.5.2	Paramètres non partagés par le cluster	60
6.3.6	Formation du cluster	60
6.3.7	Taille de cluster et appartenance	61
6.3.8	Sécurité Intra-Cluster	61
6.4	Présentation des paramètres de point d'accès	61
6.4.1	Modification de la description d'emplacement	63

6.4.2	Définition du nom du cluster	63
6.5	Démarrage de la mise en cluster	63
6.6	Arrêt de la mise en cluster	64
6.7	Informations de configuration pour un point d'accès spécifique et gestion des points d'accès autonomes	64
6.7.1	Accès à un point d'accès en utilisant son adresse IP dans une URL.....	65
6.8	Surveillance de session	65
6.8.1	Accès à la surveillance de session	65
6.8.2	Présentation des informations de surveillance de session.....	65
6.8.3	Affichage des informations de session pour les points d'accès.....	67
6.8.4	Tri des informations de session	68
6.8.5	Actualisation des informations de session.....	68

Chapitre 7 : Gestion des comptes d'utilisateur

7.1	Présentation	71
7.2	Accès à la gestion des utilisateurs	71
7.2.1	Affichage des comptes d'utilisateur	72
7.2.2	Ajout d'un utilisateur	72
7.2.3	Modification d'un compte d'utilisateur	74
7.2.4	Activation et désactivation des comptes d'utilisateur	74
7.2.5	Activation d'un compte d'utilisateur.....	74
7.2.6	Désactivation d'un compte d'utilisateur	75
7.2.7	Suppression d'un compte d'utilisateur	75
7.3	Sauvegarde et restauration d'une base de données utilisateur	75
7.3.1	Sauvegarde de la base de données utilisateur.....	75
7.3.2	Restauration d'une base de données utilisateur depuis un fichier de sauvegarde	76

Chapitre 8 : Gestion des canaux

8.1	Accès à la gestion des canaux	79
8.2	Présentation de la gestion des canaux	79
8.2.1	Fonctionnement en quelques mots	79
8.2.2	Pour les curieux : plus de détails sur les canaux avec chevauchement	80
8.2.3	Exemple : un réseau avant et après la gestion des canaux	80
8.3	Configuration et affichage des paramètres de gestion des canaux	81

8.3.1	Arrêt/démarrage de l'affectation automatique des canaux	82
8.3.2	Affichage des affectations de canaux actuelles et définition de verrouillages	82
8.3.2.1	Mettre à jour les paramètres actuels de canal (manuel).....	83
8.3.3	Affichage du dernier ensemble de modifications proposé	83
8.3.4	Configuration des paramètres avancés (Personnalisation/programmation de plans de canaux).....	84
8.3.4.1	Mise à jour des paramètres avancés	86

Chapitre 9 : Voisinage sans fil

9.1	Accès au voisinage sans fil.....	89
9.2	Présentation des informations du voisinage sans fil.....	89
9.3	Affichage du voisinage sans fil.....	90
9.4	Affichage des détails d'un membre du cluster	92

Chapitre 10 : Configuration de la sécurité

10.1	Présentation des problèmes de sécurité sur les réseaux sans fil	97
10.1.1	Comment puis-je savoir quel mode de sécurité utiliser ?	97
10.1.2	Comparaison des modes de sécurité pour la gestion des clés, algorithmes d'authentification et de cryptage.....	98
10.1.2.1	Quand utiliser le mode non crypté (aucune sécurité).....	99
10.1.2.2	Quand utiliser le mode WEP statique.....	99
10.1.2.3	Quand utiliser le mode IEEE 802.1x	100
10.1.2.4	Quand utiliser le mode WPA Personal	102
10.1.2.5	Quand utiliser le mode WPA Enterprise	103
10.1.3	Interdire le SSID de diffusion améliore-t-il la sécurité ?.....	104
10.1.4	Comment l'isolation de station protège-t-elle le réseau ?	105
10.2	Configuration des paramètres de sécurité	105
10.2.1	Broadcast SSID (SSID de diffusion), Station Isolation (Isolation de station) et Security Mode (Mode de sécurité)	106
10.2.2	Modes de sécurité	107
10.2.2.1	None (Plain-text) (Aucun (texte brut))	108
10.2.2.2	Static WEP (WEP statique)	109
10.2.2.3	IEEE 802.1x	114
10.2.2.4	WPA Personal	117
10.2.2.5	WPA Enterprise	119

10.3	Mise à jour des paramètres.....	124
------	---------------------------------	-----

Chapitre 11 : Maintenance et surveillance

11.1	Interfaces	127
11.1.1	Paramètres Ethernet (filaire).....	128
11.1.2	Paramètres sans fil	128
11.2	Journaux des événements	128
11.2.1	Activation ou désactivation de la persistance	129
11.2.2	Severity (Gravité)	130
11.2.3	Profondeur	130
11.2.4	Hôte de relais de journal pour les messages du noyau	131
11.2.4.1	Présentation de la journalisation à distance	131
11.2.4.2	Configuration de l'hôte de relais de journal	131
11.2.4.3	Activation/désactivation de l'hôte de relais de journal sur la page Status > Events (État > Événements)	132
11.2.5	Journal des événements.....	133
11.3	Statistiques d'émission/réception	134
11.4	Clients sans fil associés	136
11.4.1	Contrôle d'intégrité de la liaison	136
11.5	Points d'accès voisins	136

Chapitre 12 : L'interface Ethernet (filaire)

12.1	Accès aux paramètres Ethernet (filaire)	143
12.1.1	DNS Hostname (Nom d'hôte DNS).....	144
12.1.2	Accès invité	144
12.1.2.1	Configuration d'un réseau LAN interne et d'un réseau invité.....	144
12.1.2.2	Activation ou désactivation de l'accès invité	145
12.1.2.3	Spécification d'un réseau invité virtuel	145
12.1.3	Réseaux sans fil virtuels (VLAN).....	146
12.1.4	Paramètres de l'interface interne	147
12.1.5	Paramètres de l'interface invité	150
12.1.6	Mise à jour des paramètres	150

Chapitre 13 : Définition de l'interface sans fil

13.1	Accès aux paramètres sans fil	153
------	-------------------------------------	-----

13.2	Configuration de la prise en charge du domaine réglementaire 802.11d.....	154
13.3	802.11h Regulatory Domain Control (Contrôle du domaine réglementaire 802.11h)....	155
13.4	Configuration de l'interface radio	156
13.5	Configuration des paramètres de LAN sans fil « interne ».....	157
13.6	Configuration des paramètres sans fil de réseau « invité ».....	158
13.7	Mise à jour des paramètres sans fil.....	158

Chapitre 14 : Configuration de l'accès invité

14.1	Présentation de l'interface invité.....	161
14.2	Configuration de l'interface invité.....	162
14.2.1	Configuration d'un réseau invité sur un VLAN	162
14.2.2	Configuration de l'écran d'accueil (portail captif)	163
14.3	Utilisation du réseau invité en tant que client.....	164
14.4	Exemple de déploiement.....	165

Chapitre 15 : Configuration de VLAN

15.1	Accès aux paramètres de réseau sans fil virtuels.....	169
15.2	Configuration de VLAN	169
15.3	Mise à jour des paramètres.....	171

Chapitre 16 : Configuration des paramètres radio 802.11

16.1	Présentation des paramètres radio	175
16.2	Accès aux paramètres radio	175
16.3	Configuration des paramètres radio	177
16.4	Mise à jour des paramètres.....	182

Chapitre 17 : Filtrage d'adresses MAC

17.1	Accès aux paramètres de filtrage MAC	185
17.2	Utilisation du filtrage MAC.....	186
17.3	Mise à jour des paramètres.....	186

Chapitre 18 : Équilibrage de la charge

18.1	Présentation de l'équilibrage de la charge.....	189
18.1.1	Identification d'un déséquilibre : points d'accès souvent encombrés ou sous-utilisés	189
18.1.2	Définition de limites pour l'utilisation et les associations de client.....	190

18.1.3	Équilibrage de la charge et qualité de service (QoS)	190
18.2	Navigation vers les paramètres de l'équilibrage de la charge	190
18.3	Configuration de l'équilibrage	191
18.4	Mise à jour des paramètres	193

Chapitre 19 : Qualité de service (QoS)

19.1	Présentation de QoS	197
19.1.1	QoS et équilibrage de la charge	197
19.1.2	Prise en charge des normes 802.11e et WMM	197
19.1.3	Files d'attente et paramètres QoS pour coordonner le flux de trafic	198
19.1.3.1	Files d'attente QoS et type de service (ToS) pour les paquets	198
19.1.3.2	Contrôle EDCF des trames de données et espaces indépendant d'arbitrage	200
19.1.3.3	Interruption aléatoire et fenêtres de contention minimale/maximale	201
19.1.3.4	Salve de paquets pour de meilleures performances	202
19.1.3.5	Intervalle Transmission Opportunity (TXOP) pour stations client	202
19.1.4	802.1p et balises DSCP	202
19.1.4.1	Priorité VLAN	204
19.1.4.2	Priorité DSCP	205
19.2	Configuration des files d'attente QoS	205
19.2.1	Configuration des paramètres EDCA du point d'accès	208
19.2.2	Activation/désactivation de Wi-Fi Multimedia	210
19.2.3	Configuration des paramètres EDCA de la station	210
19.3	Mise à jour des paramètres	212

Chapitre 20 : Système de distribution sans fil (WDS)

20.1	Présentation du système de distribution sans fil (WDS)	215
20.1.1	Utilisation de WDS pour ponter les réseaux locaux filaires distants	215
20.1.2	Utilisation de WDS pour étendre réseau au-delà de la zone de couverture filaire	216
20.1.3	Utilisation de WDS pour la création de liaisons de sauvegarde	217
20.2	Remarques relatives à la sécurité associées aux liaisons WDS	217
20.2.1	Présentation du cryptage de données WEP statique	218
20.2.2	Présentation du cryptage de données WPA (PSK)	218

20.3	Configuration des paramètres WDS	219
20.3.1	Exemple de configuration d'une liaison WDS	222
20.4	Mise à jour des paramètres	223

Chapitre 21 : Configuration de SNMP

21.1	Présentation des paramètres SNMP	227
21.2	Accès aux paramètres SNMP	228
21.3	Configuration des paramètres SNMP	229
21.3.1	Configuration des alertes SNMP	232
21.3.2	Mise à jour des paramètres SNMP	233

Chapitre 22 : La 9160 G2 comme station de base

22.1	Présentation	237
22.2	Protocoles radio	238
22.2.1	Protocole d'interrogation adaptative/de contention	238
22.3	Menus Narrow Band (Bande étroite)	239
22.3.1	Paramètres de configuration de radio à bande étroite	239
22.3.1.1	Paramètres de radio RA1001A	241
22.3.2	Options de connectivité	242
22.3.3	Options de connectivité : mode station de base	242
22.3.3.1	Paramètres de protocole d'interrogation	244
22.3.3.2	Paramètres radio	247
22.3.4	Options de connectivité : mode MRR	248
22.4	Menus de connectivité	248
22.4.1	Paramètres de configuration de station de base	250
22.4.2	Paramètres de configuration des groupes MRR	251
22.4.2.1	RRM Groups (Groupes MRR)	253
22.4.2.2	Paramètres de protocole d'interrogation	254
22.4.2.3	Paramètres radio	256
22.4.2.4	Paramètres de groupe	257
22.4.2.5	Remote Radio Modules (Modules radio à distance (MRR))	258
22.4.3	Paramètres de configuration des fonctionnalités de liaison radio	258
22.4.3.1	Fonctionnalités de liaison radio	260
22.4.3.2	Automatic Radio Address (Adresse radio automatique)	261
22.4.3.3	Automatic Terminal Number (Numéro de terminal automatique)	262

22.4.4	Menu Hosts (Hôtes)	263
22.4.4.1	Configuration 9010	266

Chapitre 23 : Configuration du mini-contrôleur

23.1	Présentation	269
23.2	Menu de configuration du mini-contrôleur	270
23.3	Menu Hosts (Hôtes)	270
23.4	Options du menu de l'hôte	274
23.4.1	Émulation 3274	274
23.4.1.1	Options d'émulation	274
23.4.1.2	Options TESS	275
23.4.1.3	Options de protocole Telnet	285
23.4.1.4	Configurations des touches de fonction	289
23.4.2	Émulation 5250	290
23.4.2.1	Options d'émulation	290
23.4.2.2	Options TESS	291
23.4.2.3	Options de protocole Telnet	301
23.4.2.4	Configurations des touches de fonction	305
23.4.3	Émulation ANSI	306
23.4.3.1	Options d'émulation	306
23.4.3.2	Options de protocole Telnet	310
23.4.3.3	Auto-Telnet/Auto-login (Telnet automatique/Connexion automatique)	312
23.4.3.4	Configurations des touches de fonction	316

Chapitre 24 : Paramètres 802.IQ

24.1	Fonctionnalités 802.IQ	319
24.1.1	Fonctionnalités communes 802.IQ v1/v2	319
24.1.2	Fonctionnalités 802.IQ v1	322
24.1.3	Menu des fonctionnalités 802.IQ v2	323
24.2	Mise à jour des paramètres 802.IQ	323

Chapitre 25 : Serveur Network Time Protocol (NTP)

25.1	Accès aux paramètres horaires	327
25.2	Activation ou désactivation d'un serveur NTP (Network Time Protocol)	328

25.3	Mise à jour des paramètres.....	329
------	---------------------------------	-----

Chapitre 26 : Sauvegarder et restaurer la configuration

26.1	Accès aux paramètres de configuration du point d'accès	333
26.2	Réinitialisation de la configuration d'usine par défaut	334
26.3	Enregistrement de la configuration en cours dans un fichier de sauvegarde	334
26.4	Restauration de la configuration à partir d'un fichier enregistré précédemment	335
26.5	Redémarrage du point d'accès.....	335
26.6	Mise à niveau du firmware.....	336
26.6.1	Mise à jour	337
26.6.2	Vérification de la mise à niveau du firmware	337

Chapitre 27 : Spécifications

27.1	Description physique	341
27.2	Exigences en termes d'environnement.....	341
27.3	Exigences en termes d'alimentation CA	341
27.4	Exigences en termes d'alimentation Power Over Ethernet	342
27.5	Processeur et mémoire	342
27.6	Interfaces réseau	342
27.7	Radios	342

Annexe A : Brochages de port et diagrammes des câbles

A.1	Port de console	A-1
A.2	Descriptions des câbles série.....	A-1
A.3	Brochages des connecteurs RJ-45 (Ethernet 10BaseT/100BaseT)	A-3

Annexe B : Paramètres de sécurité sur clients sans fil/serveur RADIUS

B.1	Infrastructure réseau ; choix entre un serveur d'authentification intégré ou externe.....	B-8
B.1.1	Utilisation du serveur d'authentification intégré (EAP-PEAP)	B-8
B.1.2	Utilisation d'un serveur RADIUS externe avec des certificats EAP-TLS ou EAP-PEAP.....	B-8
B.2	Assurez-vous que le logiciel client sans fil est à jour.....	B-9
B.3	Accès aux paramètres de sécurité client sans fil Microsoft Windows	B-9
B.4	Configuration d'un client pour accéder à un réseau non sécurisé (aucune sécurité).....	B-11
B.5	Configuration de la sécurité WEP statique sur un client.....	B-12

B.6	Configuration de la sécurité IEEE 802.1x sur un client	B-15
B.6.1	Client IEEE 802.1x utilisant EAP/PEAP	B-15
B.6.2	Client IEEE 802.1x utilisant un certificat EAP/TLS	B-19
B.7	Configuration de la sécurité WPA/WPA2 Entreprise (RADIUS) sur un client	B-23
B.7.1	Client WPA/WPA2 Entreprise (RADIUS) utilisant EAP/PEAP	B-23
B.7.2	Client WPA/WPA2 Entreprise (RADIUS) utilisant un certificat EAP-TLS	B-27
B.8	Configuration de la sécurité WPA/WPA2 Personal (PSK) sur un client	B-31
B.9	Configuration d'un serveur RADIUS externe pour reconnaître la 9160 G2	B-34
B.10	Obtention d'un certificat TLS-EAP pour un client	B-38
B.11	Configuration du serveur RADIUS pour les balises VLAN	B-43
B.11.1	Configuration d'un serveur RADIUS	B-43

Annexe C : Dépannage

C.1	Problèmes et solutions relatifs au système de distribution sans fil (WDS)	C-47
C.2	Rétablissement de cluster	C-48
C.2.1	Redémarrer ou réinitialiser le point d'accès	C-48

Annexe D : Glossaire

Index	1
--------------------	---

SYNTHÈSE DE SÉCURITÉ ET DES HOMOLOGATIONS

DÉCLARATION DE CONFORMITÉ

Produit :	9160 G2 Wireless Gateway - RA2050, RA2060 et RA1001A
Application des directives du conseil :	Directive CEM : 2004/108/CE Directive sur les basses tensions : 2006/95/CE Directive européenne sur la réduction de l'utilisation de substances dangereuses : 2002/95/CE Directive R&TTE : 1999/5/CEE
Conformité déclarée aux normes :	EN 55022, classe B EN 61000-3-2 ; EN 61000-3-3 EN 55024 ETSI EN 300 113-1 : V1.6.1 (2006-08) EN 301 893 : 2003-08 V1.2.3 EN 300 328 : 2004-11 V1.6.1 EN 301 489-1/17 : 2004-11 V1.5.1/ 2002-08 V1.2.1 ETSI EN 301 489-5 V1.3.1 (2002-08) EN 60950-1
Fabricant :	PSION TEKLOGIX INC. 2100 Meadowvale Blvd. Mississauga, Ontario ; Canada L5N 7J9
Année de fabrication :	2006
Adresse du fabricant dans la Communauté européenne :	PSION TEKLOGIX Bourne End Business Centre Cores End Road, Bourne End, SL8 5AR Royaume-Uni
Type d'équipement :	Équipement informatique
Classe d'équipement :	Commerciale et industrielle légère

Déclaration FCC

DÉCLARATION DE CONFORMITÉ DE LA FCC (DoC)

Nom et adresse postale du demandeur : PSION TEKLOGIX
2100 Meadowvale Blvd.
Mississauga, Ontario ; Canada L5N 7J9
N° de téléphone : (905) 813-9900

Représentant légal aux États-Unis : Psion Teklogix Corp.
Nom et adresse : 1810 Airport Exchange Blvd., Suite 500
Erlanger, Kentucky, 41018, États-Unis
N° de téléphone : (859) 372-4329

Type d'équipement/environnement
d'utilisation : Appareils informatiques

Nom de marque / n° de modèle : **9160 G2 Wireless Gateway**

Année de fabrication : 2005

Normes auxquelles la conformité est déclarée :

La passerelle sans fil **9160 G2 Wireless Gateway**, fournie par Psion Teklogix, a été testée et déclarée conforme aux normes **FCC SECTION 15, SOUS-PARTIE B - RADIATEURS NON DÉLIBÉRÉS, APPAREILS INFORMATIQUES DE CLASSE B POUR UNE UTILISATION DOMESTIQUE OU PROFESSIONNELLE**.

Fabricant : Psion Teklogix Inc.
Mississauga, Ontario, Canada

Représentant légal aux États-Unis : Psion Teklogix Corp.
Erlanger, Kentucky, États-Unis

La passerelle sans fil 9160 G2 Wireless Gateway a été testée et déclarée conforme aux caractéristiques pour un appareil numérique de classe B, conformément à la section 15 des règles de la FCC. Son fonctionnement est assujéti au respect des deux conditions suivantes :

1. Cet appareil ne doit pas provoquer d'interférences dangereuses et
2. Cet appareil doit accepter toutes les interférences reçues, y compris celles qui risquent de provoquer un fonctionnement non souhaité.

Ces limites sont conçues pour offrir une protection raisonnable contre les interférences dangereuses dans une installation résidentielle. Cet appareil produit, utilise et peut émettre une énergie de fréquence radio et, s'il n'est pas installé et utilisé en conformité avec ces consignes, peut provoquer des interférences dangereuses pour les communications radios. Cependant, il est impossible de garantir qu'aucune interférence ne se produira dans certaines installations. Si cet appareil provoque des interférences qui affectent la réception d'un poste de radio ou de télévision, ce que vous pouvez déterminer en allumant puis en éteignant l'appareil, nous vous encourageons à essayer de les corriger en employant au moins l'une des méthodes suivantes :

- Réorientez ou déplacez l'antenne de réception.
- Éloignez l'appareil des équipements.
- Branchez cet équipement sur la prise autre que celle sur laquelle le récepteur est branché.
- Consultez le revendeur ou un technicien en radio et télévision expérimenté pour obtenir une assistance.



Important : Toute modification apportée au produit non expressément approuvée par Psion Teklogix est susceptible d'entraîner la révocation du droit d'utilisation de l'appareil.

Déclaration d'exposition aux rayonnements RF

Afin de respecter les critères de limites d'exposition aux rayonnements RF de la FCC et ANSI C95.1, les antennes de cet appareil doivent être conformes avec ce qui suit :

- Toutes les antennes de point d'accès doivent être utilisées à une distance d'au moins 25 cm (9,8 po.) de toutes les personnes à l'aide du câble fourni, et ne doivent pas être colocalisées ou fonctionner en même temps qu'une autre antenne ou un autre émetteur.
- L'antenne parabolique Gabriel (P/N 9002006) nécessite une distance minimale de séparation de 63,2 cm (24,9 po.).



Remarque : Deux antennes utilisées pour des opérations diverses ne sont pas considérés comme étant colocalisées.

Industrie Canada (IC) Avis du ministère des communications

This Class B digital apparatus complies with Canadian ICES-003 and RSS-210.

“To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors is subject to licensing.”

Cet appareil numérique de classe B est conforme aux normes ICES-003 et RSS-210 du Canada. « Pour empêcher que cet appareil cause du brouillage au service faisant l'objet d'une licence, il doit être utilisé à l'intérieur et devrait être placé loin des fenêtres afin de fournir un écran de blindage maximal. Si le matériel (ou son antenne d'émission) est installé à l'extérieur, il doit faire l'objet d'une licence. »

Homologations de sécurité

CSA, NRTL/C et CB.

Marquage CE

Lors d'une utilisation dans un environnement résidentiel, commercial ou d'industrie légère, le produit et ses périphériques approuvés au Royaume-Uni et en Europe répondent à toutes les conditions de marquage CE.

Directive R&TTE 1999/5/EEC

This equipment complies with the essential requirements of EU Directive 1999/5/EC (Declaration available: www.pSIONteklogix.com).

Cet équipement est conforme aux principales caractéristiques définies dans la Directive européenne RTTE 1999/5/CE. (Déclaration disponible sur le site : www.pSIONteklogix.com).

Die Geräte erfüllen die grundlegenden Anforderungen der RTTE-Richtlinie (1999/5/EG). (Den Wortlaut der Richtlinie finden Sie unter: www.pSIONteklogix.com).

Questa apparecchiatura è conforme ai requisiti essenziali della Direttiva Europea R&TTE 1999/5/CE. (Dichiarazione disponibile sul sito: www.pSIONteklogix.com).

Este equipo cumple los requisitos principales de la Directiva 1995/5/CE de la UE, "Equipos de Terminales de Radio y Telecomunicaciones". (Declaración disponible en: www.pSIONteklogix.com).

Este equipamento cumpre os requisitos essenciais da Directiva 1999/5/CE do Parlamento Europeu e do Conselho (Directiva RTT). (Declaração disponível no endereço: www.pSIONteklogix.com).

Ο εξοπλισμός αυτός πληροί τις βασικές απαιτήσεις της κοινοτικής οδηγίας EU R&TTE 1999/5/EK. (Η δήλωση συμμόρφωσης διατίθεται στη διεύθυνση: www.pSIONteklogix.com)

Deze apparatuur voldoet aan de noodzakelijke vereisten van EU-richtlijn betreffende radioapparatuur en telecommunicatie-eindapparatuur 199/5/EG. (verklaring beschikbaar: www.pSIONteklogix.com).

Dette udstyr opfylder de Væsentlige krav i EU's direktiv 1999/5/EC om Radio- og teleterminaludstyr. (Erklæring findes på: www.pSIONteklogix.com).

Dette utstyret er i overensstemmelse med hovedkravene i R&TTE-direktivet (1999/5/EC) fra EU. (Erklæring finnes på: www.pSIONteklogix.com).

Utrustningen uppfyller kraven för EU-direktivet 1999/5/EC om ansluten teleutrustning och ömsesidigt erkännande av utrustningens överensstämmelse (R&TTE). (Förklaringen finns att läsa på: www.pSIONteklogix.com).

Tämä laite vastaa EU:n radio- ja telepäätelaitedirektiivin (EU R&TTE Directive 1999/5/EC) vaatimuksia. (Julkilausuma nähtävillä osoitteessa: www.psionteklogix.com).

Psion Teklogix tímto prohlašuje, že 9160 G2 Wireless Gateway je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1995/5/ES (NV č. 426/2000 Sb.) a Prohlášení o shodě je k dispozici na www.psionteklogix.com.

Toto zařízení lze provozovat v České republice na základě generální licence č. GL-12/R/2000.

Psion Teklogix tímto vyhlasuje, že 9160 G2 Wireless Gateway spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1995/5/ES (NV č. 443/2001 Z.z.) a Vyhlásenie o zhode je k dispozícii na www.psionteklogix.com.

Toto zariadenie je možné prevádzkovať v Slovenskej republike na základe Všeobecného povolenia č. VPR-01/2001.



Consignes de sécurité importantes

Ces informations de sécurité concernent la protection du personnel d'exploitation et d'entretien.

- La 9160 G2 doit être installée par un installateur professionnel qualifié Psion Teklogix. Une 9160 G2 mal installée annulerait la garantie du fabricant.
- Le cordon d'alimentation secteur (s'il est vendu séparément) doit être conforme aux règles de sécurité nationales du pays où l'équipement doit être utilisé.
- L'utilisation d'un accessoire qui n'est ni recommandé ni vendu par le fabricant pourrait provoquer un incendie, une électrocution ou des blessures.
- Afin de réduire les risques d'endommagement de la prise d'alimentation et du cordon lorsque vous débranchez la 9160 G2, il est recommandé de tirer sur la prise et non sur le cordon.
- Assurez-vous que le cordon d'alimentation est positionné de façon à ce qu'il ne soit pas piétiné, arraché ou encore endommagé ou soumis à d'autres contraintes.
- Ne faites pas fonctionner la 9160 G2 avec une prise ou un cordon d'alimentation endommagé. Remplacez-le immédiatement.
- Ne faites pas fonctionner la 9160 G2 si elle a reçu un choc, si elle est tombée ou si elle a été endommagée de quelque manière. Elle doit être inspectée par du personnel qualifié.
- Ne démontez pas la 9160 G2 ; elle doit être réparée par un personnel d'entretien qualifié. Une erreur de réassemblage pourrait provoquer une électrocution ou un incendie.
- Pour éviter tout risque d'électrocution, débranchez la 9160 G2 de la prise secteur avant de tenter d'effectuer toute opération d'entretien ou de nettoyage.

- N'utilisez pas de cordon d'extension sauf si nécessaire. L'utilisation d'un cordon d'extension inapproprié pourrait entraîner un risque d'incendie ou d'électrocution. Si un cordon d'extension doit être utilisé, assurez-vous que :
 - Les broches du cordon d'extension sont du même nombre, de la même taille et de la même forme que celles de l'adaptateur.
 - Le cordon d'extension est correctement câblé, en bon état électrique, et la taille des fils est supérieure à 16 AWG.
- La 9160 G2 est conçue pour une utilisation en intérieur uniquement ; ne pas l'exposer à la pluie ou la neige.

L'option de fibres optiques de la passerelle sans fil 9160 G2 Wireless Gateway est :

CLASS 1 LED PRODUCT
APPAREIL À LED DE CLASSE 1

Ne pas faire fonctionner dans une atmosphère explosive

Utiliser des équipements Psion Teklogix là où des gaz explosifs sont présents peut provoquer une explosion.

Ne pas retirer les couvercles ou ouvrir les boîtiers

Pour éviter tout risque de blessure, les couvercles et boîtiers doivent toujours être retirés par du personnel qualifié uniquement. N'utilisez pas l'équipement sans que les couvercles et boîtiers soient correctement installés.

Ne pas tenir l'antenne

Afin d'éviter les désagréments en raison de l'effet de chaleur de l'énergie des fréquences radio, ne touchez pas l'antenne lorsqu'une 9160 G2 est en cours de transmission.

Connexion pour antenne extérieure

L'antenne extérieure ne doit être installée que par des professionnels de service Psion Teklogix.

Installation de l'antenne extérieure et d'alimentation électrique par Power over Ethernet (PoE)



Mise à la terre

Avertissement : Une connexion à un conducteur de terre est essentielle avant de procéder à une connexion d'antenne extérieure ou PoE.

1. Un conducteur de terre supplémentaire doit être installé entre la 9160 et la terre, c'est-à-dire en plus du conducteur de terre du cordon d'alimentation.
2. Le conducteur de terre supplémentaire ne peut pas être plus petit que les conducteurs d'alimentation du circuit de dérivation non reliés à la terre (section transversale nominale 0,75 mm² min. ou 18 AWG). Le conducteur de terre supplémentaire doit être relié à la 9160 au niveau de la borne prévue à cet effet, et relié à la terre d'une manière qui conservera la connexion de mise à la terre lorsque la 9160 sera alimentée par Ethernet (PoE, Power over Ethernet) ou utilisera les antennes extérieures. La connexion à la terre du conducteur de terre supplémentaire doit être conforme aux règles appropriées pour les cavaliers de terminaison de masse dans le pays d'utilisation. La terminaison du conducteur de terre supplémentaire peut être sur de l'acier de construction, un système de conduites électriques métalliques ou n'importe quel élément relié à la terre en permanence et connecté de façon fiable à l'équipement de service électrique relié à la terre.
3. Les conducteurs de terre dénudés, couverts ou isolés sont acceptables. Un conducteur de terre couvert ou isolé aura une finition extérieure verte, ou verte avec une ou plusieurs bandes jaunes.
4. Évitez de procéder à l'entretien pendant un orage. Il pourrait y avoir un risque de choc électrique à la foudre.

INTRODUCTION

1

1.1 À propos de ce manuel	3
1.2 Fonctionnalités d'aide en ligne, navigateurs pris en charge et limitations	6
1.3 Conventions de texte	7
1.4 Présentation de la passerelle sans fil 9160 G2 Wireless Gateway	7
1.4.1 Radios	8
1.4.2 Fonctionnalités du point d'accès	9
1.4.3 Fonctionnalités de la station de base	9
1.4.4 Fonctionnalités du mini-contrôleur.	9
1.5 Fonctionnalités et avantages	10
1.5.1 Conformité Wi-Fi et prise en charge des normes IEEE	10
1.5.2 Fonctionnalités sans fil	10
1.5.2.1 Le protocole Psion Teklogix 802.IQ	11
1.5.3 Fonctionnalités de sécurité	11
1.5.4 Interface Invité prête à l'emploi	12
1.5.5 Mise en cluster et gestion automatique.	12
1.5.6 Mise en réseau	13
1.5.7 Prise en charge SNMP	13
1.5.8 Capacité de maintenance	14
1.6 Quelle est la prochaine étape ?	14

1.1 À propos de ce manuel

Ce manuel décrit la configuration, l'administration et la maintenance d'une ou plusieurs Passerelle sans fil 9160 G2 Wireless Gateway sur un réseau sans fil.

Chapitre 1 : Introduction

offre une présentation de ce manuel et des fonctionnalités de la passerelle sans fil 9160 G2 Wireless Gateway.

Chapitre 2 : « Configuration d'installation requise »

présente l'installation physique de la passerelle sans fil 9160 G2 Wireless Gateway, et la manière de la connecter pour des diagnostics.

Chapitre 3 : « Liste de contrôle du pré-lancement »

offre une vérification rapide des composants matériels, des logiciels, des configurations client nécessaires, et des problèmes de compatibilité.

Chapitre 4 : « Étapes rapides de configuration et de lancement »

est un guide pas-à-pas de la configuration de vos passerelles sans fil 9160 G2 Wireless Gateway et du réseau sans fil résultant.

Chapitre 5 : « Configuration des paramètres de base »

fournit des instructions sur la configuration des paramètres d'accès administrateur et des nouveaux paramètres de point d'accès.

Chapitre 6 : « Gestion des points d'accès et des clusters »

décrit les clusters de point d'accès et la navigation vers des points d'accès spécifiques dans les clusters.

Chapitre 7 : « Gestion des comptes d'utilisateur »

illustre les capacités de gestion des utilisateurs pour le contrôle d'accès client aux points d'accès.

Chapitre 8 : « Gestion des canaux »

décrit comment la passerelle sans fil 9160 G2 Wireless Gateway attribue automatiquement les canaux radio utilisés par les points d'accès en cluster pour réduire les interférences mutuelles ou les interférences avec d'autres points d'accès en dehors de son cluster.

Chapitre 9 : « Voisinage sans fil »

fournit une vue détaillée des points d'accès voisins, y compris les informations d'identification, l'état du cluster et des informations statistiques.

Chapitre 10 : « Configuration de la sécurité »

offre un certain nombre de schémas de cryptage et d'authentification pour vous assurer que votre infrastructure sans fil soit uniquement accessible par les utilisateurs concernés. Chaque mode de sécurité est décrit en détail.

Chapitre 11 : « Maintenance et surveillance »

décrit la maintenance et la surveillance des tâches pour les points d'accès individuels (pas pour les configurations cluster).

Chapitre 12 : « L'interface Ethernet (filaire) »

décrit comment configurer les paramètres de l'interface filaire sur la passerelle sans fil 9160 G2 Wireless Gateway.

Chapitre 13 : « Définition de l'interface sans fil »

décrit comment configurer l'adresse réseau sans fil et les paramètres associés sur la passerelle sans fil 9160 G2 Wireless Gateway.

Chapitre 14 : « Configuration de l'accès invité »

vous permet de configurer la passerelle sans fil 9160 G2 Wireless Gateway afin de contrôler l'accès invité à un réseau isolé.

Chapitre 15 : « Configuration de VLAN »

décrit comment configurer plusieurs réseaux sans fil LAN virtuels (VLAN).

Chapitre 16 : « Configuration des paramètres radio 802.11 »

décrit la procédure à suivre pour configurer les paramètres radio sur la passerelle sans fil 9160 G2 Wireless Gateway.

Chapitre 17 : « Filtrage d'adresses MAC »

explique comment vous pouvez utiliser le filtrage d'adresses MAC pour contrôler l'accès client à votre réseau sans fil.

Chapitre 18 : « Équilibrage de la charge »

décrit comment configurer l'équilibrage de la charge sur votre réseau sans fil, pour vous permettre d'équilibrer la distribution des connexions client sans fil sur plusieurs points d'accès.

Chapitre 19 : « Qualité de service (QoS) »

fournit des instructions sur la configuration des paramètres sur plusieurs files d'attente pour améliorer le rendement et les performances du trafic sans fil différencié.

Chapitre 20 : « Système de distribution sans fil (WDS) »

décrit la procédure à suivre pour configurer le système de distribution sans fil (WDS) sur la passerelle sans fil 9160 G2 Wireless Gateway, vous permettant de connecter plusieurs points d'accès qui peuvent ensuite communiquer les uns avec les autres sans fil de manière normalisée.

Chapitre 21 : « Configuration de SNMP »

décrit la procédure à suivre pour configurer SNMP et les paramètres associés à l'API Enterprise-Manager de la passerelle sans fil 9160 G2 Wireless Gateway.

Chapitre 22 : « La 9160 G2 comme station de base »

décrit la procédure à suivre pour configurer la passerelle sans fil 9160 G2 Wireless Gateway comme une station de base filaire ou sans fil, ou comme un module radio à distance (MRR). Ce chapitre décrit également les paramètres de configuration de radio à bande étroite.

Chapitre 23 : « Configuration du mini-contrôleur »

décrit la configuration de la passerelle sans fil 9160 G2 Wireless Gateway lorsqu'elle est utilisée comme mini-contrôleur.

Chapitre 24 : « Paramètres 802.IQ »

décrit les paramètres pour le protocole sans fil propriétaire 802.IQ pour les stations de base et mini-contrôleurs 9160 G2.

Chapitre 25 : « Serveur Network Time Protocol (NTP) »

décrit la procédure à suivre pour configurer la passerelle sans fil 9160 G2 Wireless Gateway pour utiliser un serveur NTP (Network Time Protocol) spécifié afin de synchroniser l'heure des horloges des ordinateurs de votre réseau.

Chapitre 26 : « Sauvegarder et restaurer la configuration »

indique la procédure à suivre pour sauvegarder un fichier de configuration qui peut être utilisé à une date ultérieure pour restaurer le point d'accès à la configuration précédemment enregistrée.

Chapitre 27 : « Spécifications »

explique les caractéristiques physiques, environnementales et de différents fonctionnements de la passerelle sans fil 9160 G2 Wireless Gateway et de ses radios.

Annexe A : Brochages de port et diagrammes des câbles

inclut les brochages et les diagrammes des ports et des câbles pour la 9160 G2.

Annexe B : Paramètres de sécurité sur clients sans fil/serveur RADIUS

explique comment configurer les paramètres de sécurité sur le client pour correspondre au mode de sécurité utilisé par chaque connexion réseau (AP).

Annexe C : Dépannage

décrit la procédure à suivre pour résoudre les problèmes courants éventuellement rencontrés lors de la mise à jour des configurations réseau sur les réseaux desservis par plusieurs points d'accès en cluster.

Annexe D : Glossaire

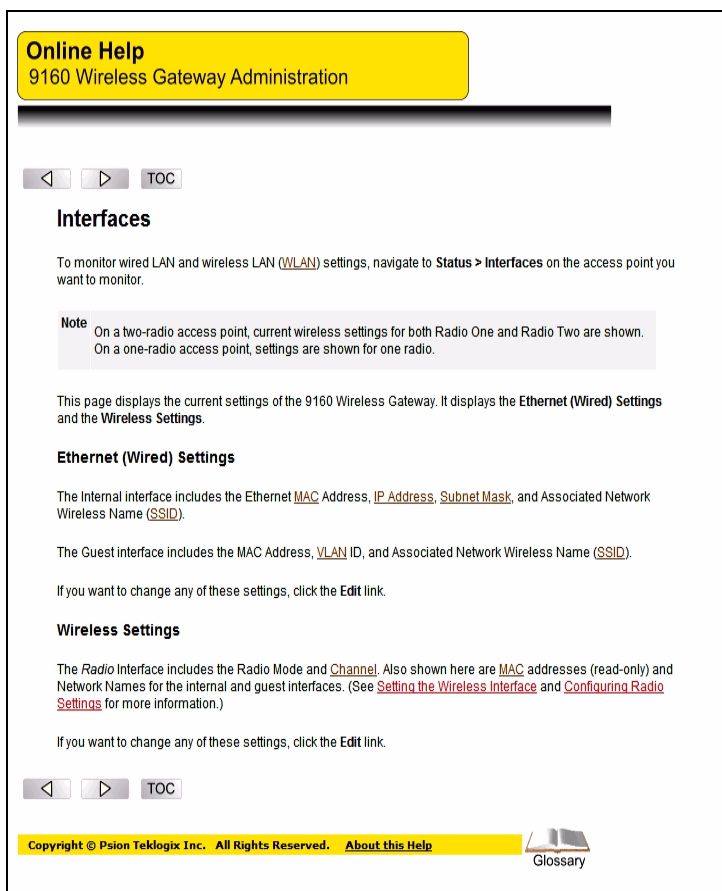
fournit des définitions et plus de détails sur les termes figurant en italique et en gras dans l'ensemble du manuel.

1.2 Fonctionnalités d'aide en ligne, navigateurs pris en charge et limitations

L'aide en ligne de Passerelle sans fil 9160 G2 Wireless Gateway fournit des informations sur tous les champs et les fonctionnalités disponibles dans l'interface utilisateur. Les informations de l'aide en ligne constituent un sous-ensemble des informations disponibles dans le manuel d'utilisation complet.

Les informations de l'aide en ligne correspondent à chaque onglet de l'interface utilisateur d'administration de la Passerelle sans fil 9160 G2 Wireless Gateway. Cliquez sur le bouton **Help** (Aide) sur un onglet ou le lien « More. . . » (Plus...) au bas du panneau de l'aide en ligne sur l'interface utilisateur pour obtenir des informations d'aide sur les paramètres concernant l'onglet actuel.

Figure 1.1 Écran d'aide en ligne



1.3 Conventions de texte



Remarque : les remarques mettent en évidence d'autres informations utiles.



Important : *Ces déclarations fournissent des instructions particulièrement importantes ou des informations supplémentaires qui sont vitales pour le bon fonctionnement de l'ordinateur et d'autres équipements.*



Avertissement : *Ces déclarations fournissent des informations importantes qui peuvent prévenir les accidents, les dommages sur l'équipement ou la perte de données.*



Une flèche en regard d'une information de description de champ (généralement dans les tableaux) indique un paramètre de configuration recommandé ou suggéré pour une option sur l'Access Point - Point d'accès (AP).

Italiques et gras Lorsque vous voyez un terme écrit en *italique et en gras*, il existe une entrée pour celui-ci dans l'Annexe D : « Glossaire », avec une définition et des détails supplémentaires. Tous les termes ne sont pas mis en évidence dans le manuel, mais le glossaire est complet. Par conséquent, veuillez le consulter pour les mots ou expressions que vous ne connaissez pas.

1.4 Présentation de la passerelle sans fil 9160 G2 Wireless Gateway

La Passerelle sans fil 9160 G2 Wireless Gateway fournit un accès à grande vitesse et en continu entre vos appareils sans fil et Ethernet. Il s'agit d'une solution avancée et basée sur des normes pour la mise en réseau sans fil dans les petites et moyennes entreprises. La Passerelle sans fil 9160 G2 Wireless Gateway permet le déploiement sans administration d'un réseau local sans fil (**WLAN**) tout en fournissant des fonctionnalités de réseau sans fil de pointe.

La Passerelle sans fil 9160 G2 Wireless Gateway offre une sécurité de pointe, une grande facilité d'administration et les normes de l'industrie, fournissant un réseau sans fil autonome et entièrement sécurisé sans devoir ajouter des logiciels de serveur de sécurité et de gestion supplémentaires.

La passerelle sans fil 9160 G2 Wireless Gateway est conçue pour prendre en charge un large éventail de configurations système. Utilisant les normes LAN sans fil IEEE 802.11, la 9160 G2 peut fonctionner comme un pont transparent (point d'accès) entre des réseaux filaires et sans fil. Cela permet aux clients sans fil d'accéder au réseau et de se déplacer en toute transparence entre les 9160 G2 du réseau. La 9160 G2 peut fonctionner comme un mini-contrôleur, une station de base, un module radio à distance (MRR), et faire partie d'un système MapRF.

1.4.1 Radios

La 9160 G2 peut prendre en charge le fonctionnement de radios simples ou doubles. Les modules radios disponibles sont la radio 802.11a/g, la radio 802.11g, et la radio à bande étroite RA1001A. Pour les caractéristiques détaillées de ces radios, reportez-vous à la section « Radios » à la page 342.

En fonction des radios installées, le point d'accès est capable de fonctionner dans les modes suivants :

- Mode **802.11b** IEEE.
- Mode **802.11g** IEEE.
- Mode **802.11a** IEEE.
- Atheros Turbo 5 GHz.
- Atheros Dynamic Turbo 5 GHz.
- Atheros Turbo 2,4 GHz.
- Atheros Dynamic Turbo 2,4 GHz.
- Zone de couverture étendue.
- Protocole d'interrogation bande étroite Psion Teklogix.



Important : *Les terminaux mobiles Psion Teklogix ne prennent pas en charge les modes Atheros Turbo et, pour prévenir un temps système radio inutile, l'utilisation du mode Turbo n'est pas recommandée.*

La passerelle sans fil 9160 G2 Wireless Gateway prend en charge quatre configurations radio différentes : 802.11g, 802.11g + 802.11ag, NB (bande étroite) et NB + 802.11ag.

Ces différentes variantes sont identifiées par la valeur « Model » (Modèle), qui est affichée sur la page Web *Maintenance > Upgrade* (Maintenance > Mise à niveau) (voir la Figure 1.2 à la page 9). Les modèles sont définis comme suit :

- 9160 Wireless Gateway = 802.11g.
- 9160 Wireless Gateway (radio double) = 802.11g + 802.11ag.
- 9160 Wireless Gateway NB = NB.
- 9160 Wireless Gateway NB (radio double) = NB + 802.11g.



Remarque : *Dans le cas « NB uniquement », il est possible que la page Web affiche la page de configuration pour une radio simple 802.11. Vous pouvez l'ignorer. Cependant, si vous tentez de configurer cette radio inexistante, cela ne causera aucun problème dans la 9160 G2.*

Figure 1.2 Page Web de mise à niveau du firmware

Upgrade firmware

Model	9160 Wireless Gateway NB (Dual Radio)
Platform	PTX9160G2
Firmware Version	E187k

New Firmware Image

Please note: Uploading the new firmware may take up to 20 seconds. Please do not refresh the page or navigate to another page while uploading the new firmware, or the firmware upload will be aborted. When the upload is complete, a page will be displayed indicating whether the new firmware was uploaded successfully. If successful, the upgrade will proceed automatically.

1.4.2 Fonctionnalités du point d'accès

En point d'accès connecté à un réseau filaire, la passerelle sans fil 9160 G2 Wireless Gateway forme une liaison de communication entre les terminaux mobiles RF Psion Teklogix clients ou entre les clients à point d'accès sans fil et un contrôleur réseau ou un ordinateur hôte Psion Teklogix. Elle communique par liaison de données RF IEEE 802.11 avec des terminaux mobiles, et par câble avec le contrôleur réseau ou un ordinateur hôte. La 9160 G2 peut être connectée au réseau via une connexion Ethernet.

1.4.3 Fonctionnalités de la station de base

En station de base ou module radio à distance (MRR), la 9160 G2 fournit un lien entre le réseau local sans fil et les terminaux mobiles utilisant des protocoles radio propriétaires Psion Teklogix. Sur le réseau local, la station de base 9160 G2 (ou MRR) communique avec un hôte 9500 Communications Server (ou un hôte utilisant un kit de développement logiciel Psion Teklogix) à l'aide du protocole propriétaire 9010 sur les protocoles TCP/IP.

Pour plus d'informations sur la configuration de la 9160 G2 en station de base ou MRR, reportez-vous à la section Chapitre 22 : « La 9160 G2 comme station de base ».

1.4.4 Fonctionnalités du mini-contrôleur

La 9160 G2 est dotée de capacités d'émulation lui permettant d'agir comme un mini-contrôleur. Lorsqu'une 9160 G2 est configurée comme un mini-contrôleur, les terminaux mobiles Psion Teklogix peuvent émuler un terminal mobile ANSI, 5250 ou 3274 via la 9160 G2 plutôt que via un serveur de communication 9500.

Pour configurer la passerelle sans fil 9160 G2 Wireless Gateway comme un mini-contrôleur, reportez-vous à la section Chapitre 23 : « Configuration du mini-contrôleur ».

1.5 Fonctionnalités et avantages

1.5.1 Conformité Wi-Fi et prise en charge des normes IEEE

- Prise en charge des normes de mise en réseau sans fil *IEEE 802.11a*, *IEEE 802.11b*, *IEEE 802.11g*, *IEEE 802.11i*, et *IEEE 802.3af*.
- Fournit une bande passante de 54 Mbit/s pour *IEEE 802.11a* ou *IEEE 802.11g* (11 Mbit/s pour *IEEE 802.11b*, 108 Mbit/s pour Atheros *802.11a Turbo*).
- Conformité Wi-Fi requise pour la certification.

1.5.2 Fonctionnalités sans fil

- Sélection automatique des canaux au démarrage.
- Ajustement d'alimentation d'émission.
- Système de distribution sans fil (**WDS**) pour la connexion de plusieurs points d'accès sans fil. Étend votre réseau avec moins de câblage.
- Qualité de service (**QoS**) pour un débit accru et de meilleures performances de trafic sans fil urgent tel que vidéo, audio, voix sur IP (VoIP) et la diffusion de contenus multimédias. Notre qualité de service (QoS) est conforme à Wi-Fi Multimedia (WMM).
- Équilibrage de la charge.
- La prise en charge de plusieurs **SSID** (noms de réseau) et de plusieurs **BSSID** (Basic Service Set ID) sur le même point d'accès.
Deux BSSID spéciaux sont pris en charge, l'un pour le réseau interne (principal et gestion), l'autre pour le réseau invité. Six BSSID d'usage général supplémentaires (appelés réseaux sans fil virtuels ou VWN) sont pris en charge via des réseaux VLAN.
- Gestion des canaux pour la coordination automatique des affectations de canaux radio de point à point pour réduire les interférences entre points d'accès sur le réseau et optimiser la bande passante Wi-Fi.
- Détection des points d'accès voisins (également connu sous le nom de détection des points d'accès « indésirables »).
- Prise en charge de la sélection du domaine réglementaire *IEEE 802.11d* (codes pays pour un fonctionnement global).
- Prise en charge de *IEEE 802.11h*, intégrant TPC et DFS.
IEEE 802.11h est une norme qui offre deux services requis pour satisfaire à certains domaines réglementaires pour la bande 5 GHz. Ces deux services sont TPC (Transmit Power Control, ou contrôle de la puissance de transmission) et DFS (Dynamic Frequency Selection, ou sélection dynamique des fréquences).
- Prise en charge de plage étendue (XR).

- Priorité voix SpectraLink (SVP).
La priorité voix SpectraLink (SVP) est une approche QoS pour les déploiements Wi-Fi. SVP est une spécification ouverte qui est conforme à la norme IEEE 802.11b. SVP réduit le délai et donne la priorité aux paquets voix sur les paquets de données sur le réseau local (LAN) sans fil, ce qui augmente la probabilité de meilleures performances réseau.

1.5.2.1 Le protocole Psion Teklogix 802.IQ

802.IQ est un protocole propriétaire Psion Teklogix qui permet aux terminaux mobiles de fonctionner dans un LAN sans fil sur un réseau qui prend simultanément en charge les protocoles TCP/IP et 802.IQ. Le protocole 802.IQ est disponible en deux versions : 802.IQ v1 et 802.IQ v2. La passerelle sans fil 9160 G2 Wireless Gateway peut prendre en charge les deux versions du protocole simultanément (les terminaux mobiles ne doivent en utiliser qu'un).

Le protocole 802.IQ v1 est un plan d'acheminement LAN sans fil qui offre de meilleures performances dans un réseau sans fil 802.11 qu'il n'est possible avec un routage TCP/IP. Un terminal mobile peut communiquer avec le point d'accès 9160 G2 via le protocole TCP/IP ou 802.IQ v1, ce qui rend un système à double opérabilité possible.

Le protocole 802.IQ v2 est une version améliorée du protocole 802.IQ v1 qui transporte des paquets sur la couche UDP. Il fournit toutes les fonctionnalités 802.IQ v1, avec les fonctions supplémentaires de capacité de mise à niveau de logiciels sur RF, la possibilité d'ajouter des points d'accès tiers entre les contrôleurs et les terminaux mobiles et l'intégration dans le système MapRF si vous le souhaitez.

Pour plus d'informations et les menus de configuration pour 802.IQ, reportez-vous à la section Chapitre 24 : « Paramètres 802.IQ ».

1.5.3 Fonctionnalités de sécurité

- Supprimer la diffusion SSID.
- Ignorer la diffusion SSID.
- Faible contournement IV.
- Wired Equivalent Privacy (**WEP**).
- Certifié Wi-Fi pour les normes suivantes :
 - Normes IEEE : 802.11b, 802.11g, 802.11d
 - Sécurité :
 - WPA™ - Individuel
 - WPA™ - Entreprise
 - WPA2™ - Individuel
 - WPA2™ - Entreprise

- Types EAP :
 - EAP-TLS
 - EAP-TTLS/MSCHAPv2
 - PEAPv0/EAP-MSCHAPv2
 - PEAPv1/EAP-GTC
 - EAP-SIM
- Advanced Encryption Standard (**AES**).
- Contrôle d'accès basé sur l'utilisateur avec serveur d'authentification local.
- Base de données utilisateur locale et gestion utilisateur du cycle de vie.
- Filtrage d'adresses MAC.
- WPA/WPA2 sur **WDS**.
- Secure Sockets Shell (SSH).
- Secure Sockets Layer (SSL).

1.5.4 Interface Invité prête à l'emploi

- Nom de réseau unique (**SSID**) pour l'interface client.
- Portail captif pour guider les invités vers une page Web invité personnalisable.
- Options VLAN et Ethernet.

1.5.5 Mise en cluster et gestion automatique

- Mise en service et configuration automatique des points d'accès via une mise en cluster et un « point de rendez-vous » cluster.

L'administrateur peut spécifier comment les nouveaux points d'accès doivent être configurés avant qu'ils soient ajoutés au réseau. Lorsque de nouveaux points d'accès sont ajoutés, ils peuvent automatiquement atteindre le « point de rendez-vous » avec le cluster et télécharger la bonne configuration. Le processus ne nécessite aucune intervention manuelle, mais est sous le contrôle de l'administrateur.

- Vue universelle unique des points d'accès en cluster et des paramètres de configuration.

La configuration de tous les points d'accès dans un cluster peut être gérée depuis une seule et même interface. Les modifications apportées aux paramètres communs sont automatiquement répercutées dans tous les membres du groupe.

- Points d'accès auto-gérés avec synchronisation de configuration automatique.

Les points d'accès dans un cluster vérifient périodiquement que la configuration du cluster est constante, et vérifient la présence et la disponibilité des autres membres du cluster. L'administrateur peut surveiller ces informations via l'interface utilisateur.

- Authentification locale améliorée utilisant 802.1x sans configuration informatique supplémentaire.

Un cluster peut maintenir un serveur d'authentification d'utilisateur et une base de données stockés sur les points d'accès. Cela vous évite d'avoir à installer, configurer et gérer une infrastructure **RADIUS** et simplifie la tâche d'administration de déploiement d'un réseau sans fil sécurisé.

1.5.6 Mise en réseau

- Prise en charge Dynamic Host Configuration Protocol (Protocole de configuration dynamique des hôtes) (**DHCP**) pour obtenir de manière dynamique les informations de configuration du réseau.
- Prise en charge réseau local virtuel (VLAN).
- Réseaux sans fil virtuels (VLAN).
- Spanning Tree Protocol (**STP**).
- **802.1p**.
- Prise en charge fibres optiques 100BASE-FX.

1.5.7 Prise en charge SNMP

La Passerelle sans fil 9160 G2 Wireless Gateway inclut les bases de données Management Information Base (**MIB**) Simple Network Management Protocol (**SNMP**) standard suivantes :

- Pont MIB 802.1d (RFC 1493).
- SNMPv2 MIB (RFC 3418).
- MIB IEEE 802.11 Std (base).
- Groupe d'interfaces MIB (RFC 2233).
- Deux MIB propriétaires (MIB sans fil et MIB système), basées sur la MIB IEEE 802.11k à venir. Elles fournissent des informations à propos de la liste d'association client Passerelle sans fil 9160 G2 Wireless Gateway et le tableau de détection des points d'accès, respectivement. La MIB système propriétaire contient des fonctionnalités de maintenance telles que le redémarrage du système ou la mise à niveau du firmware.

1.5.8 Capacité de maintenance

- Des vues d'état, de surveillance et de suivi du réseau, notamment la surveillance de session, les associations client, la transmission/réception des statistiques et le journal des événements.
- Liaison du contrôle d'intégrité pour vérifier en permanence la connexion au client, quel que soit les niveaux d'activité du trafic réseau.
- Option de réinitialisation de la configuration.
- Mise à niveau du firmware.
- Sauvegarde et restauration de la configuration des points d'accès.
- Sauvegarde et restauration de la base de données utilisateur pour le serveur RADIUS intégré (applicable aux modes de sécurité IEEE 802.1x et WPA/WPA2 Enterprise (RADIUS)).

1.6 Quelle est la prochaine étape ?

Êtes-vous prêt à commencer une mise en réseau sans fil ? Une fois que votre passerelle sans fil 9160 G2 Wireless Gateway sera installée (voir le Chapitre 2 : « Configuration d'installation requise »), lisez le Chapitre 3 : « Liste de contrôle du pré-lancement » et suivez les étapes du Chapitre 4 : « Étapes rapides de configuration et de lancement ».

CONFIGURATION D'INSTALLATION REQUISE **2**

2.1 Choix de l'emplacement adéquat	17
2.1.1 Environnement	17
2.1.2 Maintenance	18
2.1.3 Radios	18
2.1.4 Alimentation et câbles d'antenne	18
2.1.4.1 Alimentation.	18
2.1.4.2 Antennes.	19
2.2 Connexion à des appareils externes	20
2.2.1 Ports	20
2.2.2 Installation du réseau local (LAN) : présentation	21
2.2.3 Installation d'un LAN : Ethernet	21
2.2.3.1 Câblage Ethernet	22
2.2.3.2 Port Ethernet à fibres optiques 100Base-FX	22
2.2.4 Indicateurs d'état (LED)	23
2.2.5 Connexion d'un terminal à affichage vidéo	23
2.3 Modification de la configuration avec un navigateur Web.	24



Avertissement : La 9160 G2 doit être installée par un installateur professionnel qualifié Psion Teklogix.

2.1 Choix de l'emplacement adéquat

Généralement, Psion Teklogix réalise une étude de site et recommande ensuite les emplacements préférés pour les 9160 G2. Ces emplacements disposent d'une bonne couverture radio, réduisent la distance à l'ordinateur hôte ou au contrôleur réseau, et répondent aux exigences environnementales.

2.1.1 Environnement

La 9160 G2 doit se trouver dans une zone bien ventilée et doit être protégée des fluctuations extrêmes de température (c'est-à-dire sortie de chauffage directe, portes d'expédition ou lumière directe du soleil). Si un couvercle de protection est nécessaire, il doit avoir une ventilation suffisante pour maintenir le fonctionnement régulier de l'appareil.

Reportez-vous au Chapitre 27 : « Spécifications » pour une description plus détaillée des exigences environnementales. Gardez à l'esprit que la stabilité à long terme de cet équipement sera améliorée si les conditions environnementales sont moins graves que celles répertoriées dans ce manuel.

La 9160 G2 doit être placée hors de la trajectoire d'un quelconque véhicule et à l'abri des projections d'eau ou de poussière. La 9160 G2 doit uniquement être montée dans la position verticale, comme illustré dans la Figure 2.1 à la page 18. Cette orientation réduit les risques d'infiltration d'eau dans la 9160 G2, si l'unité était aspergée accidentellement.

La 9160 G2 est fixée à une surface verticale à l'aide de quatre fixations sur la plaque arrière (le type de fixations dépend de la surface de montage). Les deux trous supérieurs de la plaque arrière sont des slots qui permettent à l'unité d'être accrochée en position avant de fixer les boulons restants, ce qui facilite l'installation. Les boulons utilisés pour l'installation sont de type SAE 1/4-20.

Figure 2.1 Position d'installation de la 9160 G2



2.1.2 Maintenance

La 9160 G2 n'a aucun commutateur optionnel interne et ne requiert pas d'accès physique ; tous les paramètres de configuration sont effectués à distance (reportez-vous à la section « Accès aux paramètres de base » à la page 49). Les considérations relatives à l'environnement et aux communications radio continuent à s'appliquer.

2.1.3 Radios

- Radio 802.11g sans antenne intégrée (standard).
- Radio 802.11a/g sans antenne intégrée (deuxième radio optionnelle).
- RA1001A - Radio à bande étroite (NB).

2.1.4 Alimentation et câbles d'antenne

2.1.4.1 Alimentation

Pour éviter toute déconnexion et contrainte accidentelle sur la 9160 G2, l'antenne et les câbles d'alimentation doivent être fixés à moins de 30 cm de l'appareil. Fixez les câbles avec des serre-câbles aux supports d'attache de câble de la 9160 G2 (reportez-vous à la Figure 2.1). Une prise d'alimentation monophasée (de 100 à 240 Vca nominal 1,0 A minimum) doit être installée à moins d'un mètre (3,1 pieds) de la 9160 G2. La 9160 G2 s'adapte automatiquement à l'entrée dans cette plage de puissance. Le câble d'alimentation est amovible et disponible dans le type d'alimentation spécifique à votre emplacement. L'alimentation secteur de la 9160 G2 a une entrée universelle via un connecteur IEC320 standard.

Pour éliminer le besoin de câblages secteur, la passerelle sans fil 9160 G2 Wireless Gateway est conforme à IEEE 802.3af et peut être alimentée via sa connexion Ethernet. Pour plus d'informations, reportez-vous à la section « Exigences en termes d'alimentation Power Over Ethernet » à la page 342.



Avertissement : *Pour éviter des chocs électriques, le fil de terre de protection du câble d'alimentation doit toujours être relié à la terre.*

2.1.4.2 Antennes

Le type d'antenne requis pour chaque installation dépend de la couverture requise et des fréquences utilisées. Un maximum de quatre éléments d'antenne peuvent être utilisés. Ces antennes peuvent être une combinaison de diverses SMA à filetage inversé « à visser » ou d'antennes WDS à gain élevé. Plusieurs antennes omnidirectionnelles et des antennes directionnelles spéciales sont disponibles auprès de Psion Teklogix. En règle générale, une étude de site détermine l'antenne appropriée. Consultez le service d'assistance Psion Teklogix pour plus d'informations.



Avertissement : *n'utilisez jamais la 9160 G2 sans antenne ou charge fictive.*

Connexion à l'antenne extérieure (Kit, référence 1916641)

L'antenne doit être installée par du personnel qualifié, conformément aux codes d'installation électrique locaux. L'antenne doit être située de telle sorte qu'elle soit toujours au moins à une hauteur de 4,6 m (15 pieds) et à plus de 3 m (10 pieds) des utilisateurs et des autres personnes travaillant dans la zone.

Pour une 9160 G2 reliée à une antenne extérieure, toutes les remarques suivantes sont applicables :

1. Le blindage du câble coaxial d'antenne extérieure doit être raccordé à la terre (indépendamment de la 9160 G2) dans l'installation du bâtiment, à condition que l'installation soit acceptable pour les autorités compétentes dans le pays d'utilisation.
2. Un conducteur relié à la terre supplémentaire doit être installé entre la 9160 G2 et la terre, c'est-à-dire en plus du conducteur de terre du cordon d'alimentation.
3. Le conducteur de terre supplémentaire ne peut pas être plus petit que les conducteurs d'alimentation du circuit de dérivation non reliés à la terre (section transversale nominale 0,75 mm² min. ou 18 AWG). Le conducteur de terre supplémentaire doit être connecté à la 9160 G2 au terminal fourni, et relié à la terre d'une manière qui conserve la connexion de mise à la terre lorsque le cordon d'alimentation est débranché. La connexion à la terre du conducteur de terre supplémentaire doit être conforme aux règles appropriées pour les cavaliers de terminaison de masse dans le pays d'utilisation. La terminaison du conducteur de mise à la terre supplémentaire peut être sur de l'acier de construction, un système de conduites électriques métalliques ou n'importe quel élément relié à la terre en permanence et connecté de façon fiable à l'équipement de service électrique relié à la terre.

4. Les conducteurs de masse dénudés, couverts ou isolés sont acceptables. Un conducteur de masse couvert ou isolé aura une finition extérieure verte (Canada et États-Unis uniquement), ou verte avec une ou plusieurs bandes jaunes (dans tous les pays).
5. Évitez un entretien pendant un orage. Il pourrait y avoir un risque de choc électrique à la foudre.
6. Pour la Finlande, la Norvège et la Suède, l'équipement doit être utilisé dans une ZONE À ACCÈS RESTREINT où une liaison équipotentielle a été appliquée. Le CONDUCTEUR DE TERRE DE PROTECTION branché en permanence doit être installé par un TECHNICIEN QUALIFIÉ.



Avertissement : *Pour des raisons de sécurité RF, les utilisateurs ne sont pas autorisés à approcher à proximité de l'antenne.*

Psion Teklogix fournit le câble coaxial nécessaire pour connecter la 9160 G2 à l'antenne. Lors de la détermination de l'emplacement de l'antenne, les exigences en matière de couverture de l'antenne sont considérées en fonction des exigences environnementales de la 9160 G2.

Le câble coaxial doit être routé et fixé à l'aide de chevilles et/ou de clips pour câble coaxial. Quelques centimètres de câble supplémentaires sont nécessaires près de l'antenne et de la 9160 G2 pour faciliter une déconnexion.

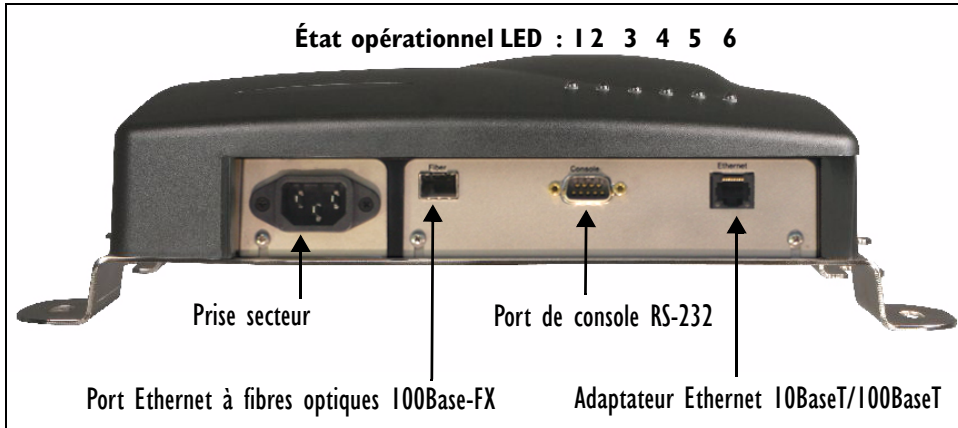
2.2 Connexion à des appareils externes

Cette section contient des directives générales pour le raccordement de la 9160 G2 à des appareils externes tels que contrôleurs réseau, stations de base, ordinateurs hôtes, ordinateurs et terminaux d'affichage vidéo.

2.2.1 Ports

La Figure 2.2 à la page 21 indique les emplacements des connecteurs d'alimentation et de port sur le socle de la 9160 G2. Les brochages de port sont décrits dans l'Annexe A : « Brochages de port et diagrammes des câbles » .

Figure 2.2 Emplacement des ports et des LED sur la 9160 G2



* Remarque : les versions antérieures de la 9160 G2 n'ont pas de port à fibres optiques

2.2.2 Installation du réseau local (LAN) : présentation

Comme la 9160 G2 fournit une connectivité Ethernet, elle peut être ajoutée à un réseau LAN existant. En règle générale, les installations LAN sont traitées avec l'aide d'administrateurs réseau, car ils sont familiarisés avec leur réseau et sa configuration. Une fois que la 9160 G2 est installée, connectée et sous tension, l'administrateur système peut accéder à l'unité pour vérifier la configuration et attribuer à la 9160 G2 son adresse IP unique. Cette opération peut être effectuée via le réseau (reportez-vous à la section « Modification de la configuration avec un navigateur Web » à la page 24). Les autres modifications du réseau, telles que l'ajout de stations ou d'utilisateurs, exigeraient également que la configuration de la 9160 G2 soit modifiée.



Important : Une fois que la 9160 G2 a été configurée et redémarrée pour la première fois, le serveur DHCP doit être désactivé à moins que la 9160 G2 n'obtienne son adresse IP auprès d'un serveur.

2.2.3 Installation d'un LAN : Ethernet

La 9160 G2 est un point d'accès hautes performances qui prend en charge les réseaux LAN Ethernet rapides 100 Mo/s, ainsi que 10 Mo/s, à la fois en fonctionnement duplex et semi-duplex. Elle est équipée de :

- Une carte 10BaseT/100BaseT (utilisant un câble à paire torsadée de catégorie 5, un connecteur RJ-45, exécutant à un débit de 10 ou 100 Mo/s). Pour les brochages de port, reportez-vous à l'Annexe A : « Brochages de port et diagrammes des câbles » .

- Un port à fibres optiques 100Base-FX (pour plus de détails, reportez-vous à la Section 2.2.3.2).



Remarque : La 9160 G2 ne prend en charge aucun type de connexion autre qu'Ethernet 10Base-T, 100 Base-T et 100Base-FX.

2.2.3.1 Câblage Ethernet

La longueur maximale du segment de câble autorisée entre les relais pour la 9160 G2 (câblage Ethernet 10BaseT/100BaseT) est de 100 m.

2.2.3.2 Port Ethernet à fibres optiques 100Base-FX

La passerelle sans fil 9160 G2 Wireless Gateway prend en charge la mise en réseau à fibres optiques 100Base-FX. Pour utiliser le port Ethernet à fibres optiques, l'utilisateur doit installer un module SFP (Small Form Pluggable) 100Base-FX dans le slot d'extension de la 9160 G2. Les SFP sont des émetteurs-récepteurs optiques et compacts modulaires qui permettent les transmissions à haute vitesse.

Lorsque le matériel est installé, la fonctionnalité est activée : aucune configuration n'est requise pour le port. Le logiciel de la 9160 G2 détecte automatiquement la présence du module SFP au démarrage et l'utilise au lieu du port 10/100Base-T standard.

Le module est inséré, interface électrique en premier, sur pression du doigt. Le module SFP n'est pas remplaçable à chaud. Insérez-le ou retirez-le uniquement lorsque la 9160 G2 est hors tension.

Au démarrage, la 9160 G2 indiquera l'un des deux messages suivants au niveau du port de console série, selon que le module SFP est installé ou non :

ixp425_eth : 100BASE-FX SFP fiber module detected (module SFP 100BASE-FX à fibres optiques détecté)

ixp425_eth : 100BASE-FX SFP fiber module not detected (module SFP 100BASE-FX à fibres optiques non détecté)

Lors de l'utilisation de l'interface à fibres optiques, la 9160 G2 ne prend en charge que le fonctionnement 100 Mo/s. Quel que soit le port Ethernet utilisé, la 9160 G2 utilise la même adresse MAC filaire.

Le fonctionnement simultané de deux ports Ethernet n'est pas pris en charge. L'utilisation de la technologie PoE (via le port 10/100BaseT) et de l'interface à fibres optiques est prise en charge. Dans cette configuration, le port 10/100BaseT est uniquement utilisé pour l'alimentation.

2.2.4 Indicateurs d'état (LED)

La 9160 G2 hautes performances dispose de six indicateurs d'état sur l'avant du boîtier, comme illustré dans la Figure 2.2 à la page 21. Les LED numérotées et colorées à l'avant de l'unité indiquent l'état de fonctionnement de chaque port, comme décrit dans le Tableau 2.1 à la page 23.

Tableau 2.1 Fonctions des LED de la 9160 G2 : boîtier avant

Numéro de LED	Nom	Fonction	Couleur
1	Liaison Ethernet	Indicateur de liaison pour 10BaseT/ 100BaseT : ON (Allumée) = liaison correcte ; OFF (Éteinte) = pas de liaison	jaune *
2	Activité Ethernet	Activité LAN Ethernet (Rx/Tx)	vert
3	1er état de la radio 802.11	1ère activité de la radio 802.11 (Rx/Tx)	vert
4	2e état de la radio 802.11	2e activité de la radio 802.11 (Rx/Tx)	vert
5	État de la radio NB	Activité de la radio NB (Rx/Tx)	vert
6	Alimentation	LED allumée fixe = unité sous tension LED éteinte = aucune alimentation de l'appareil	vert

* La couleur de la LED 1 indique l'orientation des LED lorsqu'on les regarde à distance.

2.2.5 Connexion d'un terminal à affichage vidéo

Un terminal à affichage vidéo compatible ANSI (par ex., DEC VT220 ou supérieur), ou un PC exécutant une émulation de terminal, est utilisé à des fins de diagnostic.

Le terminal est connecté au port RS-232 de la 9160 G2 (reportez-vous à la Figure 2.2.2 à la page 21). Ce port est généralement configuré pour fonctionner à 115 200 bauds, 8 bits, 1 bit d'arrêt, pas de bit de parité. Pour se conformer à la section 15 des règles de la FCC pour un appareil informatique de classe B, seul le câble fourni (référence 19387) doit être utilisé.

2.3 Modification de la configuration avec un navigateur Web

La mémoire Flash de la 9160 G2 peut être reconfigurée à distance via le réseau au moyen d'un navigateur Web HTML standard tel que MS Internet Explorer (version 4.0 ou ultérieure) ou Firefox. Reportez-vous au Chapitre 4 : « Étapes rapides de configuration et de lancement » pour obtenir des instructions sur la modification des paramètres et les paramètres de configuration généraux.

LISTE DE CONTRÔLE DU PRÉ-LANCEMENT

3

3.1 La passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway	27
3.1.1 Paramètres par défaut de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway	27
3.1.2 Ce que le point d'accès ne fournit pas	31
3.2 Ordinateur de l'administrateur	31
3.3 Ordinateurs client sans fil	32
3.4 Présentation de l'adressage IP statique et dynamique sur la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway	33
3.4.1 Comment le point d'accès obtient-il une adresse IP au démarrage ?.	34
3.4.2 Adressage IP dynamique	34
3.4.3 Adressage IP statique.	34
3.4.4 Restauration d'une adresse IP	35

Avant de brancher et de démarrer un nouveau **Access Point - Point d'accès**, reportez-vous aux sections suivantes pour faire une vérification rapide des composants matériels, des logiciels, des configurations de client nécessaires et des problèmes de compatibilité. Veillez à disposer de tout ce dont vous avez besoin pour assurer le succès du lancement et du test de votre nouveau réseau sans fil (ou étendu).

3.1 La passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway

La passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway est un concentrateur de communications sans fil pour les appareils de votre réseau. Elle fournit un accès à grande vitesse en continu entre vos appareils sans fil et Ethernet en modes **802.11a IEEE**, **802.11b**, **802.11g** et **802.11a Turbo**.

La passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway offre une fonctionnalité d'*interface invité* prête à l'emploi qui vous permet de configurer des points d'accès afin de contrôler l'accès invité au réseau sans fil via des réseaux LAN virtuels.

Pour plus d'informations sur l'interface client, reportez-vous au Chapitre 14 :
« Configuration de l'accès invité » et à la section « Une remarque sur la configuration de connexions pour un réseau invité » à la page 42.

3.1.1 Paramètres par défaut de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway

Tableau 3.1 Paramètres par défaut de la 9160 G2

Option	Paramètres par défaut	Informations associées
<i>System Name</i> (Nom du système)	PTX9160-Wireless-AP	« DNS Hostname (Nom d'hôte DNS) » à la page 144 dans « L'interface Ethernet (filaire) » à la page 141
<i>User Name</i> (Nom d'utilisateur)	admin Le nom d'utilisateur est en lecture seule. Il ne peut pas être modifié.	
<i>Password</i> (Mot de passe)	admin	« Fournir des paramètres réseau » à la page 51 dans « Configuration des paramètres de base » à la page 47

Tableau 3.1 Paramètres par défaut de la 9160 G2 (Suite)

Option	Paramètres par défaut	Informations associées
<i>Network Name (SSID) (Nom de réseau (SSID))</i>	« TEKLOGIX » pour l'interface interne « TEKLOGIX Guest » pour l'interface Invité	« Révision / Description du point d'accès » à la page 50 dans « Configuration des paramètres de base » à la page 47 « Configuration des paramètres de LAN sans fil « interne » » à la page 157 dans « Définition de l'interface sans fil » à la page 151 « Configuration des paramètres sans fil de réseau « invité » » à la page 158 dans « Définition de l'interface sans fil » à la page 151
<i>Network Time Protocol (NTP)</i>	None (Aucun)	« Serveur Network Time Protocol (NTP) » à la page 325
<i>IP Address (Adresse IP)</i>	192.168.1.10 L'adresse IP par défaut est utilisée si vous n'utilisez pas un serveur <i>Dynamic Host Configuration Protocol (Protocole de configuration dynamique des hôtes) (DHCP)</i> . Vous pouvez attribuer une nouvelle adresse IP statique via les pages Web d'administration. Si vous disposez d'un serveur <i>DHCP</i> sur le réseau, une adresse IP sera affectée de façon dynamique par le serveur au démarrage du point d'accès.	« Présentation de l'adressage IP statique et dynamique sur la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway » à la page 33
<i>Connection Type (Type de connexion)</i>	<i>Dynamic Host Configuration Protocol (Protocole de configuration dynamique des hôtes) (DHCP)</i> Si vous ne disposez pas d'un serveur <i>DHCP</i> sur le réseau interne et que vous n'avez pas l'intention d'en utiliser un, la première chose à faire depuis le point d'accès est de changer le type de connexion « DHCP » en « Static IP » (IP statique). Le réseau invité doit disposer d'un serveur DHCP.	« Présentation de l'adressage IP statique et dynamique sur la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway » à la page 33 Pour plus d'informations sur la manière de reconfigurer le type de connexion, reportez-vous à la section « Paramètres de l'interface interne » à la page 147.

Tableau 3.1 Paramètres par défaut de la 9160 G2 (Suite)

Option	Paramètres par défaut	Informations associées
<i>Subnet Mask</i> (Masque de sous-réseau)	None (Aucun) Ce paramètre est déterminé par la configuration du réseau et du serveur DHCP.	« L'interface Ethernet (filaire) » à la page 141
<i>Radio (Radio)</i>	On (Activée)	« Configuration des paramètres radio 802.11 » à la page 173
<i>IEEE 802.11 Mode</i> (Mode IEEE 802.11)	802.11g ou 802.11a+g	« Configuration des paramètres radio 802.11 » à la page 173
<i>Canal 802.11g</i>	Auto (Auto)	« Configuration des paramètres radio 802.11 » à la page 173
<i>Beacon Interval</i> (Intervalle de balise)	100	« Configuration des paramètres radio 802.11 » à la page 173
<i>DTIM Period</i> (Période DTIM)	2	« Configuration des paramètres radio 802.11 » à la page 173
<i>Fragmentation Threshold</i> (Seuil de fragmentation)	2346	« Configuration des paramètres radio 802.11 » à la page 173
<i>Regulatory Domain</i> (Domaine de réglementation)	FCC	« Configuration des paramètres radio 802.11 » à la page 173
<i>RTS Threshold</i> (Seuil RTS)	2347	« Configuration des paramètres radio 802.11 » à la page 173
<i>MAX Stations</i> (Stations MAX)	2007	« Configuration des paramètres radio 802.11 » à la page 173
<i>Transmit Power</i> (Puissance de transmission)	100 %	« Configuration des paramètres radio 802.11 » à la page 173

Tableau 3.1 Paramètres par défaut de la 9160 G2 (Suite)

Option	Paramètres par défaut	Informations associées
<i>Rate Sets Supported (Mbps) (Ensembles de débits pris en charge (Mbit/s))</i>	<ul style="list-style-type: none"> • IEEE 802.1a : 54, 48, 36, 24, 18, 12, 9, 6 • IEEE 802.1g : 54, 48, 36, 24, 18, 12, 11, 9, 6, 5,5, 2, 1 • IEEE 802.1b : 11, 5,5, 2, 1 	« Configuration des paramètres radio 802.11 » à la page 173
<i>Rate Sets (Mbps) (Ensembles de débits (Mbit/s)) (Basic/Advertised) (Base/annoncés)</i>	<ul style="list-style-type: none"> • IEEE 802.1a : 24, 12, 6 • IEEE 802.1g : 11, 5,5, 2, 1 • IEEE 802.1b : 2, 1 	« Configuration des paramètres radio 802.11 » à la page 173
<i>Broadcast SSID (SSID de diffusion)</i>	Allow (Autoriser)	« Configuration des paramètres de sécurité » à la page 105.
<i>Security Mode (Mode de sécurité)</i>	None (Aucun) (texte brut)	« Configuration des paramètres de sécurité » à la page 105.
<i>Authentication Type (Type d'authentification)</i>	None (Aucun)	
<i>MAC Filtering (Filtrage des adresses MAC)</i>	Allow any station unless in list (Autoriser toute station sauf si elle est dans la liste)	« Filtrage d'adresses MAC » à la page 183
<i>Guest Login and Management (Connexion et gestion invité)</i>	Disabled (Désactive)	« Configuration de l'accès invité » à la page 159
<i>Load Balancing (Équilibrage de la charge)</i>	Disabled (Désactivé)	« Équilibrage de la charge » à la page 187
<i>WDS Settings (Paramètres WDS)</i>	None (Aucun)	« Système de distribution sans fil (WDS) » à la page 213

3.1.2 Ce que le point d'accès ne fournit pas

La passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway n'est pas conçue pour fonctionner comme une **Gateway - Passerelle** Internet. Pour connecter votre LAN sans fil (**WLAN**) à d'autres **LAN** ou à Internet, vous avez besoin d'un appareil de passerelle.

3.2 Ordinateur de l'administrateur

La configuration et l'administration de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway est effectuée grâce à une interface utilisateur basée sur Internet (IU). Le Tableau 3.2 décrit la configuration minimale requise pour l'ordinateur de l'administrateur.

Tableau 3.2 Logiciel et matériel administrateur de point d'accès requis

Éléments requis	Description
<i>Ethernet Connection to the First Access Point (Connexion Ethernet au premier point d'accès)</i>	<p>L'ordinateur utilisé pour configurer le premier point d'accès doit être connecté au point d'accès (directement ou via un concentrateur) par un câble Ethernet.</p> <p>Pour plus d'informations, reportez-vous à la section « Connecter le point d'accès au réseau et à l'alimentation » à la page 40 dans « Étapes rapides de configuration et de lancement ».</p>
<i>Wireless Connection to the Network (Connexion sans fil au réseau)</i>	<p>Après la configuration initiale et le lancement des premiers points d'accès sur votre nouveau réseau sans fil, vous pouvez apporter d'autres modifications de configuration dans les pages Web d'administration via une connexion sans fil au réseau « interne ». Pour ouvrir une connexion sans fil au point d'accès, votre appareil d'administration devra disposer de fonctionnalités Wi-Fi similaires à celle de tout client sans fil :</p> <ul style="list-style-type: none">• Adaptateur client portable ou Wi-Fi intégrée qui prend en charge au moins un des modes IEEE 802.11 dans lequel vous avez l'intention d'exécuter le point d'accès. (Les modes IEEE 802.11a, 802.11b802.11a, 802.11g802.11b, 802.11a Turbo802.11g 802.11a Turbo sont pris en charge.)• Logiciel de client sans fil tel que Microsoft® Windows® XP ou client sans fil Funk Odyssey configuré pour s'associer avec la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway. <p>Pour plus de détails sur la configuration du client Wi-Fi, reportez-vous à la section « Ordinateurs client sans fil » à la page 32.</p>

Tableau 3.2 Logiciel et matériel administrateur de point d'accès requis (Suite)

Éléments requis	Description
<i>Web Browser / Operating System (Navigateur Web/Système d'exploitation)</i>	<p>La configuration et l'administration de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway sont fournies via une interface utilisateur Internet hébergée sur le point d'accès. Nous vous recommandons d'utiliser l'un des navigateurs Web suivants pour accéder aux pages Web d'administration des points d'accès :</p> <ul style="list-style-type: none">• Microsoft Internet Explorer version 5.5 ou 6.x (avec niveau de correctif mis à jour pour chaque version majeure) sur Microsoft Windows XP ou Microsoft Windows 2000• Netscape® Mozilla 1.7.x sur RedHat Linux Version 2.4 <p>JavaScript doit être activé dans le navigateur Web d'administration pour prendre en charge les fonctionnalités interactives de l'interface d'administration. Il doit également prendre en charge les téléchargements HTTP pour utiliser la fonction de mise à niveau du firmware.</p>
<i>Security Settings (Paramètres de sécurité)</i>	<p>Assurez-vous que la sécurité est désactivée sur le client sans fil utilisé pour configurer le point d'accès.</p>

3.3 Ordinateurs client sans fil

La passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway offre un accès sans fil à n'importe quel client équipé d'un adaptateur client Wi-Fi correctement configuré pour le mode 802.11 dans lequel le point d'accès est en cours d'exécution.

Plusieurs systèmes d'exploitation client sont pris en charge. Les clients peuvent être des ordinateurs portables ou de bureau, des assistants numériques personnels (PDA), ou tout autre appareil portatif, mobile ou fixe équipé d'un adaptateur Wi-Fi et de pilotes de prise en charge.

Afin de se connecter au point d'accès, les clients sans fil ont besoin des logiciels et matériels décrits dans le Tableau 3.3.

Tableau 3.3 Logiciel et matériel administrateur de point d'accès requis

Éléments requis	Description
<i>Wi-Fi Client Adaptor (Adaptateur client Wi-Fi)</i>	<p>Adaptateur client portable ou Wi-Fi intégrée qui prend en charge au moins un des modes IEEE 802.11 dans lequel vous avez l'intention d'exécuter le point d'accès. (Les modes IEEE 802.11a, 802.11b et 802.11g sont pris en charge.)</p> <p>Les adaptateurs client Wi-Fi varient de façon significative. L'adaptateur peut être une carte PC intégrée dans l'appareil client, une carte portable PCMCIA ou PCI (types de MC), ou appareil terminal externe tel qu'un adaptateur USB ou Ethernet que vous connectez au client au moyen d'un câble.</p> <p>Le point d'accès prend en charge les modes 802.11a/b/g, mais vous devrez probablement prendre une décision pendant la phase de conception du réseau concernant le mode à utiliser. La condition fondamentale pour les clients est de disposer de tous les adaptateurs configurés qui correspondent au mode 802.11 pour lesquels vos points d'accès sont configurés.</p>
<i>Wireless Client Software (Logiciel client sans fil)</i>	<p>Logiciel de client sans fil tel que Microsoft® Windows Suppliquant ou client sans fil Funk Odyssey configuré pour s'associer avec la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway.</p>
<i>Client Security Settings (Paramètres de sécurité client)</i>	<p>La sécurité doit être désactivée sur le client utilisé pour établir la configuration initiale du point d'accès.</p> <p>Si le mode de sécurité sur le point d'accès est défini sur un paramètre autre que le texte brut, les clients sans fil devront définir un profil pour le mode d'authentification utilisé par le point d'accès et fournir un nom d'utilisateur et un mot de passe, un certificat ou une preuve d'identité similaire valide. Les modes de sécurité sont Static (Statique) WEP, IEEE 802.1x, WPA avec serveur RADIUS et WPA2PSK.</p> <p>Pour plus d'informations sur la configuration de la sécurité sur le point d'accès, reportez-vous à la section « Configuration de la sécurité » à la page 95.</p>

3.4

Présentation de l'adressage IP statique et dynamique sur la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway

Les passerelles sans fil Passerelle sans fil 9160 G2 Wireless Gateway sont conçues pour la configuration automatique, avec une configuration minimale requise pour le premier point d'accès et aucune pour les points d'accès supplémentaires qui rejoignent un *cluster* préconfiguré.

3.4.1 Comment le point d'accès obtient-il une adresse IP au démarrage ?

Lorsque vous déployez le point d'accès, il recherche un serveur réseau **DHCP** et, s'il le trouve, obtient une **IP Address - Adresse IP** auprès du serveur DHCP. Si aucun serveur DHCP n'est détecté sur le réseau, le point d'accès va continuer à utiliser son **Static IP Address - Adresse IP statique** (192.168.1.10) par défaut jusqu'à ce que vous lui attribuez une nouvelle adresse IP statique (et que vous spécifiez une stratégie d'adressage IP statique) ou jusqu'à ce qu'un serveur DHCP soit mis en ligne.



Remarques : Si vous configurez un réseau interne et un réseau invité et que vous envisagez d'utiliser une stratégie d'adressage dynamique, des serveurs DHCP différents doivent être exécutés sur chaque réseau.

Un serveur DHCP est une condition requise pour le réseau invité.

3.4.2 Adressage IP dynamique

La passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway s'attend généralement à ce qu'un serveur **DHCP** soit en cours d'exécution sur le réseau où le point d'accès est déployé. La plupart des réseaux grand public et petites entreprises ont déjà un service DHCP fourni via un appareil de passerelle ou un serveur centralisé. Cependant, si aucun serveur DHCP n'est présent sur le réseau interne, le point d'accès va utiliser l'**Static IP Address - Adresse IP statique** par défaut pour le premier démarrage.

De même, les clients sans fil et autres appareils réseau (comme les imprimantes) recevront leurs adresses IP du serveur DHCP, le cas échéant. Si aucun serveur DHCP n'existe déjà sur le réseau, vous devez affecter manuellement les adresses IP statiques à vos clients sans fil et aux autres appareils réseau.

Le réseau invité doit disposer d'un serveur DHCP.

3.4.3 Adressage IP statique

La passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway est livrée avec une **Static IP Address - Adresse IP statique** par défaut de 192.168.1.10. (Reportez-vous à la section « Paramètres par défaut de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway » à la page 27.) Si aucun serveur **DHCP** n'est trouvé sur le réseau, le point d'accès conserve cette adresse IP statique au premier démarrage.

Après le démarrage du point d'accès, vous avez la possibilité d'indiquer une stratégie d'adressage IP statique sur les passerelles sans fil Passerelle sans fil 9160 G2 Wireless Gateway et d'attribuer des adresses IP statiques aux points d'accès sur le réseau interne via les pages Web d'administration des points d'accès. (Reportez-vous aux informations sur le champ « Connection Type » (Type de connexion) et les champs associés dans la section « Paramètres de l'interface interne » à la page 147.)



Important : Si vous ne disposez pas d'un serveur sur le réseau interne et que vous n'avez pas l'intention d'en utiliser un, la première chose à faire depuis le point d'accès est de changer le type de connexion DHCP en IP statique. Vous pouvez attribuer une nouvelle adresse IP statique au point d'accès ou continuer à utiliser l'adresse par défaut. Nous vous recommandons l'affectation d'une nouvelle adresse IP statique de sorte que si plus tard que vous ajoutez une autre passerelle sans fil 9160 G2 Wireless Gateway sur le même réseau, l'adresse IP de chaque point d'accès reste unique.

3.4.4 Restauration d'une adresse IP

Si vous rencontrez un problème de communication avec le point d'accès, vous pouvez récupérer une **Static IP Address - Adresse IP statique** en réinitialisant le point d'accès à la configuration d'usine par défaut (reportez-vous à la section « Réinitialisation de la configuration d'usine par défaut » à la page 334), ou vous pouvez obtenir une adresse attribuée de manière dynamique en connectant le point d'accès à un réseau qui a **DHCP**.

ÉTAPES RAPIDES DE CONFIGURATION ET DE LANCEMENT

4

4.1 Déballer la passerelle sans fil 9160 G2 Wireless Gateway.	39
4.1.1 Matériel et ports de la passerelle sans fil 9160 G2 Wireless Gateway.	39
4.1.2 Qu'y a-t-il dans la passerelle sans fil 9160 G2 Wireless Gateway ?	39
4.2 Connecter le point d'accès au réseau et à l'alimentation	40
4.2.1 Une remarque sur la configuration de connexions pour un réseau invité	42
4.2.1.1 Connexions matérielles pour un VLAN invité	42
4.3 Mise sous tension du point d'accès	42
4.4 Se connecter aux pages Web d'administration	42
4.4.1 Affichage des paramètres de base des points d'accès	43
4.5 Configurer les paramètres de base et démarrer le réseau sans fil	44
4.5.1 Configuration par défaut	44
4.6 Quelle est la prochaine étape ?	44
4.6.1 Vérifier que le point d'accès est connecté au réseau local	44
4.6.2 Tester la connectivité LAN avec les clients sans fil	45
4.6.3 Sécuriser et affiner le point d'accès avec des fonctions avancées	45

Configurer et déployer une ou plusieurs passerelles sans fil Passerelle sans fil 9160 G2 Wireless Gateway équivaut à créer et lancer un *réseau sans fil*. La page Web d'administration *Basic Settings* (Paramètres de base) simplifie ce processus. Voici un guide pas-à-pas de la configuration de vos passerelles sans fil Passerelle sans fil 9160 G2 Wireless Gateway et du réseau sans fil résultant. Familiarisez-vous avec le Chapitre 3 : « Liste de contrôle du pré-lancement » si vous ne l'avez pas déjà fait.

Les thèmes abordés ici sont les suivants :

- Étape 1 : *Déballer la passerelle sans fil 9160 G2 Wireless Gateway*.
- Étape 2 : *Connecter le point d'accès au réseau et à l'alimentation*.
- Étape 3 : *Mise sous tension du point d'accès*.
- Étape 5 : *Se connecter aux pages Web d'administration*.
- Étape 6 : *Configurer les paramètres de base et démarrer le réseau sans fil*.
- *Quelle est la prochaine étape ?*

4.1 Déballer la passerelle sans fil 9160 G2 Wireless Gateway

Déballer la passerelle sans fil 9160 G2 Wireless Gateway et familiarisez-vous avec ses ports matériels, ses câbles associés et ses accessoires.

4.1.1 Matériel et ports de la passerelle sans fil 9160 G2 Wireless Gateway

La passerelle sans fil 9160 G2 Wireless Gateway inclut :

- Port Ethernet pour la connexion au réseau local (LAN) via un câble réseau Ethernet.
- Port d'alimentation et adaptateur secteur.
- Interrupteur Marche/Arrêt d'alimentation.
- Une ou deux radios en fonction du modèle du produit que vous avez.

4.1.2 Qu'y a-t-il dans la passerelle sans fil 9160 G2 Wireless Gateway ?

La passerelle sans fil 9160 G2 Wireless Gateway, en tant que *Access Point - Point d'accès* (AP), est un ordinateur universel conçu pour fonctionner comme un concentrateur sans fil. Ce point d'accès contient un système radio Wi-Fi et un microprocesseur. Le point d'accès démarre depuis FlashROM via un firmware alimenté avec les fonctionnalités d'exécution configurables résumées dans la section « Présentation de la passerelle sans fil 9160 G2 Wireless Gateway » à la page 7.

Dès que de nouvelles fonctionnalités et améliorations sont disponibles, vous pouvez mettre à niveau le firmware pour ajouter de nouvelles fonctionnalités et améliorations des performances pour les points d'accès qui constituent votre réseau sans fil. (Reportez-vous à la section « Mise à niveau du firmware » à la page 336.)

4.2 Connecter le point d'accès au réseau et à l'alimentation

L'étape suivante consiste à configurer le réseau et les connexions d'alimentation.

1. Effectuez l'une des opérations suivantes pour créer une connexion Ethernet entre le point d'accès et l'ordinateur :

Branchez une extrémité du câble Ethernet au port réseau sur le point d'accès et l'autre extrémité au concentrateur auquel votre ordinateur est connecté. (Reportez-vous à la Figure 4.2 à la page 41.)

Ou

Branchez une extrémité d'un câble croisé¹ au port réseau sur le point d'accès et l'autre extrémité au port Ethernet de l'ordinateur. (Reportez-vous à la Figure 2 à la page 41.)



Remarques : Si vous utilisez un concentrateur, l'appareil utilisé doit permettre aux signaux de diffusion du point d'accès d'atteindre tous les autres appareils du réseau. Un concentrateur standard devrait faire l'affaire. Certains commutateurs, cependant, ne permettent pas les diffusions dirigées ou de sous-réseau. Vous pourriez être amené à configurer le commutateur pour une diffusion dirigée.

Pour une configuration initiale avec une connexion Ethernet directe sans serveur DHCP, assurez-vous de définir votre PC sur une adresse IP statique dans le même sous-réseau que l'adresse IP par défaut du point d'accès. (L'adresse IP par défaut pour le point d'accès est 192.168.1.10.)

Si vous utilisez une connexion Ethernet directe (filaire) pour la configuration initiale (via un câble croisé) entre le point d'accès et l'ordinateur, vous devrez reconfigurer le câblage pour le démarrage et le déploiement du point d'accès de sorte que le point d'accès ne soit plus connecté directement à l'ordinateur, mais au LAN (via un concentrateur comme illustré dans la Figure 4.2, ou directement).

¹ Si le matériel du point d'accès prend en charge les fonctionnalités automatiques **MDI** et **MDI-X**, vous pouvez utiliser un câble Ethernet simple pour une connexion directe d'un PC au point d'accès. Un câble croisé fonctionne également, mais il n'est pas nécessaire si vous avez des ports de détection automatique MDI et MDI-X.

Figure 4.1 Connexions Ethernet utilisant DHCP

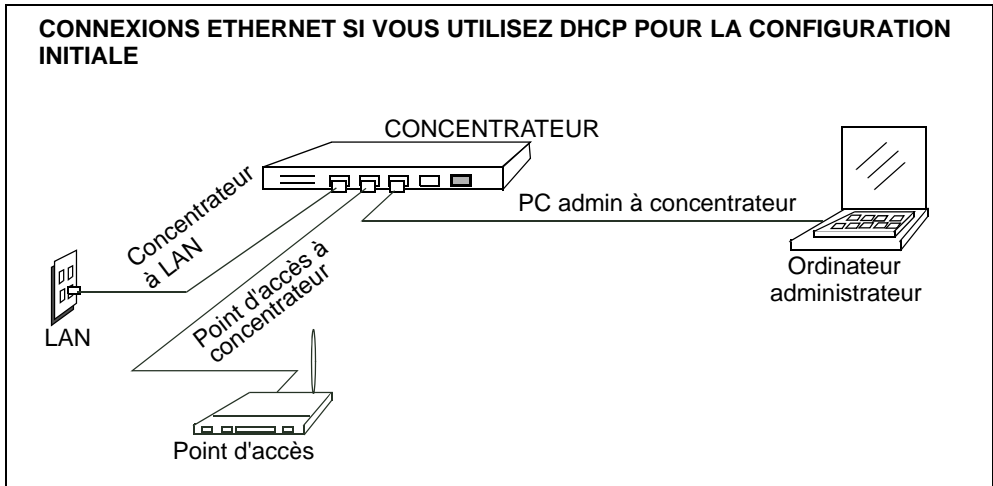
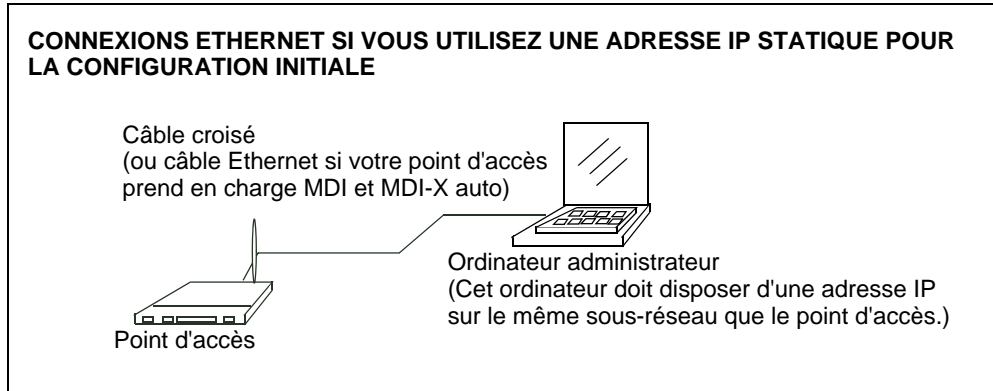


Figure 4.2 Connexions Ethernet utilisant une adresse IP statique



2. Branchez l'adaptateur secteur au port d'alimentation situé à l'arrière du point d'accès, puis branchez l'autre extrémité du cordon d'alimentation à une prise de courant (de préférence, via un parasurtenseur).

4.2.1 Une remarque sur la configuration de connexions pour un réseau invité

La passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway offre une interface invité prête à l'emploi qui vous permet de configurer un point d'accès afin de contrôler l'accès invité au réseau. Le même point d'accès peut fonctionner comme un pont pour deux réseaux sans fil différents : un réseau « interne » local et un réseau « invité » public. Cette opération peut être réalisée virtuellement en définissant deux réseaux LAN virtuels différents via l'interface d'administration.

Pour plus d'informations sur la configuration des paramètres de l'interface invité depuis l'interface d'administration, reportez-vous au Chapitre 14 : « Configuration de l'accès invité ».

4.2.1.1 Connexions matérielles pour un VLAN invité

Si vous envisagez de configurer un réseau invité utilisant des réseaux VLAN, procédez comme suit :

- Connectez un port réseau sur le point d'accès à un commutateur VLAN.
- Définissez les réseaux locaux virtuels (VLAN) sur ce commutateur.

4.3 Mise sous tension du point d'accès

La passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway s'allume et s'initialise lorsque vous la branchez.

4.4 Se connecter aux pages Web d'administration

Lorsque vous accédez à l'adresse IP des pages Web d'administration de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway, vous êtes invité à entrer un nom d'utilisateur et un mot de passe.



Les valeurs par défaut pour le nom d'utilisateur et le mot de passe sont les suivantes.

Tableau 4.1 Nom d'utilisateur et mot de passe

Champ	Paramètre par défaut
<i>User name (Nom d'utilisateur)</i>	admin
<i>Password (Mot de passe)</i>	admin (Le nom d'utilisateur est en lecture seule. Il ne peut pas être modifié.)

Entrez le nom d'utilisateur et le mot de passe, puis cliquez sur **OK**.

4.4.1 Affichage des paramètres de base des points d'accès

Lors de votre première connexion, la page *Basic Settings* (Paramètres de base) pour l'administration de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway s'affiche. Ces sont des paramètres généraux pour tous les points d'accès qui sont membres du cluster et, si la configuration automatique est spécifiée, pour tous les nouveaux points d'accès qui sont ajoutés ultérieurement.

Figure 4.3 Paramètres de base des points d'accès

Basic Settings

Provide basic settings

1 Review Description of this Access Point ...

These fields show information specific to this access point.

IP Address: 10.128.75.4
MAC Address: 00:08:A2:01:4B:52
Firmware Version: E187k

2 Provide Network Settings ...

These settings apply to this access point. The same settings will apply to new access points joining the cluster.

Current Password
New Password
Confirm new password
Network Name (SSID)

3 Settings ...

Click "Update" to save the new settings.

4.5 Configurer les paramètres de base et démarrer le réseau sans fil

Fournissez un ensemble minimal d'informations de configuration en définissant les paramètres de base de votre réseau sans fil. Ces paramètres sont tous disponibles sur la page *Basic Settings* ((Paramètres de base) de l'interface Web d'administration, et sont classés en étapes 1 à 3 sur la page Web.

Pour obtenir une description détaillée de ces « paramètres de base » et la manière de les configurer correctement, reportez-vous au Chapitre 5 : « Configuration des paramètres de base ». Ces étapes, résumées brièvement ici, sont les suivantes :

1. Vérifiez la description de ce point d'accès.
Fournissez les informations d'adressage IP. Pour plus d'informations, reportez-vous à la section « Révision / Description du point d'accès » à la page 50.
2. Fournissez des paramètres réseau.
Fournissez un nouveau mot de passe administrateur pour les points d'accès en cluster. Pour plus d'informations, reportez-vous à la section « Fournir des paramètres réseau » à la page 51.
3. Paramètres.
Cliquez sur le bouton **Update** (Mettre à jour) pour activer le réseau sans fil avec les nouveaux paramètres. Pour plus d'informations, reportez-vous à la section « Mise à jour des paramètres de base » à la page 52.

4.5.1 Configuration par défaut

Si vous suivez les étapes ci-dessus en acceptant tous les paramètres par défaut, le point d'accès aura la configuration par défaut indiquée dans la section « Paramètres par défaut de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway » à la page 27.

4.6 Quelle est la prochaine étape ?

Assurez-vous ensuite que le point d'accès est connecté au réseau local, ajoutez des clients sans fil et connectez les clients au réseau. Une fois que vous avez testé les éléments de base de votre réseau sans fil, vous pouvez activer plus de sécurité et affiner en modifiant les fonctions de configuration avancées du point d'accès.

4.6.1 Vérifier que le point d'accès est connecté au réseau local

Si vous avez configuré le point d'accès et le PC administrateur en les connectant à un concentrateur de réseau, votre point d'accès est déjà connecté au LAN. C'est tout — vous êtes prêt ! L'étape suivante consiste à tester des clients sans fil.

Si vous avez configuré le point d'accès avec une connexion filaire directe via un câble croisé entre votre ordinateur et le point d'accès, procédez comme suit :

1. Débranchez le câble croisé de l'ordinateur et du point d'accès.
2. Branchez un câble Ethernet entre le point d'accès et le **LAN**.
3. Connectez votre ordinateur au réseau local via un câble Ethernet ou une carte client sans fil.

4.6.2 Tester la connectivité LAN avec les clients sans fil

Testez la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway en essayant de la détecter et de l'associer à certains appareils client sans fil. (Reportez-vous à la section « Ordinateurs client sans fil » à la page 32 dans le *Liste de contrôle du pré-lancement* pour obtenir des informations sur la configuration requise pour ces clients.)

4.6.3 Sécuriser et affiner le point d'accès avec des fonctions avancées

Une fois que votre le réseau sans fil fonctionne et que vous avez testé le point d'accès avec des clients sans fil, vous pouvez ajouter des couches de sécurité supplémentaires, ajouter des utilisateurs, configurer une interface invité et affiner les paramètres de performances.

CONFIGURATION DES PARAMÈTRES DE BASE

5

5.1 Accès aux paramètres de base	49
5.2 Révision / Description du point d'accès	50
5.3 Fournir des paramètres réseau	51
5.4 Mise à jour des paramètres de base.	52
5.5 Paramètres de base pour un point d'accès autonome.	52
5.6 Votre réseau d'un coup d'œil : Présentation des icônes d'indicateur	52

5.1 Accès aux paramètres de base

Pour configurer les paramètres initiaux, cliquez sur **Basic Settings** (Paramètres de base).

Si vous saisissez l'adresse IP du point d'accès dans votre navigateur, la page *Basic Settings* (Paramètres de base) est la page qui s'affiche par défaut.

Figure 5.1 Paramètres de base

9160 Wireless Gateway

Basic Settings

Provide basic settings

1 Review Description of this Access Point ...

These fields show information specific to this access point.

IP Address: 10.128.75.4
MAC Address: 00:08:A2:01:4B:52
Firmware Version: E187k

2 Provide Network Settings ...

These settings apply to this access point. The same settings will apply to new access points joining the cluster.

Current Password
New Password
Confirm new password
Network Name (SSID)

3 Settings ...

Click "Update" to save the new settings.

Remplissez les champs de la page *Basic Settings* (Paramètres de base) comme indiqué dans la section « Révision / Description du point d'accès » à la page 50.

5.2 Révision / Description du point d'accès

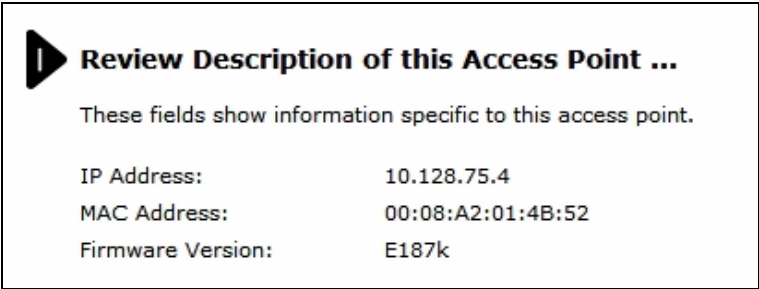


Tableau 5.1 Options de l'écran Basic Settings (Paramètres de base)

Champ	Description
<i>IP Address</i> (Adresse IP)	Affiche l'adresse IP attribuée à ce point d'accès. Ce champ n'est pas modifiable car l'adresse IP est déjà affectée (soit via DHCP, ou en version statique via les paramètres Ethernet (filaire), comme décrit dans la section « Paramètres de l'interface invité » à la page 150).
<i>MAC Address</i> (Adresse MAC)	<p>Affiche l'adresse <i>MAC</i> du point d'accès.</p> <p>Une adresse MAC est une adresse matérielle unique et permanente pour tout appareil qui représente une interface pour le réseau. L'adresse MAC est attribuée par le fabricant. Vous ne pouvez pas modifier l'adresse MAC. Elle est fournie ici à titre d'information comme identifiant unique pour une interface.</p> <p>L'adresse affichée ici est l'adresse MAC du pont (br0). C'est l'adresse par laquelle le point d'accès est connu en externe par d'autres réseaux.</p> <p>Pour voir les adresses MAC des interfaces interne et invité du point d'accès, reportez-vous à l'onglet <i>Status > interfaces</i> (État > interfaces).</p>
<i>Firmware Version</i> (Version du firmware)	<p>Informations de version du firmware actuellement installé sur le point d'accès.</p> <p>Dès que de nouvelles versions du firmware de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway sont disponibles, vous pouvez mettre à niveau le firmware sur vos points d'accès pour bénéficier de nouvelles fonctionnalités et améliorations.</p> <p>Pour obtenir des instructions sur la mise à niveau du firmware, reportez-vous à la section « Mise à niveau du firmware » à la page 336.</p>

5.3 Fournir des paramètres réseau

2

Provide Network Settings ...

These settings apply to this access point. The same settings will apply to new access points joining the cluster.

Current Password


New Password

Confirm new password

Network Name (SSID)

Psion Teklogix

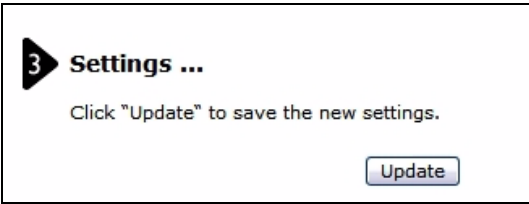
Tableau 5.2 Mot de passe administrateur et réseau sans fil

Champ	Description
<i>Current Password</i> (Mot de passe actuel)	Saisissez le mot de passe administrateur actuel. Vous devez entrer correctement le mot de passe actuel avant de pouvoir le modifier.
<i>New Password</i> (Nouveau mot de passe)	Saisissez un nouveau mot de passe administrateur. Le texte que vous saisissez s'affiche sous la forme de caractères « * » afin d'empêcher d'autres personnes de voir le mot de passe que vous entrez. Le mot de passe administrateur doit être une chaîne alphanumérique de 8 caractères maximum. N'utilisez pas de caractères spéciaux ni d'espaces.  En première étape de sécurisation immédiate de votre réseau sans fil, nous vous recommandons de modifier le mot de passe administrateur pour remplacer la valeur par défaut.
<i>Confirm New Password</i> (Confirmation du nouveau mot de passe)	Entrez une nouvelle fois le nouveau mot de passe administrateur afin de confirmer que vous l'avez saisi comme prévu.
<i>Network Name (SSID)</i> (Nom de réseau (SSID))	Entrez un nom pour le réseau sans fil sous forme de chaîne de caractères. Ce nom s'applique à tous les points d'accès sur ce réseau. À mesure que vous ajoutez d'autres points d'accès, ils partagent ce SSID . Le <i>Service Set Identifier (SSID)</i> est une chaîne alphanumérique de 32 caractères maximum Remarque : Si vous êtes connecté en tant que client sans fil au point d'accès que vous administrez, réinitialiser le SSID entraînera la perte de connectivité du point d'accès. Vous devrez vous reconnecter au nouveau SSID après l'enregistrement de ce nouveau paramètre.



Remarque : La passerelle sans fil 9160 G2 Wireless Gateway n'est pas conçue pour plusieurs modifications de configuration simultanées. Si vous disposez d'un réseau qui inclut plusieurs points d'accès, et que plus d'un administrateur est connecté aux pages Web d'administration pour apporter des modifications de configuration, tous les points d'accès du cluster restent synchronisés, mais il n'est pas garanti que toutes les modifications de configuration spécifiées par plusieurs utilisateurs soient appliquées.

5.4 Mise à jour des paramètres de base



Une fois que vous avez examiné la nouvelle configuration, cliquez sur **Update** (Mettre à jour) pour appliquer les paramètres et déployer les points d'accès comme un réseau sans fil.

5.5 Paramètres de base pour un point d'accès autonome

L'onglet *Basic Settings* (Paramètres de base) d'un point d'accès autonome indique uniquement que le mode actuel est autonome. Si vous souhaitez ajouter le point d'accès actuel à un cluster existant, accédez à l'onglet *Cluster > Access* (Cluster > Accès).

Pour plus d'informations, reportez-vous à la section « Démarrage de la mise en cluster » à la page 63.

5.6 Votre réseau d'un coup d'œil : Présentation des icônes d'indicateur

Tous les onglets des paramètres de cluster sur les pages Web d'administration comprennent des icônes d'indicateur visuel indiquant l'activité actuelle du réseau.

5.7 Affichage de l'interface utilisateur avec des couleurs et styles différents

Tableau 5.3 Icônes d'indicateur

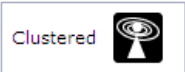


Icône	Description
	<p>Lorsqu'au moins un point d'accès sur votre réseau est disponible pour le service, l'icône « Wireless Network Available » (Réseau sans fil disponible) s'affiche. L'icône de mise en cluster indique si le point d'accès actuel est « Clustered » (En cluster) ou « Not Clustered » (Pas en cluster) (c'est-à-dire, autonome ou lorsqu'un état de modification est en cours).</p> <p>Pour plus d'informations sur la mise en cluster, reportez-vous à la section « Présentation de la mise en cluster » à la page 58.</p>

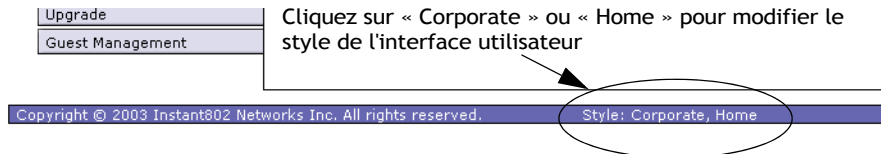
Tableau 5.3 Icônes d'indicateur (Suite)

Icône	Description
	<p>Le nombre de points d'accès disponibles pour le service sur ce réseau est indiqué par l'icône « Access Points » (Points d'accès).</p> <p>Pour plus d'informations sur la gestion des points d'accès, reportez-vous au Chapitre 6 : « Gestion des points d'accès et des clusters ».</p>
	<p>Le nombre de comptes d'utilisateur client créés et activés sur ce réseau est indiqué par l'icône « User Accounts » (Comptes d'utilisateur).</p> <p>Pour plus d'informations sur la configuration de comptes d'utilisateur sur le point d'accès à utiliser avec le serveur d'authentification intégré, reportez-vous au Chapitre 7 : « Gestion des comptes d'utilisateur ». Reportez-vous également aux sections « IEEE 802.1x » à la page 114 et « WPA Enterprise » à la page 119, qui sont les deux modes de sécurité qui offrent la possibilité d'utiliser le serveur d'authentification intégré.</p>

Les pages Web d'administration de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway sont fournies en deux thèmes de couleur et styles différents : (1) type Corporate et (2) style Home.

Vous pouvez modifier le style de l'interface utilisateur que vous êtes en train de visionner en fonction de vos préférences.

Pour changer de style, cherchez les boutons « Style : Corporate, Home » situés au bas des pages Web d'administration, et cliquez sur **Corporate** ou **Home**.



GESTION DES POINTS D'ACCÈS ET DES CLUSTERS

6

6.1 Présentation.	57
6.2 Accès à la gestion des points d'accès.	57
6.3 Présentation de la mise en cluster	58
6.3.1 Qu'est-ce qu'un cluster ?	58
6.3.2 Combien de points d'accès un cluster peut-il prendre en charge ?	58
6.3.3 Quels types de points d'accès peuvent être mis en cluster ensemble ?	58
6.3.4 Quelle est la relation entre le point d'accès coordinateur et les autres membres du cluster ?	59
6.3.5 Quels paramètres sont/ne sont pas partagés dans le cadre de la configuration du cluster ?	59
6.3.5.1 Paramètres partagés dans la configuration du cluster.	59
6.3.5.2 Paramètres non partagés par le cluster	60
6.3.6 Formation du cluster	60
6.3.7 Taille de cluster et appartenance	61
6.3.8 Sécurité Intra-Cluster.	61
6.4 Présentation des paramètres de point d'accès	61
6.4.1 Modification de la description d'emplacement.	63
6.4.2 Définition du nom du cluster.	63
6.5 Démarrage de la mise en cluster	63
6.6 Arrêt de la mise en cluster	64
6.7 Informations de configuration pour un point d'accès spécifique et gestion des points d'accès autonomes.	64
6.7.1 Accès à un point d'accès en utilisant son adresse IP dans une URL	65
6.8 Surveillance de session.	65
6.8.1 Accès à la surveillance de session	65
6.8.2 Présentation des informations de surveillance de session	65
6.8.3 Affichage des informations de session pour les points d'accès	67
6.8.4 Tri des informations de session.	68
6.8.5 Actualisation des informations de session	68

6.1 Présentation

La passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway affiche les paramètres de configuration des points d'accès en cluster (emplacement, adresse IP, adresse MAC, état et disponibilité) et fournit un moyen d'accès à la configuration complète de points d'accès spécifiques s'ils sont membres du cluster.

Les points d'accès autonomes ou ceux qui ne sont pas les membres de ce cluster ne s'affichent pas dans cette liste. Pour configurer les points d'accès autonomes, vous devez connaître l'adresse IP du point d'accès et l'utiliser dans une URL (<http://AdresseIPduPointdAccès>).



Remarque : La passerelle sans fil 9160 G2 Wireless Gateway n'est pas conçue pour plusieurs modifications de configuration simultanées. Si vous disposez d'un réseau qui inclut plusieurs points d'accès, et que plus d'un administrateur est connecté aux pages Web d'administration pour effectuer des modifications de configuration, tous les points d'accès du cluster restent synchronisés, mais il n'est pas garanti que toutes les modifications de configuration spécifiées par plusieurs utilisateurs seront appliquées.

6.2 Accès à la gestion des points d'accès

Pour afficher ou modifier des informations sur les points d'accès dans un cluster, cliquez sur l'onglet **Cluster > Access Points** (Cluster > Points d'accès).

Figure 6.1 Paramètres de cluster pour les points d'accès

Location	MAC Address	IP Address
Vicky's Office - top shelf	00:0C:41:16:A3:12	10.10.100.238
Vicky's Office - lower shelf	00:00:04:7F:00:00	10.10.100.245

6.3 Présentation de la mise en cluster

Une fonctionnalité clé de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway est la possibilité de former un groupe dynamique reconnaissant la configuration (appelé *cluster*) avec d'autres passerelles sans fil Passerelle sans fil 9160 G2 Wireless Gateway dans un réseau, dans le même sous-réseau. Les points d'accès peuvent participer à un cluster d'auto-organisation qui facilite le déploiement, la gestion et la sécurisation de votre réseau sans fil. Le cluster fournit un point d'administration unique et vous permet d'afficher le déploiement de points d'accès comme un seul réseau sans fil au lieu d'une série d'appareils sans fil distincts.

6.3.1 Qu'est-ce qu'un cluster ?

Un cluster est un groupe de points d'accès qui sont coordonnés comme un seul groupe via l'administration de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway. Vous pouvez avoir plusieurs clusters sur le même sous-réseau s'ils ont des « noms » de cluster différents.

6.3.2 Combien de points d'accès un cluster peut-il prendre en charge ?

Actuellement, il n'existe pas de limite au nombre de points d'accès dans un cluster. Des tests de validation ont vérifié au moins une douzaine de points d'accès pris en charge sur le même sous-réseau. Vous pouvez inclure autant de points d'accès que nécessaire dans un cluster à tout moment.

6.3.3 Quels types de points d'accès peuvent être mis en cluster ensemble ?

Une passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway peut former un cluster avec elle-même (un « cluster d'un ») et avec d'autres passerelles sans fil Passerelle sans fil 9160 G2 Wireless Gateway. Pour être membres du même cluster, les points d'accès doivent :

- Être des appareils compatibles selon les indications du fabricant (les points d'accès doivent avoir des caractéristiques de conception compatibles).
- Avoir la même configuration radio (tous les points d'accès de radio unique ou de radio professionnelle).
- Avoir la même configuration de bande (tous les points d'accès monobandes ou bibandes).
- Être sur le même *LAN*.

Le fait de disposer de points d'accès divers sur le réseau n'affecte aucunement la mise en cluster de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway. Cependant, il est utile de comprendre le comportement de la mise en cluster à des fins d'administration :

- Les points d'accès rejoignant le cluster doivent avoir le même nom. Pour plus d'informations sur la définition du nom du cluster, reportez-vous à la page 63.
- Les points d'accès d'autres marques ne peuvent pas rejoindre le cluster. Ces points d'accès doivent être administrés avec leurs propres outils d'administration associés.

6.3.4 Quelle est la relation entre le point d'accès coordinateur et les autres membres du cluster ?

La configuration du cluster, le partage des mises à jour de configuration, et le suivi des points d'accès qui rejoignent ou quittent le groupe sont gérés par un point d'accès *coordinateur* qui est choisi parmi les membres du cluster. Si un point d'accès coordinateur est indisponible, un nouveau membre du cluster se voit attribuer les responsabilités de coordinateur. Ce processus est entièrement automatisé, basé sur un ensemble de règles qui prend en compte l'ancienneté, la taille du cluster, ainsi que d'autres facteurs pour déterminer quel point d'accès est le plus adapté à la tâche à un moment donné.

Il n'est pas nécessaire de suivre ou de gérer quel point d'accès est le coordinateur car cet état est sujet à modification à tout moment en fonction des besoins du cluster. Nous mentionnons ce concept uniquement parce que vous remarquerez peut-être de légères différences entre les informations de configuration affichées sur les pages Web d'administration pour un point d'accès coordinateur par rapport à d'autres membres du cluster.

6.3.5 Quels paramètres sont/ne sont pas partagés dans le cadre de la configuration du cluster ?

La plupart des paramètres de configuration définis via les pages Web d'administration de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway sera propagée aux membres du cluster dans le cadre de la *configuration du cluster*.

6.3.5.1 Paramètres partagés dans la configuration du cluster

La configuration du cluster comprend :

- Nom de réseau (SSID).
- Mot de passe de l'administrateur.
- Comptes d'utilisateur et authentification.
- Paramètres de l'interface sans fil.
- Paramètres de l'écran d'accueil invité.
- Paramètres Network Time Protocol (NTP).

- Paramètres radio.
Les paramètres Only Mode (Mode unique), Channel (Canal), Fragmentation Threshold (Seuil de fragmentation), RTS Threshold (Seuil RTS) et Rate Sets (Ensembles de débits) sont synchronisés sur le cluster. Beacon Interval (Intervalle de balise), DTIM Period (Période DTIM), Maximum Stations (Nbre maximal de stations) et Transmit Power (Puissance de transmission) ne sont pas mis en cluster.



Remarque : Lorsque le paramètre Channel Planning (Planification de canal) est activé, le canal radio n'est pas synchronisé sur le cluster. Reportez-vous à la section « Arrêt/démarrage de l'affectation automatique des canaux » à la page 82.

- Paramètres de sécurité.
- Paramètres de files d'attente *QoS*.
- Filtrage d'adresses MAC.

6.3.5.2 Paramètres non partagés par le cluster

Les quelques exceptions (de paramètres *non* partagés par les points d'accès en cluster) sont les suivantes, la plupart d'entre eux devant, par nature, être unique :

- Adresses IP.
- Adresses MAC.
- Descriptions d'emplacement.
- Paramètres d'équilibrage de la charge.
- Ponts WDS.
- Paramètres Ethernet (filaire).
- Configuration de l'interface invité.

Les paramètres qui ne sont pas partagés doivent être configurés individuellement sur les pages d'administration pour chaque point d'accès. Pour trouver les pages d'administration pour un point d'accès qui est membre du cluster en cours, cliquez sur son lien d'adresse IP dans la page *Cluster > Access Points* (Cluster > Points d'accès) du point d'accès en cours.

6.3.6 Formation du cluster

Un cluster est formé lorsque le premier point d'accès est déployé avec la mise en cluster activée. Le point d'accès tente d'atteindre un « point de rendez-vous » avec un cluster existant. S'il ne parvient pas à localiser d'autres points d'accès ayant le même nom de cluster sur le sous-réseau, il établit un nouveau cluster.

6.3.7 Taille de cluster et appartenance

Il n'existe actuellement pas de limite au nombre de points d'accès dans un cluster. Des tests de validation ont vérifié au moins une douzaine de points d'accès pris en charge sur le même sous-réseau. Vous pouvez inclure autant de points d'accès que nécessaire dans un cluster à tout moment.

L'appartenance au cluster est déterminée par les éléments suivants :

- Nom du cluster : les points d'accès avec le même nom se connecteront au même cluster (reportez-vous à la section « Définition du nom du cluster » à la page 63).
- Si la mise en cluster est activée : seuls les points d'accès pour lesquels la mise en cluster est activée pourront rejoindre un cluster (reportez-vous aux sections « Démarrage de la mise en cluster » à la page 63 et « Arrêt de la mise en cluster » à la page 64).

6.3.8 Sécurité Intra-Cluster

À des fins de simplicité d'utilisation, le composant de mise en cluster est conçu pour permettre à de nouveaux appareils de rejoindre un cluster sans authentification forte. Toutefois, les communications de toutes les données entre les points d'accès dans un cluster sont protégées contre l'écoute occasionnelle en utilisant SSL (Secure Sockets Layer). L'hypothèse est que le réseau filaire privé auquel les appareils sont connectés est sécurisé. Le fichier de configuration du cluster et la base de données utilisateur sont transmises entre les points d'accès via SSL.

6.4 Présentation des paramètres de point d'accès

L'onglet Access Points (Points d'accès) fournit des informations sur tous les points d'accès dans le cluster. Depuis cet onglet, vous pouvez afficher les descriptions d'emplacement, les adresses MAC, les adresses IP, activer ou désactiver les points d'accès *en cluster* et supprimer des points d'accès du cluster. Vous pouvez également modifier la description d'emplacement pour un point d'accès. Les liens d'adresse IP fournissent un moyen d'accéder aux paramètres de configuration et aux données sur un point d'accès.

Les points d'accès autonomes (qui ne sont pas membres du cluster) ne sont pas indiqués sur cette page.

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Manage access points in the cluster

Access Points...

Status: Clustering is online...

Location	MAC Address	IP Address
Vicky's Office - top shelf	00:0C:41:16:A3:12	10.10.100.238
Vicky's Office - lower shelf	00:00:04:7F:00:00	10.10.100.245

Stop Clustering

Clustering Options...

Enter the location of this AP.

Location:

Enter the name of the cluster for this AP to join.

Cluster Name:

Update

Le Tableau 6.1 décrit en détails les paramètres du point d'accès et l'écran d'informations.

Tableau 6.1 Paramètres de point d'accès

Champ	Description
Location (Emplacement)	Description de l'endroit où le point d'accès se trouve physiquement.
MACAddress (Adresse MAC)	<p>Adresse Media Access Control (<i>MAC</i>) du point d'accès.</p> <p>Une adresse MAC est une adresse matérielle unique et permanente pour tout appareil qui représente une interface pour le réseau. L'adresse MAC est attribuée par le fabricant. Vous ne pouvez pas modifier l'adresse MAC. Elle est fournie ici à titre d'information comme identifiant unique pour le point d'accès.</p> <p>L'adresse affichée ici est l'adresse MAC du pont (<i>br0</i>). C'est l'adresse par laquelle le point d'accès est connu en externe par d'autres réseaux.</p> <p>Pour voir les adresses MAC des interfaces interne et invité du point d'accès, reportez-vous à l'onglet <i>Status > Interfaces</i> (État > interfaces).</p>
IP Address (Adresse IP)	<p>Spécifie l'adresse IP du point d'accès. Chaque adresse IP est un lien vers les pages Web d'administration pour ce point d'accès. Vous pouvez utiliser ces liens pour accéder aux pages Web d'administration pour un point d'accès spécifique. Cette fonction est utile pour visualiser ces données sur un point d'accès spécifique et vous assurer qu'un membre de cluster reçoit les modifications de configuration du cluster, configurer les paramètres avancés sur un point d'accès particulier ou faire passer un point d'accès autonome en mode cluster.</p>

6.4.1 Modification de la description d'emplacement

Pour apporter des modifications à la description d'emplacement :

1. Accédez à l'onglet *Cluster > Access Points* (Cluster > Points d'accès).
2. Dans la section *Clustering Options* (Options de mise en cluster), saisissez le nouvel emplacement du point d'accès dans le champ *Location* (Emplacement).
3. Cliquez sur le bouton **Update** (Mettre à jour) pour appliquer les modifications.

6.4.2 Définition du nom du cluster

Pour définir le nom du cluster que vous souhaitez que votre point d'accès rejoigne, procédez comme suit :

1. Accédez à l'onglet *Cluster > Access Points* (Cluster > Points d'accès).
2. Dans la section *Clustering Options* (Options de mise en cluster), saisissez le nouveau nom de cluster dans le champ *Cluster Name* (Nom du cluster).
3. Cliquez sur le bouton **Update** (Mettre à jour) pour appliquer les modifications.



Remarque : Si vous souhaitez que plusieurs points d'accès rejoignent un cluster particulier, tous ces points d'accès doivent avoir le même nom de cluster spécifié dans le champ Cluster Name (Nom de cluster). Si le nom de cluster est différent, le point d'accès ne pourra pas rejoindre le cluster.

6.5 Démarrage de la mise en cluster

Pour démarrer la mise en cluster et ajouter un point d'accès particulier à un cluster, procédez comme suit.

1. Accédez aux pages Web d'administration pour le point d'accès autonome. (Reportez-vous à la section « Accès à un point d'accès en utilisant son adresse IP dans une URL » à la page 65.)

Les pages Web d'administration pour le point d'accès autonome sont affichées.

2. Cliquez sur l'onglet **Cluster > Access Points** (Cluster > Points d'accès) pour le point d'accès autonome.
3. Cliquez sur le bouton **Start Clustering** (Démarrer la mise en cluster).
Le point d'accès est maintenant un membre du cluster. Il apparaît dans la liste des points d'accès en cluster dans l'onglet *Cluster > Access Points* (Cluster > Points d'accès).



Remarque : Dans certaines situations, il est possible que le cluster devienne désynchronisé. Si après avoir ajouté un point d'accès au cluster, la liste des points d'accès ne reflète pas le point d'accès ajouté ou présente un affichage incomplet, reportez-vous aux informations de restauration du cluster dans l'Annexe C : « Dépannage ».

6.6 Arrêt de la mise en cluster

Pour arrêter la mise en cluster et supprimer un point d'accès particulier d'un cluster, procédez comme suit.

1. Accédez au pages Web d'administration pour le point d'accès que vous voulez supprimer du cluster.
2. Accédez à l'onglet **Cluster > Access Points** (Cluster > Points d'accès).
3. Cliquez sur le bouton **Stop Clustering** (Arrêt de la mise en cluster) pour supprimer le point d'accès du cluster.

La modification sera reflétée sous *Status* (État) pour ce point d'accès ; le point d'accès s'affichera maintenant comme *standalone* (autonome) (au lieu de *cluster*).



Remarque : Dans certaines situations, il est possible que le cluster devienne désynchronisé. Si après avoir supprimé un point d'accès du cluster, la liste des points d'accès indique toujours le point d'accès supprimé ou présente un affichage incomplet, actualisez votre navigateur. Si vous rencontrez encore des problèmes, reportez-vous aux informations sur de restauration du cluster dans l'Annexe C : « Dépannage ».

6.7 Informations de configuration pour un point d'accès spécifique et gestion des points d'accès autonomes

En général, la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway est conçue pour la gestion centralisée de points d'accès *en cluster*. Pour les points d'accès en cluster, tous les points d'accès du cluster reflètent la même configuration. Dans ce cas, peu importe le point d'accès auquel vous vous connectez pour l'administration.

Il y a peut-être des cas, toutefois, où vous voudrez visualiser ou gérer des informations sur un point d'accès particulier. Par exemple, vous pourriez vouloir vérifier les informations d'état telles que les associations client ou les événements pour un point d'accès. Ou encore, vous pourriez vouloir configurer et gérer les fonctionnalités sur un point d'accès qui s'exécute en mode *autonome*. Dans ces cas, vous pouvez accéder à l'interface Web d'administration pour des points d'accès individuels en cliquant sur les liens d'adresse IP dans l'onglet Access Points (Points d'accès).

Tous les points d'accès en cluster sont affichés dans la page *Cluster > Access Points* (Cluster > Points d'accès). Pour accéder à des points d'accès en cluster, vous pouvez simplement cliquer sur l'adresse IP d'un membre du cluster spécifique affiché dans la liste.

6.7.1 Accès à un point d'accès en utilisant son adresse IP dans une URL

Vous pouvez également accéder aux pages Web d'administration d'un point d'accès spécifique en saisissant l'adresse IP de ce point d'accès comme une URL directement dans la barre d'adresse d'un navigateur Web au format suivant :

`http://AdresseIPduPointdAccès`

AdresseIPduPointdAccès étant l'adresse du point d'accès particulier que vous souhaitez contrôler ou configurer. Pour les points d'accès autonomes, c'est le seul moyen d'accéder à leurs informations de configuration.

6.8 Surveillance de session

La passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway fournit des informations de surveillance de session en temps réel, y compris quels clients sont associés à un point d'accès particulier, les débits de données, les statistiques de transmission/réception, la puissance du signal et le temps d'inactivité.

6.8.1 Accès à la surveillance de session

Pour afficher les informations de surveillance de session, cliquez sur l'onglet **Cluster > Sessions**.

Figure 6.2 Informations de surveillance de session

Manage sessions associated with the cluster


Sessions...


You may sort the following table by clicking on any of the column names.


Display

User	AP Location	User MAC	Idle	Rate (Mbps)	Signal	Utilization	Rx Total	Tx Total	Error Rate	Idle
Ciara	not set	00:90:4b:93:f4:35	150	54	44	0.1 %	78944	107640	0	150
Sean	not set	00:0c:f1:3e:99:ae	190	11	44	0.4 %	4462	3147	0	190

You may restrict the number of columns displayed by selecting a field other than "all" in the choice box above. By selecting a specific field, the table will show only "User", "AP Location", "User MAC" and the selected field for each session. Click the "Go" button to apply the new selection.

Clustered 

1 Access Points 

0 User Accounts 

6.8.2 Présentation des informations de surveillance de session

La page *Sessions* affiche des informations sur les stations client associées aux points d'accès du cluster. Chaque client est identifié par nom d'utilisateur et adresse *MAC*, ainsi que le point d'accès (emplacement) auquel il est actuellement connecté.

Pour afficher une statistique spécifique de session client, sélectionnez un élément à partir de la liste déroulante Display (Affichage) et cliquez sur **Go** (OK). Vous pouvez afficher des informations des paramètres *Idle Time* (Durée d'inactivité), *Data Rate* (Débit), *Signal*, *Utilization* (Utilisation), etc., tous décrits en détail dans le Tableau 6.2 à la page 66.

Dans ce contexte, une « session » correspond à l'intervalle de temps pendant lequel un utilisateur d'appareil client (station) avec une adresse MAC unique maintient une connexion avec le réseau sans fil. La session commence lorsque le client l'ouvre sur le réseau et s'arrête lorsqu'il se déconnecte intentionnellement ou perd la connexion pour une autre raison.



Remarque : Une session n'est pas la même chose qu'une association, qui décrit une connexion client à un point d'accès particulier. Une connexion réseau client peut passer d'un point d'accès en cluster à un autre au cours de la même session. Une station client peut se déplacer entre les points d'accès et maintenir la session. Pour plus d'informations sur la surveillance des associations et le contrôle de l'intégrité de la liaison, reportez-vous à la section « Clients sans fil associés » à la page 136.

Tableau 6.2 Informations de session

Champ	Description
<i>User Name (Nom d'utilisateur)</i>	Indique le nom d'utilisateur client des clients IEEE 802.1x. <i>Remarque : Ce champ s'applique uniquement aux clients qui sont connectés aux points d'accès en utilisant le mode de sécurité IEEE 802.1x et un serveur d'authentification local. (Pour plus d'informations sur ce mode, reportez-vous à la section « IEEE 802.1x » à la page 114.) Pour les clients de points d'accès utilisant IEEE 802.1x avec un serveur RADIUS ou d'autres modes de sécurité, aucun nom d'utilisateur n'est indiqué ici.</i>
<i>AP Location (Emplacement du point d'accès)</i>	Indique l'emplacement du point d'accès. Ce paramètre est dérivé de la description d'emplacement indiquée dans l'onglet <i>Basic Settings</i> (Paramètres de base).
<i>User MAC Address (Adresse MAC de l'utilisateur)</i>	Indique l'adresse MAC de l'appareil client de l'utilisateur (station). Une adresse <i>MAC</i> est une adresse matérielle qui identifie de façon unique chaque nœud d'un réseau.
<i>Idle Time (Temps d'inactivité)</i>	Indique le laps de temps pendant lequel cette station est restée inactive. Une station est considérée « inactive » lorsqu'elle ne reçoit pas ou ne transmet pas de données.

Tableau 6.2 Informations de session (Suite)

Champ	Description
<i>Data Rate (Débit)</i>	<p>La vitesse à laquelle ce point d'accès transfère des données au client spécifié.</p> <p>Le débit de transmission des données est mesuré en <i>mégabits par seconde</i> (Mbits/s).</p> <p>Cette valeur doit tomber dans la plage de la configuration de l'ensemble de débits annoncé pour le mode <i>IEEE802.1x</i> en cours d'utilisation sur le point d'accès. Par exemple, 6 à 54 Mbits/s pour 802.11a.</p>
<i>Signal</i>	<p>Indique l'intensité du signal de la fréquence radio (RF) que le client reçoit du point d'accès.</p> <p>La mesure utilisée est une valeur <i>IEEE802.1x</i> connue sous le nom de <i>RSSI (Received Signal Strength Indication, Indicateur de niveau de signal reçu)</i>, et sera une valeur comprise entre 0 et 100.</p> <p>RSSI est déterminé par un mécanisme IEEE 802.1x mis en œuvre sur la carte d'interface réseau (<i>NIC</i>) de la station client.</p>
<i>Utilization (Utilisation)</i>	<p>Fréquence d'utilisation pour cette station.</p> <p>Par exemple, si la station est « active » (qu'elle émet et reçoit des données) 90 % du temps et inactive 10 % du temps, sa « fréquence d'utilisation » est 90 %.</p>
<i>Receive Total (Total reçu)</i>	Indique le nombre total de paquets reçus par le client pendant la session en cours.
<i>Transmit Total (Total transmis)</i>	Indique le nombre total de paquets émis par le client pendant la session en cours.
<i>Error Rate (Taux d'erreurs)</i>	Indique le pourcentage de trames temporelles perdues lors de la transmission sur ce point d'accès.

6.8.3 Affichage des informations de session pour les points d'accès

Vous pouvez afficher les informations de la session pour tous les points d'accès sur le réseau en même temps, ou définir l'écran pour afficher les informations de session pour un point d'accès spécifique choisi dans le menu déroulant en haut de l'écran.

Pour afficher des informations relatives à tous les points d'accès, sélectionnez le bouton radio **Show all access points** (Afficher tous les points d'accès) en haut de la page.

Pour afficher les informations de la session pour un point d'accès particulier, sélectionnez le bouton radio **Show only this access point** (Afficher uniquement ce point d'accès) et choisissez le nom du point d'accès dans le menu déroulant.

6.8.4 Tri des informations de session

Pour ordonner (trier) les informations affichées dans les tableaux par un indicateur particulier, cliquez sur l'étiquette de la colonne en fonction de laquelle vous souhaitez trier les informations. Par exemple, si vous souhaitez voir les rangées du tableau classées par fréquence d'utilisation, cliquez sur l'étiquette de colonne **Utilization** (Utilisation). Les entrées sont classées en fonction par fréquence d'utilisation.

6.8.5 Actualisation des informations de session

Vous pouvez forcer une mise à jour des informations affichées sur la page *Session Monitoring* (Surveillance de session) en cliquant sur le bouton **Refresh** (Actualiser).

GESTION DES COMPTES D'UTILISATEUR

7

7.1 Présentation	71
7.2 Accès à la gestion des utilisateurs	71
7.2.1 Affichage des comptes d'utilisateur	72
7.2.2 Ajout d'un utilisateur	72
7.2.3 Modification d'un compte d'utilisateur	74
7.2.4 Activation et désactivation des comptes d'utilisateur	74
7.2.5 Activation d'un compte d'utilisateur	74
7.2.6 Désactivation d'un compte d'utilisateur	75
7.2.7 Suppression d'un compte d'utilisateur	75
7.3 Sauvegarde et restauration d'une base de données utilisateur	75
7.3.1 Sauvegarde de la base de données utilisateur	75
7.3.2 Restauration d'une base de données utilisateur depuis un fichier de sauvegarde	76

7.1 Présentation

La passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway inclut des fonctionnalités de gestion des utilisateurs pour contrôler les accès client aux points d'accès.

La gestion et l'authentification des utilisateurs doivent toujours être utilisées en conjonction avec les deux modes de sécurité suivants, qui nécessitent l'utilisation d'un serveur **RADIUS** pour l'authentification et la gestion des utilisateurs.

- Mode IEEE 802.1x (reportez-vous à la section « IEEE 802.1x » à la page 114 dans le Chapitre 10 : « Configuration de la sécurité »).
- Mode WPA avec RADIUS (reportez-vous à la section « WPA Enterprise » à la page 119 dans le Chapitre 10 : « Configuration de la sécurité »).

Vous avez la possibilité d'utiliser le serveur RADIUS interne intégré à la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway ou un serveur RADIUS externe que vous fournissez. Si vous utilisez le serveur RADIUS intégré, utilisez la page Web d'administration du point d'accès pour configurer et gérer les comptes d'utilisateur. Si vous utilisez un serveur RADIUS externe, vous devez configurer et gérer les comptes d'utilisateur sur l'interface d'administration de ce serveur.

Sur la page User Management (Gestion des utilisateurs), vous pouvez créer, modifier, supprimer et afficher les *comptes d'utilisateur* client. Chaque compte d'utilisateur se compose d'un nom d'utilisateur et d'un mot de passe. L'ensemble des utilisateurs spécifiés ici représentent *les clients agréés* qui peuvent se connecter et utiliser un ou plusieurs points d'accès pour accéder aux réseaux locaux et éventuellement externes via votre réseau sans fil.



Remarque : Les utilisateurs spécifiés ici sont des clients des points d'accès qui utilisent les points d'accès comme concentrateur de connectivité, pas les administrateurs du réseau sans fil. Seuls les utilisateurs qui ont le nom d'utilisateur et le mot de passe de l'administrateur et la connaissance de l'URL d'administration peuvent se connecter en tant qu'administrateur et afficher ou modifier les paramètres de configuration.

7.2 Accès à la gestion des utilisateurs

Pour configurer ou modifier les comptes d'utilisateur, cliquez sur l'onglet **User Management** (Gestion des utilisateurs).

Figure 7.1 Gestion des comptes d'utilisateur

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

Manage user accounts

User Accounts...

0 User Accounts

To enable or disable a user, click the "Enable" or "Disable" button. Likewise, to remove a user, click the "Remove" button. Ensure that you have selected at least one user prior to any of these actions.
Note: These user accounts apply only when the security mode is set to "IEEE 802.1x" or "WPA with RADIUS" and the Built-In authentication server is chosen. See the Help panel for more information.

☐ Edit

Username

Real name

Status

Selected users:

Enable

Disable

Remove

[\[backup or restore the user database\]](#)

Add a user...

To add a user, fill in the fields below and click: "Add Account".

Username

Real name

Password

Password (again for safety)

Cancel

Add Account

7.2.1 Affichage des comptes d'utilisateur

Les comptes d'utilisateur sont affichés en haut de l'écran, sous *User Accounts...* (Comptes d'utilisateur...). Les champs Username (Nom d'utilisateur), Real Name (Vrai nom) et Status (enabled or disabled) (État (activé ou désactivé)) de l'utilisateur sont affichés. Vous apportez des modifications à un compte d'utilisateur existant en sélectionnant d'abord la case en regard d'un nom d'utilisateur, puis en choisissant une action. (Reportez-vous à la section « Modification d'un compte d'utilisateur » à la page 74.)

7.2.2 Ajout d'un utilisateur

Pour créer un nouvel utilisateur, procédez comme suit :

1. Sous *Add a User..* (Ajouter un utilisateur...), fournissez des informations dans les champs suivants.

72 Manuel d'utilisation de la passerelle sans fil 9160 G2 Wireless Gateway Psion Teklogix

Tableau 7.1 Champs de nouvel utilisateur

Champ	Description
<i>Username</i> (Nom d'utilisateur)	Fournissez un nom d'utilisateur. Les noms d'utilisateur sont des chaînes alphanumériques d'un maximum de 237 caractères. N'utilisez pas de caractères spéciaux ni d'espaces.
<i>Real name</i> (Vrai nom)	À des fins d'information, indiquez le nom complet de l'utilisateur. Il y a une limite de 256 caractères pour les vrais noms.
<i>Password</i> (Mot de passe)	Indiquez un mot de passe pour cet utilisateur. Les mots de passe sont des chaînes alphanumériques d'un maximum de 256 caractères. N'utilisez pas de caractères spéciaux ni d'espaces.

2. Lorsque vous avez rempli les champs, cliquez sur **Add Account** (Ajouter un compte) pour ajouter le compte.

Le nouvel utilisateur s'affiche alors dans *User Accounts...* (Comptes utilisateur...).

Le compte d'utilisateur est **activé** par défaut lorsque vous le créez.



Remarque : Une limite de 100 comptes d'utilisateur par point d'accès est imposée par l'interface utilisateur d'administration. L'utilisation du réseau peut imposer une limite plus pratique, en fonction de la demande pour chaque utilisateur.

7.2.3 Modification d'un compte d'utilisateur

Une fois que vous avez créé un compte d'utilisateur, il est affiché sous *User Accounts...* (Comptes utilisateur ...) en haut de la page Web d'administration *User Management* (Gestion des utilisateurs). Pour apporter des modifications à un compte d'utilisateur existant, cliquez tout d'abord sur la case en regard du nom d'utilisateur pour la cocher.

User Accounts...

To enable or disable a user, click the "Enable" or "Disable" button. Likewise, to remove a user, click the "Remove" button. Ensure that you have selected at least one user prior to any of these actions. **Note:** These user accounts apply only when the security mode is set to "IEEE 802.1x" or "WPA with RADIUS" and the Built-In authentication server is chosen. See the Help panel for more information.

<input type="checkbox"/>	Edit	Username	Real name	Status
<input type="checkbox"/>	[Edit]	Engineer	Mary SMith	enabled
<input type="checkbox"/>	[Edit]	Manager	Tom Jones	enabled
<input type="checkbox"/>	[Edit]	Tester	Joe Bloggs	enabled

Selected users:

[\[backup or restore the user database\]](#)

Ensuite, choisissez une action comme **modifier**, **activer**, **désactiver** ou **supprimer**.

7.2.4 Activation et désactivation des comptes d'utilisateur

Un compte d'utilisateur doit être activé pour que l'utilisateur puisse se connecter comme client et utiliser le point d'accès.

Vous pouvez **activer** ou **désactiver** un compte d'utilisateur. Grâce à cette fonctionnalité, vous pouvez gérer un ensemble de comptes d'utilisateur et autoriser ou empêcher des utilisateurs d'accéder au réseau sans avoir à supprimer ou recréer de comptes. Cela peut être très utile dans les cas où les utilisateurs ont un besoin occasionnel d'accès au réseau. Par exemple, les entrepreneurs qui travaillent pour votre société régulièrement, mais de façon intermittente, pourraient avoir besoin d'un accès au réseau pendant 3 mois, puis se déconnecter pendant 3 mois, et revenir pour une autre mission. Vous pouvez activer et désactiver ces comptes d'utilisateur en fonction des besoins, et contrôler l'accès selon les besoins.

7.2.5 Activation d'un compte d'utilisateur

Pour activer un compte d'utilisateur, cliquez sur la case à cocher en regard du nom d'utilisateur et cliquez sur **Enable** (Activer). Un utilisateur avec un compte *activé* peut se connecter aux points d'accès sans fil de votre réseau comme un client.

7.2.6 Désactivation d'un compte d'utilisateur

Pour désactiver un compte d'utilisateur, cliquez sur la case à cocher en regard du nom d'utilisateur et cliquez sur **Disable** (Désactiver).

Un utilisateur avec un compte *désactivé* ne peut pas se connecter aux points d'accès sans fil de votre réseau comme un client. Cependant, l'utilisateur reste dans la base de données et peut être activé ultérieurement si nécessaire.

7.2.7 Suppression d'un compte d'utilisateur

Pour supprimer un compte d'utilisateur, cliquez sur la case à cocher en regard du nom d'utilisateur et cliquez sur **Remove** (Supprimer).

Si vous pensez que vous souhaitez ajouter à nouveau cet utilisateur à une date ultérieure, vous pourriez envisager de *désactiver* l'utilisateur plutôt que supprimer le compte.

7.3 Sauvegarde et restauration d'une base de données utilisateur

Vous pouvez enregistrer une copie de l'ensemble de comptes d'utilisateur actuel dans un fichier de configuration de sauvegarde. Le fichier de sauvegarde peut être utilisé à une date ultérieure pour restaurer les comptes d'utilisateur sur le point d'accès à la configuration précédemment enregistrée.

7.3.1 Sauvegarde de la base de données utilisateur

Pour créer une copie de sauvegarde des comptes d'utilisateur pour ce point d'accès :

1. Cliquez sur le lien **[sauvegarder ou restaurer la base de données utilisateur]**.

Une boîte de dialogue *File Download or Open* (Télécharger ou ouvrir le fichier) s'affiche.

2. Choisissez l'option **Save** (Enregistrer) dans cette première boîte de dialogue.

Un navigateur de fichiers s'affiche.

Utilisez le navigateur de fichiers pour accéder au répertoire dans lequel vous souhaitez enregistrer le fichier et cliquez sur **OK** pour enregistrer le fichier.

Vous pouvez conserver le nom de fichier par défaut (wirelessUsers.ubk) ou renommer le fichier de sauvegarde, mais assurez-vous d'enregistrer le fichier avec une extension .ubk.

7.3.2 Restauration d'une base de données utilisateur depuis un fichier de sauvegarde

Pour restaurer une base de données utilisateur depuis un fichier de sauvegarde :

1. Sélectionnez le fichier de configuration de sauvegarde que vous souhaitez utiliser, en tapant le chemin d'accès complet et le nom du fichier dans le champ Restore (Restaurer) ou en cliquant sur **Browse** (Parcourir) et en sélectionnant le fichier.

(Seuls les fichiers qui ont été créés avec la fonctionnalité de sauvegarde de base de données utilisateur et enregistrés comme fichiers de configuration de sauvegarde .ubk sont valides pour être utilisés avec la fonction de restauration ; par exemple, wirelessUsers.ubk.)

2. Cliquez sur le bouton **Restore** (Restaurer).

Lorsque le processus de restauration de la sauvegarde est terminé, un message s'affiche pour indiquer que la base de données utilisateur a été restaurée avec succès. (Ce processus ne prend pas beaucoup de temps ; la restauration devrait se terminer presque immédiatement.)

Cliquez sur l'onglet **User Management** (Gestion des utilisateurs) pour afficher les comptes d'utilisateur restaurés.

8.1 Accès à la gestion des canaux	79
8.2 Présentation de la gestion des canaux	79
8.2.1 Fonctionnement en quelques mots	79
8.2.2 Pour les curieux : plus de détails sur les canaux avec chevauchement	80
8.2.3 Exemple : un réseau avant et après la gestion des canaux	80
8.3 Configuration et affichage des paramètres de gestion des canaux	81
8.3.1 Arrêt/démarrage de l'affectation automatique des canaux	82
8.3.2 Affichage des affectations de canaux actuelles et définition de verrouillages	82
8.3.3 Affichage du dernier ensemble de modifications proposé	83
8.3.4 Configuration des paramètres avancés (Personnalisation/programmation de plans de canaux)	84

8.1 Accès à la gestion des canaux

Pour afficher les informations de surveillance de session, cliquez sur l'onglet **Cluster > Channel Management** (Cluster > Gestion des canaux).

Figure 8.1 Gestion des affectations de canal

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

Automatically manage channel assignments

Channels ...

Start

 automatically re-assigning channels

Current Channel Assignments

IP Address	Radio	Band	Channel	Locked
10.10.100.238	00:0C:41:16:A3:12	G	2	<input type="checkbox"/>
10.10.100.245	00:00:04:7F:00:00	G	3	<input type="checkbox"/>

Apply

Proposed Channel Assignments (3 hours, 40 minutes and 52 seconds old)

IP Address	Radio	Proposed Channel
10.10.100.238	00:0C:41:16:A3:12	2

Advanced

Change channels if interference is reduced by at least 5%

Determine if there is better set of channel settings every 1 Minute

Update

Clustered

2 Access Points

3 User Accounts

8.2 Présentation de la gestion des canaux

Lorsque *Channel Management* (Gestion des canaux) est activé, la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway affecte automatiquement les canaux radio utilisés par les points d'accès en cluster pour réduire les interférences mutuelles (ou les interférences avec d'autres points d'accès en dehors de son cluster). Cela permet d'optimiser la bande passante Wi-Fi et de préserver l'efficacité des communications sur votre réseau sans fil. (Vous devez démarrer la gestion des canaux pour obtenir l'affectation automatique des canaux ; elle est désactivée par défaut sur un nouveau point d'accès. Reportez-vous à la section « Arrêt/démarrage de l'affectation automatique des canaux » à la page 82.)

8.2.1 Fonctionnement en quelques mots

À un intervalle spécifié (la valeur par défaut est **1 heure**) ou à la demande (clic sur **Update** (Mettre à jour)), le gestionnaire de canaux configure des points d'accès à utiliser sur les canaux et mesure les interférences des niveaux dans le cluster. Si des interférences importantes entre les canaux sont détectées, le gestionnaire de canaux réattribue automatiquement certains ou tous les points d'accès à de nouveaux canaux par un algorithme d'efficacité (ou *plan de canal automatique*).

8.2.2 Pour les curieux : plus de détails sur les canaux avec chevauchement

Le **Channel - Canal** de diffusion de fréquence radio (RF) définit la partie du spectre que la radio du point d'accès utilise pour émettre et recevoir. La plage de canaux disponibles pour un point d'accès est déterminée par le mode **IEEE802.11** (également appelé bande) du point d'accès.

Les modes IEEE **802.11b/802.11g** (802.11 b/g) prennent en charge l'utilisation des canaux 1 à 11 inclus, alors que le mode IEEE **802.11a** prend en charge une quantité de canaux non consécutifs plus importante (36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165).

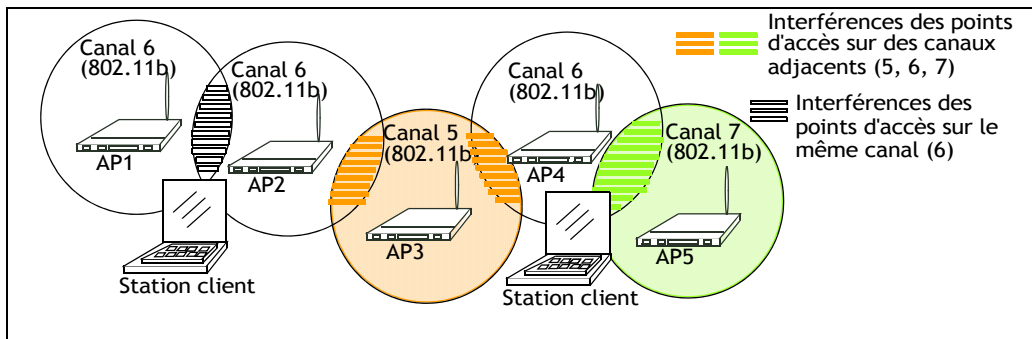
Des interférences peuvent se produire lorsque plusieurs points d'accès à portée les uns des autres émettent sur le même canal ou sur des canaux qui se *chevauchent*. L'impact de ces interférences sur les performances du réseau peut s'intensifier pendant les heures de pointe lorsqu'une grande quantité de trafic données et multimédia partagent la bande passante.

Le gestionnaire de canaux détecte les bandes (b/g ou a) sur lesquelles les points d'accès en cluster se trouvent, et utilise un ensemble de canaux prédéfinis qui n'interféreront pas les uns avec les autres. Pour la bande radio « b/g », l'ensemble classique de canaux non parasites est 1, 6, 11. Les canaux 1, 4, 8, 11 produisent un chevauchement minimum. Un ensemble similaire de canaux non parasites est utilisé pour la bande radio « a », qui comprend tous les canaux pour ce mode car ils ne se chevauchent pas.

8.2.3 Exemple : un réseau avant et après la gestion des canaux

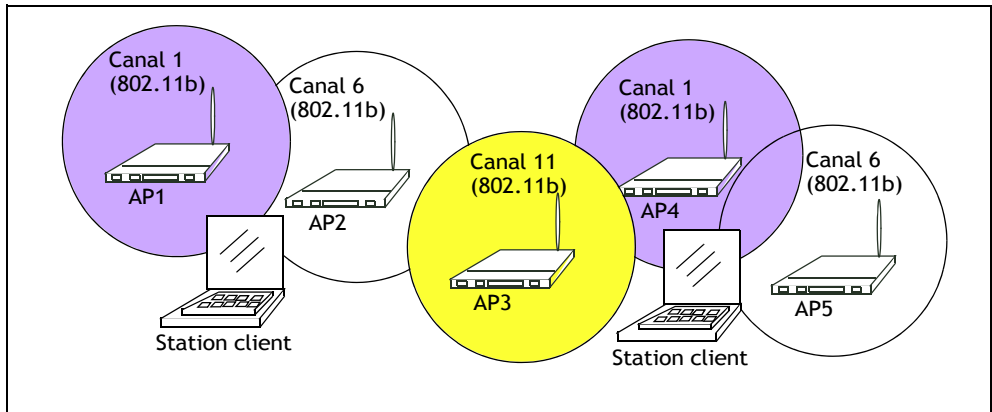
Sans gestion automatisée des canaux en cluster, les affectations de canaux aux points d'accès en cluster peuvent être effectuées sur des *canaux consécutifs*, qui risquent de se chevaucher et de provoquer des interférences. Par exemple, AP1 peut être attribué au canal 6, AP2 au canal 6, et AP3 au canal 5 comme illustré dans la Figure 8.2.

Figure 8.2 Sans gestion automatique des canaux



Avec la gestion automatisée des canaux, les points d'accès du cluster sont automatiquement affectés à des canaux non parasites comme indiqué dans 8.3.

Figure 8.3 Avec la gestion des canaux activée



8.3 Configuration et affichage des paramètres de gestion des canaux

La page Channel Management (Gestion des canaux) affiche les affectations précédentes, courantes et prévues pour les points d'accès en cluster. Par défaut, l'affectation automatique des canaux est désactivée. Vous pouvez démarrer la gestion des canaux pour optimiser l'utilisation des canaux sur le cluster selon un intervalle planifié.

Dans cette page, vous pouvez afficher les affectations de canaux pour tous les points d'accès du cluster, arrêter/démarrer la gestion automatique des canaux et « mettre à jour » manuellement la carte de canaux actuelle (points d'accès à canaux). Pendant une mise à jour manuelle, le gestionnaire de canaux évalue l'utilisation des canaux et, si nécessaire, réaffecte les points d'accès à de nouveaux canaux pour réduire les interférences en fonction des paramètres avancés actuels.

En utilisant les paramètres avancés, vous pouvez modifier le potentiel de réduction des interférences qui déclenchent la réaffectation des canaux, modifier la planification des mises à jour automatiques et reconfigurer l'ensemble des canaux utilisés pour les affectations.

Les sections suivantes décrivent comment configurer et utiliser la gestion des canaux sur votre réseau :

- « Arrêt/démarrage de l'affectation automatique des canaux » à la page 82.

- « Affichage des affectations de canaux actuelles et définition de verrouillages » à la page 82.
- « Mettre à jour les paramètres actuels de canal (manuel) » à la page 83.
- « Affichage du dernier ensemble de modifications proposé » à la page 83.
- « Configuration des paramètres avancés (Personnalisation/programmation de plans de canaux) » à la page 84.
- « Mise à jour des paramètres avancés » à la page 86.

8.3.1 Arrêt/démarrage de l'affectation automatique des canaux

Par défaut, l'affectation automatique des canaux est désactivée (off).

- Cliquez sur **Start** (Démarrer) pour reprendre l'affectation automatique des canaux. Lorsque l'affectation automatique des canaux est activée, le gestionnaire de canaux configure régulièrement les canaux radio utilisés par les points d'accès en cluster et, si nécessaire, réaffecte des canaux aux points d'accès en cluster afin de réduire les interférences (avec des membres du cluster ou d'autres points d'accès en dehors du cluster).



Remarque : La gestion des canaux est prioritaire sur le fonctionnement par défaut du cluster, qui est de synchroniser les canaux radio de tous les points d'accès sur un cluster. Lorsque la gestion des canaux est activée, le canal radio n'est pas synchronisé sur le cluster à d'autres points d'accès. Reportez-vous à la remarque sous Paramètres radio dans la section « Paramètres partagés dans la configuration du cluster » à la page 59.

- Cliquez sur **Stop** (Arrêter) pour arrêter l'affectation automatique des canaux. (Aucune configuration d'utilisation des canaux ou affectation de canal ne sera effectuée. Seules les mises à jour manuelles affectent l'affectation de canaux.)

8.3.2 Affichage des affectations de canaux actuelles et définition de verrouillages

Current Channel Settings (Paramètres actuels de canal) affiche une liste de tous les points d'accès dans le cluster par adresse IP. L'écran indique la bande sur laquelle chaque point d'accès diffuse, le canal actuel utilisé par chaque point d'accès et une option de « verrouillage » d'un point d'accès sur son canal radio actuel afin qu'il ne puisse pas être réaffecté à un autre. Des détails sur les paramètres actuels de canal sont fournis ci-dessous.

Tableau 8.1 Paramètres actuels de canal

Champ	Description
<i>IP Address</i> (Adresse IP)	Indique l' <i>IP Address</i> - Adresse IP du point d'accès.
<i>Radio</i>	Indique l'adresse <i>MAC</i> du point d'accès.
<i>Band (Bande)</i>	Indique la bande (b/g ou a) sur laquelle le point d'accès diffuse.
<i>Channel</i> (Canal)	Indique le <i>Channel</i> - Canal radio sur lequel ce point d'accès est actuellement diffusé.
<i>Locked</i> (Verrouillé)	<p>Cliquez sur Locked (Verrouillé) si vous souhaitez que ce point d'accès reste sur le canal actuel.</p> <p>Lorsque la case « Locked » (Verrouillé) est cochée (activée) pour un point d'accès, les plans de gestion automatisée des canaux ne réaffectent pas le point d'accès à un canal différent dans le cadre de la stratégie d'optimisation. Au lieu de cela, les points d'accès avec des canaux verrouillés sont pris en compte dans les conditions requises pour le plan.</p> <p>Si vous cliquez sur Update (Mettre à jour), vous verrez que les points d'accès verrouillés indiquent le même canal pour « Current Channel » (Canal actuel) et « Proposed Channel » (Canal proposé). Les points d'accès verrouillés conservent leurs canaux actuels.</p>

8.3.2.1 Mettre à jour les paramètres actuels de canal (manuel)

Vous pouvez exécuter une mise à jour manuelle de la gestion des canaux à tout moment en cliquant sur **Update** (Mettre à jour) dans l'écran *Current Channel Settings* (Paramètres actuels de canal).

8.3.3 Affichage du dernier ensemble de modifications proposé

Last Proposed Set of Channel Changes (Dernier ensemble de modifications de canaux proposé) indique le dernier plan de canaux. Le plan contient tous les points d'accès dans le cluster par adresse IP et montre les canaux actuels et proposés pour chaque point d'accès. Les canaux verrouillés ne peuvent pas être réaffectés et l'optimisation d'affectation des canaux entre points d'accès prend en compte le fait que les points d'accès verrouillés doivent rester sur leurs canaux actuels. Les points d'accès qui ne sont pas « verrouillés » peuvent être affectés à des canaux différents de ceux qu'ils utilisaient précédemment, selon les résultats du plan.

Tableau 8.2 Plan de canaux des points d'accès

Champ	Description
<i>IP Address</i> (Adresse IP)	Indique l' <i>IP Address</i> - <i>Adresse IP</i> du point d'accès.
<i>Current</i> (Actuel)	Indique le canal radio sur lequel ce point d'accès est actuellement diffusé.
<i>Proposed</i> (Proposé)	Indique le canal radio auquel ce point d'accès serait réaffecté si le plan de canaux est exécuté.

8.3.4 Configuration des paramètres avancés (Personnalisation/programmation de plans de canaux)

Si vous utilisez *Channel Management* (Gestion des canaux) telle que fournie (sans mettre à jour les *Advanced Settings* (Paramètres avancés)), les canaux sont automatiquement réglés une fois toutes les heures si les interférences peuvent être réduites de 25 % ou plus. Les canaux seront réaffectés même si le réseau est occupé. Les paramètres du canal approprié seront utilisés (« b/g » pour les points d'accès utilisant IEEE 802.11b/g et « a » pour les points d'accès utilisant IEEE 802.11a).

Ces paramètres par défaut sont conçus pour satisfaire la plupart des scénarios dans lesquels vous devez mettre en œuvre la gestion des canaux.

Grâce aux *Advanced Settings* (Paramètres avancés), vous pouvez modifier le potentiel de réduction des interférences qui déclenchent la réaffectation des canaux, modifier la planification des mises à jour automatiques et reconfigurer l'ensemble des canaux utilisés pour les affectations.

Tableau 8.3 Paramètres avancés

Champ	Description
<i>Advanced</i> (Avancé)	Cliquez sur le bouton « Advanced » (Avancé) pour afficher/masquer les paramètres d'affichage qui modifient la temporisation et les détails de l'algorithme de planification des canaux. Par défaut, ces paramètres sont masqués .

Tableau 8.3 Paramètres avancés (Suite)

Champ	Description
<i>Change channels if interference is reduced by at least__ (Changer de canal si les interférences sont réduites d'au moins__)</i>	<p>Indiquez le pourcentage minimal de réduction des interférences qu'un plan proposé doit atteindre pour être appliqué. La valeur par défaut est 25 %.</p> <p>Utilisez le menu déroulant pour choisir des pourcentages allant de 25 % à 75 %.</p> <p>Ce paramètre vous permet de définir un facteur de blocage pour la réaffectation des canaux afin que le réseau ne soit pas constamment interrompu pour un minimum de gains d'efficacité.</p> <p>Par exemple, si les interférences entre canaux doivent être réduites de 75 %, et que les affectations de canal proposées ne réduisent les interférences que de 30 %, les canaux ne seront pas réaffectés. Cependant, si vous réinitialisez l'avantage minimal d'interférences entre canaux à 25 % et que vous cliquez sur Update (Mettre à jour), le plan de canaux proposé sera mis en place et les canaux seront réaffectés en fonction de vos besoins.</p>
<i>Determine if there is better set of channel settings every__ (Déterminer s'il y a un meilleur ensemble de paramètres de canaux chaque__)</i>	<p>Utilisez le menu déroulant pour spécifier le programme des mises à jour automatiques.</p> <p>Une plage d'intervalles est proposée, allant de « 1 minute » à « 6 mois ». La valeur par défaut est « 1 Hour » (1 heure) (l'utilisation des canaux est réévaluée et le plan de canaux obtenu est appliqué toutes les heures).</p>
<i>Use these channels when applying channel assignments (Utiliser ces canaux lors de l'application d'affectations de canal)</i>	<p>Choisissez un ensemble de canaux non parasites sur une bande spécifique (« b/g » ou « a »). Les choix possibles sont les suivants :</p> <ul style="list-style-type: none"> • Canaux b/g 1-6-11 • Canaux b/g 1-4-8-11 • a <p>Les modes IEEE 802.11b/802.11g (802.11 b/g) prennent en charge l'utilisation des canaux 1 à 11. Pour la bande radio « b/g », l'ensemble classique de canaux non parasites est 1, 6, 11. Les canaux 1, 4, 8, 11 produisent un chevauchement minimum.</p> <p>Le mode IEEE 802.11a prend en charge une quantité de canaux non consécutifs plus importante (36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165). Tous les canaux à bande « a » sont non parasites.</p>
<i>Apply channel modifications even when the network is busy (Appliquer les modifications de canal, même lorsque le réseau est chargé)</i>	<p>Cliquez pour activer ou désactiver ce paramètre.</p> <p>Une coche indique que celui-ci est activé et que les modifications de canal seront appliquées, même lorsque le réseau est chargé. Si ce paramètre n'est pas coché, les modifications de canal ne seront pas appliquées sur un réseau chargé.</p> <p>Ce paramètre (avec le paramètre de réduction des interférences) est conçu pour vous aider à comparer l'impact coût/avantage de la réaffectation des canaux sur les performances du réseau avec les perturbations inhérentes qu'elle peut entraîner sur les clients pendant une heure de pointe.</p>

8.3.4.1 Mise à jour des paramètres avancés

Cliquez sur **Update** (Mettre à jour) dans *Advanced Settings* (Paramètres avancés) pour appliquer ces paramètres.

Les paramètres avancés sont pris en compte lorsqu'ils sont appliqués, et ils influent sur la façon dont la gestion automatique des canaux est exécutée. (Les nouveaux paramètres de réduction minimale des interférences, de réglage d'intervalle programmé, de définition de canal et de réseau chargé seront pris en compte pour les mises à jour automatiques et manuelles.)

VOISINAGE SANS FIL

9

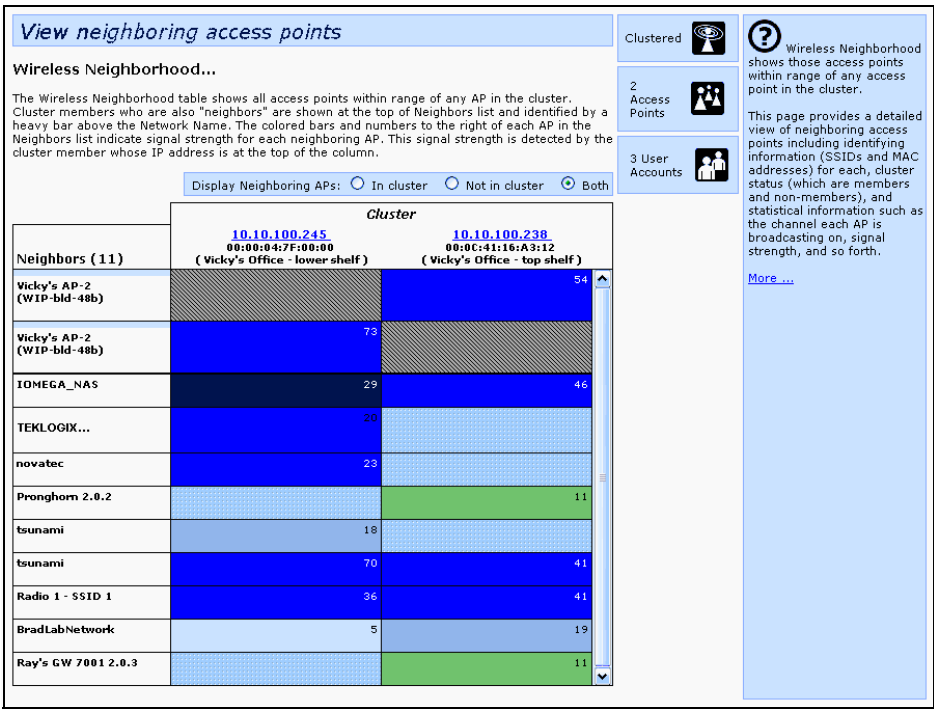
9.1 Accès au voisinage sans fil	89
9.2 Présentation des informations du voisinage sans fil	89
9.3 Affichage du voisinage sans fil.	90
9.4 Affichage des détails d'un membre du cluster	92

L'écran *Wireless Neighborhood* (Voisinage sans fil) affiche les points d'accès à portée de n'importe quel point d'accès du cluster. Cette page fournit une vue détaillée des points d'accès voisins, y compris les informations d'identification (SSID et adresses MAC) pour chacun d'eux, l'état de cluster (membres et non-membres) et des informations de statistiques telles que le canal de diffusion de chaque point d'accès, la puissance du signal, etc.

9.1 Accès au voisinage sans fil

Pour afficher le *voisinage sans fil*, cliquez sur l'onglet **Cluster > Wireless Neighborhood** (Cluster > Voisinage sans fil).

Figure 9.1 Points d'accès voisins dans le cluster et hors du cluster



9.2 Présentation des informations du voisinage sans fil

L'écran *Wireless Neighborhood* (Voisinage sans fil) affiche tous les points d'accès à portée de tous les membres du cluster, indique quels points d'accès sont à portée de quels membres du cluster, et fait la distinction entre les membres et les non-membres du cluster.

Pour chaque point d'accès voisin, l'écran Wireless Neighborhood (Voisinage sans fil) affiche les informations d'identification (*SSID* ou nom de réseau, *IP Address - Adresse IP*, adresse *MAC*), ainsi que les statistiques radio (puissance du signal, canal, intervalle de balise). Vous pouvez cliquer sur un point d'accès pour obtenir des statistiques supplémentaires sur les points d'accès à portée radio du point d'accès sélectionné.

L'écran Wireless Neighborhood (Voisinage sans fil) peut vous aider à :

- Détecter et localiser des points d'accès imprévus (ou *indésirables*) dans un domaine sans fil de façon à ce que vous puissiez agir pour limiter les risques associés.
- Vérifier les attentes de couverture. En évaluant quels points d'accès sont visibles par d'autres points d'accès et à quelle puissance du signal, vous pouvez vérifier que le déploiement répond à vos objectifs de planification.
- Détecter des défaillances. Les changements inattendus dans le modèle de couverture sont évidents en un coup d'œil dans le tableau à code de couleur.

9.3 Affichage du voisinage sans fil

Les détails sur les informations du voisinage sans fil affichés sont décrits ci-dessous.

Tableau 9.1 Statistiques de voisinage sans fil

Champ	Description
<i>Display Neighboring APs (Afficher les points d'accès voisins)</i>	<p>Cliquez sur l'un des boutons radio suivants pour modifier l'affichage :</p> <ul style="list-style-type: none">• <i>In cluster</i> (Dans le cluster) - Affiche uniquement les points d'accès voisins qui sont membres du cluster.• <i>Not in cluster</i> (Hors du cluster) - Affiche uniquement les points d'accès voisins qui ne sont pas membres du cluster.• <i>Both</i> (Les deux) - Affiche tous les points d'accès voisins (membres et non-membres du cluster).
<i>Cluster</i>	<p>La liste « Cluster » en haut du tableau affiche les adresses IP de tous les points d'accès du cluster. (Il s'agit de la même liste des membres du cluster affichée sur l'onglet <i>Cluster > Access Points</i> (Cluster > Points d'accès) décrit dans la section « Accès à la gestion des points d'accès » à la page 57).</p> <p>S'il n'y a qu'un seul point d'accès dans le cluster, une seule colonne d'adresses IP s'affiche ici ; indiquant que le point d'accès est « en cluster avec lui-même ».</p> <p>Vous pouvez cliquer sur une adresse IP pour afficher plus de détails sur un point d'accès spécifique, comme illustré dans la Figure 9.2 à la page 92.</p>

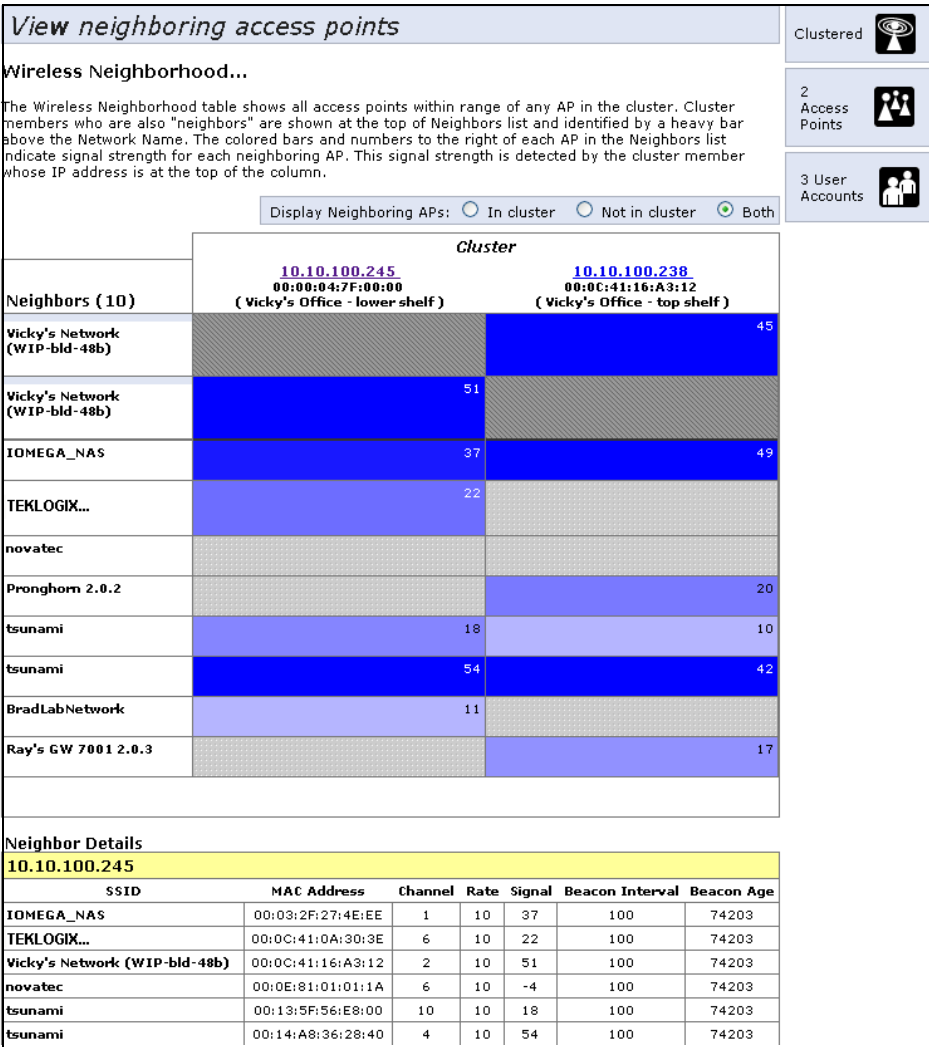
Tableau 9.1 Statistiques de voisinage sans fil

Champ	Description																																															
Neighbors (Voisins)	<p>Les points d'accès qui sont voisins d'au moins un des points en cluster sont répertoriés dans la colonne de gauche par SSID (nom de réseau). Un point d'accès qui est détecté comme voisin d'un membre de cluster peut également être membre du cluster lui-même. Les voisins qui sont également membres du cluster sont toujours affichés en haut de la liste en-dessous d'une barre épaisse et avec un indicateur d'emplacement.</p> <p>Les barres de couleur à droite de chaque point d'accès dans la liste Neighbors (Voisins) indiquent la puissance du signal pour chacun des points d'accès voisins détectés par le membre du cluster dont l'adresse IP est indiquée dans la partie supérieure de la colonne :</p> <p>Ce point d'accès (un membre du cluster) est visible par le point d'accès dont l'adresse IP est 10.10.100.246 (à une puissance du signal de 54). . .</p> <p>. . . mais pas par le point d'accès dont l'adresse est 10.10.100.223</p> <table><tr><th rowspan="2">Neighbors (88)</th><th colspan="3">Cluster</th></tr><tr><th>10.10.100.246 (not set)</th><th>10.10.100.223 (not set)</th><th>10.10.100.213 (not set)</th></tr><tr><td>TEKLOGIX... (not set)</td><td></td><td>3</td><td>48</td></tr><tr><td>TEKLOGIX... (not set)</td><td></td><td></td><td></td></tr><tr><td>TEKLOGIX... (not set)</td><td>54</td><td>0</td><td></td></tr><tr><td>TEKLOGIX... (not set)</td><td>34</td><td>5</td><td>26</td></tr><tr><td>TEKLOGIX... (not set)</td><td>22</td><td></td><td>50</td></tr><tr><td>Bread Lab 105</td><td>20</td><td>18</td><td>27</td></tr><tr><td>wi-fi-a</td><td>46</td><td></td><td>34</td></tr><tr><td>guest</td><td>4</td><td>6</td><td>48</td></tr><tr><td>int</td><td>4</td><td>5</td><td>48</td></tr><tr><td>g10_wgt624_guest</td><td>21</td><td>14</td><td>33</td></tr></table>	Neighbors (88)	Cluster			10.10.100.246 (not set)	10.10.100.223 (not set)	10.10.100.213 (not set)	TEKLOGIX... (not set)		3	48	TEKLOGIX... (not set)				TEKLOGIX... (not set)	54	0		TEKLOGIX... (not set)	34	5	26	TEKLOGIX... (not set)	22		50	Bread Lab 105	20	18	27	wi-fi-a	46		34	guest	4	6	48	int	4	5	48	g10_wgt624_guest	21	14	33
Neighbors (88)	Cluster																																															
	10.10.100.246 (not set)	10.10.100.223 (not set)	10.10.100.213 (not set)																																													
TEKLOGIX... (not set)		3	48																																													
TEKLOGIX... (not set)																																																
TEKLOGIX... (not set)	54	0																																														
TEKLOGIX... (not set)	34	5	26																																													
TEKLOGIX... (not set)	22		50																																													
Bread Lab 105	20	18	27																																													
wi-fi-a	46		34																																													
guest	4	6	48																																													
int	4	5	48																																													
g10_wgt624_guest	21	14	33																																													
	<ul style="list-style-type: none">• Barre bleu foncé - Une barre bleu foncé et une valeur de puissance du signal élevée (par exemple 50) indique la détection d'une bonne puissance du signal du voisin visible par le point d'accès dont l'adresse IP est répertoriée au-dessus de cette colonne.• Barre bleu clair - Une barre bleu clair et une valeur de puissance du signal faible (par exemple 20) indique la détection d'une puissance du signal faible ou moyenne du voisin visible par le point d'accès dont l'adresse IP est répertoriée au-dessus de cette colonne.• Barre blanche - Une barre blanche et la valeur 0 indiquent qu'un point d'accès voisin qui a été détecté par l'un des membres du cluster ne peut pas être détecté par le point d'accès dont l'adresse IP est répertoriée au-dessus de cette colonne.• Bande gris clair - Une bande gris clair et aucune valeur de puissance du signal indique un voisin qui est détecté par d'autres membres du cluster mais pas par le point d'accès dont l'adresse IP est répertoriée au-dessus de cette colonne.• Barre gris foncé - Une barre gris foncé et aucune valeur de puissance du signal indique que c'est le point d'accès dont l'adresse IP est répertoriée au-dessus de cette colonne (comme il n'est pas applicable d'afficher la capacité du point d'accès à se détecter lui-même).																																															

9.4 Affichage des détails d'un membre du cluster

Pour afficher des détails relatifs à un point d'accès membre du cluster, cliquez sur l'adresse IP d'un membre du cluster en haut de la page.

Figure 9.2 Détails d'un point d'accès membre du cluster



Le tableau ci-dessous explique les détails affichés pour le point d'accès sélectionné.

Tableau 9.2 Statistiques du point d'accès

Champ	Description
<i>SSID</i>	<p>Le <i>Service Set Identifier (SSID)</i> du point d'accès.</p> <p>Le SSID est une chaîne alphanumérique de 32 caractères maximum qui identifie de façon unique un réseau local sans fil. Il est également appelé <i>nom de réseau</i>.</p> <p>Le SSID est défini dans Basic Settings (Paramètres de base) (Chapitre 5 : « Configuration des paramètres de base ») ou dans <i>Manage > 802.11 Settings</i> (Gérer > Paramètres 802.11) (Chapitre 13 : « Définition de l'interface sans fil ».)</p> <p>Un réseau invité et un réseau interne exécutés sur le même point d'accès doivent toujours avoir deux différents noms de réseau.</p>
<i>MAC Address</i> (Adresse MAC)	<p>Affiche l'adresse <i>MAC</i> du point d'accès voisin.</p> <p>Une adresse <i>MAC</i> est une adresse matérielle qui identifie de façon unique chaque nœud d'un réseau.</p>
<i>Channel</i> (Canal)	<p>Affiche le canal sur lequel le point d'accès diffuse actuellement.</p> <p>Le <i>Channel - Canal</i> définit la partie du spectre que la radio utilise pour émettre et recevoir.</p> <p>Le canal est défini dans <i>Manage > 802.11 Advanced Settings</i> (Gérer > Paramètres avancés 802.11). (Reportez-vous au Chapitre 16 : « Configuration des paramètres radio 802.11 ».)</p>
<i>Rate (Débit)</i>	<p>Indique le débit (en mégabits par seconde) à laquelle le point d'accès émet actuellement.</p> <p>Le débit actuel sera toujours l'un des débits pris en charge dans <i>Supported Rates</i> (Débits pris en charge).</p>
<i>Signal</i>	<p>Indique la puissance du signal radio de transmission de ce point d'accès, mesurée en décibels (dB).</p>
<i>Beacon Interval</i> (Intervalle de balise)	<p>Affiche l'intervalle de <i>Beacon - Balise</i> utilisé par ce point d'accès.</p> <p>Les trames de balise sont transmises par un point d'accès à intervalles réguliers pour annoncer l'existence du réseau sans fil. Le fonctionnement par défaut consiste à envoyer une trame de balise une fois toutes les 100 millisecondes (soit 10 par seconde).</p> <p>L'intervalle de balise est défini dans <i>Manage > 802.11 Advanced Settings</i> (Gérer > Paramètres avancés 802.11). (Reportez-vous au Chapitre 16 : « Configuration des paramètres radio 802.11 ».)</p>
<i>Capability</i> (Capacité)	<p>Un nombre hexadécimal qui, une fois converti en binaire, indique chaque fonction ou fonctionnalité <i>IEEE 802.11</i> et si elle est « activée » ou « désactivée » sur ce point d'accès.</p>
<i>Beacon Age</i> (Âge de la balise)	<p>Indique la date et l'heure d'émission de la balise la plus récente depuis le point d'accès.</p>

10.1 Présentation des problèmes de sécurité sur les réseaux sans fil.	97
10.1.1 Comment puis-je savoir quel mode de sécurité utiliser ?	97
10.1.2 Comparaison des modes de sécurité pour la gestion des clés, algorithmes d'authentification et de cryptage	98
10.1.2.1 Quand utiliser le mode non crypté (aucune sécurité)	99
10.1.2.2 Quand utiliser le mode WEP statique	99
10.1.2.3 Quand utiliser le mode IEEE 802.1x	100
10.1.2.4 Quand utiliser le mode WPA Personal.	102
10.1.2.5 Quand utiliser le mode WPA Enterprise.	103
10.1.3 Interdire le SSID de diffusion améliore-t-il la sécurité ?	104
10.1.4 Comment l'isolation de station protège-t-elle le réseau ?	105
10.2 Configuration des paramètres de sécurité.	105
10.2.1 Broadcast SSID (SSID de diffusion), Station Isolation (Isolation de station) et Security Mode (Mode de sécurité).	106
10.2.2 Modes de sécurité	107
10.2.2.1 None (Plain-text) (Aucun (texte brut)).	108
10.2.2.2 Static WEP (WEP statique)	109
10.2.2.3 IEEE 802.1x	114
10.2.2.4 WPA Personal	117
10.2.2.5 WPA Enterprise	119
10.3 Mise à jour des paramètres	124

Les sections suivantes décrivent comment configurer les paramètres de sécurité sur la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway.

10.1 Présentation des problèmes de sécurité sur les réseaux sans fil

Les supports sans fil sont intrinsèquement moins sûrs que les supports filaires. Par exemple, un *NIC* Ethernet transmet ses paquets via un support physique comme un câble coaxial ou une paire torsadée. Une carte réseau (NIC) sans fil diffuse les signaux radio par liaison radio, ce qui permet de se connecter facilement à un LAN sans fil sans accès physique ou sans équipement sophistiqué. Un pirate équipé d'un ordinateur portable, d'une carte réseau sans fil et de quelques connaissances peut facilement tenter de compromettre votre réseau sans fil. Il n'est même pas utile d'être à portée normale du point d'accès. En orientant une antenne sophistiquée sur le client, un pirate a la possibilité de se connecter au réseau depuis plusieurs kilomètres.

La passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway offre un certain nombre de schémas de cryptage et d'authentification pour vous assurer que votre infrastructure sans fil soit uniquement accessible par les utilisateurs concernés. Les détails de chaque mode de sécurité sont décrits dans les sections ci-dessous.

Reportez-vous également à la rubrique associée, Annexe B : « Paramètres de sécurité sur clients sans fil/serveur RADIUS ».

10.1.1 Comment puis-je savoir quel mode de sécurité utiliser ?

En général, nous recommandons que vous utilisiez sur votre réseau interne le mode de sécurité le plus robuste possible dans votre environnement. Lors de la configuration de la sécurité sur le point d'accès, vous devez d'abord choisir le mode de sécurité, puis un algorithme d'authentification dans certains modes, et autoriser ou non l'association des clients qui n'utilisent pas le mode de sécurité spécifié.

Wi-Fi Protected Access (WPA), avec *Remote Authentication Dial-In User Service (RADIUS)* via l'algorithme de cryptage CCMP (AES), fournit la meilleure protection des données disponible. C'est clairement la meilleure option si toutes les stations client sont équipées de demandeurs WPA. Cependant, les problèmes de rétrocompatibilité et d'interopérabilité avec des clients ou même d'autres points d'accès peuvent nécessiter que vous configuriez WPA avec RADIUS via un autre algorithme de cryptage ou que vous choisissiez l'un des autres modes de sécurité.

Cependant, cela dit, la sécurité pourrait ne pas être une priorité aussi importante sur certains types de réseaux. Si vous fournissez simplement un accès imprimante et Internet, comme sur un réseau invité, définir le mode de sécurité sur *None (Plain text)* (Aucun (texte brut)) peut être le choix approprié. Pour empêcher les clients de découvrir et de se connecter de manière accidentelle à votre réseau, vous pouvez désactiver la diffusion SSID pour que votre nom de réseau ne soit pas diffusé. Si le réseau est suffisamment isolé de l'accès à des informations sensibles, cela peut offrir une protection suffisante dans certaines situations. Ce niveau de protection est le seul proposé pour les réseaux invité, et peut également être le compromis le plus pratique pour d'autres scénarios où la priorité est de rendre la connexion client la plus simple possible. (Reportez-vous à la section « Interdire le SSID de diffusion améliore-t-il la sécurité ? » à la page 104.)

Vous trouverez ci-après une brève discussion sur les facteurs qui font qu'un mode est plus sûr qu'un autre, une description de chaque mode proposé, et à quel moment utiliser chaque mode.

10.1.2 Comparaison des modes de sécurité pour la gestion des clés, algorithmes d'authentification et de cryptage

Les trois facteurs majeurs qui déterminent l'efficacité d'un protocole de sécurité sont les suivants :

- La manière dont le protocole gère les clés.
- La présence ou l'absence d'authentification de l'utilisateur intégrée dans le protocole.
- L'algorithme ou la formule de cryptage que le protocole utilise pour coder/décoder les données.

Voici la liste des modes de sécurité disponibles sur la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway, ainsi qu'une description de la gestion des clés, de l'authentification et des algorithmes de cryptage utilisés dans chaque mode. Nous suggérons aussi quelques cas dans lesquels un mode est peut-être plus approprié qu'un autre.

- « Quand utiliser le mode non crypté (aucune sécurité) » à la page 99.
- « Quand utiliser le mode WEP statique » à la page 99.
- « Quand utiliser le mode IEEE 802.1x » à la page 100.
- « Quand utiliser le mode WPA Personal » à la page 102.
- « Quand utiliser le mode WPA Enterprise » à la page 103.

10.1.2.1 Quand utiliser le mode non crypté (aucune sécurité)

Définir le mode de sécurité sur *None (Plain-text)* (Aucun (texte brut)) n'assure par définition aucune sécurité. Dans ce mode, les données ne sont pas cryptées mais envoyées en tant que « texte brut » sur le réseau. Aucune gestion des clés, aucun cryptage des données ou aucune authentification utilisateur n'est utilisée.

Recommandations

Le mode non crypté, c'est-à-dire *None (Plain-text)* (Aucun (texte brut)), n'est pas recommandé pour une utilisation normale sur le réseau interne car il n'est pas sécurisé. C'est le seul mode dans lequel vous pouvez exécuter le réseau invité, qui est par définition un LAN non sécurisé, toujours séparé virtuellement ou physiquement des informations sensibles du LAN interne.

Par conséquent, définissez uniquement le mode de sécurité sur *None (Plain-text)* (Aucun (texte brut)) sur le réseau invité, et sur le réseau interne uniquement lors de la configuration initiale, des tests, et de la résolution des problèmes.

Voir aussi

Pour plus d'informations sur la configuration du mode de sécurité non crypté, reportez-vous à la section « *None (Plain-text)* (Aucun (texte brut)) » à la page 108.

10.1.2.2 Quand utiliser le mode WEP statique

Wired Equivalent Privacy statique (WEP) est un protocole de cryptage pour les réseaux sans fil 802.11. Toutes les stations et les points d'accès sans fil sur le réseau sont configurés avec une clé partagée statique 64 bits (clé secrète 40 bits + vecteur d'initialisation (IV) 24 bits) ou 128 bits (clé secrète 104 bits + IV 24 bits) pour le cryptage des données.

Tableau 10.1 Mode de sécurité WEP statique

Gestion des clés	Algorithme de cryptage	Authentification de l'utilisateur
<p>Le mode <i>WEP</i> statique utilise une clé fixe fournie par l'administrateur. Les clés WEP sont indexées dans différents slots (jusqu'à quatre sur la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway).</p> <p>Les stations client doivent avoir la même clé indexée dans le même slot pour accéder aux données sur le point d'accès.</p>	<p>Un chiffrement de flux <i>RC4</i> est utilisé pour crypter le corps de la trame et le contrôle de redondance cyclique (CRC) de chaque trame 802.11.</p>	<p>Si vous définissez l'algorithme d'authentification sur « Shared Key » (Clé partagée), ce protocole offre une forme rudimentaire d'authentification des utilisateurs.</p> <p>Toutefois, si l'algorithme d'authentification est défini sur « Open System » (Système ouvert), aucune authentification n'est effectuée.</p> <p>Si l'algorithme est défini sur « Both » (Les deux), seuls les clients WEP sont authentifiés.</p>

Recommandations

Le mode WEP statique a été conçu pour offrir une sécurité équivalente à l'envoi de données non cryptées via une connexion Ethernet. Toutefois, il a des défauts majeurs et ne fournit pas ce niveau de sécurité prévu.

Par conséquent, le mode **WEP statique n'est pas recommandé** comme mode sécurisé. Le mode WEP statique peut uniquement être utilisé lorsque les problèmes d'interopérabilité font que c'est la seule option disponible et qu'exposer potentiellement les données de votre réseau ne vous inquiète pas.

Voir aussi

Pour plus d'informations sur la configuration du mode de sécurité WEP statique, reportez-vous à la section « Static WEP (WEP statique) » à la page 109.

10.1.2.3 Quand utiliser le mode IEEE 802.1x

IEEE 802.1x est la norme de transfert du protocole Extensible Authentication Protocol (*EAP*) sur un réseau sans fil 802.11 en utilisant un protocole appelé EAP Encapsulation Over LANs (EAPOL). Il s'agit d'une norme plus récente et plus sécurisée que WEP statique.

Tableau 10.2 Mode de sécurité IEEE 801.1x

Gestion des clés	Algorithme de cryptage	Authentification de l'utilisateur
IEEE 802.1x fournit des clés générées dynamiquement qui sont régulièrement actualisées. Il existe différentes clés <i>Unicast</i> - <i>Monodiffusion</i> pour chaque station.	Un chiffrement de flux <i>RC4</i> est utilisé pour crypter le corps de la trame et le contrôle de redondance cyclique (CRC) de chaque trame 802.11.	Le mode IEEE 802.1x prend en charge un grand choix de méthodes d'authentification, comme les certificats, Kerberos et l'authentification de clé publique avec un serveur RADIUS. Vous avez le choix d'utiliser le serveur RADIUS intégré à la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway ou un serveur RADIUS externe. Le serveur RADIUS intégré prend en charge le protocole <i>EAP</i> protégé (PEAP) et MSCHAP V2.

Recommandations

Le mode IEEE 802.1x est un choix plus judicieux que le mode WEP statique parce que les clés sont générées dynamiquement et modifiées à intervalles réguliers. Cependant, l'algorithme de cryptage utilisé est le même que celui du mode WEP statique et il n'est par conséquent pas aussi fiable que les méthodes de cryptage plus avancées telles que *TKIP* et *CCMP* (*AES*) utilisées dans *Wi-Fi Protected Access* (*WPA*) ou *WPA2*.

En outre, les problèmes de compatibilité peuvent être contraignants en raison de la variété des méthodes d'authentification prises en charge et de l'absence de méthode de mise en œuvre standard.

Par conséquent, le mode IEEE 802.1x n'est pas une solution aussi sécurisée que *Wi-Fi Protected Access* (*WPA*) ou *WPA2*. Si vous ne pouvez pas utiliser *WPA* parce que certaines de vos stations client n'ont pas WPA, **utiliser le mode WPA Enterprise** est une meilleure solution que le mode IEEE 802.1x.

Si vous disposez d'un serveur RADIUS externe sur votre réseau, nous vous recommandons de l'utiliser du serveur RADIUS intégré sur le point d'accès. Un serveur RADIUS externe offrira une meilleure sécurité que le serveur d'authentification local.

Voir aussi

Pour plus d'informations sur la configuration du mode de sécurité IEEE 802.1x, reportez-vous à la section « IEEE 802.1x » à la page 114.

10.1.2.4 Quand utiliser le mode WPA Personal

Pre-Shared Key (Clé prépartagée) (PSK) Wi-Fi Protected Access Personal est une mise en œuvre de la norme Wi-Fi Alliance IEEE 802.11h, qui comprend les mécanismes AES (Advanced Encryption Algorithm), CCMP (Counter mode/CBC-MAC Protocol) et Temporal Key Integrity Protocol (TKIP). Ce mode présente les mêmes algorithmes de cryptage que WPA 2 avec RADIUS, mais sans la possibilité d'intégrer un serveur RADIUS pour l'authentification de l'utilisateur.

Ce mode de sécurité est rétrocompatible pour les clients sans fil qui ne prennent en charge que le **WPA** d'origine.

Tableau 10.3 Mode de sécurité WPA Personal

Gestion des clés	Algorithmes de cryptage	Authentification de l'utilisateur
WPA Personal fournit des clés générées dynamiquement qui sont régulièrement actualisées. Il existe différentes clés <i>Unicast - Monodiffusion</i> pour chaque station.	<ul style="list-style-type: none">• Temporal Key Integrity Protocol (<i>TKIP</i>).• Counter mode/CBC-MAC Protocol (<i>CCMP</i>) <i>Advanced Encryption Standard (AES)</i>.	L'utilisation d'une clé prépartagée (<i>PSK</i>) offre une authentification de l'utilisateur similaire à celle des clés partagées dans <i>WEP</i> .

Recommandations

WPA Personal n'est pas recommandé pour une utilisation avec la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway lorsque WPA Enterprise est une option.

Nous vous recommandons d'utiliser plutôt le mode WPA Enterprise, sauf si vous avez des problèmes d'interopérabilité qui vous empêchent d'utiliser ce mode.

Par exemple, certains appareils sur votre réseau ne prennent peut-être pas en charge WPA ou WPA2 avec **EAP** en relation avec un serveur **RADIUS**. Les serveurs d'impression intégrés ou d'autres petits appareils client avec très peu d'espace de mise en œuvre ne prennent peut-être pas en charge RADIUS. Dans de tels cas, nous vous recommandons d'utiliser WPA Personal.

Voir aussi

Pour plus d'informations sur la configuration de ce mode de sécurité, reportez-vous à la section « WPA Personal » à la page 117.

10.1.2.5 Quand utiliser le mode WPA Enterprise

Remote Authentication Dial In User Service (RADIUS) Wi-Fi Protected Access Personal est une mise en œuvre de la norme Wi-Fi Alliance IEEE **802.11h**, qui comprend les mécanismes *Advanced Encryption Algorithm (AES)*, *Counter mode/CBC-MAC Protocol (CCMP)* et *Temporal Key Integrity Protocol (TKIP)*. Ce mode nécessite l'utilisation d'un serveur RADIUS pour authentifier les utilisateurs. WPA Enterprise offre la meilleure sécurité disponible pour les réseaux sans fil.

Ce mode de sécurité est rétrocompatible pour les clients sans fil qui ne prennent en charge que le **WPA** d'origine.

Tableau 10.4 Mode de sécurité WPA Enterprise

Gestion des clés	Algorithmes de cryptage	Authentification de l'utilisateur
Le mode WPA Enterprise fournit des clés générées dynamiquement qui sont régulièrement actualisées. Il existe différentes clés <i>Unicast - Monodiffusion</i> pour chaque station.	<ul style="list-style-type: none">• Temporal Key Integrity Protocol (<i>TKIP</i>).• Counter mode/CBC-MAC Protocol (<i>CCMP</i>) Advanced Encryption Standard (<i>AES</i>).	Remote Authentication Dial-In User Service (<i>RADIUS</i>) Vous avez le choix d'utiliser le serveur RADIUS intégré à la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway ou un serveur RADIUS externe. Le serveur RADIUS intégré prend en charge le protocole <i>EAP</i> protégé (PEAP) et MSCHAP V2.

Recommandations

Le mode WPA Enterprise est le **mode recommandé**. Les algorithmes de cryptage **CCMP (AES)** et **TKIP** utilisés avec les modes WPA sont de loin supérieurs à l'algorithme **RC4** utilisé pour les modes **WEP** statique ou IEEE 802.1x. Par conséquent, CCMP (AES) ou TKIP devrait être utilisé si possible. Tous les modes WPA vous permettent d'utiliser ces schémas de cryptage. Par conséquent, les modes de sécurité WPA sont recommandés prioritairement aux autres lorsque l'utilisation de WPA est une option. En outre, ce mode intègre un serveur RADIUS pour l'authentification de l'utilisateur, ce qui lui confère un avantage sur le mode WPA Personal.

Si vous disposez d'un serveur RADIUS externe sur votre réseau, nous vous recommandons de l'utiliser du serveur RADIUS intégré sur le point d'accès. Un serveur RADIUS externe offrira une meilleure sécurité que le serveur d'authentification local.

Respectez les directives ci-dessous pour choisir les options dans le mode de sécurité du mode WPA Enterprise :

1. La meilleure sécurité disponible aujourd'hui sur un réseau sans fil est le mode WPA Entreprise utilisant l'algorithme de cryptage CCMP (AES). AES est une technique de cryptage de blocs de données 128 bits symétriques qui fonctionne sur plusieurs couches du réseau. C'est le système de cryptage le plus efficace actuellement disponible pour les réseaux sans fil. Si tous les clients ou autres points d'accès sur le réseau sont compatibles WPA/CCMP, utilisez cet algorithme de cryptage. (Si tous les clients sont compatibles WPA2, choisissez de ne prendre en charge que les clients WPA2.)
2. Le deuxième meilleur choix est WPA Entreprise avec l'algorithme de cryptage défini sur TKIP et CCMP. Cette option permet aux stations client WPA sans CCMP de s'associer, utilise TKIP pour crypter les trames **Multicast** et **Broadcast - Diffusion**, et permet aux clients de choisir d'utiliser ou non CCMP ou TKIP pour les trames **Unicast - Monodiffusion** (point d'accès vers un seul poste). Cette configuration WPA permet une meilleure interopérabilité, aux dépens d'une certaine sécurité. Les stations client qui prennent en charge CCMP peuvent l'utiliser pour leurs trames **Unicast - Monodiffusion**. Si vous rencontrez des problèmes d'interopérabilité du point d'accès vers la station avec le paramètre d'algorithme de cryptage « Both » (Les deux), vous devez sélectionner TKIP à la place. (Voir l'option suivante.)
3. Le troisième meilleur choix est WPA Entreprise avec l'algorithme de cryptage défini sur **TKIP**. Certains clients ont des problèmes d'interopérabilité si CCMP et TKIP sont activés en même temps. Si vous rencontrez ce problème, choisissez TKIP comme algorithme de cryptage. Il s'agit du mode WPA standard et du mode le plus interopérable avec les fonctionnalités de sécurité du logiciel client sans fil. TKIP est le seul algorithme de cryptage qui est en cours de test de certification **WPA WI-FI**.

Voir aussi

Pour plus d'informations sur la configuration de ce mode de sécurité, reportez-vous à la section « WPA Entreprise » à la page 119.

10.1.3 Interdire le SSID de diffusion améliore-t-il la sécurité ?

Vous pouvez supprimer (interdire) cette diffusion pour décourager la détection automatique de votre point d'accès par les stations. Lorsque le SSID de diffusion du point d'accès est supprimé, le nom du réseau ne s'affiche pas dans la liste des réseaux disponibles sur une station client. Au lieu de cela, le client doit avoir le nom exact du réseau configuré dans le demandeur avant de pouvoir se connecter.

La désactivation du SSID de diffusion est suffisante pour empêcher les clients de se connecter accidentellement à votre réseau, mais elle n'empêche pas les tentatives les plus simples de connexion par un pirate, ou de contrôler le trafic non crypté.

Ceci offre un niveau minimal de protection sur un réseau autrement exposé (comme un réseau invité) où la priorité va à une connexion facile pour les clients et où aucune information sensible n'est disponible.

(Voir aussi la section « Guest Network (Réseau invité) » à la page 108.)

10.1.4 Comment l'isolation de station protège-t-elle le réseau ?

Lorsque l'option *Station Isolation* (Isolation de station) est activée, le point d'accès bloque la communication entre les clients sans fil. Le point d'accès autorise toujours le trafic de données entre ses clients sans fil et les appareils filaires sur le réseau, mais pas entre les clients sans fil.

Le blocage de trafic s'étend aux clients sans fil connectés au réseau via des liaisons **WDS** ; ces clients ne peuvent pas communiquer avec les autres lorsque l'isolation de station est activée.

Reportez-vous au Chapitre 20 : « Système de distribution sans fil (WDS) » pour plus d'informations sur WDS.

10.2 Configuration des paramètres de sécurité

Pour définir le mode de sécurité, accédez à l'onglet *Security* (Sécurité) et mettez à jour les champs comme décrit ci-dessous.

Figure 10.1 Page de paramètres de sécurité

Basic Settings	Modify Internal Network security settings	
User Management	<input checked="" type="checkbox"/> Broadcast SSID <input type="checkbox"/> Station Isolation	
Cluster	Mode: WPA Personal	
Access Points	WPA Versions: <input checked="" type="checkbox"/> WPA <input checked="" type="checkbox"/> WPA2	
Sessions	Cipher Suites: <input checked="" type="checkbox"/> TKIP <input type="checkbox"/> CCMP (AES)	
Channel Management	Key: reoreore	
Wireless Neighborhood	Update	
Security		
Status		
Interfaces		

Les informations de configuration suivantes vous expliquent comment configurer les modes de sécurité sur le point d'accès. Gardez à l'esprit que chaque client sans fil qui souhaite échanger des données avec le point d'accès doit être configuré avec le mode de sécurité et la clé de cryptage conformes aux paramètres de sécurité du point d'accès.

Sur un point d'accès de radio professionnelle, ces paramètres de sécurité s'appliquent aux deux radios.



Remarque : Les modes de sécurité autres que Plain-Text (Texte brut) s'appliquent uniquement à la configuration du réseau « interne ». Sur le réseau « invité », vous pouvez utiliser uniquement le mode Plain-text (Texte brut). (Pour plus d'informations sur les réseaux invité, reportez-vous au Chapitre 14 : « Configuration de l'accès invité ».)

10.2.1 Broadcast SSID (SSID de diffusion), Station Isolation (Isolation de station) et Security Mode (Mode de sécurité)

Pour configurer la sécurité sur le point d'accès, sélectionnez un mode de sécurité et remplissez les champs associés, comme indiqué dans le Tableau 10.5.



Remarque : Vous pouvez également autoriser ou interdire le SSID de diffusion et activer/désactiver l'isolation de station en précautions supplémentaires, comme indiqué dans le Tableau 10.5 à la page 106.

Tableau 10.5 Paramètres de sécurité

Champ	Description
Broadcast SSID (SSID de diffusion)	<p>Pour activer le SSID de diffusion, cochez la case directement en regard du champ. Par défaut, le point d'accès diffuse (autorise) le <i>Service Set Identifier (SSID)</i> dans ses trames de balise.</p> <p>Vous pouvez supprimer (interdire) cette diffusion pour décourager la détection automatique de votre point d'accès par les stations. Lorsque le SSID de diffusion du point d'accès est supprimé, le nom du réseau ne s'affiche pas dans la liste des réseaux disponibles sur une station client. Au lieu de cela, le client doit avoir le nom exact du réseau configuré dans le demandeur avant de pouvoir se connecter.</p>

Tableau 10.5 Paramètres de sécurité (Suite)

Champ	Description
<i>Station Isolation (Isolation de station)</i>	<p>Pour activer l'isolation de station, cochez la case directement en regard du champ.</p> <ul style="list-style-type: none"> Lorsque l'option Station Isolation (Isolation de station) est <i>désactivée</i>, les clients sans fil peuvent communiquer les uns avec les autres normalement en envoyant du trafic via le point d'accès. Lorsque l'option Station Isolation (Isolation de station) est <i>activée</i>, le point d'accès bloque la communication entre les clients sans fil. Le point d'accès autorise toujours le trafic de données entre ses clients sans fil et les appareils filaires sur le réseau, mais pas entre les clients sans fil. Le blocage de trafic s'étend aux clients sans fil connectés au réseau via des liaisons WDS ; ces clients ne peuvent pas communiquer avec les autres lorsque l'isolation de station est activée. Reportez-vous au Chapitre 20 : « Système de distribution sans fil (WDS) » pour plus d'informations sur WDS.
<i>Security Mode (Mode de sécurité)</i>	<p>Sélectionnez le <i>Security Mode</i> (Mode de sécurité). Sélectionnez l'une des options suivantes :</p> <ul style="list-style-type: none"> « None (Plain-text) (Aucun (texte brut)) » à la page 108. « Static WEP (WEP statique) » à la page 109. « IEEE 802.1x » à la page 114. « WPA Personal » à la page 117. « WPA Enterprise » à la page 119. <p>Pour un réseau invité, le seul mode de sécurité qui puisse être appliqué est « None (Plain-text) » (Aucun (texte brut)). (Pour plus d'informations, reportez-vous au Chapitre 14 : « Configuration de l'accès invité ».)</p> <p>Les modes de sécurité autres que « None (Plain-text) » (Aucun (texte brut)) s'appliquent uniquement à la configuration du réseau « Interne ».</p>

10.2.2 Modes de sécurité

The screenshot shows a configuration window for wireless security. At the top, there are two checkboxes: 'Broadcast SSID' (checked) and 'Station Isolation' (unchecked). Below these, the 'Mode:' dropdown menu is open, showing options: 'None (Plain-text)', 'Static WEP', 'IEEE802.1x', 'WPA Personal' (highlighted), and 'WPA Enterprise'. To the right of the dropdown, there are two checkboxes: 'WPA2' (checked) and 'CCMP (AES)' (unchecked). Below the 'Mode:' dropdown, there is a 'Cipher:' label and a 'Key:' label with a text input field containing the text 'reoreore'.

10.2.2.1 None (Plain-text) (Aucun (texte brut))

None (Plain-text) (Aucun (texte brut)) signifie que toutes les données transférées vers et depuis la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway ne sont pas cryptées.

Si vous sélectionnez *None (Plain-text)* (Aucun (texte brut)) comme mode de sécurité, aucune autre option n'est configurable sur le point d'accès. Ce mode de sécurité peut être utile lors de la première configuration réseau ou pour la résolution de problèmes, mais il n'est pas recommandé pour une utilisation normale sur le réseau interne car il n'est pas sécurisé.

Guest Network (Réseau invité)

Définir la sécurité sur « None (Plain-text) » (Aucun (texte brut)) est le seul mode dans lequel vous pouvez exécuter le réseau invité, qui est par définition un **LAN** non sécurisé, toujours séparé virtuellement ou physiquement des informations sensibles du LAN interne. Par exemple, le réseau invité peut simplement fournir l'accès Internet et imprimante aux visiteurs quotidiens.

L'absence de sécurité sur le point d'accès invité est conçue pour simplifier le plus possible une connexion pour les invités sans avoir à programmer les paramètres de sécurité de leurs clients.

Pour un niveau minimum de protection sur un réseau invité, vous pouvez choisir de supprimer (interdire) la diffusion du SSID (nom de réseau) pour décourager la détection automatique votre point d'accès par les stations client. (Voir aussi la section « Interdire le SSID de diffusion améliore-t-il la sécurité ? » à la page 104.)

Pour plus d'informations sur le réseau invité, reportez-vous au Chapitre 14 : « Configuration de l'accès invité ».

10.2.2.2 Static WEP (WEP statique)

☒ Broadcast SSID ☐ Station Isolation

Mode: Static WEP

Transfer key index: 1

Key Length: ☐ 64 bits ☒ 128 bits ☐ 152 bits

Key Type: ☐ ASCII ☒ Hex

WEP Keys: (Characters required: 26)

1:

2:

3:

4:

Authentication : ☒ Open system ☐ Shared key

Wired Equivalent Privacy statique (WEP) est un protocole de cryptage des données pour les réseaux sans fil 802.11. Toutes les stations et les points d'accès sans fil sur le réseau sont configurés avec une clé partagée statique 64 bits (clé secrète 40 bits + vecteur d'initialisation (IV) 24 bits) ou 128 bits (clé secrète 104 bits + IV 24 bits) pour le cryptage des données. Vous ne pouvez pas mélanger les clés WEP 64 bits et 128 bits entre le point d'accès et ses stations client.

WEP statique n'est pas le mode le plus sécurisé disponible, mais il offre une meilleure protection que définir les paramètres de sécurité sur « None (Plain-text) » (Aucun (texte brut)), car il évite qu'un intrus puisse renifler facilement le trafic sans fil non crypté. (Pour des modes plus sécurisés, reportez-vous aux sections « IEEE 802.1x » à la page 114, « WPA Personal » à la page 117, ou « WPA Enterprise » à la page 119.)

WEP crypte les données en déplacement dans le réseau sans fil en utilisant une clé statique. (L'algorithme de cryptage est un chiffrement de « flux » appelé RC4.) Le point d'accès utilise une clé pour transmettre les données aux stations client. Chaque station client doit utiliser cette même clé pour décrypter les données qu'elle reçoit du point d'accès.

Les stations client peuvent utiliser plusieurs clés pour transmettre les données au point d'accès. (Ou elles peuvent toutes utiliser la même clé, mais c'est moins sécurisé, car cela signifie qu'une station peut décrypter les données envoyées par une autre.) Si vous avez sélectionné le mode de sécurité *Static WEP* (WEP statique), fournissez les informations dans les paramètres du point d'accès, comme indiqué dans la figure ci-dessous et décrit dans le Tableau 10.6 à la page 110.

Tableau 10.6 Paramètres de sécurité WEP statique

Champ	Description
<i>Transfer Key Index (Index de clé de transfert)</i>	<p>Sélectionnez un index de clé dans le menu déroulant. Les index de clé 1 à 4 sont disponibles. La valeur par défaut est 1.</p> <p>L'index de clé de transfert indique quelle clé WEP le point d'accès peut utiliser pour crypter les données qu'il transmet.</p>
<i>Key Length (Longueur de la clé)</i>	<p>Déterminez la longueur de la clé en cliquant sur l'un des boutons radio suivants :</p> <ul style="list-style-type: none">• 64 bits• 128 bits
<i>Key Type (Type de clé)</i>	<p>Sélectionnez le type de clé en cliquant sur l'un des boutons radio suivants :</p> <ul style="list-style-type: none">• ASCII• Hex
<i>Characters Required (Caractères requis)</i>	<p>Indique le nombre de caractères requis dans la clé WEP.</p> <p>Le nombre de caractères requis est mis à jour automatiquement en fonction de la manière dont vous avez défini les champs Key Length (Longueur de la clé) et Key Type (Type de clé).</p>
<i>WEP Keys (Clés WEP)</i>	<p>Vous pouvez spécifier jusqu'à quatre clés WEP. Dans chaque zone de texte, saisissez une chaîne de caractères pour chaque clé.</p> <p>Si vous avez sélectionné « ASCII », entrez n'importe quelle combinaison de nombres entiers et de lettres 0 à 9, a à z et A à Z. Si vous avez sélectionné « HEX », entrez des caractères hexadécimaux (toute combinaison de caractères compris entre 0 et 9 et a et f ou A et F).</p> <p>Utilisez le même nombre de caractères pour chaque clé, comme spécifié dans le champ « Characters Required » (Caractères requis). Ce sont les clés WEP RC4 partagées avec les stations utilisant le point d'accès.</p> <p>Chaque station client doit être configurée pour utiliser l'une de ces mêmes clés WEP dans le même slot, comme indiqué ici sur le point d'accès. (Reportez-vous à la section « Règles à retenir pour le mode WEP statique » à la page 111.)</p>

Tableau 10.6 Paramètres de sécurité WEP statique (Suite)

Champ	Description
<i>Authentication Algorithm (Algorithme d'authentification)</i>	<p>L'algorithme d'authentification définit la méthode utilisée pour déterminer si une station client est autorisée à s'associer à un point d'accès lorsque WEP statique est le mode de sécurité. Indiquez l'algorithme d'authentification que vous souhaitez utiliser en choisissant l'une des options suivantes dans le menu déroulant :</p> <ul style="list-style-type: none"> • Open System (Système ouvert). • Shared Key (Clé partagée). • Both (Les deux). <p>L'authentification Open System (Système ouvert) autorise n'importe quelle station client à associer avec le point d'accès que cette station client ait la clé WEP appropriée ou non. Cet algorithme est également utilisé dans les modes texte brut, IEEE 802.1x et WPA. Lorsque l'algorithme d'authentification est défini sur « Open System » (Système ouvert), tout client peut s'associer avec le point d'accès.</p> <p>Remarquez que le fait qu'une station client soit autorisée à s'associer ne garantit pas qu'elle puisse échanger du trafic avec un point d'accès. Une station doit avoir la clé WEP appropriée pour pouvoir accéder à un point d'accès et décrypter ses données, et pour transmettre des données lisibles au point d'accès.</p> <p>L'authentification Shared Key (Clé partagée) nécessite que la station client dispose de la clé WEP appropriée pour s'associer avec le point d'accès. Lorsque l'algorithme d'authentification est défini sur « Shared Key » (Clé partagée), une station avec une clé WEP incorrecte ne sera pas en mesure de s'associer avec le point d'accès.</p> <p>Both (Les deux) est le paramètre par défaut. Lorsque l'algorithme d'authentification est défini sur « Both » (Les deux) :</p> <ul style="list-style-type: none"> • Les stations client configurées pour utiliser WEP en mode clé partagée doivent disposer d'une clé WEP valide pour pouvoir s'associer avec le point d'accès. • Les stations client configurées pour utiliser WEP comme système ouvert (le mode clé partagée n'étant pas activé) pourront s'associer avec le point d'accès même si elles n'ont pas la clé WEP appropriée.

Règles à retenir pour le mode WEP statique

- Toutes les stations client doivent avoir la sécurité LAN sans fil (WLAN) configurée sur WEP et tous les clients doivent avoir l'une des clés WEP spécifiées sur le point d'accès pour décoder les transmissions de données du point d'accès vers la station.
- Le point d'accès doit avoir toutes les clés utilisées par les clients pour les transmissions station à point d'accès afin de pouvoir décoder les transmissions de la station.
- La même clé doit occuper le même slot sur tous les nœuds (point d'accès et clients). Par exemple, si le point d'accès définit la clé abc123 comme clé WEP 3, les stations client doivent définir cette même chaîne comme clé WEP 3.

- Sur certains logiciels client sans fil (comme Funk Odyssey), vous pouvez configurer plusieurs clés WEP et définir un « index de clé de transfert » de station client, puis définir les stations pour crypter les données qu'elles transmettent via différentes clés. Cela garantit que les points d'accès voisins ne puissent pas décoder les transmissions les uns des autres.

Exemple d'utilisation de WEP statique

Pour un exemple simple, supposons que vous configurez trois clés WEP sur le point d'accès. Dans notre exemple, l'index de clé de transfert pour le point d'accès est défini sur **3**. Cela signifie que la clé WEP dans le slot « 3 » est la clé que le point d'accès peut utiliser pour crypter les données qu'il envoie.

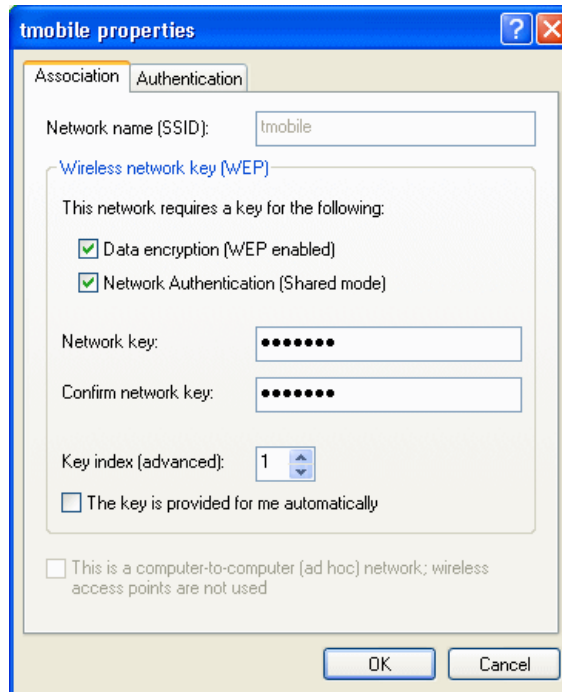
Figure 10.2 Définir la clé de transfert du point d'accès sur le point d'accès

The screenshot shows a configuration window for WEP. At the top, there are two checkboxes: "Broadcast SSID" (checked) and "Station Isolation" (unchecked). Below this is a "Mode:" dropdown menu set to "Static WEP". Underneath is a "Transfer key index:" dropdown menu set to "3". Then, there are three radio buttons for "Key Length": "64 bits" (selected), "128 bits", and "152 bits". Below that are two radio buttons for "Key Type": "ASCII" (selected) and "Hex". The "WEP Keys:" section has a note "(Characters required: 5)" and four input fields labeled 1 through 4. Field 1 contains "abcde", field 2 contains "fghij", field 3 contains "klmno", and field 4 is empty. At the bottom, there are two checkboxes for "Authentication": "Open system" (checked) and "Shared key" (unchecked).

Vous devez ensuite configurer toutes les stations client pour utiliser WEP et fournir à chaque client l'une des combinaisons slot/clé que vous avez définies sur le point d'accès.

Pour cet exemple, nous allons définir la clé WEP 1 sur un client Windows.

Figure 10.3 Fournir une clé WEP à un client sans fil



Si vous disposez d'une deuxième station client, elle doit également disposer de l'une des clés WEP définies sur le point d'accès. Vous pouvez lui donner la même clé WEP que celle que vous avez donnée à la première station. Ou, pour une solution plus sécurisée, vous pouvez donner à la deuxième station une autre clé WEP (clé 2, par exemple) afin que les deux stations ne puissent pas décrypter les transmissions l'une de l'autre.

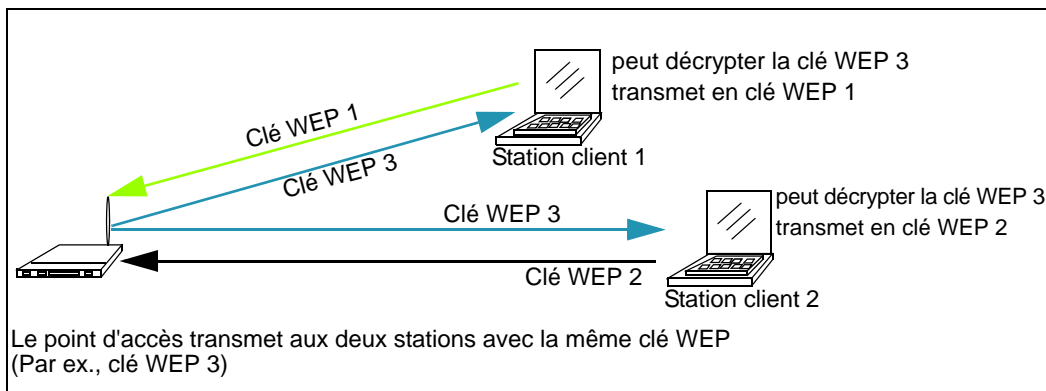
WEP statique avec index de clé de transfert sur les stations client

Certains logiciels client sans fil (comme Funk Odyssey) permettent de configurer plusieurs clés WEP et de définir un index de transfert sur la station client ; vous pouvez spécifier ensuite plusieurs clés à utiliser pour les transmissions de station à point d'accès. (Le logiciel client sans fil standard de Windows ne vous permet pas d'effectuer cette opération.)

Pour développer notre exemple, à l'aide du logiciel client Funk Odyssey, vous pouvez donner à chacun des clients la clé WEP 3 afin qu'ils puissent décoder les transmissions du point d'accès avec cette clé et donner également au client 1 la clé WEP 1 et la définir comme clé de transfert. Vous pouvez ensuite donner au client 2 la clé WEP 2 et la définir comme son index de clé de transfert.

La Figure 10.2.2.3 illustre la dynamique entre le point d'accès et deux stations client utilisant plusieurs clés WEP et un index de clé de transfert.

Figure 10.4 Exemple d'utilisation de plusieurs clés WEP et de l'index de clé de transfert sur des stations client



10.2.2.3 IEEE 802.1x

IEEE 802.1x est l'authentification basée sur le port de définition et l'infrastructure de gestion des clés standard. Les messages Extensible Authentication Protocol (**EAP**) envoyés via un réseau sans fil **IEEE 802.11** utilisant un protocole appelé EAPOL (EAP Encapsulation Over LANs). IEEE 802.1x fournit des clés générées dynamiquement qui sont régulièrement actualisées. Un chiffrement de flux RC4 est utilisé pour crypter le corps de la trame et le contrôle de redondance cyclique (CRC) de chaque trame 802.11.

Ce mode nécessite l'utilisation d'un serveur **RADIUS** pour authentifier les utilisateurs. Si l'option pour le serveur RADIUS interne est activée, configurez les comptes d'utilisateur sur le point d'accès via l'onglet *Cluster > User Management* (Cluster > Gestion des utilisateurs). Dans le cas contraire, configurez les comptes d'utilisateur sur le serveur RADIUS externe.

Le point d'accès requiert un serveur RADIUS compatible **EAP**, tel que le serveur Microsoft Internet Authentication Server ou le serveur d'authentification interne de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway. Pour fonctionner avec des clients Windows, le serveur d'authentification doit prendre en charge le protocole EAP protégé (PEAP) et **MSCHAP V2**.

Lors de la configuration du mode IEEE 802.1x, vous avez la possibilité de choisir d'utiliser le serveur RADIUS intégré ou un serveur RADIUS externe que vous fournissez. Le serveur RADIUS intégré de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway prend en charge le protocole **EAP** protégé (PEAP) et MSCHAP V2.

Si vous utilisez votre propre serveur RADIUS, vous avez la possibilité d'utiliser un grand choix de méthodes d'authentification que le mode IEEE 802.1x prend en charge, y compris les certificats, Kerberos et l'authentification de clé publique. N'oubliez pas, toutefois, que les stations client doivent être configurées pour utiliser la même méthode d'authentification que le point d'accès.

Si vous avez sélectionné le mode de sécurité *IEEE 802.1x*, fournissez les informations suivantes :

This screenshot shows the configuration interface for IEEE 802.1x security. At the top, the 'Security Mode' is set to 'IEEE 802.1x'. Below this, the 'Authentication Server' is set to 'Built-in'. The 'Radius IP' is configured as 127.0.0.1. The 'Radius Key' is represented by a series of dots. At the bottom, there is an unchecked checkbox labeled 'Enable radius accounting'.

This screenshot shows another configuration interface for IEEE802.1x security. At the top, there are two checkboxes: 'Broadcast SSID' (checked) and 'Station Isolation' (unchecked). Below these, the 'Mode' is set to 'IEEE802.1x'. A section with a grey header contains an unchecked checkbox 'Use internal radius server'. Below this, the 'Radius IP' is set to 10.128.14.14, and the 'Radius Key' is represented by a series of dots. At the bottom, there is an unchecked checkbox labeled 'Enable radius accounting'.

Tableau 10.7 Paramètres de sécurité IEEE 802.1x


Champ	Description
<i>Use internal radius server (Utiliser le serveur radius interne)</i>	<p>Sélectionnez l'une des options suivantes dans le menu déroulant :</p> <ul style="list-style-type: none">• Pour utiliser le serveur d'authentification fourni avec la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway, assurez-vous que la case en regard du champ Use internal radius server (Utiliser serveur radius interne) est sélectionnée. Si cette option est sélectionnée, vous n'avez pas besoin de renseigner les champs Radius IP (IP Radius) et Radius Key (Clé Radius) ; ils sont renseignés automatiquement. Si l'option pour le serveur RADIUS interne est activée, configurez les comptes d'utilisateur sur le point d'accès via l'onglet <i>Cluster > User Management</i> (Cluster > Gestion des utilisateurs). Pour plus d'informations, reportez-vous au Chapitre 7 : « Gestion des comptes d'utilisateur ».• Pour utiliser un serveur d'authentification externe, assurez-vous que la case en regard du champ Use internal radius server (Utiliser serveur radius interne) est désactivée. Si vous désactivez cette case, vous devez renseigner les champs Radius IP (IP Radius) et Radius Key (Clé Radius) pour le serveur que vous souhaitez utiliser. <p><i>Remarque : Le serveur RADIUS est identifié par son adresse IP et les numéros de port UDP des différents services qu'il offre. Sur la version actuelle de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway, les ports UDP (User Datagram Protocol) du serveur RADIUS utilisés par le point d'accès ne sont pas configurables. (La passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway est codée en dur pour utiliser le port UDP 1812 du serveur RADIUS pour l'authentification et le port 1813 pour l'audit.)</i></p>
<i>Radius IP (IP Radius)</i>	<p>Entrez l'IP Radius dans la zone de texte.</p> <p>L'IP Radius est l'adresse IP du serveur RADIUS.</p> <p>(Le serveur d'authentification interne de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway est 127.0.0.1.)</p> <div><p>Si vous disposez d'un serveur RADIUS externe sur votre réseau, nous vous recommandons de l'utiliser du serveur RADIUS intégré sur le point d'accès. Un serveur RADIUS externe offrira une meilleure sécurité que le serveur d'authentification local.</p></div> <p>Pour plus d'informations sur la configuration de comptes d'utilisateur, reportez-vous au Chapitre 7 : « Gestion des comptes d'utilisateur ».</p>

Tableau 10.7 Paramètres de sécurité IEEE 802.1x (Suite)

Champ	Description
<i>Radius Key</i> (Clé Radius)	<p>Entrez la clé Radius dans la zone de texte.</p> <p>La <i>clé Radius</i> est la clé secrète partagée du serveur RADIUS. Le texte que vous saisissez s'affiche sous la forme de caractères « * » afin d'empêcher d'autres personnes de voir la clé RADIUS que vous entrez.</p> <p>(La clé du serveur d'authentification interne de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway est secrète.)</p> <p>Cette valeur n'est jamais envoyée sur le réseau.</p>
<i>Enable radius accounting</i> (Activer l'audit Radius)	<p>Cliquez sur la case à cocher en regard du champ « Enable radius accounting » (Activer l'audit Radius) si vous souhaitez suivre et mesurer les ressources qu'un utilisateur particulier a consommé, par exemple l'heure système, la quantité de données transmises et reçues, etc.</p>

10.2.2.4 WPA Personal

Wi-Fi Protected Access Personal est une norme Wi-Fi Alliance IEEE **802.11i**, qui inclut les mécanismes *Counter mode/CBC-MAC Protocol-Advanced Encryption Algorithm (CCMP-AES)* et *Temporal Key Integrity Protocol (TKIP)*.

La version Personal de WPA utilise une clé prépartagée (au lieu de IEEE **802.1x** et **EAP** qui sont utilisés dans le mode de sécurité WPA Enterprise). PSK est utilisé uniquement pour une vérification initiale des informations d'identification. Ce mode de sécurité est rétrocompatible pour les clients sans fil qui prennent en charge le **WPA** d'origine.

Si vous avez sélectionné le *mode de sécurité WPA Personal*, remplissez les paramètres comme indiqué dans le Tableau 10.8 à la page 118.

Security Mode		WPA/WPA2 Personal (PSK) ▼
<hr/>		
Supported Client Stations	Both ▼	
Cipher Suites	TKIP ▼	
Key	<input type="text"/>	

☒ Broadcast SSID ☐ Station Isolation

Mode:

WPA Personal

WPAVersions: ☒ WPA ☒ WPA2

Cipher Suites: ☒ TKIP ☐ CCMP (AES)

Key:

reoreore

Tableau 10.8 Paramètres du mode de sécurité WPA Personal

Champ	Description
WPA Versions (Versions WPA)	<p>Sélectionnez les types de stations client vous souhaitez prendre en charge :</p> <ul style="list-style-type: none">• WPA• WPA2• Both (Les deux) <p>WPA. Si toutes les stations client sur le réseau prennent en charge le <i>WPA</i> d'origine mais pas le <i>WPA2</i> plus récent, sélectionnez WPA.</p> <p>WPA2. Si toutes les stations client sur le réseau prennent en charge <i>WPA2</i>, nous vous suggérons d'utiliser WPA2 qui offre une sécurité optimale pour la norme <i>IEEE 802.11i</i>.</p> <p>Both (Les deux). Si vous avez une combinaison de clients, certains prenant en charge <i>WPA2</i> et d'autres prenant uniquement en charge le <i>WPA</i> d'origine, sélectionnez les deux. Cette option permet aux stations client WPA et WPA2 de s'associer et de s'authentifier, mais utilise le mode WPA2 plus robuste pour les clients qui le prennent en charge. Cette configuration WPA permet une meilleure interopérabilité, aux dépens d'une certaine sécurité.</p>

Tableau 10.8 Paramètres du mode de sécurité WPA Personal (Suite)

Champ	Description
<i>Cipher Suites</i> (Suites de chiffrement)	<p>Sélectionnez la suite de chiffrement que vous souhaitez utiliser :</p> <ul style="list-style-type: none"> • TKIP • CCMP (AES) • Both (Les deux) <p>Temporal Key Integrity Protocol (TKIP) est le paramètre par défaut.</p> <p>TKIP fournit une solution de cryptage plus sécurisée que les clés WEP. Le traitement TKIP modifie plus fréquemment la clé de cryptage utilisée et assure une meilleure garantie que la même clé ne sera pas réutilisée pour crypter des données (une faiblesse de WEP). TKIP utilise une « clé temporelle » 128 bits partagée par les clients et les points d'accès. La clé temporelle est associée à l'adresse MAC du client et à un vecteur d'initialisation 16 octets pour produire la clé qui va crypter les données. Ceci permet de s'assurer que chaque station client utilise une clé différente pour crypter les données. TKIP utilise RC4 pour effectuer le cryptage, qui est la même que WEP. Mais TKIP modifie les clés temporelles tous les 10 000 paquets et les distribue, ce qui améliore considérablement la sécurité du réseau.</p> <p>Counter mode/CBC-MAC Protocol (CCMP) est une méthode de cryptage pour IEEE 802.11i qui utilise Advanced Encryption Algorithm (AES). Elle utilise un CCM combiné au mode Cipher Block Chaining Counter (CBC-CTR) et du code Cipher Block Chaining Message Authentication Code (CBC-MAC) pour le cryptage et l'intégrité des messages.</p> <p>Si vous sélectionnez à la fois TKIP et CCMP(AES), le chiffrement Pairwise (par paires) est AES et le chiffrement Groupwise (par groupes) est TKIP. Le chiffrement Pairwise est utilisé pour le trafic monodiffusion et le chiffrement Groupwise est utilisé pour le trafic diffusion/multidiffusion. Les clients TKIP et AES peuvent s'associer au point d'accès. Les clients WPA doit avoir l'un des éléments suivants pour s'associer au point d'accès :</p> <ul style="list-style-type: none"> • Une clé TKIP valide • Une clé CCMP (AES) valide <p>Les clients non configurés pour utiliser WPA Personal ne pourront pas s'associer au point d'accès.</p>
<i>Key (Clé)</i>	<p>La <i>clé prépartagée</i> est la clé secrète partagée pour WPA Personal. Saisissez une chaîne d'au moins 8 caractères avec un maximum de 63 caractères.</p>

10.2.2.5 WPA Enterprise

Remote Authentication Dial In User Service (RADIUS) Wi-Fi Protected Access Enterprise est une mise en œuvre de la norme Wi-Fi Alliance IEEE **802.11h**, qui comprend les mécanismes *Advanced Encryption Algorithm (AES)*, *Counter mode/CBC-MAC Protocol (CCMP)* et *Temporal Key Integrity Protocol (TKIP)*. Le mode Enterprise nécessite l'utilisation d'un serveur RADIUS pour authentifier les utilisateurs, et la configuration de comptes d'utilisateur via l'onglet *Cluster, User Management* (Cluster, Gestion des utilisateurs).

Ce mode de sécurité est rétrocompatible pour les clients sans fil qui prennent en charge le **WPA** d'origine.

Lors de la configuration du mode WPA Enterprise, vous avez la possibilité de choisir d'utiliser le serveur RADIUS intégré ou un serveur RADIUS externe que vous fournissez. Le serveur RADIUS intégré de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway prend en charge le protocole **EAP** protégé (PEAP) et MSCHAP V2.

Si vous avez sélectionné le mode de sécurité « *WPA Enterprise* », remplissez les paramètres comme indiqué dans le Tableau 10.9 à la page 121.

This screenshot shows the configuration interface for WPA/WPA2 Enterprise (RADIUS) security mode. The 'Security Mode' dropdown is set to 'WPA/WPA2 Enterprise (RADIUS)'. Below this, the 'Supported Client Stations' dropdown is set to 'WPA'. There are two checkboxes: 'Enable pre-authentication' (unchecked) and 'Enable radius accounting' (unchecked). The 'Cipher Suites' dropdown is set to 'TKIP'. The 'Authentication Server' dropdown is set to 'Built-in'. The 'Radius IP' is configured as '127.0.0.1' using four input fields. The 'Radius Key' is a text field containing a series of asterisks. At the bottom, there is a checkbox for 'Allow non-WPA IEEE 802.1x clients' which is checked.

This screenshot shows the configuration interface for WPA Enterprise security mode. At the top, there are two checkboxes: 'Broadcast SSID' (checked) and 'Station Isolation' (unchecked). The 'Mode' dropdown is set to 'WPA Enterprise'. Under 'WPA Versions', both 'WPA' and 'WPA2' are checked. There are two checkboxes: 'Enable pre-authentication' (unchecked) and 'Enable radius accounting' (unchecked). Under 'Cipher Suites', 'TKIP' is checked and 'CCMP (AES)' is unchecked. A section titled 'Use internal radius server' (with an unchecked checkbox) contains the 'Radius IP' field set to '10.128.14.14' and the 'Radius Key' field filled with asterisks.

Tableau 10.9 Paramètres de sécurité WPA Enterprise

Champ	Description
<i>WPA Versions (Versions WPA)</i>	<p>Sélectionnez les types de stations client que vous souhaitez prendre en charge :</p> <ul style="list-style-type: none">• WPA• WPA2• Both (Les deux) <p>WPA. Si toutes les stations client sur le réseau prennent en charge le WPA d'origine mais pas le WPA2 plus récent, sélectionnez WPA.</p> <p>WPA2. Si toutes les stations client sur le réseau prennent en charge WPA2, nous vous suggérons d'utiliser WPA2 qui offre une sécurité optimale pour la norme IEEE 802.11i.</p> <p>Both (Les deux). Si vous avez une combinaison de clients, certains prenant en charge WPA2 et d'autres prenant uniquement en charge le WPA d'origine, sélectionnez WPA et WPA2. Cette option permet aux stations client WPA et WPA2 de s'associer et de s'authentifier, mais utilise le mode WPA2 plus robuste pour les clients qui le prennent en charge. Cette configuration WPA permet une meilleure interopérabilité, aux dépens d'une certaine sécurité.</p>
<i>Enable pre-authentication (Activer la pré-authentication)</i>	<p>Si pour les versions WPA, vous sélectionnez uniquement WPA2 ou WPA et WPA2, vous pouvez activer la pré-authentication pour les clients WPA2.</p> <p>Cliquez sur Enable pre-authentication (Activer la pré-authentication) si vous souhaitez que les clients sans fil WPA2 envoient un paquet de pré-authentication. Les informations de pré-authentication seront transmises à partir du point d'accès que le client utilise actuellement vers le point d'accès cible. L'activation de cette fonctionnalité permet d'accélérer l'authentification pour les clients itinérants qui se connectent à plusieurs points d'accès.</p> <p>Cette option ne s'applique pas si vous avez sélectionné « WPA » pour les versions WPA car le mode WPA d'origine ne prend pas en charge cette fonctionnalité.</p>

Tableau 10.9 Paramètres de sécurité WPA Enterprise (Suite)

Champ	Description
<i>Cipher Suites (Suites de chiffrement)</i>	<p>Sélectionnez le chiffrement que vous souhaitez utiliser :</p> <ul style="list-style-type: none">• TKIP• CCMP (AES)• Both (Les deux) <p>Temporal Key Integrity Protocol (TKIP) est le paramètre par défaut.</p> <p>TKIP fournit une solution de cryptage plus sécurisée que les clés WEP. Le traitement TKIP modifie plus fréquemment la clé de cryptage utilisée et assure une meilleure garantie que la même clé ne sera pas réutilisée pour crypter des données (une faiblesse de WEP). TKIP utilise une « clé temporelle » 128 bits partagée par les clients et les points d'accès. La clé temporelle est associée à l'adresse MAC du client et à un vecteur d'initialisation 16 octets pour produire la clé qui va crypter les données. Ceci permet de s'assurer que chaque station client utilise une clé différente pour crypter les données. TKIP utilise RC4 pour effectuer le cryptage, qui est la même que WEP. Mais TKIP modifie les clés temporelles tous les 10 000 paquets et les distribue, ce qui améliore considérablement la sécurité du réseau.</p> <p>Counter mode/CBC-MAC Protocol (CCMP) est une méthode de cryptage pour IEEE 802.11i qui utilise Advanced Encryption Algorithm (AES). Elle utilise un CCM combiné au mode Cipher Block Chaining Counter (CBC-CTR) et du code Cipher Block Chaining Message Authentication Code (CBC-MAC) pour le cryptage et l'intégrité des messages.</p> <p>Lorsque TKIP et CCMP sont tous deux sélectionnés, les clients TKIP et AES peuvent s'associer au point d'accès. Les stations client configurées pour utiliser WPA avec RADIUS doivent être associées à l'un des éléments suivants pour être en mesure de s'associer au point d'accès :</p> <ul style="list-style-type: none">• Une adresse IP RADIUS TKIP et une clé partagée valides.• Une adresse IP CCMP (AES) et une clé partagée valides. <p>Les clients non configurés pour utiliser WPA avec RADIUS ne pourront pas s'associer au point d'accès.</p> <p>Par défaut, TKIP et CCMP sont tous les deux sélectionnés. Lorsque les deux TKIP et CCMP sont sélectionnés, les stations client configurées pour utiliser WPA avec RADIUS doit avoir l'un des éléments suivants :</p> <ul style="list-style-type: none">• Une adresse IP RADIUS TKIP et une clé RADIUS valides.• Une adresse IP CCMP (AES) et une clé RADIUS valides.

Tableau 10.9 Paramètres de sécurité WPA Enterprise (Suite)


Champ	Description
<i>Use internal radius server (Utiliser le serveur radius interne)</i>	<p>Vous pouvez choisir d'utiliser le serveur d'authentification intégré fourni avec la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway ou vous pouvez utiliser un serveur radius externe.</p> <ul style="list-style-type: none"> Pour utiliser le serveur d'authentification fourni avec la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway, assurez-vous que la case en regard du champ Use internal radius server (Utiliser serveur radius interne) est sélectionnée. Si cette option est sélectionnée, vous n'avez pas besoin de renseigner les champs Radius IP (IP Radius) et Radius Key (Clé Radius) ; ils sont renseignés automatiquement. Si l'option pour le serveur RADIUS interne est activée, configurez les comptes d'utilisateur sur le point d'accès via l'onglet <i>Cluster > User Management</i> (Cluster > Gestion des utilisateurs). Pour plus d'informations, reportez-vous au Chapitre 7 : « Gestion des comptes d'utilisateur ». Pour utiliser un serveur d'authentification externe, assurez-vous que la case en regard du champ Use internal radius server (Utiliser serveur radius interne) est désactivée. Si vous désactivez cette case, vous devez renseigner les champs Radius IP (IP Radius) et Radius Key (Clé Radius) pour le serveur que vous souhaitez utiliser. <p><i>Remarque : Le serveur RADIUS est identifié par son adresse IP et les numéros de port UDP des différents services qu'il offre. Sur la version actuelle de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway, les ports UDP (User Datagram Protocol) du serveur RADIUS utilisés par le point d'accès ne sont pas configurables. (La passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway est codée en dur pour utiliser le port UDP 1812 du serveur RADIUS pour l'authentification et le port 1813 pour l'audit.)</i></p>
<i>Radius IP (IP Radius)</i>	<p>Entrez l'IP Radius dans la zone de texte. L'<i>IP Radius</i> est l'adresse IP du serveur RADIUS.</p> <p>(Le serveur d'authentification interne de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway est 127.0.0.1.)</p> <p> Si vous disposez d'un serveur RADIUS externe sur votre réseau, nous vous recommandons de l'utiliser du serveur RADIUS intégré sur le point d'accès. Un serveur RADIUS externe offrira une meilleure sécurité que le serveur d'authentification local.</p> <p>Pour plus d'informations sur la configuration de comptes d'utilisateur, reportez-vous au Chapitre 7 : « Gestion des comptes d'utilisateur ».</p>
<i>Radius Key (Clé Radius)</i>	<p>Entrez la clé Radius dans la zone de texte.</p> <p>La <i>clé Radius</i> est la clé secrète partagée du serveur RADIUS. Le texte que vous saisissez s'affiche sous la forme de caractères « * » afin d'empêcher d'autres personnes de voir la clé RADIUS que vous entrez.</p> <p>(La clé du serveur d'authentification interne de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway est secrète.)</p> <p>Cette valeur n'est jamais envoyée sur le réseau.</p>

Tableau 10.9 Paramètres de sécurité WPA Enterprise (Suite)

Champ	Description
<i>Enable RADIUS Accounting (Activer l'audit RADIUS)</i>	Cliquez sur Enable RADIUS Accounting (Activer l'audit RADIUS) si vous souhaitez appliquer l'authentification pour les stations client <i>WPA</i> avec des noms d'utilisateur et des mots de passe pour chaque station. Voir aussi le Chapitre 7 : « Gestion des comptes d'utilisateur ».

10.3 Mise à jour des paramètres

Pour mettre à jour les paramètres de sécurité :

1. Accédez à l'onglet *Security* (Sécurité).
2. Configurez les paramètres de sécurité selon les besoins.
3. Cliquez sur le bouton **Update** (Mettre à jour) pour appliquer les modifications.

11.1 Interfaces	127
11.1.1 Paramètres Ethernet (filaire)	128
11.1.2 Paramètres sans fil	128
11.2 Journaux des événements	128
11.2.1 Activation ou désactivation de la persistance	129
11.2.2 Severity (Gravité)	130
11.2.3 Profondeur	130
11.2.4 Hôte de relais de journal pour les messages du noyau.	131
11.2.4.1 Présentation de la journalisation à distance	131
11.2.4.2 Configuration de l'hôte de relais de journal	131
11.2.4.3 Activation/désactivation de l'hôte de relais de journal sur la page Status > Events (État > Événements).	132
11.2.5 Journal des événements	133
11.3 Statistiques d'émission/réception	134
11.4 Clients sans fil associés	136
11.4.1 Contrôle d'intégrité de la liaison	136
11.5 Points d'accès voisins	136



Important : Les tâches de maintenance et de surveillance décrites dans cette section se rapportent à l'affichage et à la modification des paramètres de points d'accès spécifiques, et non à une configuration de cluster qui est automatiquement partagée par plusieurs points d'accès. Par conséquent, il est important de veiller à ce que vous accédiez aux pages Web d'administration du point d'accès particulier que vous souhaitez configurer. Pour plus d'informations à ce sujet, reportez-vous à la section « Informations de configuration pour un point d'accès spécifique et gestion des points d'accès autonomes » on page 64.

11.1 Interfaces

Pour contrôler les paramètres LAN filaire et sans fil (**WLAN**), accédez à *Status > Interfaces* (État > Interfaces) sur le point d'accès que vous souhaitez surveiller.



Remarque : Sur un point d'accès de radio professionnelle, les paramètres sans fil actuels pour les radios un et deux sont affichés. Sur un point d'accès de radio unique, les paramètres sont affichés pour une radio. La page Interfaces (Interfaces) pour un point d'accès de radio professionnelle est affichée dans la figure suivante.

Figure 11.1 Page Network Interfaces (Interfaces réseau)

View settings for network interfaces

Wired Settings

(Edit)

LAN or Internal Interface

MAC Address00:08:A2:01:10:AC

VLAN ID

IP Address10.128.75.98

Subnet Mask255.255.0.0

Guest Interface

MAC Address00:00:00:00:00:00

VLAN ID

Subnet

Wireless Settings

(Edit)

Radio

ModeIEEE 802.11g

Channel5 (2432 MHz)

Internal Interface

MAC Address00:08:A2:01:10:B0

Network Name (SSID)SFGWPA /

Guest Interface

MAC Addressn/a

Network Name (SSID)TEKLOGIX GUEST /

?

This page displays current Ethernet (Wired) and Wireless settings on the access point.

To configure Ethernet Settings, go to the [Ethernet \(Wired\) Settings](#) tab.

To configure Wireless Settings, go to the [Wireless Settings](#) tab.

[More ...](#)

Cette page affiche les paramètres actuels de la passerelle sans fil 9160 G2 Wireless Gateway. Elle affiche les paramètres Ethernet (filaire) et les paramètres sans fil.

11.1.1 Paramètres Ethernet (filaire)

L'interface *Internal* (Interne) comprend l'adresse Ethernet **MAC**, **IP Address - Adresse IP**, **Subnet Mask - Masque de sous-réseau** et le nom du réseau sans fil associé (**SSID**).

L'interface *Guest* (Invité) comprend l'adresse **MAC**, l'**ID VLAN**, et le nom du réseau sans fil associé (**SSID**).

Si vous souhaitez modifier l'un de ces paramètres, cliquez sur le lien **Edit** (Modifier).

11.1.2 Paramètres sans fil

L'interface *Radio* (Radio) inclut le mode *radio* et **Channel - Canal**. Les adresses **MAC** (en lecture seule) et les noms des réseaux pour les interfaces interne et invité sont également indiquées ici. (Pour plus d'informations, reportez-vous au Chapitre 13 : « Définition de l'interface sans fil » et au Chapitre 16 : « Configuration des paramètres radio 802.11 ».)

Si vous souhaitez modifier l'un de ces paramètres, cliquez sur le lien **Edit** (Modifier).

11.2 Journaux des événements

Pour afficher le journal du noyau et des événements système d'un point d'accès particulier, accédez à *Status > Events* (États > Événements) sur les pages Web d'administration pour le point d'accès que vous souhaitez contrôler.

Figure 11.2 Événements de point d'accès

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

View events generated by this access point

Options

Persistence ☐ Enabled ☒ Disabled

Severity 7

Depth 128

Update

☐ Relay Log

Relay Host

Relay Port 514

Update

Events

Clear All

Time	Type	Service	Description
Jun 4 19:14:29	info	dropbear [3074]	exit after auth (admin): Exited normally
Jun 4 19:14:29	err	dropbear [3074]	chown /dev/tty0 0 0 failed: Read-only file system
Jun 4 18:25:30	info	hostapd	wlan0: STA 00:10:c6:36:6f:1f WPA: group key poll timed out (no reply was received)
Jun 4 18:24:00	info	hostapd	wlan0: STA 00:10:c6:36:6f:1f WPA: group key exchange completed

L'onglet *Events* (Événements) vous permet d'activer ou de désactiver la *persistance*. Cette page vous offre également la possibilité d'activer un « hôte de relais de journal » pour capturer tous les événements et erreurs du système sur un journal de noyau. (Cela nécessite d'abord de configurer un hôte de relais à distance. Reportez-vous à la section « Hôte de relais de journal pour les messages du noyau » on page 131.) L'onglet *Events* (Événements) répertorie également les événements les plus récents générés par ce point d'accès (reportez-vous à la section « Journal des événements » on page 133).



Remarque : La passerelle sans fil 9160 G2 Wireless Gateway reçoit ses informations relatives à la date et à l'heure via NTP (Network Time Protocol). Ces données sont signalées au format UTC (également appelé Temps moyen de Greenwich). Vous devez convertir l'heure signalée à votre heure locale. Pour plus d'informations sur la définition du protocole NTP, reportez-vous au Chapitre 25 : « Serveur Network Time Protocol (NTP) ».

11.2.1 Activation ou désactivation de la persistance

La *persistance* peut être activée ou désactivée depuis l'onglet *Events* (Événements). Le journal permanent est enregistré dans la mémoire NVRAM. Même après un redémarrage, tous les journaux permanents sont toujours réservés dans la mémoire NVRAM. Les journaux non permanents ne sont conservés que pendant la période d'exécution. Si vous redémarrez la 9160 G2, tous les journaux non permanents seront perdus.

Activer la *persistance* depuis l'onglet *Events* (Événements) garantit que tous les journaux sont écrits dans la mémoire NVRAM et que même après un redémarrage, ils sont récupérables.



Remarque : Il faut se rappeler que l'activation de la persistance aura pour résultat une opération d'écriture en continu. Il y a un risque que cela use l'élément Flash du point d'accès ; vous devez décider si activer la persistance est plus adapté à vos besoins, étant donné ce risque élevé.

Tableau 11.1 Paramètres de configuration de la persistance

Champ	Description
<i>Relay Log (Journal de relais)</i>	Choisissez d'activer ou de désactiver la <i>persistance</i> .
<i>Relay Host (Hôte de relais)</i>	Vous pouvez choisir un niveau de <i>gravité</i> entre 0 et 7. <i>Severity</i> 7 (Gravité 7) est le niveau le moins grave et <i>Severity</i> 0 (Gravité 0) est le plus grave. Pour plus d'informations sur les niveaux de gravité, reportez-vous à la section « <i>Severity</i> (Gravité) » à la page 130.
<i>Relay Port (Port de relais)</i>	Vous pouvez entrer une valeur comprise entre 1 et 128. Pour plus d'informations sur la profondeur, reportez-vous à la section « <i>Profondeur</i> » à la page 130.

11.2.2 Severity (Gravité)

Le but de configuration de la gravité est de filtrer ou de limiter les messages de sécurité qui s'affichent dans le journal des événements. Il est peu probable que vous souhaitiez voir une liste de tous les messages. Les messages moins graves ou de moindre importance peuvent être filtrés en utilisant la fonction de configuration de la *gravité*.

Si vous définissez le niveau de *gravité* à 7, tous les messages avec un niveau de gravité situé entre 7 et 0 apparaîtront dans le journal des événements. Sinon, si vous souhaitez filtrer les messages, vous pouvez définir le niveau de *gravité* à 4. Dans cet exemple, tous les messages avec un niveau de gravité situé entre 4 et 0 s'affichent dans le journal des événements. Par conséquent, les messages et les notifications moins importants seront ignorés.

Tableau 11.2 Paramètres de configuration de la gravité

Niveau de gravité	Description
0	<i>Urgence</i> : le système est inutilisable
1	<i>Alerte</i> : une action doit être entreprise immédiatement
2	<i>Critique</i> : condition critique
3	<i>Erreur</i> : condition d'erreur
4	<i>Avertissement</i> : conditions d'avertissement
5	<i>Avertissement</i> : condition normale mais significative
6	<i>Informative</i> : messages d'information
7	<i>Débogage</i> : messages de débogage

11.2.3 Profondeur

La valeur indiquée dans le champ *Depth* (Profondeur) détermine le nombre d'entrées de journal qui peuvent être enregistrées dans la mémoire NVRAM. Vous pouvez enregistrer un maximum de 128 entrées. Si vous comptez sur les messages de journal pour contrôler les performances de votre point d'accès, vous devez définir la *profondeur* à sa valeur maximale de **128**.

11.2.4 Hôte de relais de journal pour les messages du noyau

- « Présentation de la journalisation à distance » à la page 131.
- « Configuration de l'hôte de relais de journal » à la page 131.
- « Activation/désactivation de l'hôte de relais de journal sur la page Status > Events (État > Événements) » à la page 132.

11.2.4.1 Présentation de la journalisation à distance

Le journal du noyau est une liste complète des événements système (indiqués dans le journal système) et des messages du noyau, tels que les conditions d'erreur comme les pertes d'images.

Vous ne pouvez pas afficher les messages du journal du noyau directement à partir de l'interface utilisateur Web d'administration d'un point d'accès. Vous devez d'abord configurer un serveur distant exécutant un processus syslog agissant comme un « hôte de relais de journal » sur votre réseau. Ensuite, vous pouvez configurer la passerelle sans fil 9160 G2 Wireless Gateway pour envoyer ses messages syslog au serveur distant.

L'utilisation d'un serveur distant pour collecter les messages syslog d'un point d'accès vous offre plusieurs avantages. Vous pouvez :

- regrouper les messages syslog provenant de plusieurs points d'accès ;
- stocker un historique des messages plus long que celui qui est conservé sur un point d'accès ;
- déclencher des alertes et des opérations de gestion par scripts.

11.2.4.2 Configuration de l'hôte de relais de journal

Pour utiliser le relayage de journal du noyau, vous devez configurer un serveur distant pour recevoir les messages syslog. Cette procédure peut varier en fonction du type de machine utilisée comme hôte pour le journal distant. L'exemple suivant montre comment configurer un serveur Linux distant en utilisant le programme syslog.

Exemple d'utilisation d'un syslogd Linux

Les étapes suivantes activent le programme syslog sur un serveur Linux. Assurez-vous que vous avez bien une identité d'utilisateur racine pour ces tâches.

1. Connectez-vous en tant qu'utilisateur racine à la machine que vous souhaitez utiliser comme hôte de relais syslog.

Les opérations suivantes exigent des permissions d'utilisateur racine. Si vous n'êtes pas déjà connecté en tant qu'utilisateur racine, tapez su à l'invite de ligne de commande pour devenir racine (« super utilisateur »).

2. Modifiez `/etc/init.d/syslogd` et ajoutez « -r » à la variable `SYSLOGD` en haut du fichier. La ligne que vous modifiez ressemblera à ceci :

`SYSLOGD= « -r »`

Consultez les pages man pour obtenir plus d'informations sur les options de commande `syslogd`. (Entrez `man syslogd` dans la ligne de commande.)

3. Si vous souhaitez envoyer tous les messages dans un fichier, modifiez `/etc/syslog.conf`.

Par exemple, vous pouvez ajouter cette ligne pour envoyer tous les messages à un fichier journal appelé « `AP_syslog` » :

`*.* -/tmp/AP_syslog`

Consultez les pages man pour obtenir plus d'informations sur les options de commande `syslogd.conf`. (Entrez `man syslogd.conf` dans la ligne de commande.)

4. Redémarrez le serveur syslog en tapant le code suivant dans l'invite de ligne de commande :

`/etc/init.d/syslogd restart`



*Remarque : Le processus syslog utilisera par défaut le port **514**. Nous vous conseillons de conserver ce port par défaut. Cependant, si vous choisissez de reconfigurer le port du journal, assurez-vous que le numéro de port que vous avez attribué à syslog n'est pas utilisé par un autre processus.*

11.2.4.3 Activation/désactivation de l'hôte de relais de journal sur la page Status > Events (État > Événements)

Pour activer et configurer le relayage de journal sur la page *Status > Events* (État > Événements), définissez les options *Log Relay* (Relais de journal) et procédez comme indiqué ci-dessous, puis cliquez sur **Update** (Mettre à jour).

☒ Relay Log

Relay Host

Relay Port

Tableau 11.3 Paramètres de l'hôte de relais de journal

Champ	Description
<i>Relay Log</i> (Journal de relais)	Choisissez d'activer ou de désactiver l'utilisation de l'hôte de relais de journal : Si vous cochez la case Relay log (Relais de journal), l'hôte de relais de journal est activé et les champs <i>Relay Host</i> (Hôte de relais) et <i>Relay Port</i> (Port de relais) sont modifiables.
<i>Relay Host</i> (Hôte de relais)	Spécifiez le nom <i>IP Address - Adresse IP</i> ou <i>DNS</i> de l'hôte de relais. <i>Remarque : Si vous utilisez Devicescape Wireless Operations Center, le serveur de référentiel doit recevoir les messages syslog de tous les points d'accès. Dans ce cas, utilisez l'adresse IP du serveur de référentiel du centre d'opérations comme hôte de relais.</i>
<i>Relay Port</i> (Port de relais)	Indiquez le numéro de port pour le processus syslog sur l'hôte de relais. Le port par défaut est 514 .

Mettre à jour les paramètres

Pour appliquer vos modifications, cliquez sur **Update** (Mettre à jour).

Si vous avez *activé* l'hôte de relais de journal, cliquer sur **Update** (Mettre à jour) activera la journalisation à distance. Le point d'accès envoie ses messages du noyau en temps réel pour l'affichage à l'écran du serveur de journal distant, dans un fichier journal de noyau spécifié ou un autre périphérique, selon la manière dont vous avez configuré l'hôte de relais de journal.

Si vous avez *désactivé* l'hôte de relais de journal, cliquer sur **Update** (Mettre à jour) désactivera la journalisation à distance.

11.2.5 Journal des événements

Le journal des événements indique les événements système sur le point d'accès comme l'association des stations, leur authentification, ainsi que d'autres occurrences. Le journal des événements en temps réel est toujours affiché sur la page d'interface utilisateur Web d'administration *Status > Events* (États > Événements) pour le point d'accès que vous contrôlez.

11.3 Statistiques d'émission/réception

Pour afficher les statistiques d'émission/réception d'un point d'accès particulier, accédez à *Status > Transmit/Receive* (États > Émission/réception) sur les pages Web d'administration pour le point d'accès que vous souhaitez contrôler.



Remarque : La Figure 11.3 montre la page d'émission/réception pour un point d'accès de radio professionnelle. La page Web d'administration pour le point d'accès de radio unique est légèrement différent.

Figure 11.3 Page de statistiques d'émission et de réception

Basic Settings	View transmit and receive statistics for this access point			
User Management				
Cluster				
Access Points				
Sessions				
Channel Management				
Wireless Neighborhood				
Security				
Status				
Interfaces				
Events				
Transmit/Receive				
Client Associations				
Neighboring Access Points				
Manage				
Ethernet Settings				
802.11 Settings				
802.11 Advanced Settings				
VWN				

Type	Ethernet		Radio	
Name	Guest	Internal	Guest	
IP Address	10.128.75.4			
MAC Address	00:08:A2:01:4B:52	00:00:00:00:00:00	00:08:A2:01:4B:56	n/a
VLAN ID				
Name (SSID)		SFG	TEKLOGIX GUEST	

Transmit

Type	Ethernet		Radio	
Name	Guest	Internal	Guest	
Total packets	11329	0	4622	0
Total bytes	3482589	0	649463	0
Errors	0	0	2	0

Receive

Type	Ethernet		Radio	
Name	Guest	Internal	Guest	
Total packets	833047	0	37	0
Total bytes	89628621	0	3190	0
Errors	0	0	0	0

Cette page fournit des informations de base sur le point d'accès et un affichage en temps réel des statistiques d'émission et de réception pour ce point d'accès comme indiqué dans le tableau 11.4 à la page 135. Toutes les statistiques d'émission et de réception présentées sont des totaux remontant au dernier démarrage du point d'accès. Si le point d'accès est redémarré, ces chiffres indiquent les totaux d'émission/réception totaux depuis le redémarrage.

Tableau 11.4 Statistiques d'émission/réception

Champ	Description
<i>IP Address</i> (Adresse IP)	<i>IP Address - Adresse IP</i> pour le point d'accès.
<i>MAC Address</i> (Adresse MAC)	Adresse Media Access Control (MAC) pour l'interface spécifiée. Une adresse MAC est un adresse matérielle unique et permanent pour tout appareil qui représente une interface pour le réseau. L'adresse MAC est attribuée par le fabricant. La passerelle sans fil 9160 G2 Wireless Gateway dispose d'une adresse MAC unique pour chaque interface. Un point d'accès radio professionnelle dispose d'une adresse MAC différente pour chaque interface sur chacune de ses deux radios.
<i>VLAN ID</i> (ID VLAN)	ID <i>LAN</i> virtuel (VLAN). Un réseau local virtuel (VLAN) est un regroupement logique et logiciel d'appareils sur un réseau qui leur permet d'agir comme s'ils étaient connectés à un seul réseau physique, même si ce n'est peut-être pas le cas. Les VLAN peuvent être utilisés pour établir des réseaux internes et invité sur le même point d'accès.
<i>Name (SSID)</i> (Nom (SSID))	Nom de réseau sans fil. Également appelé SSID , cette touche alphanumérique identifie de manière unique un réseau local sans fil. Le SSID est défini sur l'onglet Basic Settings (Paramètres de base). (Reportez-vous au « Fournir des paramètres réseau » on page 51.)
Informations d'émission et de réception	
<i>Total Packets</i> (Nombre total de paquets)	Indique le nombre total de paquets envoyés (dans le tableau d'émission) ou reçus (dans le tableau de réception) par ce point d'accès.
<i>Total Bytes</i> (Nombre total d'octets)	Indique le nombre total d'octets envoyés (dans le tableau d'émission) ou reçus (dans le tableau de réception) par ce point d'accès.
<i>Errors</i> (Erreurs)	Indique le nombre total d'erreurs associées à l'envoi et la réception de données sur ce point d'accès.

11.4 Clients sans fil associés

Pour afficher les stations client associées à un point d'accès particulier, accédez à *Status > Client associations* (État > Associations client) sur les pages Web d'administration pour le point d'accès que vous souhaitez contrôler.

Les stations associées s'affichent avec des informations sur le trafic de paquets émis et reçus pour chaque station (voir la Figure 11.4 à la page 136).

Figure 11.4 Stations client associées

Basic Settings	View list of currently associated client stations							
User Management								
Cluster								
Access Points	Network	Station	Status		From Station		To Station	
Sessions			Authenticated	Associated	Packets	Bytes	Packets	Bytes
Channel Management	wlan0	00:0c:f1:3e:99:ae	Yes	Yes	1732	261063	1517	510274
Wireless Neighborhood	wlan0	00:90:4b:93:f4:35	Yes	Yes	687	123005	572	155409
Security								
Status								
Interfaces								
Events								
Transmit/Receive								
Client Associations								
Neighboring Access Points								

11.4.1 Contrôle d'intégrité de la liaison

La passerelle sans fil 9160 G2 Wireless Gateway assure *le contrôle d'intégrité de la liaison* pour vérifier en permanence sa connexion à chaque client associé (même lorsqu'il n'y a aucun échange de données en cours). Pour ce faire, le point d'accès envoie des paquets de données aux clients à quelques secondes d'intervalles lorsqu'il n'y a aucun autre trafic. Cela permet au point d'accès de détecter lorsqu'un client est hors de portée, même pendant des périodes où aucun trafic normal n'a lieu. La connexion du client est supprimée de la liste des clients associés dans les 300 secondes qui suivent la disparition d'un client, même s'il n'est pas dissocié (mais qu'il est hors de portée).

11.5 Points d'accès voisins

La page d'état des « points d'accès voisins » fournit des statistiques en temps réel pour tous les points d'accès à portée du point d'accès dont vous consultez les pages Web d'administration. Pour afficher des informations sur d'autres points d'accès sur le réseau sans fil, accédez à *Status > Neighboring Access Points* (État > Points d'accès voisins) (voir la Figure 11.5 à la page 137).

Figure 11.5 État des points d'accès voisins

View neighboring access points													
AP Detection <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled <input type="button" value="Update"/>													
MAC	Beacon Int.	Type	SSID	Privacy	WPA	Band	Channel	Rate	Signal	Beacons	Last Beacon	Rates	
00:08:a2:01:13:20	100	AP		On	Off	2.4	11	1		2	Fri Jan 2 06:33:01 1970	1,2,5,5,6,9,11,12,18,24,36,48,54	
00:08:a2:01:22:34	100	AP		On	On	2.4	3	1		3	Fri Jan 2 06:31:23 1970	1,2,5,5,6,9,11,12,18,24,36,48,54	
00:08:a2:01:12:fc	100	AP		On	Off	2.4	6	1		1	Fri Jan 2 06:26:45 1970	1,2,5,5,6,9,11,12,18,24,36,48,54	
00:08:a2:01:22:30	100	AP		On	On	2.4	6	1		1	Fri Jan 2 06:26:07 1970	1,2,5,5,6,9,11,12,18,24,36,48,54	
00:08:a2:02:73:e4	100	AP	steve	On	On	2.4	6	1		6616	Fri Jan 2 06:34:40 1970	1,2,5,5,6,9,11,12,18,24,36,48,54	

Les informations fournies sur les points d'accès voisins sont décrites dans le Tableau 11.5.

Tableau 11.5 Statistiques des points d'accès voisins

Champ	Description
<i>MAC (MAC)</i>	<p>Affiche l'adresse MAC du point d'accès voisin.</p> <p>Une adresse MAC est une adresse matérielle qui identifie de façon unique chaque nœud d'un réseau.</p>
<i>Radio (Radio)</i>	<p>Points d'accès de radio professionnelle</p> <p>Si le point d'accès qui « fait la détection » de points d'accès voisins est un point d'accès de radio professionnelle, le champ Radio (Radio) est inclus.</p> <p>Le champ Radio (Radio) indique sur quelle radio le point d'accès voisin a été détecté :</p> <ul style="list-style-type: none">• wlan0 (radio un)• wlan1 (radio deux) <p>Points d'accès de radio unique</p> <p>Ce champ n'est pas inclus sur les pages <i>Neighboring Access Points</i> (Points d'accès voisins) des points d'accès d'une radio unique.</p>
<i>Beacon Int. (Interv. de balise)</i>	<p>Affiche l'intervalle Beacon - Balise utilisé par ce point d'accès.</p> <p>Les trames de balise sont transmises par un point d'accès à intervalles réguliers pour annoncer l'existence du réseau sans fil. Le comportement par défaut est d'envoyer une trame de balise une fois toutes les 100 millisecondes (soit 10 par seconde).</p> <p>L'intervalle de balise est défini sur l'onglet <i>Manage > 802.11 Advanced Settings</i> (Gérer > Paramètres avancés 802.11). (Reportez-vous au Chapitre 16 : « Configuration des paramètres radio 802.11 ».)</p>
<i>Capability (Capacité)</i>	<p>Un nombre hexadécimal qui, une fois converti en binaire, indique chaque fonction ou fonctionnalité IEEE 802.11 et si elle est « activée » ou « désactivée » sur ce point d'accès.</p>

Tableau 11.5 Statistiques des points d'accès voisins (Suite)

Champ	Description
Type (Type)	<p>Indique le type d'appareil :</p> <ul style="list-style-type: none">• AP (point d'accès) indique que l'appareil voisin est un point d'accès qui prend en charge la norme IEEE 802.11 <i>Wireless Networking Framework - Infrastructure de réseau sans fil</i> dans <i>Infrastructure Mode - Mode infrastructure</i>.• Ad hoc indique une station voisine s'exécutant dans <i>Ad hoc Mode - Mode Ad-hoc</i>. Les stations définies sur le mode ad-hoc communiquent directement entre elles sans l'utilisation d'un point d'accès traditionnel. Le mode ad-hoc est une norme <i>Wireless Networking Framework - Infrastructure de réseau sans fil</i> IEEE 802.11 également appelée mode « <i>poste-à-poste</i> » ou <i>Independent Basic Service Set (IBSS)</i>.
SSID (SSID)	<p>Le <i>Service Set Identifier ou identifiant d'ensemble de services (SSID)</i> pour le point d'accès.</p> <p>Le SSID est une chaîne alphanumérique d'un maximum de 32 caractères qui identifie de façon unique un réseau local sans fil. Il est également appelé « <i>nom de réseau</i> ».</p> <p>Le SSID est défini dans les paramètres de base. (Reportez-vous au Chapitre 5 : « Configuration des paramètres de base ») ou dans <i>Manage > Wireless Settings</i> (Gérer > Paramètres sans fil) (reportez-vous au Chapitre 13 : « Définition de l'interface sans fil ».)</p> <p>Un réseau invité et un réseau interne exécutés sur le même point d'accès doivent toujours avoir deux noms de réseau différents.</p>
Privacy (Confidentialité)	<p>Indique si l'appareil voisin est sécurisé ou non.</p> <ul style="list-style-type: none">• Off (Désactivé) indique que le mode de sécurité de l'appareil voisin est défini sur « <i>None</i> » (Aucun) (pas de sécurité).• On (Activé) indique que l'appareil voisin a une sécurité en place. <p>La sécurité est configurée sur le point d'accès dans l'onglet <i>Security</i> (Sécurité). Pour plus d'informations sur les paramètres de sécurité, reportez-vous au Chapitre 10 : « Configuration de la sécurité ».</p>
WPA (WPA)	<p>Indique si la sécurité <i>WPA</i> est activée ou désactivée sur ce point d'accès.</p>
Band (Bande)	<p>Cette option indique le mode IEEE 802.11 utilisé sur ce point d'accès. (Par exemple, <i>IEEE 802.11a</i>, <i>IEEE 802.11b</i>, <i>IEEE 802.11g</i>.)</p> <p>Le nombre affiché indique le mode selon la carte suivante :</p> <ul style="list-style-type: none">• 2.4 Indique le mode IEEE 802.11b ou IEEE 802.11g.• 5 Indique le mode IEEE 802.11a.

Tableau 11.5 Statistiques des points d'accès voisins (Suite)

Champ	Description
<i>PHY (PHY)</i>	<p>Cette option indique le mode IEEE 802.11 utilisé sur ce point d'accès. (Par exemple, <i>IEEE 802.11a</i>, <i>IEEE 802.11b</i>, <i>IEEE 802.11g</i>)</p> <p>Le nombre affiché indique le mode selon la carte suivante :</p> <ul style="list-style-type: none">• 4 indique le mode IEEE 802.11b• 7 indique le mode IEEE 802.11g• 8 indique le mode IEEE 802.11a• 256 indique le mode Atheros Turbo
<i>Channel (Canal)</i>	<p>Affiche le canal sur lequel le point d'accès diffuse actuellement.</p> <p>Le Channel - Canal définit la partie du spectre que la radio utilise pour émettre et recevoir.</p> <p>Le canal est défini dans les <i>paramètres de la radio</i>. (Reportez-vous au Chapitre 16 : « Configuration des paramètres radio 802.11 ».)</p>
<i>Rate (Débit)</i>	<p>Indique le débit (en mégabits par seconde) auquel le point d'accès émet actuellement.</p> <p>Le débit actuel sera toujours l'un des débits pris en charge dans <i>Rates</i> (Débits).</p>
<i>Signal (Signal)</i>	<p>Indique la force du signal radio émettant de ce point d'accès, mesuré en décibels (dB).</p>

Tableau 11.5 Statistiques des points d'accès voisins (Suite)

Champ	Description
<i>ERP (ERP)</i>	<p>Le <i>protocole ERP (Extended Rate Protocol) (ERP)</i> fait référence au protocole utilisé par les stations <i>IEEE802.11g</i>.</p> <p>Ce champ indique comment une station client 802.11g <i>IEEE</i> qui utilise ce point d'accès doit envoyer des données lorsqu'il y a des stations ou des points d'accès <i>IEEE 802.11b</i> (non ERP) présents sur le même canal que la station <i>IEEE 802.11g</i> (ERP).</p> <p>Si une station <i>IEEE 802.11g</i> détermine qu'il existe un ou plusieurs nœuds <i>IEEE 802.11b</i> sur le réseau qui utilisent le même canal qu'elle, elle activera la protection <i>Request to Send (RTS)</i> et <i>Clear to Send (CTS)</i>.</p> <p>Le numéro qui apparaît sur l'interface utilisateur actuelle est un nombre hexadécimal qui, une fois converti en binaire, indique comment l'indicateur ERP est défini.</p> <p>Utilisez la carte suivante pour déterminer le paramètre ERP actuel pour ce point d'accès.</p> <ul style="list-style-type: none">• 0X0 indique « Aucun ». Il n'y a aucune station <i>IEEE 802.11b</i> (non ERP) présente.• 0X1 indique qu'un appareil <i>IEEE 802.11b</i> (non ERP) est présent. Ce point d'accès dispose d'une station <i>IEEE 802.11b</i> uniquement. (Cet indicateur ne doit jamais être utilisé de manière autonome.)• 0X2 indique que les stations <i>IEEE 802.11g</i> doivent utiliser la protection RTS/CTS. Il y a un autre point d'accès sur le même canal avec des stations client <i>IEEE 802.11b</i>.• 0X3 indique qu'il y a un appareil non ERP présent et que les stations <i>IEEE 802.11g</i> doivent utiliser la protection RTS/CTS.• 0X4 indique que les stations <i>IEEE 802.11g</i> radio doivent utiliser le préambule Barker.• 0X5 indique que les stations <i>IEEE 802.11g</i> doivent utiliser le même protocole que 0x1 mais avec le préambule Barker.• 0X6 indique que les stations <i>IEEE 802.11g</i> doivent utiliser le même protocole que 0x2 mais avec le préambule Barker.• 0X7 indique que les stations <i>IEEE 802.11g</i> doivent utiliser le même protocole que 0x3 mais avec le préambule Barker.
<i>Beacons (Balises)</i>	<p>Affiche le nombre total de balises émises par ce point d'accès depuis son dernier démarrage.</p>
<i>Last Beacon (Dernière balise)</i>	<p>Indique la date et l'heure de l'émission de la balise la plus récente depuis le point d'accès.</p>
<i>Rates (Débits)</i>	<p>Affiche les ensembles de débits pris en charge et basiques (annoncés) pour le point d'accès voisin. Les débits sont affichés en mégabits par seconde (Mbit/s).</p> <p>Tous les débits pris en charge sont répertoriés, avec les débits de base affichés en gras.</p> <p>Les ensembles de débits sont configurés dans les <i>paramètres de la radio</i>. (Reportez-vous au Chapitre 16 : « Configuration des paramètres radio 802.11 ».) Les débits indiqués pour un point d'accès seront toujours les débits actuellement définis pour ce point d'accès dans les <i>paramètres de la radio</i>.</p>

L'INTERFACE ÉTHERNET (FILAIRE)

12

12.1 Accès aux paramètres Ethernet (filaire).	143
12.1.1 DNS Hostname (Nom d'hôte DNS).	144
12.1.2 Accès invité	144
12.1.2.1 Configuration d'un réseau LAN interne et d'un réseau invité	144
12.1.2.2 Activation ou désactivation de l'accès invité	145
12.1.2.3 Spécification d'un réseau invité virtuel	145
12.1.3 Réseaux sans fil virtuels (VLAN).	146
12.1.4 Paramètres de l'interface interne	147
12.1.5 Paramètres de l'interface invité	150
12.1.6 Mise à jour des paramètres	150

Les paramètres Ethernet (filaire) décrivent la configuration de votre réseau local (**LAN Ethernet**).



*Remarque : Les paramètres Ethernet ne sont pas partagés sur le cluster. Ces paramètres doivent être configurés individuellement sur les pages d'administration pour chaque point d'accès. Pour trouver les pages d'administration pour un point d'accès qui est membre du cluster en cours, cliquez sur son lien d'**adresse IP** dans la page Cluster > Access Points (Cluster > Points d'accès) du point d'accès en cours. Pour plus d'informations sur les paramètres qui sont partagés par le cluster, reportez-vous à la section « Quels paramètres sont/ne sont pas partagés dans le cadre de la configuration du cluster ? » à la page 59.*

12.1 Accès aux paramètres Ethernet (filaire)

Pour configurer l'adresse « filaire » et les paramètres associés sur la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway, accédez à l'onglet *Manage > Ethernet Settings* (Gérer > Paramètres Ethernet) et mettez à jour les champs comme décrit dans les sections suivantes.

Figure 12.1 Présentation des paramètres Ethernet

Basic Settings	Modify Ethernet (Wired) settings	
User Management	DNS Hostname <input type="text" value="PTX9160-Wireless-AP"/>	
Cluster	Guest Access <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
Access Points	For Guest Access <input type="text" value="VLAN on Ethernet Port"/>	
Sessions	Virtual Wireless Networks (Using VLANs on Ethernet Port 1) <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
Channel Management	Internal Interface Settings	
Wireless Neighborhood	MAC Address <input type="text" value="00:08:A2:01:4B:52"/>	
Security	VLAN ID <input type="text" value="2"/>	
Status	Management VLAN ID <input type="text" value="2"/>	
Interfaces	Untagged VLAN <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Events	Untagged VLAN ID <input type="text" value="1"/>	
Transmit/Receive	Connection Type <input type="text" value="DHCP"/>	
Client Associations	Static IP Address <input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="10"/>	
Neighboring Access Points	Subnet Mask <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>	
Manage	Default Gateway <input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="254"/>	
Ethernet Settings	DNS Settings via DHCP <input checked="" type="radio"/> On <input type="radio"/> Off	
802.11 Settings	DNS Nameservers <input type="text" value=""/> . <input type="text" value=""/> . <input type="text" value=""/> . <input type="text" value=""/>	
802.11 Advanced Settings	DNS Domain <input type="text" value="example.com"/>	
VWN	Guest Interface Settings	
WDS	MAC Address <input type="text" value="00:00:00:00:00:00"/>	
Guest Login	VLAN ID <input type="text" value=""/>	
MAC Filtering	Subnet <input type="text" value="n/a"/>	
Load Balancing	<input type="button" value="Update"/>	
Services		
QoS		

12.1.1 DNS Hostname (Nom d'hôte DNS)

Tableau 12.1 Définir le nom DNS

Champ	Description
<i>DNS Hostname</i> (Nom d'hôte DNS)	<p>Saisissez le nom DNS du point d'accès dans la zone de texte.</p> <p>Il s'agit du nom d'hôte. Il peut être fourni par votre fournisseur de services Internet ou votre administrateur réseau, ou vous pouvez fournir le vôtre.</p> <p>Les règles des noms de système sont les suivantes :</p> <ul style="list-style-type: none">• Ce nom peut comporter jusqu'à 20 caractères.• Seuls des lettres, des chiffres et des tirets sont autorisés.• Le nom doit commencer par une lettre et se terminer par une lettre ou un chiffre.

12.1.2 Accès invité

Vous pouvez fournir un accès invité contrôlé sur un réseau isolé et un **LAN** interne sécurisé sur la même passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway.

12.1.2.1 Configuration d'un réseau LAN interne et d'un réseau invité

Un *réseau local (LAN)* est un réseau de communications couvrant une zone limitée, par exemple, un étage d'un bâtiment. Un LAN relie plusieurs ordinateurs et d'autres appareils réseau tels que stockage et imprimantes.

Ethernet est la technologie la plus courante mettant en œuvre un réseau local (LAN).
WI-FI (IEEE) est une autre technologie LAN très populaire.

La passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway vous permet de configurer deux LAN différents sur le même point d'accès : l'un pour un LAN *interne* sécurisé et un autre pour un réseau *invité* public sans sécurité et avec un accès limité aux ressources internes. Pour configurer ces réseaux, vous devez fournir des paramètres sans fil et Ethernet (filaire).

Des informations sur la manière de configurer les paramètres Ethernet (filaire) sont fournies dans les sections ci-dessous.

(Pour plus d'informations sur la manière de configurer les paramètres sans fil, reportez-vous au Chapitre 13 : « Définition de l'interface sans fil ». Pour une présentation de la configuration de l'interface invité, reportez-vous au Chapitre 14 : « Configuration de l'accès invité ».)

12.1.2.2 Activation ou désactivation de l'accès invité

La passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway est livrée avec la fonctionnalité d'accès invité **désactivée** par défaut. Si vous souhaitez fournir l'accès invité sur votre point d'accès, activez l'accès invité sur l'onglet *Ethernet (Wired) Settings* (Paramètres Ethernet (filaire)).

Tableau 12.2 Activation/désactivation de l'accès invité

Champ	Description
<i>Guest Access</i> (Accès invité)	Par défaut, la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway est livrée avec l'accès invité désactivé . <ul style="list-style-type: none">• Pour activer l'accès invité, cliquez sur Enabled (Activé).• Pour désactiver l'accès invité, cliquez sur Disabled (Désactivé).

12.1.2.3 Spécification d'un réseau invité virtuel

Si vous activez Guest Access (Accès invité), vous devez créer un réseau *virtuel* « interne » et « invité » sur ce point d'accès en connectant le port LAN du point d'accès à un port balisé sur un commutateur compatible **VLAN**, puis définir deux réseaux LAN virtuels différents sur cette page d'administration. (Pour plus d'informations, reportez-vous au Chapitre 14 : « Configuration de l'accès invité ».) Créez les LAN interne et invité virtuellement distincts, comme indiqué dans le Tableau 12.3.

Tableau 12.3 Spécification d'un réseau invité virtuel

Champ	Description
<i>Guest Access</i> (Accès invité)	<ul style="list-style-type: none">• Sélectionnez Enabled (Activé) pour activer l'accès invité. (Si vous choisissez cette option, vous devez sélectionner les réseaux locaux virtuels (VLAN) sur le paramètre suivant, <i>For Guest Access</i> (Pour l'accès invité), puis fournissez des détails sur le VLAN pour le réseau invité sur le reste de la page.)• Sélectionnez Disabled (Désactivé) pour désactiver l'accès invité.

Tableau 12.3 Spécification d'un réseau invité virtuel

Champ	Description
<i>For Guest Access (Pour l'accès Invité)</i>	<p>Spécifiez un réseau invité <i>virtuellement</i> distinct sur ce point d'accès :</p> <ul style="list-style-type: none">• Comme le point d'accès utilise une seule connexion physique à votre réseau LAN interne, choisissez VLAN on Ethernet Port 1 (VLAN sur le port Ethernet 1) dans le menu déroulant. Cela permet d'activer les paramètres « VLAN » où vous devez fournir un ID VLAN. Reportez-vous à la section « Paramètres de l'interface invité » à la page 150. <p><i>Important : Si vous reconfigurez les interfaces invité et interne pour utiliser des VLAN, vous risquez de perdre la connectivité au point d'accès. Pour commencer, veillez à vérifier que le commutateur et le serveur DHCP que vous utilisez peuvent prendre en charge les VLAN via la norme IEEE 802.1Q. Après avoir configuré le VLAN dans la page Manage > Ethernet Settings (Gérer > Paramètres Ethernet), rebranchez physiquement le câble Ethernet au commutateur sur le port (VLAN) paquet balisé. Ensuite, reconnectez-vous à la nouvelle adresse IP via les pages Web d'administration. (Si nécessaire, consultez l'administrateur d'assistance technique d'infrastructure au sujet des configurations VLAN et DHCP.)</i></p>

12.1.3 Réseaux sans fil virtuels (VLAN)

Si vous souhaitez configurer le réseau interne comme VLAN (que vous disposiez d'un réseau invité configuré ou non), vous pouvez activer « Virtual Wireless Networks (VLAN) » sur le point d'accès.

Vous devez activer cette fonctionnalité si vous souhaitez configurer d'autres réseaux virtuels en VLAN dans l'onglet *Manage > VWN* (Gérer > VWN) comme décrit dans la section « Configuration de VLAN » à la page 169.

Tableau 12.4 Activation des réseaux sans fil virtuels (VLAN)

Champ	Description
<i>Virtual Wireless Networks (Using VLANs on Ethernet Port 1) - VLAN (Utilisation des réseaux VLAN sur le port Ethernet 1)</i>	<ul style="list-style-type: none">• Sélectionnez <i>Enabled</i> (Activé) pour activer les VLAN pour le réseau interne et d'autres réseaux. (Si vous choisissez cette option, vous pouvez exécuter le réseau interne sur un VLAN si vous avez Guest Access (Accès invité) configuré et que vous pouvez configurer d'autres réseaux en VLAN dans l'onglet <i>Manage > VWN</i> (Gérer > VWN) comme décrit dans la section « Configuration de VLAN » à la page 169.)• Sélectionnez <i>Disabled</i> (Désactivé) pour désactiver le VLAN pour le réseau interne, et d'autres réseaux virtuels sur ce point d'accès.

12.1.4 Paramètres de l'interface interne

Pour configurer les paramètres Ethernet (filaire) pour le LAN interne, renseignez les champs comme indiqué dans le Tableau 12.5.

Tableau 12.5 Paramètres Ethernet pour réseau LAN interne

Champ	Description
<i>MAC Address</i> (Adresse MAC)	Affiche l'adresse MAC de l'interface interne pour le port Ethernet sur ce point d'accès. Il s'agit d'un champ en lecture seule que vous ne pouvez pas modifier.
<i>VLAN ID</i> (ID VLAN)	<p>Si vous choisissez de configurer les réseaux interne et invité par « VLAN », ce champ est activé.</p> <p>Fournissez un nombre entre 1 et 4094 pour le VLAN interne.</p> <p>Ainsi, le point d'accès enverra les requêtes DHCP avec la balise VLAN. Le commutateur et le serveur DHCP doivent prendre en charge les trames IEEE 802.1p VLAN. Le point d'accès pouvoir atteindre le serveur DHCP.</p> <p>Consultez l'administrateur au sujet des configurations VLAN et DHCP.</p>
<i>Management VLAN ID</i> (ID VLAN de gestion)	<p>Si vous avez activé les VWN ou l'accès invité par VLAN, ce champ est activé.</p> <p>Entrez une valeur pour Management VLAN ID (ID VLAN de gestion). Cet ID peut avoir une valeur comprise entre 1 et 4094.</p> <p>L'ID VLAN de gestion vous permet de spécifier le VLAN utilisé pour gérer les points d'accès. Vous pouvez ensuite gérer le point d'accès via l'interface utilisateur Web, l'interface de ligne de commande et SNMP en utilisant ce VLAN.</p> <p>Si Connection Type (Type de connexion) est défini sur DHCP, le point d'accès enverra des requêtes DHCP avec la balise VLAN. Le commutateur et le serveur DHCP doivent prendre en charge les trames IEEE 802.1Q VLAN. Le point d'accès pouvoir atteindre le serveur DHCP.</p> <p>Il n'y a aucune restriction sur l'ID VLAN de gestion que vous spécifiez. L'ID VLAN de gestion peut être le même que l'ID VLAN interne, l'ID VLAN invité, un ID VLAN VWN ou l'ID VLAN non balisé.</p>
<i>Untagged VLAN</i> (VLAN non balisé)	<p>Si vous avez activé des VWN ou un accès invité via VLAN, vous pouvez activer ou désactiver les VLAN non balisés.</p> <p>Sélectionnez Enabled (Activé) pour activer <i>Untagged VLAN</i> (VLAN non balisé).</p> <p>Sélectionnez Disabled (Désactivé) pour désactiver <i>Untagged VLAN</i> (VLAN non balisé).</p> <p>Si <i>Untagged VLAN</i> (VLAN non balisé) est activé, les paquets reçus sans balise VLAN seront traités comme s'ils étaient reçus avec l'ID VLAN non balisé spécifié.</p> <p>Si <i>Untagged VLAN</i> (VLAN non balisé) est désactivé, les paquets reçus sans balise VLAN sont pontés vers des liaisons WDS, mais ne sont pas autrement utilisés par le point d'accès.</p>

Tableau 12.5 Paramètres Ethernet pour réseau LAN interne (Suite)

Champ	Description
<i>Untagged VLAN ID (ID VLAN non balisé)</i>	<p>Si vous avez activé <i>Untagged VLAN</i> (VLAN non balisé), ce champ est activé.</p> <p>Entrez une valeur pour <i>Untagged VLAN ID</i> (ID VLAN non balisé). Cet ID peut avoir une valeur comprise entre 1 et 4094.</p> <p>Il n'y a aucune restriction sur l'ID VLAN non balisé que vous spécifiez. L'ID VLAN non balisé peut être le même que l'ID VLAN interne, l'ID VLAN invité, un ID VLAN VWN ou l'ID VLAN de gestion.</p>
<i>Connection Type (Type de connexion)</i>	<p>Vous pouvez sélectionner DHCP ou Static IP (IP statique).</p> <p><i>Dynamic Host Configuration Protocol (DHCP)</i> est un protocole définissant la manière dont un serveur centralisé peut fournir les informations de configuration du réseau aux appareils du réseau. Un serveur DHCP « offre » une « location » au système client. Les informations fournies incluent les adresses IP et le masque réseau, plus l'adresse de ses serveurs DNS et de sa passerelle.</p> <p><i>Static IP</i> (IP statique) indique que tous les paramètres du réseau sont fournis manuellement. Vous devez fournir l'adresse IP pour la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway, son masque de sous-réseau, l'adresse IP de la passerelle par défaut et l'adresse IP d'au moins un serveur de noms DNS.</p> <p>Si vous sélectionnez DHCP, la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway acquerra son adresse IP, masque de sous-réseau et ses informations DNS et de passerelle des serveurs DHCP.</p> <p>Dans le cas contraire, si vous sélectionnez Static IP (IP statique), renseignez les éléments décrits dans <i>Static IP Settings</i> (Paramètres IP statique).</p> <p>Important : <i>Si vous ne disposez pas d'un serveur DHCP sur le réseau interne et que vous n'avez pas l'intention d'en utiliser un, la première chose à faire depuis le point d'accès est de changer le type de connexion DHCP en IP statique. Lorsque vous modifiez le type de connexion à IP statique, vous pouvez attribuer une nouvelle Static IP Address - Adresse IP statique au point d'accès ou continuer à utiliser l'adresse par défaut. Nous vous recommandons d'attribuer une nouvelle adresse pour que, si plus tard vous ajoutez une autre Passerelle sans fil 9160 G2 Wireless Gateway sur le même réseau, les adresses IP des deux points d'accès restent uniques.</i></p> <p>Si vous avez besoin de restaurer l'adresse IP statique par défaut, vous pouvez le faire en réinitialisant le point d'accès aux paramètres d'usine par défaut, comme indiqué dans la section « Réinitialisation de la configuration d'usine par défaut » à la page 334.</p>
<i>Static IP Address (Adresse IP statique)</i>	<p>Si vous avez choisi Static IP (IP statique) comme type de connexion, ces champs sont activés.</p> <p>Saisissez l'adresse IP statique dans les zones de texte.</p>

Tableau 12.5 Paramètres Ethernet pour réseau LAN interne (Suite)

Champ	Description
<i>Subnet Mask</i> (Masque de sous-réseau)	Entrez le masque de sous-réseau dans les zones de texte. Vous devez obtenir ces informations auprès de votre fournisseur de services Internet ou votre administrateur réseau.
<i>Default Gateway</i> (Passerelle par défaut)	Entrez la passerelle par défaut dans les zones de texte.
<i>DNS Settings via DHCP</i> (Paramètres DNS via DHCP)	<p><i>Domain Name Service (DNS)</i> est un système qui résout le nom descriptif d'une ressource réseau à son adresse IP numérique. Vous pouvez choisir d'activer cette option ; les adresses IP des serveurs DNS seront automatiquement attribuées via DHCP. (Cette option est disponible uniquement si vous avez spécifié DHCP pour le champ <i>Connection Type</i> (Type de connexion).)</p> <p>Si vous choisissez Off (Désactivé), vous devez attribuer des adresses IP statiques manuellement.</p>
<i>DNS Nameservers</i> (Serveurs de noms DNS)	<p><i>Domain Name Service (DNS)</i> est un système qui résout le nom descriptif (<i>nomdedomaine</i>) d'une ressource réseau (par exemple, <i>www.psionteklogix.com</i>) à son adresse IP numérique (par exemple, 66.93.138.219). Un serveur DNS est appelé un <i>Nameserver</i> (<i>serveur de noms</i>).</p> <p>Il y a généralement deux serveurs de noms ; un serveur de noms principal et un serveur de noms secondaire.</p>
<i>DNS Domain</i> (Domaine DNS)	Identifiez le domaine des serveurs DNS.

12.1.5 Paramètres de l'interface invité

Pour configurer les paramètres Ethernet (filaire) pour l'interface « invité », renseignez les champs comme indiqué ci-dessous.

Tableau 12.6 Configuration des paramètres Ethernet de l'interface invité

Champ	Description
<i>MAC Address</i> (Adresse MAC)	Affiche l'adresse MAC de l'interface invité pour le port Ethernet sur ce point d'accès. Il s'agit d'un champ en lecture seule que vous ne pouvez pas modifier.
<i>VLAN ID</i> (ID VLAN)	Si vous choisissez de configurer les réseaux interne et invité par « VLAN », ce champ est activé . Fournissez un nombre entre 1 et 4094 pour le VLAN invité.
<i>Subnet</i> (Sous-réseau)	Affiche l'adresse de sous-réseau de l'interface invité. Par exemple, 192 . 168 . 1 . 0.

12.1.6 Mise à jour des paramètres

Pour mettre à jour les paramètres Ethernet :

1. Accédez à la page *Ethernet Settings* (Paramètres Ethernet).
2. Configurez les paramètres Ethernet selon les besoins.
3. Cliquez sur le bouton **Update** (Mettre à jour) pour appliquer les modifications.

DÉFINITION DE L'INTERFACE SANS FIL 13

13.1 Accès aux paramètres sans fil	153
13.2 Configuration de la prise en charge du domaine réglementaire 802.11d	154
13.3 802.11h Regulatory Domain Control (Contrôle du domaine réglementaire 802.11h)	155
13.4 Configuration de l'interface radio	156
13.5 Configuration des paramètres de LAN sans fil « interne »	157
13.6 Configuration des paramètres sans fil de réseau « invité »	158
13.7 Mise à jour des paramètres sans fil	158

La page *Wireless Settings* (Paramètres sans fil) décrit les aspects du réseau local (**LAN**) spécifiquement liés à l'appareil radio au niveau du point d'accès (mode **802.11** et **Channel - Canal**) et à l'interface réseau du point d'accès (adresse **MAC** du point d'accès et nom de réseau sans fil, également appelé **SSID**).

Les sections suivantes décrivent comment configurer l'adresse « sans fil » et les paramètres associés, y compris 802.IQv1, sur la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway.

13.1 Accès aux paramètres sans fil

Pour définir l'adresse sans fil d'un point d'accès, accédez à l'onglet *Manage > 802.11 Settings* (Gérer > Paramètres 802.11) pour ouvrir la page *Wireless Settings* (Paramètres sans fil) et mettre à jour les champs comme décrit ci-dessous.



Remarque : La Figure 13.1 montre la page des paramètres sans fil d'un point d'accès de radio professionnelle. La page Web d'administration du point d'accès de radio unique est légèrement différente.

Figure 13.1 Configuration des paramètres sans fil

Basic Settings	Modify wireless settings	
User Management	802.11d Regulatory Domain Support <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Cluster	IEEE802.11h support present.	
Access Points	Radio Interface	
Sessions	Mode	IEEE 802.11g ▼
Channel Management	Channel	6 ▼
Wireless Neighborhood	Internal Settings	
Security	MAC Address	00:08:A2:01:4B:56
Status	SSID	SFG
Interfaces	Guest Settings	
Events	MAC Address	
Transmit/Receive	SSID	TEKLOGIX GUEST
Client Associations	<input type="button" value="Update"/>	
Neighboring Access Points		
Manage		
Ethernet Settings		
802.11 Settings		
802.11 Advanced Settings		

13.2 Configuration de la prise en charge du domaine réglementaire 802.11d

Vous pouvez activer ou désactiver la prise en charge du domaine réglementaire IEEE *802.11d* pour diffuser les informations de code pays du point d'accès comme décrit ci-dessous.

Tableau 13.1 Activation de la prise en charge de la norme 802.11d

Champ	Description
<i>802.11d Regulatory Domain Support (Prise en charge du domaine réglementaire 802.11d)</i>	<p>L'activation de la prise en charge de la norme IEEE 802.11d sur le point d'accès déclenche la diffusion par le point d'accès du pays dans lequel il fonctionne parmi ses balises :</p> <ul style="list-style-type: none">• Pour activer la prise en charge du domaine réglementaire 802.11d, cliquez sur Enabled (Activé).• Pour désactiver la prise en charge du domaine réglementaire 802.11d, cliquez sur Disabled (Désactivé). Pour les points d'accès de radio professionnelle, deux adresses MAC sont affichées : une pour chaque radio sur l'interface interne. <p><i>Remarque : La norme IEEE 802.11d définit des règles standard pour le fonctionnement des réseaux LAN sans fil IEEE 802.11 dans n'importe quel pays sans devoir procéder à une nouvelle configuration. IEEE 802.11d permet aux stations client de fonctionner dans n'importe quel pays sans devoir procéder à une nouvelle configuration. Le point d'accès de référence Devicescape doit être configuré par le fabricant par l'intermédiaire des codes pays de l'interface de ligne de commande (CLI) pour fonctionner dans un pays donné.</i></p>

13.3 802.11h Regulatory Domain Control (Contrôle du domaine réglementaire 802.11h)

Tableau 13.2 Norme IEEE 802.11h

Champ	Description
<i>IEEE 802.11h</i>	<p>L'interface d'administration indique si le contrôle du domaine réglementaire IEEE 802.11h est en vigueur sur le point d'accès. IEEE 802.11h ne peut pas être désactivé par un administrateur utilisateur final. Les détails suivants ne sont fournis qu'à titre d'information.</p> <p>IEEE 802.11h est une norme qui offre deux services requis pour satisfaire certains domaines réglementaires pour la bande 5 GHz. Ces deux services sont le contrôle de la puissance de transmission (TPC) et la sélection dynamique des fréquences (DFS).</p> <ul style="list-style-type: none">• TPC nécessite que les réseaux radio (RLAN) fonctionnant sur la bande 5 GHz utilisent le contrôle de puissance de l'émetteur. Cela implique d'adhérer à une puissance de sortie maximale de transmission réglementaire et à une atténuation requise pour chaque canal autorisé. Il en résulte une réduction des interférences des services par satellite.• DFS nécessite que les RLAN fonctionnant dans la bande 5 GHz mettent en œuvre un mécanisme pour éviter un fonctionnement de canal commun avec des systèmes de radar et assurer une utilisation uniforme de tous les canaux disponibles. <p><i>Remarque : 802.11H est activé automatiquement si le point d'accès est configuré pour fonctionner dans n'importe quel pays qui nécessite 802.11h comme norme minimale. Cette norme n'est actuellement requise que par les pays appartenant à la catégorie European Telecommunications Standard Institute (ETSI). 802.11H est également activé pour le Japon.</i></p>

Pour le développeur de points d'accès, un certain nombre de points clés doivent être mémorisés par rapport à la norme IEEE **802.11h** :

- 802.11H ne fonctionne que pour la bande 802.11a. Ce n'est pas nécessaire pour 802.11b ou 802.11g.
- Si vous vous trouvez dans un domaine compatible 802.11h, la sélection de canal du BSS sera toujours « Auto » (Automatique). Même si un autre canal a été configuré, il est ignoré et la sélection automatique de canal aura lieu.
- Lorsque 802.11h est activé, le temps de démarrage initial augmente d'un minimum de soixante secondes. Il s'agit du délai minimum nécessaire pour balayer le canal sélectionné à la recherche d'interférences radar.
- Configurer les liaisons WDS peut être difficile lorsque 802.11h est opérationnel. Cela est dû au fait que les canaux de fonctionnement des deux points d'accès de la liaison WDS peuvent changer en fonction de l'utilisation des canaux et des interférences radar. WDS ne fonctionne que si les deux les points d'accès fonctionnent sur le même canal. Pour plus d'informations sur WDS, reportez-vous au Chapitre 20 : « Système de distribution sans fil (WDS) ».

13.4 Configuration de l'interface radio

L'interface radio vous permet de définir le **Channel - Canal** radio et le mode **802.11** selon la procédure décrite dans le Tableau 13.3.



Remarque : Sur un point d'accès de radio professionnelle, vous devez configurer ces paramètres d'interface radio pour l'interface radio un et l'interface radio deux.

Tableau 13.3 Paramètres de l'interface radio

Champ	Description
<i>MAC Addresses (Adresses MAC) (uniquement sur les points d'accès de radio professionnelle)</i>	<p>Indique les adresses Media Access Control (MAC) de l'interface.</p> <p>Sur les points d'accès de radio professionnelle, les adresses MAC de l'interface radio un (interne/invité) et l'interface radio deux (interne/invité) sont affichées.</p> <p>Une adresse MAC est une adresse matérielle unique et permanente pour tout appareil qui représente une interface pour le réseau. L'adresse MAC est attribuée par le fabricant. Vous ne pouvez pas modifier l'adresse MAC. Elle est fournie ici à titre d'information comme identifiant unique pour une interface.</p>
<i>Mode</i>	<p>Le <i>mode</i> définit la norme de <i>couche physique (PHY)</i> utilisée par la radio.</p> <p>La passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway est disponible sous forme d'un point d'accès monobande ou b bande pour radio unique ou professionnelle. Les options de configuration du mode varient en fonction du produit que vous avez.</p> <p>Point d'accès monobande : Pour le point d'accès monobande, sélectionnez l'un des modes suivants :</p> <ul style="list-style-type: none">• IEEE 802.11b• IEEE 802.11g <p>Point d'accès b bande : Pour le point d'accès b bande, sélectionnez l'un des modes suivants : un mode pour chaque interface radio.</p> <ul style="list-style-type: none">• IEEE 802.11b• IEEE 802.11g• IEEE 802.11a <p>Point d'accès de radio unique ou professionnelle :</p> <p>Si vous disposez d'un point d'accès de radio professionnelle, sélectionnez un mode IEEE 802.11 pour chacune des deux interfaces radio. (Pour un point d'accès de radio unique, il n'existe qu'une seule interface radio.)</p>

Tableau 13.3 Paramètres de l'interface radio

Champ	Description
<i>Channel (Canal)</i>	<p>Sélectionnez le <i>canal</i>. La plage de canaux et le canal par défaut sont déterminés par le <i>mode</i> de l'interface radio.</p> <p>Le <i>Channel - Canal</i> définit la partie du spectre que la radio utilise pour émettre et recevoir. Chaque mode offre un certain nombre de canaux en fonction de la manière dont le spectre est sous licence par les autorités nationales et transnationales telles que la Federal Communications Commission (FCC) ou l'International Telecommunication Union (ITU-R).</p> <p>La valeur par défaut est Auto (Automatique), qui détecte le canal le moins occupé lors du démarrage.</p>

13.5 Configuration des paramètres de LAN sans fil « interne »

Les Internal Settings (Paramètres Interne) décrivent l'adresse **MAC** (en lecture seule) et le nom du réseau (également appelé **SSID**) pour le *réseau local sans fil* (WLAN) interne, comme indiqué dans le Tableau 13.4.

Tableau 13.4 Paramètres LAN

Champ	Description
<i>MAC Address (Adresse MAC)</i>	<p>Affiche les adresses MAC de l'interface interne pour ce point d'accès. Il s'agit d'un champ en lecture seule que vous ne pouvez pas modifier.</p> <p>Bien que ce point d'accès soit physiquement un appareil unique, il peut être représenté sur un réseau par deux nœuds ou plus, chacun avec une adresse MAC unique. Ceci est possible grâce à plusieurs <i>Basic Service Set Identifiers (BSSID)</i> pour un seul point d'accès.</p> <p>Les adresses MAC indiquées pour le point d'accès « interne » sont les BSSID de l'interface « interne ».</p> <p>Pour les points d'accès de radio professionnelle, deux adresses MAC sont affichées : une pour chaque radio sur l'interface interne.</p>
<i>Wireless Network Name (SSID) (Nom du réseau sans fil (SSID))</i>	<p>Entrez le SSID du WLAN interne.</p> <p>Le <i>Service Set Identifier (SSID)</i> est une chaîne alphanumérique de 32 caractères maximum qui identifie de façon unique un réseau local sans fil. Il est également appelé <i>nom de réseau</i>. Il n'y a aucune restriction sur les caractères qui peuvent être utilisés dans un SSID.</p>

13.6 Configuration des paramètres sans fil de réseau « invité »

Les Guest Settings (Paramètres Invité) décrivent l'adresse **MAC** (en lecture seule) et le nom de réseau sans fil (**SSID**) pour le *réseau invité*, comme indiqué dans le Tableau 13.5. Configurer un point d'accès avec deux noms de réseau (SSID) différents vous permet d'exploiter la fonctionnalité d'interface invité sur la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway. Pour plus d'informations, reportez-vous au Chapitre 14 : « Configuration de l'accès invité ».

Tableau 13.5 Paramètres sans fil de réseau « invité »

Champ	Description
<i>MAC Address</i> (Adresse MAC)	<p>Affiche l'adresse MAC de l'interface invité pour ce point d'accès. Il s'agit d'un champ en lecture seule que vous ne pouvez pas modifier.</p> <p>Bien que ce point d'accès soit physiquement un appareil unique, il peut être représenté sur un réseau par deux nœuds ou plus, chacun avec une adresse MAC unique. Ceci est possible à l'aide de plusieurs <i>Basic Service Set Identifiers (BSSID)</i> pour un seul point d'accès.</p> <p>Les adresses MAC indiquées pour le point d'accès « invité » sont les BSSID de l'interface « invité ».</p> <p>Pour les points d'accès de radio professionnelle, deux adresses MAC sont affichées : une pour chaque radio sur l'interface invité.</p>
<i>Wireless Network Name (SSID)</i> (Nom du réseau sans fil (SSID))	<p>Entrez le SSID du <i>réseau invité</i>.</p> <p>Le <i>Service Set Identifier (SSID)</i> est une chaîne alphanumérique de 32 caractères maximum qui identifie de façon unique un réseau local sans fil. Il est également appelé <i>nom de réseau</i>. Il n'y a aucune restriction sur les caractères qui peuvent être utilisés dans un SSID.</p> <p>Pour le réseau invité, fournissez un SSID différent du SSID interne et facilement identifiable comme réseau « invité ».</p>

13.7 Mise à jour des paramètres sans fil

Pour mettre à jour les paramètres sans fil

1. Accédez à la page *802.11 Settings* (Paramètres 802.11).
2. Configurez les paramètres sans fil selon les besoins.
3. Cliquez sur le bouton **Update** (Mettre à jour) pour appliquer les modifications.

CONFIGURATION DE L'ACCÈS INVITÉ

14

14.1 Présentation de l'interface invité	161
14.2 Configuration de l'interface invité	162
14.2.1 Configuration d'un réseau invité sur un VLAN.	162
14.2.2 Configuration de l'écran d'accueil (portail captif)	163
14.3 Utilisation du réseau invité en tant que client.	164
14.4 Exemple de déploiement	165

Les fonctionnalités de l'*interface invité* prêtes à l'emploi vous permettent de configurer la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway pour contrôler l'accès invité à un réseau isolé. Vous pouvez configurer le même point d'accès pour diffuser et fonctionner comme deux réseaux sans fil différents : un réseau « interne » sécurisé et un réseau public « invité ». Les clients invités peuvent accéder au réseau invité sans entrer de nom d'utilisateur ou de mot de passe. Lorsque les invités se connectent, ils voient un écran d'*accueil* pour les invités (également appelé « *portail captif* »).

14.1 Présentation de l'interface invité

Vous pouvez définir des paramètres uniques pour la connectivité *des invités* et isoler les clients invités des zones plus sensibles du réseau.



Important : *Aucune sécurité n'est fournie sur le réseau invité ; le mode de sécurité texte brut uniquement est autorisé.*

Simultanément, vous pouvez configurer un réseau *interne* sécurisé (utilisant le même point d'accès que votre interface invité) qui fournit un accès complet aux informations protégées par un pare-feu et nécessite une connexion sécurisée ou des certificats pour l'accès.

Vous pouvez configurer une passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway pour une interface invité en utilisant un réseau unique avec des VLAN en définissant les options de configuration de l'interface invité dans les pages Web d'administration de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway. (Pour plus de détails sur la manière de configurer ce type d'interface invité, reportez-vous à la section « Configuration d'un réseau invité sur un VLAN » à la page 162.



Remarques : *Cette méthode exploite plusieurs technologies **BSSID** et LAN virtuels (VLAN) qui sont intégrées à la passerelle sans fil 9160 G2 Wireless Gateway. Les réseaux interne et invité sont mis en œuvre comme plusieurs BSSID sur le même point d'accès, chacun avec des noms de réseau (SSID) différents sur l'interface sans fil et des ID VLAN différents sur l'interface filaire.*

Sur un point d'accès de radio professionnelle, les paramètres Guest Login (Connexion invité) and Guest Management (Gestion des invités) s'appliquent aux radios un et deux.

14.2 Configuration de l'interface invité

Pour configurer l'interface invité sur la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway, procédez comme suit :

1. Configurez le point d'accès pour représenter deux réseaux *pratiquement* distincts, comme indiqué dans la section ci-dessous, « Configuration d'un réseau invité sur un VLAN ».
2. Configurer l'écran *Welcome* (Accueil) pour le portail captif invité comme décrit dans la section « Configuration de l'écran d'accueil (portail captif) » à la page 163.



*Remarque : Les paramètres de l'interface invité ne sont pas partagés entre les points d'accès au sein du cluster. Ces paramètres doivent être configurés individuellement dans les pages d'administration de chaque point d'accès. Pour trouver les pages d'administration d'un point d'accès qui est membre du cluster en cours, cliquez sur son lien d'**adresse IP** dans la page Cluster > Access Points (Cluster > Points d'accès) du point d'accès en cours. Pour plus d'informations sur les paramètres qui sont partagés par le cluster et ceux qui ne le sont pas, reportez-vous à la section « Quels paramètres sont/ne sont pas partagés dans le cadre de la configuration du cluster ? » à la page 59.*

14.2.1 Configuration d'un réseau invité sur un VLAN



Remarques : Si vous souhaitez configurer les réseaux interne et invité sur un réseau local virtuel (VLAN), le commutateur et le serveur DHCP que vous utilisez doivent prendre en charge les réseaux locaux virtuels (VLAN).

Comme étape préalable, configurez un port sur le commutateur pour gérer les paquets VLAN comme décrit dans la norme IEEE 802.1Q.

Les paramètres de l'écran d'accueil ne sont pas partagés entre les points d'accès au sein du cluster. Lorsque vous mettez à jour ces paramètres pour un point d'accès, la configuration sera partagée avec les autres points d'accès dans le cluster. Pour plus d'informations sur les paramètres qui sont partagés par le cluster et ceux qui ne le sont pas, reportez-vous à la section « Quels paramètres sont/ne sont pas partagés dans le cadre de la configuration du cluster ? » à la page 59.

Pour configurer les réseaux interne et invité sur les VLAN, procédez comme suit :

1. N'utilisez qu'une seule connexion filaire depuis le port réseau du point d'accès au LAN. (Assurez-vous que ce port est configuré pour gérer les paquets balisés VLAN.)
2. Configurez les paramètres Ethernet (filaire) pour les réseaux interne et invité sur les réseaux locaux virtuels (VLAN) en suivant les instructions fournies dans les sections du Chapitre 12 : « L'interface Ethernet (filaire) ».
(Pour commencer, activez l'accès invité et choisissez For Internal and Guest access, use two: VLANs (*Pour accès interne et invité, utilisez deux : VLAN*) comme décrit dans la section « Spécification d'un réseau invité virtuel » à la page 145.)
3. Fournissez les paramètres de l'interface radio et les noms de réseau (SSID) pour les réseaux interne et invité, comme indiqué dans le Chapitre 13 : « Définition de l'interface sans fil ».
4. Configurez l'écran de démarrage invité en suivant la procédure décrite dans la section « Configuration de l'écran d'accueil (portail captif) » à la page 163.

14.2.2 Configuration de l'écran d'accueil (portail captif)

Vous pouvez définir ou modifier l'écran d'accueil vu par les clients invités lorsqu'ils ouvrent un navigateur Web ou qu'ils essaient de naviguer sur le Web. Pour configurer le portail captif, procédez comme suit :

1. Accédez à l'onglet *Manage > Guest Login* (Gérer > Connexion invité).

Figure 14.1 Paramètres de l'écran Guest Login (Connexion invité)

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

Modify guest welcome screen settings

Guest User Welcome Screen ☒ Enabled ☐ Disabled

Welcome Screen Text

Thank you for using wireless Guest Access as provided by this 9160 wireless AP. Upon clicking "Accept", you will gain access to our wireless guest network. This network allows

Update

2. Choisissez **Enabled** (Activé) pour activer l'écran d'accueil.
3. Dans le champ *Welcome Screen Text* (Texte de l'écran d'accueil), saisissez le message texte que vous souhaitez que les clients invités voient sur le portail captif.
4. Cliquez sur **Update** (Mettre à jour) pour appliquer les modifications.

14.3 Utilisation du réseau invité en tant que client

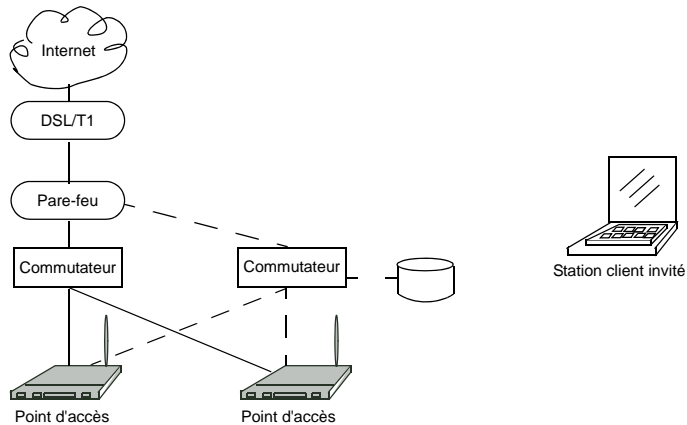
Une fois que le réseau invité est configuré, un client peut accéder au réseau invité de la manière suivante :

1. Un client invité entre dans une zone de couverture et recherche les réseaux sans fil.
2. Le réseau invité s'annonce via un SSID invité ou un nom similaire, en fonction de la manière dont le SSID invité est spécifié dans les pages Web d'administration de l'Interface invité.
3. Le client choisit Guest SSID (SSID invité).
4. Le client invité lance un navigateur Web et reçoit un écran d'accueil invité.
5. L'écran d'accueil invité fournit au client un bouton à cliquer pour continuer.
6. Le client invité est maintenant autorisé à utiliser le réseau pour utiliser le réseau « invité ».

14.4 Exemple de déploiement

Dans la Figure 14.2, les lignes en pointillés indiquent les connexions dédiées invité. Tous les points d'accès et toutes les connexions (y compris les invités) sont administrés à partir des mêmes pages Web d'administration de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway.

Figure 14.2 Connexions invité dédiées



CONFIGURATION DE VLAN

15

15.1 Accès aux paramètres de réseau sans fil virtuels	169
15.2 Configuration de VLAN	169
15.3 Mise à jour des paramètres	171

Les sections suivantes décrivent la manière de configurer plusieurs réseaux sans fil sur des réseaux LAN virtuels (**VLAN**).

15.1 Accès aux paramètres de réseau sans fil virtuels

Pour configurer plusieurs réseaux sur des VLAN, accédez à l'onglet *Manage > VWM* (Gérer > VWN) et mettez à jour les champs comme indiqué ci-dessous.

Figure 15.1 Paramètres VWN

Modify Virtual Wireless Network settings					
Virtual Wireless Networks : Disabled					
VWN	Enabled	VLAN ID	SSID	Broadcast SSID	Security
1	<input checked="" type="checkbox"/>		Virtual Wireless Network 1	<input checked="" type="checkbox"/>	None
2	<input checked="" type="checkbox"/>		Virtual Wireless Network 2	<input checked="" type="checkbox"/>	None

15.2 Configuration de VLAN



Remarque : Pour configurer d'autres réseaux sur des VLAN, vous devez d'abord activer Virtual Wireless Networks (VWN) sur la page des paramètres Ethernet. Reportez-vous à la section « Réseaux sans fil virtuels (VLAN) » à la page 146.



Important : *Si vous configurez des VLAN, vous risquez de perdre la connectivité au point d'accès. Pour commencer, assurez-vous de vérifier que le commutateur et le serveur DHCP que vous utilisez peuvent prendre en charge les VLAN via la norme IEEE 802.1Q. Après avoir configuré les VLAN, rebranchez physiquement le câble Ethernet sur le commutateur au port (VLAN) paquet balisé. Ensuite, reconnectez-vous à la nouvelle adresse IP via les pages Web d'administration. (Si nécessaire, consultez l'administrateur d'assistance technique d'infrastructure au sujet des configurations VLAN et DHCP.)*

Tableau 15.1 Paramètres Virtual Wireless Network (VWN)

Champ	Description
<i>Virtual Wireless Network (VWN)</i>	Vous pouvez configurer jusqu'à 6 VWN.
<i>Enabled (Activé)</i>	<p>Vous pouvez activer ou désactiver un réseau configuré.</p> <ul style="list-style-type: none">• Pour activer le réseau spécifié, cochez la case <i>Enabled</i> (Activé) située en regard du VWN approprié.• Pour désactiver le réseau spécifié, décochez la case <i>Enabled</i> (Activé) située en regard du VWN approprié. <p>Si vous désactivez le réseau spécifié, vous perdrez l'ID VLAN que vous avez entrée.</p>
<i>VLAN ID (ID VLAN)</i>	<p>Fournissez un nombre entre 1 et 4094 pour le VLAN interne.</p> <p>Ainsi, le point d'accès enverra les requêtes DHCP avec la balise VLAN. Le commutateur et le serveur DHCP doivent prendre en charge les trames IEEE 802.1Q VLAN. Le point d'accès doit pouvoir atteindre le serveur DHCP.</p> <p>Consultez l'administrateur au sujet des configurations VLAN et DHCP.</p>
<i>SSID</i>	<p>Entrez un nom pour le réseau sans fil sous forme de chaîne de caractères. Ce nom s'applique à tous les points d'accès sur ce réseau. À mesure que vous ajoutez d'autres points d'accès, ils partagent ce SSID.</p> <p>Le SSID (Service Set Identifier) est une chaîne alphanumérique d'un maximum de 32 caractères.</p> <p>Remarque : <i>Si vous êtes connecté en tant que client sans fil au point d'accès que vous administrez, réinitialiser le SSID entraînera la perte de connectivité du point d'accès. Vous devrez vous reconnecter au nouveau SSID après l'enregistrement de ce nouveau paramètre.</i></p>

Tableau 15.1 Paramètres Virtual Wireless Network (VWN)

Champ	Description
<i>Broadcast SSID (SSID de diffusion)</i>	<p>Sélectionnez le paramètre <i>Broadcast SSID</i> (SSID de diffusion) en sélectionnant la case Broadcast SSID (SSID de diffusion).</p> <p>Par défaut, le point d'accès diffuse (autorise) le <i>Service Set Identifier</i>(SSID) dans ses trames de balise.</p> <p>Vous pouvez supprimer (interdire) cette diffusion pour décourager la détection automatique de votre point d'accès par les stations. Lorsque le SSID de diffusion du point d'accès est supprimé, le nom du réseau ne s'affiche pas dans la <i>liste des réseaux disponibles</i> sur une station client. Au lieu de cela, le client doit avoir le nom exact du réseau configuré dans le demandeur avant de pouvoir se connecter.</p> <p><i>Remarque : Le SSID de diffusion que vous avez défini ici est spécifiquement pour ce réseau virtuel (Un ou Deux). Les autres réseaux continuent à utiliser les modes de sécurité déjà configurés :</i></p> <ul style="list-style-type: none">• Votre réseau interne d'origine (configuré dans la page <i>Ethernet Settings</i> (Paramètres Ethernet)) utilise le SSID de diffusion défini dans <i>Security</i> (Sécurité).• Si un réseau invité est configuré, le SSID de diffusion est toujours autorisé.
<i>Security (Sécurité)</i>	<p>Sélectionnez le <i>mode de sécurité</i> pour ce VLAN. Sélectionnez l'une des options suivantes :</p> <ul style="list-style-type: none">• <i>None (Plain-text) (Aucun (texte brut))</i>• <i>Static WEP (WEP statique)</i>• <i>WPA Personal</i> <p><i>Remarque : Le mode de sécurité que vous avez défini ici est spécialement pour ce réseau virtuel. Les autres réseaux continuent à utiliser les modes de sécurité déjà configurés :</i></p> <ul style="list-style-type: none">• Votre réseau interne d'origine (configuré dans la page <i>Ethernet Settings</i> (Paramètres Ethernet)) utilise le mode de sécurité défini dans <i>Security</i> (Sécurité).• Si un client réseau est configuré, définissez toujours le mode de sécurité sur « None » (Aucun).

15.3 Mise à jour des paramètres

Pour mettre à jour les paramètres VLAN :

1. Accédez à l'onglet VWN.
2. Configurez les paramètres VLAN selon les besoins.
3. Cliquez sur le bouton **Update** (Mettre à jour) pour appliquer les modifications.

16.1 Présentation des paramètres radio.	175
16.2 Accès aux paramètres radio.	175
16.3 Configuration des paramètres radio.	177
16.4 Mise à jour des paramètres	182

Les sections suivantes décrivent comment configurer les paramètres radio 802.11 sur la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway.

16.1 Présentation des paramètres radio

Les paramètres radio contrôlent directement le comportement de l'appareil radio du point d'accès et son interaction avec le support physique, c'est-à-dire quel type d'ondes électromagnétiques le point d'accès émet et comment. Vous pouvez indiquer si la radio est activée ou désactivée, le canal de diffusion de fréquence radio (RF), l'intervalle de balise (intervalle entre les transmissions de balise de point d'accès), la puissance de transmission, le mode IEEE 802.11 dans lequel la radio fonctionne, et ainsi de suite.

La passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway est fournie configurée comme un point d'accès bibande avec une radio.

Le point d'accès est capable de diffuser dans les modes suivants :

- Mode IEEE **802.11b**.
- Mode IEEE **802.11g**.
- Mode IEEE **802.11a**.
- Atheros Turbo 5 GHz.
- Atheros Dynamic Turbo 5 GHz.
- Atheros Turbo 2,4 GHz.
- Atheros Dynamic Turbo 2,4 GHz.
- Zone de couverture étendue.



Important : *Les terminaux mobiles Psion Teklogix ne prennent pas en charge les modes Atheros Turbo et, pour prévenir une surcharge radio inutile, l'utilisation du mode Turbo n'est pas recommandée.*

Le mode IEEE, ainsi que d'autres paramètres radio, sont configurés comme décrit dans les sections « Accès aux paramètres radio » à la page 175 et « Configuration des paramètres radio » à la page 177.

16.2 Accès aux paramètres radio

Pour spécifier les paramètres radio, accédez à l'onglet *Manage > 802.11 Advanced Settings* (Gérer > Paramètres avancés 802.11) afin d'ouvrir la page *Radio Settings* (Paramètres radio) et de mettre à jour les champs comme décrit dans le Tableau 16.1 à la page 177.

Figure 16.1 Présentation de la configuration des paramètres radio

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Narrow Band

Radio

Connectivity Options

Connectivity

Base Station

RRM Groups

Radio Link Features

Hosts

802.1Q

Modify radio settings

Status ☒ On ☐ Off

Mode IEEE 802.11g

Super AG ☐ Enabled ☒ Disabled

Extended Range ☐ Enabled ☒ Disabled

Channel 6

Beacon Interval 100 (Msec, Range: 20 - 2000)

DTIM Period 2 (Range: 1-255)

Fragmentation Threshold 2346 (Range: 256-2346, Even Numbers)

RTS Threshold 2347 (Range: 0-2347)

Maximum Stations 2007 (Range: 0-2007)

Transmit Power 100 Percent

Rate Supported Basic

54 Mbps ☒ ☐

48 Mbps ☒ ☐

36 Mbps ☒ ☐

24 Mbps ☒ ☐

18 Mbps ☒ ☐

12 Mbps ☒ ☐

11 Mbps ☒ ☒

9 Mbps ☒ ☐

6 Mbps ☒ ☐

5.5 Mbps ☒ ☒

2 Mbps ☒ ☒

1 Mbps ☒ ☒

Rate Sets

☐ Broadcast/Multicast Rate Limiting

Rate Limit 50 (packets per second)

Rate Limit Burst 75 (packets per second)

176 Manuel d'utilisation de la passerelle sans fil 9160 G2 Wireless Gateway Psion Teklogix

16.3 Configuration des paramètres radio

Tableau 16.1 Paramètres radio

Champ	Description
<i>Radio (Radio)</i>	<p>La passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway est disponible comme point d'accès pour une radio ou pour radio professionnelle.</p> <p>Point d'accès une radio : Si vous avez la version une radio de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway, ce champ n'est pas inclus sur l'onglet Radio (Radio).</p> <p>Point d'accès radio professionnelle : Si vous avez une version radio professionnelle de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway, précisez radio un radio deux. Sur un point d'accès radio professionnelle, le reste des paramètres de cet onglet s'appliquent à la radio sélectionnée dans ce champ. Assurez-vous de configurer les paramètres pour les deux radios.</p>
<i>Status (On/Off) (État (Activé/ Désactivé))</i>	Indiquez si vous souhaitez que la radio soit activée ou désactivée en cliquant sur On (Activé) ou Off (Désactivé).
<i>Mode (Mode)</i>	<p>Le <i>mode</i> définit la norme de <i>couche physique (PHY)</i> utilisée par la radio.</p> <p>La passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway est disponible en tant que point d'accès monobande ou b bande.</p> <p>Point d'accès monobande : Pour le point d'accès monobande, sélectionnez l'un des modes suivants :</p> <ul style="list-style-type: none"> • <i>IEEE 802.11b</i> • <i>IEEE 802.11g</i> <p>Point d'accès b bande : Pour le point d'accès b bande, sélectionnez l'un des modes suivants :</p> <ul style="list-style-type: none"> • <i>IEEE 802.11b</i> • <i>IEEE 802.11g</i> • <i>IEEE 802.11a</i> <p>Remarque : Si vous avez un point d'accès radio professionnelle, différents modes peuvent être disponibles selon que la radio un ou deux est sélectionnée dans le champ Radio (Radio) ci-dessus.</p> <p>Lorsque vous sélectionnez le mode radio, l'ensemble approprié de débits de base et pris en charge pour ce mode est sélectionné automatiquement. (Reportez-vous à la description des ensembles de débits plus bas dans ce tableau, à la page 181.)</p>

Tableau 16.1 Paramètres radio

Champ	Description
<i>Super AG</i> (<i>Super AG</i>)	Activer Super AG offre de meilleures performances en augmentant le débit radio pour un mode radio (IEEE 802.11b, g, a, etc.). Gardez à l'esprit que, avec l'option Super AG activée, les transmissions du point d'accès consommeront beaucoup plus de bande passante. <ul style="list-style-type: none">• Pour activer Super AG, cliquez sur Enabled (Activé).• Pour désactiver Super AG, cliquez sur Disabled (Désactivé).
<i>Extended Range</i> (<i>Extended Range</i>)	Atheros Extended Range (XR) est une méthode propriétaire pour la mise en œuvre de trafic à faible débit sur des distances plus longues. Elle est transparente pour les clients et les points d'accès compatibles XR et conçue pour une interopérabilité avec la norme 802.11 en modes 802.11g et 802.11a. Il n'y a pas de prise en charge d'Atheros XR dans 802.11b, Atheros Turbo 5 GHz ou Atheros Dynamic Turbo 5 GHz. Activer Atheros XR permettra d'étendre la couverture sur laquelle votre client et votre point d'accès peuvent fonctionner. <ul style="list-style-type: none">• Pour activer Extended Range, cliquez sur Enabled (Activé).• Pour désactiver Extended Range, cliquez sur Disabled (Désactivé). Cette option n'est pas disponible si vous avez sélectionné le mode matériel IEEE 802.11b, Atheros Turbo 5 GHz ou Atheros Dynamic Turbo 5 GHz. Atheros XR n'est pris en charge par ces modes matériel.
<i>Channel</i> (<i>Canal</i>)	Le Channel - Canal définit la partie du spectre que la radio utilise pour émettre et recevoir. La plage de canaux et le canal par défaut sont déterminés par le mode de l'interface radio. Pour la plupart des modes, la valeur par défaut est Auto (Auto). Le mode Auto est recommandé car il détecte automatiquement les meilleurs choix de canal en fonction de la puissance du signal, des charges du trafic, etc. Cependant, vous pouvez également sélectionner un canal entre un et onze inclus.
<i>Beacon Interval</i> (<i>Intervalle de balise</i>)	Les trames de Beacon - Balise sont transmises par un point d'accès à intervalles réguliers pour annoncer l'existence du réseau sans fil. Le comportement par défaut est d'envoyer une trame de balise une fois toutes les 100 millisecondes (soit 10 par seconde). La valeur d' <i>intervalle de balise</i> est définie en millisecondes. Entrez une valeur comprise entre 20 et 2000 .

Tableau 16.1 Paramètres radio

Champ	Description
<i>DTIM Period</i> (Période DTIM)	<p>Le message <i>Delivery Traffic Information Map</i> (DTIM) est un élément inclus dans certaines trames de Beacon - Balise. Il indique quelles stations client, actuellement en veille en mode faible puissance, ont des données mises en mémoire tampon sur le point d'accès en attente d'enlèvement.</p> <p>La période DTIM que vous spécifiez ici indique la fréquence à laquelle les clients servis par ce point d'accès doivent chercher les données en mémoire tampon qui sont toujours en attente sur le point d'accès.</p> <p>Indiquez une période DTIM dans la plage donnée (1 - 255).</p> <p>La mesure est dans les balises. Par exemple, si vous définissez ce paramètre sur 1, les clients vérifieront les données placées en mémoire tampon sur le point d'accès à chaque balise. Si vous définissez cette option sur 2, les clients vérifieront une balise sur deux. Si vous définissez cette option sur 10, les clients vérifieront une balise sur 10.</p>
<i>Fragmentation Threshold</i> (Seuil de fragmentation)	<p>Spécifiez une valeur comprise entre 256 et 2346 pour définir la taille du seuil de trame en octets.</p> <p>Le <i>seuil de fragmentation</i> est un moyen de limiter la taille des paquets (trames) transmis sur le réseau. Si un paquet dépasse le seuil de fragmentation défini ici, la fonctionnalité de fragmentation est activée et le paquet sera envoyé en plusieurs trames 802.11.</p> <p>Si le paquet en cours de transmission est inférieur ou égal au seuil, la fragmentation ne sera pas utilisée.</p> <p>Définir le seuil à la plus grande valeur (2346 octets) désactive la fragmentation.</p> <p>La fragmentation implique plus de surcharge en raison du travail supplémentaire de division et de réassemblage des trames qu'elle nécessite, et parce qu'elle augmente le trafic de messagerie sur le réseau. Toutefois, la fragmentation peut vous aider à <i>améliorer</i> la fiabilité et les performances de votre réseau si elle est correctement configurée.</p> <p>Envoyer des trames plus petites (via un seuil de fragmentation inférieur) peut aider à résoudre certains problèmes d'interférences ; par exemple, avec les fours à micro-ondes.</p> <p>Par défaut, la fragmentation est désactivée. Nous vous recommandons de ne pas utiliser la fragmentation excepté en cas d'interférences radio. Les en-têtes supplémentaires appliquées à chaque fragment augmentent la surcharge sur le réseau et peuvent réduire considérablement le débit.</p>

Tableau 16.1 Paramètres radio


Champ	Description
<i>RTS Threshold</i> (Seuil RTS)	<p>Spécifiez une valeur de <i>RTS Threshold - Seuil RTS</i> comprise entre 0 et 2347.</p> <p>Le seuil RTS spécifie la taille de paquet d'une demande d'envoi de transmission (<i>RTS</i>). Ceci permet de contrôler le flux de trafic dans le point d'accès, notamment s'il a beaucoup de clients.</p> <p>Si vous spécifiez un seuil faible, les paquets RTS seront envoyés plus fréquemment. Ceci consomme beaucoup plus de bande passante et réduit le débit du paquet.</p> <p>D'un autre côté, envoyer plus de paquets RTS peut aider le réseau à récupérer d'interférences ou de collisions qui peuvent se produire sur un réseau chargé, ou sur un réseau rencontrant des interférences électromagnétiques.</p>
<i>Maximum Stations (Nbre maximal de stations)</i>	<p>Spécifiez le nombre maximal de stations autorisées à accéder à ce point d'accès à un moment donné.</p> <p>Vous pouvez entrer une valeur comprise entre 0 et 2007.</p>
<i>Transmit Power</i> (Puissance de transmission)	<p>Indiquez une valeur sous forme de pourcentage pour définir la puissance de transmission pour ce point d'accès.</p> <p>La valeur par défaut est d'utiliser une transmission du point d'accès à 100 % de sa puissance.</p> <div>Recommandations :</div> <ul style="list-style-type: none">• Dans la plupart des cas, nous vous conseillons de garder la valeur par défaut et d'avoir la puissance de transmission définie sur 100 %. C'est plus rentable car elle donne au point d'accès un champ de diffusion maximal et réduit le nombre de points d'accès nécessaires.• Pour augmenter la capacité du réseau, rassemblez les points d'accès et réduisez la valeur de la puissance de transmission. Vous pourrez ainsi réduire les chevauchements et les interférences entre points d'accès. Un paramétrage de puissance de transmission inférieure peut également maintenir votre réseau plus sécurisé, car des signaux sans fil plus faibles sont moins susceptibles de se propager en dehors de l'emplacement physique de votre réseau.

Tableau 16.1 Paramètres radio

Champ	Description
<i>Rate Sets</i> (Ensembles de débits)	<p>Vérifiez les ensembles de débits de transmission que vous souhaitez que le point d'accès prenne en charge et les ensembles de débits de base que vous souhaitez que le point d'accès annonce.</p> <p>Les débits sont exprimés en mégabits par seconde.</p> <ul style="list-style-type: none"> • Supported Rate Sets (Ensembles de débits pris en charge) indique les débits que le point d'accès prend en charge. Vous pouvez sélectionner plusieurs débits (cliquez sur une case à cocher pour sélectionner ou désélectionner un débit). Le point d'accès choisit automatiquement la fréquence la plus efficace en fonction de facteurs tels que les taux d'erreur et la distance des stations client du point d'accès. • Basic Rate Sets (Ensembles de débits de base) indique les débits que le point d'accès annoncera sur le réseau à des fins de configuration de communications avec d'autres points d'accès et stations client sur le réseau. Il est généralement plus efficace qu'un point d'accès diffuse un sous-ensemble de ses ensembles de débits pris en charge. <p>Pour prendre en charge à la fois les clients « b » et « g », définissez le mode radio à IEEE 802.11g. L'interface utilisateur Web sélectionnera automatiquement les ensembles de débits par défaut qui permettent à la fois aux clients « b » et « g » de se connecter.</p> <p>Pour prendre en charge les clients « g » uniquement, définissez le mode radio à IEEE 802.11g. L'interface utilisateur Web sélectionnera automatiquement les ensembles de débits par défaut. Maintenant, ajoutez 24, 12, et 6 comme débits de base. Cette opération permet d'empêcher les clients « b » de se connecter comme ils ne prennent pas en charge ces débits, mais elle permettra aux clients « g » de se connecter car la norme requiert qu'ils prennent en charge ces débits.</p> <p>Pour plus d'informations, reportez-vous à la description du <i>mode</i> plus haut dans ce tableau, à la page 177.</p>
<i>Enable Broadcast/Multicast Rate Limiting</i> (Activer la limitation de débit de diffusion/multidiffusion)	<p>Activer la limitation du débit de diffusion et de multidiffusion peut améliorer les performances globales du réseau en limitant le nombre de paquets transmis sur le réseau.</p> <p>Certains protocoles utilisent des paquets de multidiffusion et de diffusion pour le trafic qui désintéresse la majorité des nœuds sur un réseau. Par exemple, les requêtes ARP pour d'autres machines, les messages DHCP ou BOOTP. Pour certains protocoles, si vous définissez un contrôle de limite de débit, vous limitez le nombre de paquets redondants transmis sur le réseau. En général, tout le trafic filtré sera retransmis à un moment ultérieur et ne créera aucune difficulté.</p> <ul style="list-style-type: none"> • Pour activer la limitation de débit de diffusion et de multidiffusion, cliquez sur Enabled (Activé). • Pour désactiver la limitation de débit de diffusion et de multidiffusion, cliquez sur Disabled (Désactivé). <p>Par défaut, la <i>limitation de débit de diffusion/multidiffusion</i> est désactivée. Jusqu'à ce que vous activiez la limitation de débit de multidiffusion/diffusion, les champs suivants seront désactivés.</p>

Tableau 16.1 Paramètres radio

Champ	Description
<i>Broadcast/Multicast Rate Limit (Limite du débit de diffusion/multi diffusion)</i>	Entrez la limite du débit que vous voulez définir pour le trafic de multidiffusion et de diffusion. Cette limite doit être supérieure à 1, mais inférieure à 50 paquets par seconde. Tout le trafic qui tombe en dessous de cette limite du débit est toujours conforme et sera transmis vers la destination appropriée. La configuration de la limite du débit par défaut et maximale est de 50 paquets par seconde.
<i>Broadcast/Multicast Rate Limit Burst (Limite de salve de débit de diffusion/multi diffusion)</i>	Définir une limite de salve de débit détermine combien de salves de trafic peuvent avoir lieu avant que tout le trafic ne dépasse la limite du débit. Cette limite de salve autorise des salves intermittentes de trafic sur un réseau au-dessus de la limite du débit. La configuration de la limite de salve de débit par défaut et maximale est de 75 paquets par seconde.

16.4 Mise à jour des paramètres

Pour mettre à jour les paramètres radio :

1. Accédez à l'onglet *802.11 Advanced settings* (Paramètres avancés 802.11).
2. Configurez les paramètres de la radio comme requis.
3. Cliquez sur le bouton **Update** (Mettre à jour) pour appliquer les modifications.



*Remarque : Si vous utilisez la version professionnelle de la passerelle sans fil 9160 G2 Wireless Gateway, gardez à l'esprit que les radios un et deux sont toutes les deux configurées sur cet onglet. Les paramètres affichés s'appliquent à la radio un ou deux, selon la radio que vous choisissez dans le champ Radio (Radio) (premier champ de l'onglet). Lorsque vous avez configuré des paramètres pour l'une des radios, cliquez sur **Update** (Mettre à jour) puis sélectionnez l'autre radio pour la configurer. Assurez-vous de cliquer sur **Update** (Mettre à jour) pour appliquer le deuxième ensemble de paramètres à l'autre radio.*

FILTRAGE D'ADRESSES MAC

17

17.1 Accès aux paramètres de filtrage MAC.	185
17.2 Utilisation du filtrage MAC.	186
17.3 Mise à jour des paramètres	186

Une adresse *MAC* (*Media Access Control*) (**MAC**) est une adresse matérielle qui identifie de façon unique chaque nœud d'un réseau. Tous les appareils de réseau IEEE 802 partagent un même format d'adresse MAC 48 bits, généralement affiché sous forme de chaîne de 12 chiffres hexadécimaux séparés par le caractère deux points, par exemple FE:CC:BA:09:87:65. Chaque carte d'interface réseau sans fil (**NIC**) utilisée par un client sans fil possède une adresse MAC unique.

Vous pouvez contrôler l'accès client à votre réseau sans fil en activant le *filtrage MAC* et en spécifiant la liste des adresses MAC approuvées. Lorsque le filtrage MAC est activé, seuls les clients avec une adresse MAC peuvent accéder au réseau.

Les sections suivantes décrivent comment utiliser le filtrage d'adresses MAC sur la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway.

17.1 Accès aux paramètres de filtrage MAC

Pour activer le filtrage par adresse MAC, accédez à l'onglet *Manage > MAC Filtering* (Gérer > Filtrage MAC) et mettez à jour les champs comme décrit ci-dessous.

Figure 17.1 Paramètres de filtrage MAC

Basic Settings	Configure MAC Filtering of client stations Filter <input type="radio"/> Allow only stations in list <input checked="" type="radio"/> Block all stations in list Stations List <table border="1"><tr><td>10:10:10:10:14:44</td></tr></table> <input type="button" value="Remove"/> <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> <input type="button" value="Add"/> <input type="button" value="Update"/>	10:10:10:10:14:44
10:10:10:10:14:44		
User Management		
Cluster		
Access Points		
Sessions		
Channel Management		
Wireless Neighborhood		
Security		
Status		
Interfaces		
Events		
Transmit/Receive		
Client Associations		
Neighboring Access Points		
Manage		
Ethernet Settings		
802.11 Settings		
802.11 Advanced Settings		
VWN		
WDS		
Guest Login		
MAC Filtering		

17.2 Utilisation du filtrage MAC

Cette page vous permet de contrôler l'accès à la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway, en fonction des adresses *MAC* (*Media Access Control*). Selon la manière dont vous avez défini le filtre, vous pouvez *autoriser* uniquement les stations client répertoriées avec une adresse MAC ou leur *empêcher* l'accès.

Pour l'interface Guest (Invité), les paramètres de filtrage **MAC** s'appliquent aux deux **BSS**. Sur un point d'accès de radio professionnelle, les paramètres de filtrage MAC s'appliquent aux deux radios.

Tableau 17.1 Paramètres de filtrage MAC

Champ	Description
<i>Filter</i> (Filtre)	Pour définir le <i>filtre</i> d'adresse MAC, cliquez sur l'un des boutons de radio suivants : <ul style="list-style-type: none">• Allow only stations in the list (Autoriser uniquement les stations de la liste)• Block all stations in list (Bloquer toutes les stations de la liste)
<i>Stations List</i> (Liste des stations)	<p>Pour ajouter une adresse MAC à la liste des stations, entrez son adresse MAC de 48 bits dans les zones de texte inférieures, puis cliquez sur Add (Ajouter).</p> <p>L'adresse MAC est ajoutée à la liste des stations.</p> <p>Pour supprimer une adresse MAC de la liste des stations, sélectionnez son adresse MAC de 48 bits, puis cliquez sur Remove (Supprimer).</p> <p>Les stations de la liste seront autorisées ou non à accéder au point d'accès en fonction de la manière dont vous configurez le filtre.</p>

17.3 Mise à jour des paramètres

Pour mettre à jour les paramètres MAC :

1. Accédez à la page d'onglet *MAC Filtering* (Filtrage MAC).
2. Configurer les paramètres MAC selon les besoins.
3. Cliquez sur le bouton **Update** (Mettre à jour) pour appliquer les modifications.

18.1 Présentation de l'équilibrage de la charge.	189
18.1.1 Identification d'un déséquilibre : points d'accès souvent encombrés ou sous-utilisés	189
18.1.2 Définition de limites pour l'utilisation et les associations de client.	190
18.1.3 Équilibrage de la charge et qualité de service (QoS)	190
18.2 Navigation vers les paramètres de l'équilibrage de la charge.	190
18.3 Configuration de l'équilibrage	191
18.4 Mise à jour des paramètres	193

La passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway vous permet d'équilibrer la distribution des connexions client sans fil sur plusieurs points d'accès. Avec l'équilibrage de la charge, vous pouvez empêcher des scénarios dans lesquels un seul point d'accès de votre réseau subit une dégradation des performances parce qu'il gère une portion disproportionnée du trafic sans fil.

Les sections suivantes décrivent comment configurer l'équilibrage de la charge sur votre réseau sans fil.

18.1 Présentation de l'équilibrage de la charge

Comme la plupart des paramètres de configuration sur la Passerelle sans fil 9160 G2 Wireless Gateway, les paramètres d'équilibrage de la charge sont partagés entre des points d'accès en cluster.



Remarque : Dans certains cas, vous souhaitez peut-être configurer des limites pour un seul point d'accès qui est toujours surexploité. Vous pouvez appliquer des paramètres uniques à un point d'accès particulier s'il fonctionne en mode autonome. (Reportez-vous aux sections « Présentation de la mise en cluster » à la page 58 et « Accès à la gestion des points d'accès » à la page 57.)

18.1.1 Identification d'un déséquilibre : points d'accès souvent encombrés ou sous-utilisés

Scénario type : une comparaison des données d'association de clients et de transmission/réception pour plusieurs points d'accès vous permet d'identifier un point d'accès qui gère toujours un pourcentage disproportionné du trafic sans fil. Cela peut se produire lorsque l'emplacement ou d'autres facteurs font qu'un point d'accès transmet le signal le plus fort à la plupart des clients sur un réseau. Par défaut, ce point d'accès recevra la plupart des demandes client alors que les autres points d'accès restent inactifs la plupart du temps.

Les déséquilibres de la distribution de trafic sans fil entre les points d'accès sont mis en évidence dans les statistiques de données d'association de clients et de transmission/réception, qui indiqueront des fréquences « d'utilisation » plus élevées sur les points d'accès encombrés et inversement, des temps « d'inactivité » plus élevés sur les points d'accès sous-utilisés. Un point d'accès qui gère trop de trafic peut également avoir des débits de transmission de données plus lents ou des débits de transmission et de réception inférieurs en raison de la surcharge.

18.1.2 Définition de limites pour l'utilisation et les associations de client

Vous pouvez corriger les déséquilibres d'utilisation des points d'accès du réseau en activant l'équilibrage de la charge et en définissant des limites pour les fréquences d'utilisation et le nombre d'associations de client autorisés par point d'accès.

18.1.3 Équilibrage de la charge et qualité de service (QoS)

L'équilibrage de la charge joue également un rôle en contribuant à *la qualité de service* (QoS) de *Voice over IP* (VoIP) et d'autres applications urgentes concurrentes pour la bande passante et à l'accès rapide aux ondes sur un réseau sans fil. Pour plus d'informations sur la configuration de votre réseau pour la qualité de service, reportez-vous au Chapitre 19 : « Qualité de service (QoS) ».

18.2 Navigation vers les paramètres de l'équilibrage de la charge

Sur l'interface d'administration, accédez à l'onglet *Manage > Load Balancing* (Gérer > Équilibrage de la charge) et mettez à jour les champs comme décrit dans la section suivante.

Figure 18.1 Paramètres d'équilibrage de la charge

Basic Settings	Modify load balancing settings
User Management	
Cluster	Load Balancing <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Access Points	Utilization for No New Associations <input type="text" value="0"/> (Percent, 0 disables)
Sessions	Utilization for Disassociation <input type="text" value="0"/> (Percent, 0 disables)
Channel Management	Station Threshold for Disassociation <input type="text" value="0"/> Range 1 - 2007, 0 disables.
Wireless Neighborhood	<input type="button" value="Update"/>
Security	
Status	
Interfaces	
Events	
Transmit/Receive	
Client Associations	
Neighboring Access Points	
Manage	
Ethernet Settings	
802.11 Settings	
802.11 Advanced Settings	
VWN	
WDS	
Guest Login	
MAC Filtering	
Load Balancing	

18.3 Configuration de l'équilibrage

Pour configurer l'équilibrage de la charge, *activez* **Load Balancing** (Équilibrage de la charge) et définissez les limites et le comportement qui seront déclenchés par une certaine fréquence d'utilisation du point d'accès.




Remarques : Même lorsque les clients sont dissociés d'un point d'accès, le réseau fournit tout de même un service continu aux stations client si un autre point d'accès se situe à portée afin que les clients puissent se reconnecter au réseau. Les clients doivent automatiquement réessayer le point d'accès auquel ils étaient initialement connectés et d'autres points d'accès sur le sous-réseau. Les clients qui sont dissociés d'un point d'accès devraient suivre une transition transparente vers un autre point d'accès sur le même sous-réseau.

Les paramètres d'équilibrage de la charge s'appliquent à la charge du point d'accès dans son ensemble. Lorsque l'accès invité est activé, les paramètres s'appliquent à la fois aux réseaux interne et invité.

Sur un point d'accès de radio professionnelle, les paramètres d'équilibrage de la charge s'appliquent aux deux radios, mais la charge de chaque radio est calculée indépendamment et comprend à la fois le réseau interne et le réseau invité (lorsque l'accès invité est activé).

Tableau 18.1 Paramètres d'équilibrage de la charge

Champ	Description
<i>Load Balancing (Équilibrage de la charge)</i>	Pour activer l'équilibrage de la charge sur ce point d'accès, cliquez sur Enable (Activer). Pour désactiver l'équilibrage de la charge sur ce point d'accès, cliquez sur Disable (Désactiver).
<i>Utilization for No New Associations (Utilisation sans nouvelles associations)</i>	Les limites de fréquence d'utilisation sont liées à l'utilisation de la bande passante sans fil. Définissez une limite de pourcentage de fréquence d'utilisation de la bande passante pour ce point d'accès afin d'indiquer quand cesser d'accepter de nouvelles associations de client. Lorsque la fréquence d'utilisation pour ce point d'accès dépasse la limite spécifiée, aucune nouvelle association de client ne sera autorisée sur ce point d'accès. Si vous indiquez 0 dans ce champ, toutes les nouvelles associations seront autorisées quelle que soit la fréquence d'utilisation.
<i>Utilization for Disassociation (Utilisation pour dissociation)</i>	Les limites de fréquence d'utilisation sont liées à l'utilisation de la bande passante sans fil. Définissez une limite de pourcentage de fréquence d'utilisation de la bande passante pour ce point d'accès afin d'indiquer quand dissocier les clients actuels. Lorsque la fréquence d'utilisation dépasse la limite spécifiée, un client actuellement associé à ce point d'accès sera déconnecté. Si vous indiquez 0 dans ce champ, les clients actuels ne seront jamais déconnectés quelle que soit la fréquence d'utilisation.
<i>Stations Threshold for Disassociation (Seuil de stations pour la dissociation)</i>	Spécifiez le nombre de stations client que vous souhaitez définir comme « seuil de stations » pour une dissociation. Si le nombre de stations client associées au point d'accès à un moment donné est inférieur ou égal au nombre que vous spécifiez ici, aucune station ne sera dissociée, quelle que soit la valeur d'utilisation pour une dissociation. En théorie, le nombre maximum de stations client autorisé est 2007 .  Nous vous recommandons de définir ce maximum sur une valeur comprise entre 30 et 50 stations client. Cela permet de réaliser une charge suffisante sur le point d'accès, la bande passante étant partagée entre les points d'accès clients.

18.4 Mise à jour des paramètres

Pour mettre à jour les paramètres d'équilibrage de la charge :

1. Accédez à la page d'onglet *Load Balancing* (Équilibrage de la charge).
2. Configurez les paramètres d'équilibrage de la charge selon les besoins.
3. Cliquez sur le bouton **Update** (Mettre à jour) pour appliquer les modifications.

19.1 Présentation de QoS.	197
19.1.1 QoS et équilibrage de la charge	197
19.1.2 Prise en charge des normes 802.11e et WMM	197
19.1.3 Files d'attente et paramètres QoS pour coordonner le flux de trafic.	198
19.1.3.1 Files d'attente QoS et type de service (ToS) pour les paquets	198
19.1.3.2 Contrôle EDCF des trames de données et espaces indépendant d'arbitrage.	200
19.1.3.3 Interruption aléatoire et fenêtres de contention minimale/maximale	201
19.1.3.4 Salve de paquets pour de meilleures performances	202
19.1.3.5 Intervalle Transmission Opportunity (TXOP) pour stations client	202
19.1.4 802.1p et balises DSCP	202
19.1.4.1 Priorité VLAN	204
19.1.4.2 Priorité DSCP	205
19.2 Configuration des files d'attente QoS.	205
19.2.1 Configuration des paramètres EDCA du point d'accès	208
19.2.2 Activation/désactivation de Wi-Fi Multimedia	210
19.2.3 Configuration des paramètres EDCA de la station	210
19.3 Mise à jour des paramètres	212

La qualité de service (**QoS**) vous permet de spécifier les paramètres sur plusieurs files d'attente pour un débit accru et de meilleures performances de trafic sans fil différencié tel que *Voice-over-IP* (VoIP), d'autres types de données audio, vidéo et la diffusion de contenus multimédias, ainsi que les données IP traditionnelles sur la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway.

Les sections suivantes décrivent comment configurer les files d'attente QoS sur la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway.

19.1 Présentation de QoS

Un des principaux facteurs qui affecte la qualité de service est la congestion du réseau due à une augmentation du nombre de clients qui tente d'accéder aux ondes et au volume plus élevé de trafic de bande passante pendant une heure de pointe dans la journée. La dégradation de service la plus visible sur un réseau chargé et saturé sera évidente dans des applications urgentes telles que la vidéo, *Voice-over-IP* (VoIP) et la diffusion de contenus multimédias.

Contrairement aux fichiers de données types qui sont moins affectés par la variabilité de la qualité de service, la vidéo, VoIP et la diffusion de contenus multimédias doivent être envoyées dans un ordre spécifique, à une vitesse régulière et avec un délai minimum entre les transmissions de **Packet - Paquet**. Si la qualité de service est compromise, le son ou l'image sera déformée.

19.1.1 QoS et équilibrage de la charge

À l'aide d'une combinaison d'équilibrage de la charge (reportez-vous au Chapitre 18 : « Équilibrage de la charge ») et de techniques QoS, vous pouvez fournir une haute qualité de service aux applications urgentes, même sur un réseau chargé. L'équilibrage de la charge est un moyen de mieux distribuer le volume de trafic entre les points d'accès. La qualité de service est un moyen d'allocation d'accès réseau et de bande passante basée sur des priorités de transmission pour les différents types de trafic sans fil dans un seul point d'accès.

19.1.2 Prise en charge des normes 802.11e et WMM

QoS décrit une gamme de technologies de contrôle des flux de données sur les connexions de réseau partagé. Le groupe de tâches **IEEE802.11e** est inclus dans le processus de définition d'une norme de qualité de service pour la qualité de transmission et la disponibilité de service sur des réseaux sans fil. La QoS est conçue pour offrir un meilleur service réseau en réduisant l'encombrement réseau ; en limitant **Jitter - Gigue**, **Latence** et **Packet Loss - Perte de paquets** ; en prenant en charge une bande passante dédiée pour les applications urgentes ou essentielles et en hiérarchisant le trafic sans fil d'accès aux canaux.

Comme avec toutes les normes de groupe de travail IEEE **802.11**, l'objectif est de fournir une méthode standard de mise en œuvre de fonctionnalités QoS afin que les composants de différentes sociétés soientinteropérables.

La passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway assure la QoS selon la spécification *Wireless Multimedia (WMM)* et les normes *Wireless Multimedia (WMM)*, qui sont les mises en œuvre d'un sous-ensemble de fonctionnalités **802.11e**.

Les deux points d'accès et les clients sans fil (ordinateurs portables, produits d'électronique grand public) peuvent être compatibles WMM.

19.1.3 Files d'attente et paramètres QoS pour coordonner le flux de trafic

Configurer les options QoS sur la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway consiste à définir des paramètres sur les files d'attente existantes pour différents types de trafic sans fil. Vous pouvez configurer des temps d'attente minimum et maximum différents pour la transmission de paquets dans chaque file d'attente en fonction des besoins du support en cours d'envoi. Les files d'attente fournissent automatiquement un délai de transmission minimum pour la voix, la vidéo, le contenu multimédia et les applications essentielles, et dépendent des paramètres de « meilleur effort » pour les données IP traditionnelles.

Par exemple, la voix, la vidéo et le contenu multimédia reçoivent une priorité plus efficace pour la transmission (temps d'attente inférieurs d'accès au canaux), tandis que d'autres applications et les données IP traditionnelles qui sont moins urgentes, mais souvent plus consommatrices de données, doivent tolérer des temps d'attente plus longs.

La passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway met en œuvre QoS selon la norme IEEE Wireless Multimedia (WMM). Une catégorie de mise en file d'attente Linux est utilisée pour marquer les paquets et établir plusieurs files d'attente. Ces files d'attente disposent d'une définition des priorités et d'un routage intégrés en fonction du type de données en cours de transmission.

L'interface d'administration vous fournit un moyen de configurer les paramètres sur les files d'attente.

19.1.3.1 Files d'attente QoS et type de service (ToS) pour les paquets

QoS sur la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway exploite les informations **WMM** contenues dans l'en-tête du paquet **IP** liée au type de service (**ToS**). Chaque paquet IP envoyé via le réseau comprend un champ ToS dans son en-tête, qui indique comment les données doivent être hiérarchisées et transmises sur le réseau. Le champ ToS est constitué d'une valeur entre 3 et 7 bits où chaque bit représente un aspect différent ou le degré de priorité pour ces données, ainsi que d'autres méta-informations (faible retard, haut débit, fiabilité élevée, faible coût, etc.).

Par exemple, le ToS pour les paquets de données FTP est susceptible d'être défini pour un débit optimal puisque la caractéristique clé de FTP est la capacité de transmettre des quantités de données relativement importantes en une seule fois. Si le retour d'informations peut être utile dans cette situation, il n'est pas essentiel. Les paquets de données VoIP sont définis pour un délai minimum car c'est un facteur essentiel de qualité et de performances pour ce type de données.

Le point d'accès examine le champ ToS dans les en-têtes de tous les paquets qui passent par le point d'accès. En fonction de la valeur du champ ToS dans un paquet, le point d'accès gère la priorité du paquet pour la transmission en lui attribuant l'une des files d'attente. Ce processus est automatique, indépendamment du fait que vous configurez QoS délibérément ou non.

Un type de données différent est associé à chaque file d'attente. La file d'attente et les priorités et paramètres de transmission associés sont comme suit :

- Données 0 (voix). File d'attente de priorité la plus élevée, délai minimum. Les données urgentes telles que Voice over IP (VoIP) sont automatiquement envoyées à cette file d'attente.
- Données 1 (vidéo). File d'attente de priorité élevée, délai minimum. Les données urgentes telles que la vidéo et autres diffusions de contenus multimédias sont automatiquement envoyées à cette file d'attente.
- Données 2 (meilleur effort). File d'attente de priorité moyenne, débit et délai moyens. La plupart des données IP sont envoyées à cette file d'attente.
- Données 3 (arrière-plan). File d'attente de priorité la plus basse, débit élevé. Les données de masse nécessitant un débit maximal et qui ne sont pas urgentes sont envoyées à cette file d'attente (données FTP, par exemple).

Les paquets envoyés dans une file d'attente de priorité supérieure seront transmis avant les paquets envoyés dans une file d'attente de priorité inférieure. Les données interactives envoyées dans les files d'attente « Données 0 » et « Données 1 » sont toujours envoyées en premier, les données meilleur effort dans « Données 2 » sont transmises ensuite, et les données d'arrière-plan (masse) dans « Données 3 » sont envoyées en dernier. Chaque file d'attente de priorité inférieure (catégorie de trafic) reçoit la bande passante restante une fois que les catégories de trafic supérieures ont été envoyées. Dans des cas extrêmes, si vous disposez de suffisamment de données interactives pour maintenir le point d'accès occupé tout le temps, le trafic de faible priorité ne sera jamais envoyé.

En utilisant les paramètres QoS dans l'interface d'administration, vous pouvez configurer les paramètres *Enhanced Distributed Channel Access* (EDCA) qui déterminent la manière dont chaque file d'attente est traitée lorsqu'elle est envoyée par le point d'accès au client ou par le client au point d'accès.



Remarque : Le trafic sans fil est acheminé :

- en aval du point d'accès vers la station client
- en amont de la station client vers le point d'accès
- en amont du point d'accès vers le réseau
- en aval du réseau vers le point d'accès

Si WMM est activé, les paramètres QoS sur la passerelle sans fil 9160 G2 Wireless Gateway affectent les deux premières catégories de trafic : le trafic en aval circulant entre le point d'accès et la station client (paramètres EDCA du point d'accès) et le trafic en amont circulant de la station vers point d'accès (paramètres EDCA de la station).

Si WMM est désactivé, vous pouvez toujours définir les paramètres sur le trafic en aval circulant du point d'accès vers la station client (paramètres EDCA du point d'accès).

Les autres phases du flux de trafic (vers et depuis le réseau) ne sont pas sous le contrôle des paramètres QoS du point d'accès.

19.1.3.2 Contrôle EDCF des trames de données et espaces indépendant d'arbitrage

Les données sont transmises sur les réseaux sans fil 802.11 dans des *trames*. Une **Frame - Trame** se compose d'une partie discrète de données ainsi que de méta-informations descriptives fournies pour la transmission sur un réseau sans fil.



Remarque : Une trame s'apparente à un paquet, à la différence qu'un paquet fonctionne sur la couche réseau (couche 3 du modèle OSI) tandis qu'une trame fonctionne sur la couche Data-Link (couche 2 du modèle OSI).

Chaque trame inclut une adresse MAC source et destination, un champ de contrôle avec la version de protocole, le type de trame, le numéro de séquence de la trame, le corps de la trame (avec les informations devant être transmises) et la séquence de contrôle de trame pour la détection d'erreur.

La norme 802.11 définit différents types de *trame* pour la gestion et le contrôle de l'infrastructure sans fil, et pour la transmission de données. Les types de trame 802.11 sont les suivantes : (1) *trames de gestion*, (2) *trames de contrôle* et (3) *trames de données*. Les trames de gestion et de contrôle (qui gèrent et contrôlent la disponibilité de l'infrastructure sans fil) ont automatiquement une priorité plus élevée pour la transmission.

802.11E utilise des *espaces indépendants* pour réguler les trames qui ont accès aux canaux disponibles et coordonner les temps d'attente pour la transmission de données de types différents.

Les trames de gestion et de contrôle attendent un minimum de temps pour la transmission ; elles patientent le temps d'un *court espace indépendant* (SIF). Ces temps d'attente sont intégrés dans 802.11 comme prise en charge d'infrastructure et ils ne sont pas configurables.

La passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway prend en charge *Enhanced Distribution Coordination Function (EDCF)* tel que défini par la norme **802.11e**. EDCF, qui est une amélioration de la norme **DCF** basée sur le protocole **CSMA/CA**, définit l'espace indépendant (IFS) entre les *trames de données*. Les trames de données attendent le temps défini comme espace indépendant d'arbitrage (AIFS) avant d'être transmises.

Ce paramètre est configurable.



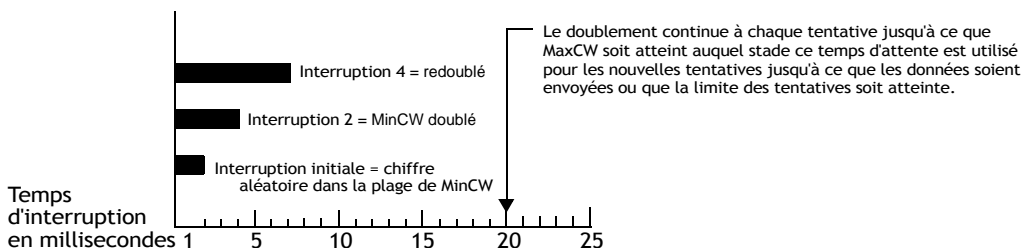
Remarque : Envoyer des trames de données dans des AIFS permet d'envoyer en premier des trames de gestion et de contrôle de priorité plus élevée dans les IFS.

L'AIFS garantit que plusieurs points d'accès n'essaient pas d'envoyer des données en même temps, mais qu'ils attendent qu'un canal soit libre.

19.1.3.3 Interruption aléatoire et fenêtres de contention minimale/maximale

Si un point d'accès détecte que le support est en cours d'utilisation (occupé), il utilise le minuteur d'*interruption aléatoire* DCF pour déterminer le délai d'attente avant la prochaine tentative d'accès à un canal donné. Chaque point d'accès attend une certaine durée aléatoire entre chaque nouvelle tentative. Le temps d'attente (initialement une valeur aléatoire dans une plage spécifiée en tant que *Minimum Contention Window - fenêtre de contention minimale*) augmente de façon exponentielle jusqu'à une limite spécifiée (*Maximum Contention Window - fenêtre de contention maximale*). Le délai aléatoire évite la plupart des collisions qui pourraient se produire si plusieurs points accédaient au support en même temps et tentaient de transmettre des données simultanément. Plus vous avez d'utilisateurs actifs sur un réseau, plus les gains de performances du minuteur d'interruption seront importants par la réduction du nombre de collisions et de retransmissions.

Figure 19.1 Minuteur d'interruption aléatoire DCF



L'interruption aléatoire utilisée par le point d'accès est un paramètre configurable. Pour décrire le délai aléatoire, une « fenêtre de contention minimale » (MinCW) et une « fenêtre de contention maximale » (MaxCW) sont définies.

- La valeur indiquée pour la *fenêtre de contention minimale* est la limite supérieure d'une plage pour le temps d'attente d'interruption aléatoire initial. Le numéro utilisé pour l'interruption aléatoire est initialement un nombre aléatoire entre 0 et le nombre défini pour la fenêtre de contention minimale.
- Si le délai de la première interruption aléatoire prend fin avant la transmission de la trame de données, le point d'accès active un nouveau compteur de tentative de reconnexion et double la valeur de la fenêtre d'interruption aléatoire. La valeur indiquée dans la *fenêtre de contention maximale* est la limite supérieure de ce doublement de l'interruption aléatoire. Ce doublement continue jusqu'à ce que la trame de données soit envoyée ou que la taille de la fenêtre de contention maximale soit atteinte.

19.1.3.4 Salve de paquets pour de meilleures performances

La passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway inclut une technologie de *salve de paquets* 802.11e qui permet d'augmenter le débit de données et la vitesse de transmission sur le réseau sans fil. La salve de paquets permet la transmission de plusieurs paquets sans la surcharge supplémentaire des informations d'en-tête. Son effet est d'augmenter la vitesse du réseau et le débit de données. La taille des salves de paquet autorisée (la longueur de salve maximale) est un paramètre configurable.

19.1.3.5 Intervalle Transmission Opportunity (TXOP) pour stations client

Transmission Opportunity (TXOP) est un intervalle de temps pendant lequel une station client Wi-Fi Multimedia (WMM) a le droit d'initier la transmission sur le support sans fil (WM).

19.1.4 802.1p et balises DSCP

IEEE **802.1p** est une extension de la norme IEEE 802 responsable de la disposition QoS. L'objectif principal de 802.1p est de hiérarchiser le trafic réseau au niveau de la couche Data-Link/MAC. 802.1P offre la possibilité de filtrer le trafic multidiffusion pour assurer qu'il n'augmente pas sur les réseaux commutés de couche 2. Il utilise des trames balises pour la hiérarchisation des priorités. Afin d'être conforme à cette norme, les commutateurs de couche 2 doivent être capables de regrouper les paquets entrants LAN en plusieurs catégories de trafic.

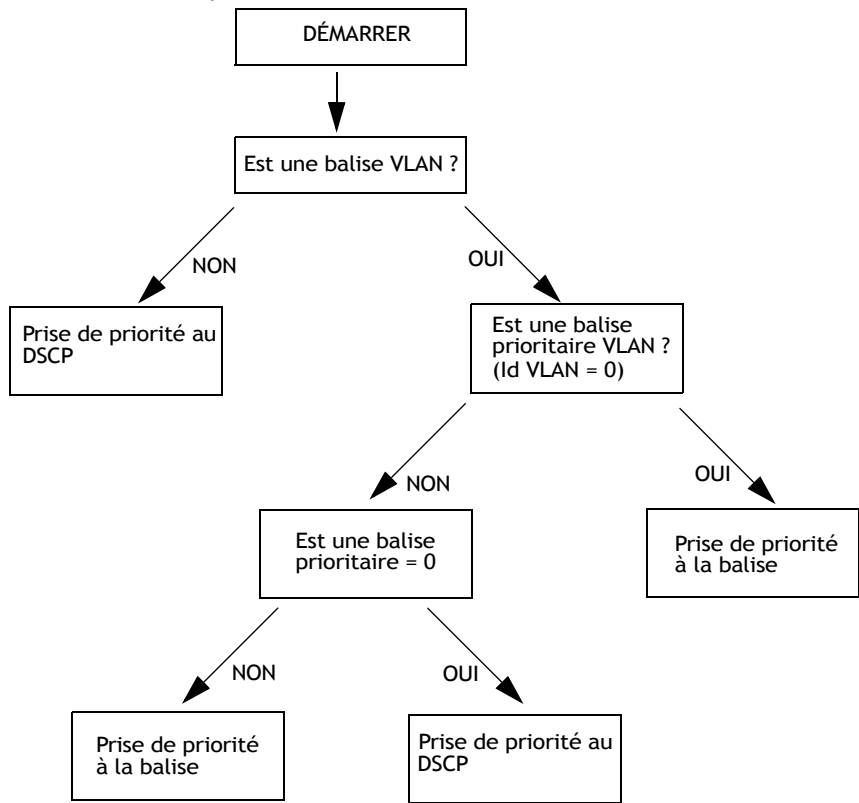
L'en-tête 802.1p inclut un champ à trois bits pour la définition des priorités, ce qui permet de regrouper les paquets en différentes catégories de trafic. Huit niveaux de priorité sont définis. La priorité la plus élevée est sept, qui peut être réservée au trafic réseau urgent (voix). Les paquets hautement prioritaires sont toujours transmis en premier. Les paquets de priorité plus faible ne sont pas transmis si les paquets hautement prioritaires sont toujours en transmission, plutôt que d'être mis dans une file d'attente jusqu'à ce que les paquets plus urgents aient bien été transmis. Le niveau de priorité le plus faible est défini sur zéro. Il est utilisé comme valeur de meilleur effort par défaut et appelé automatiquement si aucune valeur n'a été définie.



Remarque : Il est important de remarquer que 802.1p ne fonctionne pas à moins que QoS et WMM soient activés. WMM doit être activé sur le point d'accès et sur le client qui se connecte au point d'accès.

Le schéma de flux dans la Figure 19.2 décrit la manière dont les balises sont récupérées et dont le trafic est hiérarchisé sur un réseau.

Figure 19.2 Définition des priorités du trafic réseau



19.1.4.1 Priorité VLAN

Le Tableau 19.1 décrit les balises de priorité et leurs valeurs associées prises sur une balise VLAN.

Tableau 19.1 Priorités de balise VLAN

Balise ID VLAN	Priorité
0 - Valeur DHCP par défaut	Meilleur effort
1	Arrière-plan
2	Arrière-plan

Tableau 19.1 Priorités de balise VLAN

Balise ID VLAN	Priorité
3	Meilleur effort
4	Vidéo
5	Vidéo
6	Voix
7	Voix

19.1.4.2 Priorité DSCP

Le Tableau 19.2 décrit les valeurs DSCP, l'ID associé et le niveau de priorité.

Tableau 19.2 Priorités de balise DSCP

Balise ID	Priorité	Valeur DSCP
0 - Valeur DHCP par défaut	Meilleur effort	0
1	Arrière-plan	16
2	Arrière-plan	8
3	Meilleur effort	24
4	Vidéo	32
5	Vidéo	40
6	Voix	48
7	Voix	56

19.2 Configuration des files d'attente QoS

Pour configurer des files d'attente pour la qualité de service, accédez à l'onglet *Services > QoS* (Services > QoS) et configurez les paramètres comme décrit ci-dessous.

Figure 19.3 Paramètres Qualité de service (QoS)

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Modify QoS queue parameters

Queue

AIFS

cwMin

cwMax

Max. Burst

Data 0 (Voice)

1

3

7

1.5

Data 1 (Video)

1

7

15

3.0

Data 2 (Best Effort)

3

15

63

0

Data 3 (Background)

7

15

1023

0

AP EDCA parameters

Wi-Fi Multimedia (WMM)

☒ Enabled ☐ Disabled

Queue

AIFS

cwMin

cwMax

TXOP Limit

Data 0 (Voice)

2

3

7

47

Data 1 (Video)

2

7

15

94

Data 2 (Best Effort)

3

15

1023

0

Data 3 (Background)

7

15

1023

0

Station EDCA parameters

Update

Configurer la Qualité de Service (*QoS*) sur la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway consiste à définir des paramètres sur les files d'attente existantes pour différents types de trafic sans fil et à spécifier de façon efficace des temps d'attentes minimal et maximal (via des *fenêtres de contention*) pour la transmission. Les paramètres décrits ici s'appliquent au comportement de transmission de données uniquement sur le point d'accès, pas à celui des stations client.



Remarque : Pour l'interface invité, les paramètres de file d'attente QoS s'appliquent à la charge au point d'accès dans son ensemble (les deux BSS en même temps).

Sur un point d'accès pour radio professionnelle, ces paramètres s'appliquent aux deux radios mais le trafic de chaque radio est mis dans une file d'attente indépendante. (L'exception étant le trafic invité comme indiqué ci-dessous.)

Le trafic réseau interne et invité est toujours regroupé dans la même file d'attente pour chaque radio. C'est le cas à la fois sur les points d'accès pour radio unique ou radio professionnelle.

La QoS sur le point d'accès exploite les informations contenues dans l'en-tête du paquet IP liée au type de service (**ToS**). Le point d'accès examine le champ ToS dans les en-têtes de tous les paquets qui passent par le point d'accès. En fonction de la valeur du champ ToS dans un paquet, le point d'accès gère la priorité du paquet pour la transmission en lui attribuant l'une des files d'attente. Un type de données différent est associé à chaque file d'attente. Vous pouvez configurer les paramètres qui déterminent la manière dont chaque file d'attente est traitée lorsqu'elle est envoyée par le point d'accès.

La configuration de la Qualité de service (QoS) inclut :

- « Configuration des paramètres EDCA du point d'accès » à la page 208.
- « Activation/désactivation de Wi-Fi Multimedia » à la page 210.
- « Mise à jour des paramètres » à la page 212.

19.2.1 Configuration des paramètres EDCA du point d'accès

Les paramètres Enhanced Distributed Channel Access (EDCA) du point d'accès affectent le trafic circulant du point d'accès vers la station client.

Tableau 19.3 Paramètres EDCA du point d'accès

Champ	Description
<i>Queue (File d'attente)</i>	<p>Les files d'attente sont définies pour les différents types de données transmises depuis le point d'accès vers la station :</p> <p>Données 0 (voix)</p> <p>File d'attente de priorité élevée, délai minimum. Les données urgentes telles que Voice-over-IP et la diffusion de contenus multimédias sont automatiquement envoyées à cette file d'attente.</p> <p>Données 1 (vidéo)</p> <p>File d'attente de priorité élevée, délai minimum. Les données vidéo urgentes sont automatiquement envoyées à cette file d'attente.</p> <p>Données 2 (meilleur effort)</p> <p>File d'attente de priorité moyenne, débit et délai moyens. La plupart des données IP sont envoyées à cette file d'attente.</p> <p>Données 3 (arrière-plan)</p> <p>File d'attente de priorité la plus basse, débit élevé. Les données de masse nécessitant un débit maximal et qui ne sont pas urgentes sont envoyées à cette file d'attente (données FTP, par exemple).</p> <p>Pour plus d'informations, reportez-vous à la section « Files d'attente et paramètres QoS pour coordonner le flux de trafic » à la page 198.</p>
<i>AIFS (AIFS) (Interframe Space - Espace indépendant)</i>	<p>L'<i>espace indépendant d'arbitrage</i> (AIFS) précise un temps d'attente (en millisecondes) pour les <i>trames de données</i>.</p> <p>Les valeurs valides pour AIFS vont de 1 à 255.</p> <p>Pour plus d'informations, reportez-vous à la section Contrôle DCF des trames de données et des espaces indépendants.</p> <p>Pour plus d'informations, reportez-vous à la section « Contrôle EDCF des trames de données et espaces indépendant d'arbitrage » à la page 200.</p>

Tableau 19.3 Paramètres EDCA du point d'accès

Champ	Description
<i>cwMin (cwMin) (Minimum Contention Window - Fenêtre de contention minimale)</i>	<p>Ce paramètre est entré dans l'algorithme qui détermine le temps d'attente d'interruption aléatoire initial (« fenêtre ») pour réessayer une transmission.</p> <p>La valeur indiquée ici dans la <i>fenêtre de contention minimale</i> est la limite supérieure (en millisecondes) d'une plage à partir de laquelle le temps d'attente d'interruption aléatoire initial est déterminé.</p> <p>Le premier nombre aléatoire généré sera compris entre 0 et le numéro indiqué ici.</p> <p>Si le premier temps d'attente d'interruption aléatoire expire avant l'envoi de la trame de données, un compteur de tentative de reconnexion est activé et la valeur d'interruption aléatoire (fenêtre) est doublée. Le doublement continue jusqu'à ce que la taille de la valeur d'interruption aléatoire atteigne le nombre défini dans la fenêtre de contention maximale.</p> <p>Les valeurs valides pour « cwmin » sont 1, 3, 7, 15, 31, 63, 127, 255, 511 ou 1023.</p> <p>Pour plus d'informations, reportez-vous à la section « Interruption aléatoire et fenêtres de contention minimale/maximale » à la page 201.</p>
<i>cwMax (cwMax) (Maximum Contention Window - Fenêtre de contention maximale)</i>	<p>La valeur indiquée ici dans la <i>fenêtre de contention maximale</i> est la limite supérieure (en millisecondes) du doublement de la valeur d'interruption aléatoire. Ce doublement continue jusqu'à ce que la trame de données soit envoyée ou que la taille de la fenêtre de contention maximale soit atteinte.</p> <p>Une fois que la taille de la fenêtre de contention maximale est atteinte, les nouvelles tentatives se poursuivent jusqu'à ce que le nombre maximal de tentatives autorisées soit atteint.</p> <p>Les valeurs valides pour « cwmax » sont 1, 3, 7, 15, 31, 63, 127, 255, 511 ou 1023.</p> <p>Pour plus d'informations, reportez-vous à la section « Interruption aléatoire et fenêtres de contention minimale/maximale » à la page 201.</p>
<i>Max. Burst Length (Longueur max. de salve)</i>	<p>Paramètre EDCA du point d'accès uniquement (La longueur maximale de salve s'applique uniquement au trafic circulant entre le point d'accès et la station client.)</p> <p>Cette valeur indique (en millisecondes) la longueur maximale de salve autorisée pour les salves de paquets sur le réseau sans fil. Une <i>salve de paquets</i> est un ensemble de plusieurs trames transmises sans informations d'en-tête. La réduction de surcharge aboutit à un débit plus élevé et à de meilleures performances.</p> <p>Les valeurs valides pour la longueur maximale de salve vont de 0,0 à 999,9.</p> <p>Pour plus d'informations, reportez-vous à la section « Salve de paquets pour de meilleures performances » à la page 202.</p>

19.2.2 Activation/désactivation de Wi-Fi Multimedia

Par défaut, Wi-Fi Multimedia (WMM) est activé sur le point d'accès. Si WMM est activé, la définition des priorités QoS et la coordination de l'accès du support sans fil sont activés. Si WMM est activé, les paramètres QoS sur la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway contrôlent le trafic *en aval* circulant entre le point d'accès et la station client (paramètres EDCA du point d'accès) et le trafic *en amont* circulant de la station vers le point d'accès (paramètres EDCA de la station).

Désactiver WMM aura pour effet de désactiver le contrôle QoS des paramètres de contrôle de la station EDCA sur le trafic circulant *en amont* de la station vers le point d'accès. Si WMM est désactivé, vous pouvez toujours définir des paramètres sur le trafic circulant en aval du point d'accès vers la station client (paramètres EDCA du point d'accès).

- Pour désactiver les extensions WMM, cliquez sur **Disabled** (Désactivé).
- Pour activer les extensions WMM, cliquez sur **Enabled** (Activé).

19.2.3 Configuration des paramètres EDCA de la station

Les paramètres Enhanced Distributed Channel Access (EDCA) de la station affectent le trafic circulant de la station client vers le point d'accès.

Tableau 19.4 Configuration des paramètres EDCA de la station

Champ	Description
<i>Queue (File d'attente)</i>	<p>Les files d'attente sont définies pour les différents types de données transmises depuis la station vers le point d'accès :</p> <p>Données 0 (voix)</p> <p>File d'attente de priorité la plus élevée, délai minimum. Les données urgentes telles que Voice-over-IP et la diffusion de contenus multimédias sont automatiquement envoyées à cette file d'attente.</p> <p>Données 1 (vidéo)</p> <p>File d'attente de priorité la plus élevée, délai minimum. Les données vidéo urgentes sont automatiquement envoyées à cette file d'attente.</p> <p>Données 2 (meilleur effort)</p> <p>File d'attente de priorité moyenne, débit et délai moyens. La plupart des données IP sont envoyées à cette file d'attente.</p> <p>Données 3 (arrière-plan)</p> <p>File d'attente de priorité la plus basse, débit élevé. Les données de masse nécessitant un débit maximal et qui ne sont pas urgentes sont envoyées à cette file d'attente (données FTP, par exemple).</p> <p>Pour plus d'informations, reportez-vous à la section « Files d'attente et paramètres QoS pour coordonner le flux de trafic » à la page 198.</p>
<i>AIFS (AIFS) (Interframe Space - Espace indépendant)</i>	<p>L'<i>espace indépendant d'arbitrage (AIFS)</i> précise un temps d'attente (en millisecondes) pour les <i>trames de données</i>.</p> <p>Pour plus d'informations, reportez-vous à la section Contrôle DCF des trames de données et des espaces indépendants.</p> <p>Pour plus d'informations, reportez-vous à la section « Contrôle EDCF des trames de données et espaces indépendant d'arbitrage » à la page 200.</p>

Tableau 19.4 Configuration des paramètres EDCA de la station

Champ	Description
<i>cwMin (cwMin)</i> <i>(Minimum</i> <i>Contention Window -</i> <i>Fenêtre de contention</i> <i>minimale)</i>	<p>Ce paramètre est entré dans l'algorithme qui détermine le temps d'attente d'interruption aléatoire initial (« fenêtre ») pour réessayer une transmission.</p> <p>La valeur indiquée ici dans la <i>fenêtre de contention minimale</i> est la limite supérieure (en millisecondes) d'une plage à partir de laquelle le temps d'attente d'interruption aléatoire initial est déterminé.</p> <p>Le premier nombre aléatoire généré sera compris entre 0 et le numéro indiqué ici.</p> <p>Si le premier temps d'attente d'interruption aléatoire expire avant l'envoi de la trame de données, un compteur de tentative de reconnexion est activé et la valeur d'interruption aléatoire (fenêtre) est doublée. Le doublement continue jusqu'à ce que la taille de la valeur d'interruption aléatoire atteigne le nombre défini dans la fenêtre de contention maximale.</p> <p>Pour plus d'informations, reportez-vous à la section « Interruption aléatoire et fenêtres de contention minimale/maximale » à la page 201.</p>
<i>cwMax (cwMax)</i> <i>(Maximum</i> <i>Contention Window -</i> <i>Fenêtre de contention</i> <i>maximale)</i>	<p>La valeur indiquée ici dans la <i>fenêtre de contention maximale</i> est la limite supérieure (en millisecondes) du doublement de la valeur d'interruption aléatoire. Ce doublement continue jusqu'à ce que la trame de données soit envoyée ou que la taille de la fenêtre de contention maximale soit atteinte.</p> <p>Une fois que la taille de la fenêtre de contention maximale est atteinte, les nouvelles tentatives se poursuivent jusqu'à ce que le nombre maximal de tentatives autorisées soit atteint.</p> <p>Pour plus d'informations, reportez-vous à la section « Interruption aléatoire et fenêtres de contention minimale/maximale » à la page 201.</p>
<i>TXOP Limit</i> <i>(Limite TXOP)</i>	<p>Paramètre EDCA de la station uniquement (La limite TXOP s'applique uniquement au trafic circulant de la station client vers le point d'accès.)</p> <p><i>Transmission Opportunity</i> (TXOP) est un intervalle de temps pendant lequel une station client WME a le droit d'initier la transmission sur le support sans fil (WM).</p> <p>Cette valeur indique (en millisecondes) la valeur de <i>Transmission Opportunity</i> (TXOP) pour les stations client, c'est-à-dire l'intervalle de temps pendant lequel une station client WMM a le droit d'initier la transmission sur le réseau sans fil.</p>

19.3 Mise à jour des paramètres

Pour mettre à jour les paramètres QoS :

1. Accédez à l'onglet *QoS* (QoS).
2. Configurez les paramètres QoS selon les besoins.
3. Cliquez sur le bouton **Update** (Mettre à jour) pour appliquer les modifications.

SYSTÈME DE DISTRIBUTION SANS FIL (WDS) 20

20.1 Présentation du système de distribution sans fil (WDS)	215
20.1.1 Utilisation de WDS pour ponter les réseaux locaux filaires distants . . .	215
20.1.2 Utilisation de WDS pour étendre réseau au-delà de la zone de couverture filaire	216
20.1.3 Utilisation de WDS pour la création de liaisons de sauvegarde.	217
20.2 Remarques relatives à la sécurité associées aux liaisons WDS.	217
20.2.1 Présentation du cryptage de données WEP statique	218
20.2.2 Présentation du cryptage de données WPA (PSK)	218
20.3 Configuration des paramètres WDS	219
20.3.1 Exemple de configuration d'une liaison WDS.	222
20.4 Mise à jour des paramètres	223

La passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway vous permet de connecter plusieurs points d'accès en utilisant un système de distribution sans fil - Wireless Distribution System (**WDS**). WDS permet aux points d'accès de communiquer les uns avec les autres par liaison sans fil. Cette capacité est essentielle pour fournir une expérience transparente pour les clients itinérants et gérer plusieurs réseaux sans fil. Elle permet également de simplifier l'infrastructure réseau en réduisant la quantité de câblage requis.

Les sections suivantes décrivent la manière de configurer le WDS sur la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway.

20.1 Présentation du système de distribution sans fil (WDS)

Un *système de distribution sans fil (WDS)* est une technologie qui connecte les points d'accès par liaison sans fil, aussi appelé Basic Base Sets - Ensembles de services de base (**BSS**), pour former ce qu'on appelle un *Extended Service Set - Ensemble de services étendu (ESS)*.

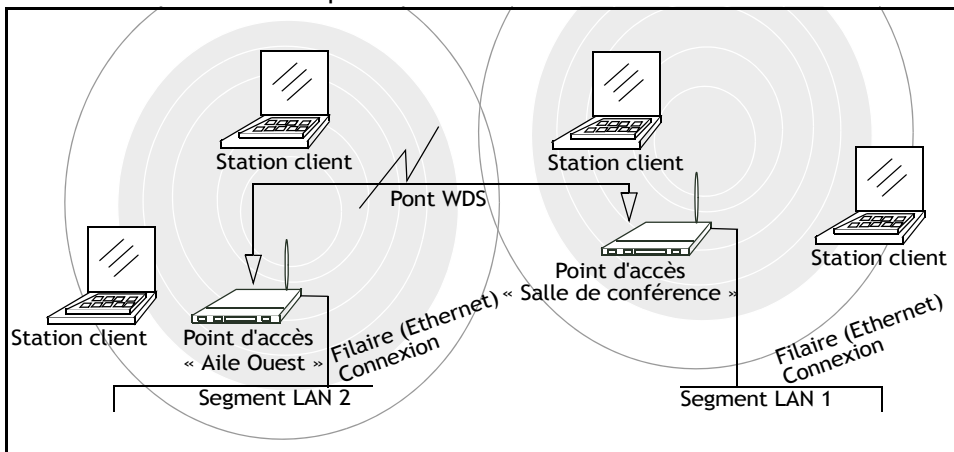


Remarque : Un BSS correspond généralement à un point d'accès (déployé comme « réseau » sans fil à point d'accès unique), sauf dans les cas où des fonctionnalités multi-BSSID font ressembler un point d'accès unique à au moins deux points d'accès pour le réseau. Dans ce cas, le point d'accès a plusieurs BSSID uniques.

20.1.1 Utilisation de WDS pour ponter les réseaux locaux filaires distants

Dans un **ESS**, un réseau à plusieurs points d'accès, chaque point d'accès dessert une partie d'une zone qui est trop grande pour être couverte par un point d'accès unique. Vous pouvez utiliser le WDS pour ponter les Ethernets distants afin de créer un **LAN** unique. Par exemple, supposons que vous disposiez d'un point d'accès qui est connecté au réseau via Ethernet et qui dessert plusieurs stations client dans la Salle de conférence (Segment LAN 1), et un autre point d'accès filaire Ethernet desservant les stations dans les bureaux de l'Aile Ouest (Segment LAN 2). Vous pouvez établir un pont reliant les points d'accès de la Salle de conférence et de l'Aile Ouest avec une liaison WDS pour créer un réseau unique pour les clients dans les deux zones (reportez-vous à la Figure 20.1 à la page 216).

Figure 20.1 LAN filaires distants pontés

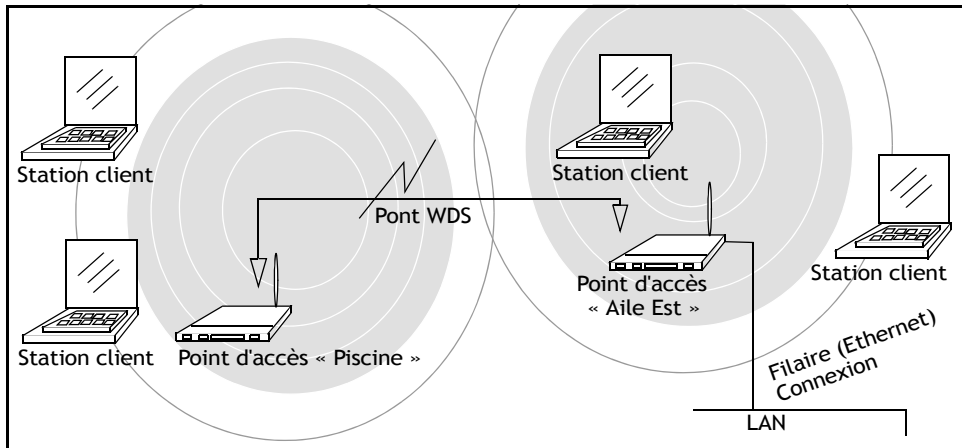


20.1.2 Utilisation de WDS pour étendre réseau au-delà de la zone de couverture filaire

Un *ESS* peut étendre la portée du réseau dans des zones où le câblage serait difficile, coûteux ou inefficace.

Par exemple, supposons que vous disposiez d'un point d'accès qui est connecté au réseau via Ethernet et qui dessert plusieurs stations client dans une zone (« Aile Est » dans notre exemple), mais qui ne peut pas en atteindre d'autres qui sont hors de portée. Supposons également qu'il est trop difficile ou trop coûteux de câbler la zone avec un câblage Ethernet. Vous pouvez résoudre ce problème en plaçant un deuxième point d'accès plus proche du deuxième groupe de stations (« Piscine » dans l'exemple de la Figure 20.2 à la page 217) et relier les deux points d'accès par une liaison WDS. Cela permet d'*étendre* votre réseau par liaison sans fil en fournissant un saut supplémentaire pour accéder aux stations distantes (reportez-vous à la Figure 20.2 à la page 217).

Figure 20.2 Réseau étendu au-delà de la zone de couverture filaire



20.1.3 Utilisation de WDS pour la création de liaisons de sauvegarde

Une autre utilisation du pontage WDS est la création de liaisons de sauvegarde. Avec *Spanning Tree Protocol (STP)* activé automatiquement sur la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway, WDS peut être utilisé pour configurer des chemins de sauvegarde entre les points d'accès sur le réseau. Par exemple, entre deux points d'accès, vous pouvez avoir à la fois un chemin principal via Ethernet et un chemin sans fil secondaire (sauvegarde) via une liaison WDS. Si la connexion Ethernet tombe en panne, STP reconfigure sa carte du réseau et répare le segment en panne en activant le chemin de sauvegarde sans fil.

20.2 Remarques relatives à la sécurité associées aux liaisons WDS

Il est important de définir un type de sécurité sur les liaisons WDS. Vous pouvez définir n'importe quel type de sécurité sur la liaison WDS, quel que soit le paramètre de sécurité appliqué aux points d'accès de la liaison. Par exemple, vous pouvez avoir la sécurité du point d'accès AP1 définie sur **None** (Aucun) et celle du point d'accès AP2 définie sur **WEP**. Même si les deux paramètres sont différents, vous pouvez choisir de définir la sécurité de la liaison WDS sur None (Aucun) ou WEP. La seule exception à cette règle survient dans le cas de WPA (PSK). Le paramètre de sécurité WPA (PSK) peut uniquement être défini sur la liaison WDS si vous avez configuré la sécurité d'AP1 et AP2 sur le mode WPA Personal ou WPA Enterprise.

20.2.1 Présentation du cryptage de données WEP statique

Wired Equivalent Privacy statique (WEP) est un protocole de cryptage pour les réseaux sans fil 802.11. Les deux points d'accès dans une liaison WDS donnée doivent être configurés avec les mêmes paramètres de sécurité. Pour WEP statique, vous devez spécifier une clé partagée 64 bits (clé secrète 40 bits + vecteur d'initialisation (IV) 24 bits) ou 128 bits (clé secrète 104 bits + IV 24 bits) pour le cryptage des données.

Vous pouvez activer *WEP* statique sur la liaison WDS (pont). Lorsque WEP est activé, toutes les données échangées entre les deux points d'accès via une liaison WDS sont cryptées à l'aide d'une clé WEP fixe que vous fournissez.

WEP statique ne fournit pas une protection des données au niveau d'autres modes de sécurité disponibles pour les stations client. Si vous utilisez WEP statique sur un *LAN* destiné à un trafic sans fil sécurisé, vous exposez votre réseau à un risque. Par conséquent, nous vous recommandons d'utiliser le cryptage WPA (PSK) sur toute liaison WDS sur un réseau interne. N'utilisez pas un WDS basé sur WEP statique pour ponter des points d'accès sur le réseau interne sauf si vous n'avez aucune inquiétude concernant la sécurité du trafic de données sur ce réseau. Pour plus d'informations sur WPA (PSK), reportez-vous à la section « Présentation du cryptage de données WPA (PSK) », ci-dessous.

Pour plus d'informations sur l'efficacité des différents modes de sécurité, reportez-vous au Chapitre 10 : « Configuration de la sécurité ». Cette rubrique couvre également l'utilisation du mode de sécurité non crypté pour le trafic du point d'accès à la station sur le réseau invité, qui est conçu pour le trafic de données moins sensible.

20.2.2 Présentation du cryptage de données WPA (PSK)

Wi-Fi Protected Access (Pre-Shared Key) ou WPA (PSK) est une forme de sécurité plus robuste que WEP statique. Anciennement appelé « WPA-Home », WPA (PSK) fonctionne grâce à une clé prépartagée qui est essentiellement un mot de passe partagé entre les points d'accès sur une liaison pontée. WPA (PSK) fournit une sécurité sans fil 802.11 sans nécessiter une infrastructure d'authentification RADIUS, qui est à la fois complexe et onéreuse à mettre en œuvre.

Le cryptage WPA (PSK) s'appuyant sur une clé partagée, les deux points d'accès de la liaison WDS doivent être définis avec la même clé ; sinon, ils ne pourront pas communiquer et partager des informations.



Remarque : Pour des raisons de sécurité, il est recommandé que vous modifiiez régulièrement les clés partagées sur votre pont WDS.

Pour plus d'informations sur l'efficacité des différents modes de sécurité, reportez-vous au Chapitre 10 : « Configuration de la sécurité ».

20.3 Configuration des paramètres WDS

Pour spécifier les informations d'échange de trafic de ce point d'accès vers d'autres, accédez à l'onglet **Manage > WDS** (Gérer > WDS) et mettez à jour les champs comme décrit ci-dessous.



Remarque : La Figure 20.3 illustre la page des paramètres WDS pour un point d'accès de radio professionnelle. La page Web d'administration pour le point d'accès de radio unique est légèrement différente.

Figure 20.3 Paramètres du système de distribution sans fil (WDS)

Basic Settings	<h3>Configure WDS bridges to other access points</h3> <div><div>Local Address00:08:A2:01:4B:56</div><div>Remote Address<input type="text"/></div><div>EncryptionNone (Plain-text)</div></div> <div><div>Remote Address<input type="text"/></div><div>EncryptionNone (Plain-text)</div></div> <div><div>Remote Address<input type="text"/></div><div>EncryptionNone (Plain-text)</div></div> <div><div>Remote Address<input type="text"/></div><div>EncryptionNone (Plain-text)</div></div> <div><div>Update</div></div>
User Management	
Cluster	
Access Points	
Sessions	
Channel Management	
Wireless Neighborhood	
Security	
Status	
Interfaces	
Events	
Transmit/Receive	
Client Associations	
Neighboring Access Points	
Manage	
Ethernet Settings	
802.11 Settings	
802.11 Advanced Settings	
VWN	
WDS	
Guest Login	

Les remarques suivantes résument certaines directives essentielles concernant la configuration de **WDS**. Veuillez lire toutes ces remarques avant de poursuivre la configuration de WDS.



Remarque : Lorsque vous utilisez WDS, assurez-vous de configurer les paramètres WDS sur les deux points d'accès participant à la liaison WDS.

Vous ne pouvez avoir qu'une seule liaison WDS entre chaque paire de points d'accès. Autrement dit, une adresse MAC distante ne peut apparaître qu'une seule fois sur la page WDS pour un point d'accès particulier.

Les deux points d'accès qui participent à une liaison WDS doivent se trouver sur le même canal radio et utiliser le même mode IEEE 802.11. (Reportez-vous au Chapitre 16 : « Configuration des paramètres radio 802.11 » pour plus d'informations sur la configuration du mode radio et canal).

Lorsque 802.11h est opérationnel, la configuration des liaisons WDS peut s'avérer difficile. Reportez-vous à la section « 802.11h Regulatory Domain Control (Contrôle du domaine réglementaire 802.11h) » à la page 155.

Pour configurer WDS sur ce point d'accès, décrivez chaque point d'accès destiné à recevoir les transferts et envoyer des informations à ce point d'accès. Chaque point d'accès destinataire doit correspondre à la description ci-dessous, comme indiqué dans le Tableau 20.1.

Tableau 20.1 Paramètres du point d'accès destinataire

Champ	Description
<i>Local Address</i> (Adresse locale)	<p>Indique les adresses Media Access Control (<i>MAC</i>) pour ce point d'accès.</p> <p>Une adresse MAC est une adresse matérielle unique et permanente pour tout appareil qui représente une interface pour le réseau. L'adresse MAC est attribuée par le fabricant. Vous ne pouvez pas modifier l'adresse MAC. Elle est fournie ici à titre d'information comme identifiant unique pour le point d'accès ou l'interface.</p> <p>Point d'accès radio unique : Sur un point d'accès radio unique, une seule adresse MAC s'affiche en haut de la page des paramètres <i>WDS</i>. L'adresse indiquée pour le point d'accès radio unique est l'adresse MAC de ce point d'accès radio. C'est l'adresse par laquelle le point d'accès est connu en externe par d'autres réseaux.</p> <p>Point d'accès radio professionnelle : Pour chaque liaison WDS sur un point d'accès de radio professionnelle, l'<i>adresse locale</i> reflète l'adresse MAC pour l'interface interne de la radio sélectionnée (Radio Un sur WLAN0 ou Radio Deux sur WLAN1).</p>

Tableau 20.1 Paramètres du point d'accès destinataire

Champ	Description
<i>Remote Address (Adresse distante)</i>	<p>Indiquez l'adresse MAC du point d'accès destinataire. En d'autres termes, le point d'accès auquel les données seront envoyées ou « transférées » et depuis lequel les données seront reçues, autrement dit, le point d'accès pour lequel vous souhaitez créer le pont WDS.</p> <p>Cliquez sur la flèche à droite du champ <i>Remote Address</i> (Adresse distante) pour afficher la liste de toutes les adresses MAC et leurs SSID associés disponibles sur le réseau. Sélectionnez l'adresse MAC appropriée dans la liste.</p> <p>Remarque : <i>Le SSID affiché dans la liste déroulante vise simplement à vous aider à identifier l'adresse MAC appropriée pour le point d'accès destinataire. Ce SSID est un SSID différent de celui que vous avez défini pour la liaison WDS. Ils n'ont pas (et ne doivent pas avoir) la même valeur ou le même nom.</i></p>
<i>Encryption (Cryptage)</i>	<p>Si vous n'avez aucune inquiétude de sécurité sur la liaison WDS, vous pouvez décider de ne pas définir de type de cryptage. Par ailleurs, si vous avez des inquiétudes concernant la sécurité, vous pouvez choisir entre WEP statique et WPA (PSK).</p> <p>Remarque : <i>Les options de types de cryptage disponibles ici dépendent des paramètres que vous avez indiqués dans l'onglet Security (Sécurité). L'option WPA (PSK) sera uniquement disponible sur la page WDS si vous définissez le mode dans l'onglet Security (Sécurité) sur WPA Personal ou WPA Enterprise.</i></p> <p>None (Plain-text) - Aucun (texte brut) : Si vous définissez le cryptage sur None (Aucun), les données envoyées entre les points d'accès sur le pont WDS ne seront pas cryptées, mais seront envoyées sous forme de texte brut.</p> <p>WEP : Indiquez si vous souhaitez que le cryptage Wired Equivalent Privacy () WEP soit activé pour la liaison WDS. Wired Equivalent Privacy statique (WEP) est un protocole de cryptage pour les réseaux sans fil 802.11. Les deux points d'accès dans la liaison WDS doivent être configurés avec les mêmes paramètres de sécurité. Pour WEP statique, une clé partagée 64 bits (clé secrète 40 bits + vecteur d'initialisation (IV) 24 bits) ou 128 bits (clé secrète 104 bits + IV 24 bits) pour le cryptage des données. Pour plus d'informations sur la sécurité WEP, reportez-vous à la section « Static WEP (WEP statique) » à la page 109.</p> <p>WPA (PSK) : Indiquez si vous souhaitez que le cryptage WPA (PSK) soit activé pour la liaison WDS. Wi-Fi Protected Access (Pre-Shared Key), ou WPA (PSK), est une forme de sécurité plus robuste que WEP. Lorsque vous utilisez le cryptage WPA (PSK), chaque point d'accès sur votre réseau doit être défini avec la même clé unique. Dans le cas contraire, les points d'accès ne pourront pas communiquer les uns avec les autres.</p> <p>L'option WPA (PSK) sera uniquement disponible sur la page <i>WDS</i> si vous définissez le mode dans l'onglet <i>Security</i> (Sécurité) sur WPA Personal ou WPA Enterprise. Pour plus d'informations sur la sécurité, reportez-vous à la section « Présentation des problèmes de sécurité sur les réseaux sans fil » à la page 97.</p> <p>Pour plus d'informations sur la sécurité WPA (PSK), reportez-vous à la section « WPA Personal » à la page 117.</p>

20.3.1 Exemple de configuration d'une liaison WDS.

Lorsque vous utilisez WDS, assurez-vous de configurer les paramètres WDS sur *les deux* points d'accès de la liaison WDS. Par exemple, pour créer une liaison WDS entre une paire de points d'accès « **MyAP1** » et « **MyAP2** », procédez comme suit :

1. Ouvrez les pages Web d'administration pour MyAP1, en entrant l'adresse IP de MyAP1 comme une URL dans la barre d'adresse du navigateur Web au format suivant :

<http://AdresseIPduPointdAccès>

AdresseIPduPointdAccès étant l'adresse de MyAP1.

2. Accédez à l'onglet *WDS* sur les pages Web d'administration de MyAP1.

L'adresse MAC de MyAP1 (le point d'accès que vous êtes en train de consulter) s'affiche comme « adresse locale » en haut de la page.

3. Configurez une interface WDS pour l'échange de données avec MyAP2.
Commencez par entrer l'adresse MAC de MyAP2 dans le champ « Remote Address » (Adresse distante) et renseignez les autres champs afin de spécifier le réseau (invité ou interne), la sécurité, etc. Enregistrez les paramètres (cliquez sur **Update** (Mettre à jour)).

4. Accédez aux paramètres radio sur les pages Web d'administration (*Manage > 802.11 Advanced Settings* (Gérer > Paramètres avancés 802.11)) pour vérifier ou définir le mode et le canal radio sur lequel vous souhaitez que MyAP1 diffuse.

N'oubliez pas que les deux points d'accès participant à la liaison, MyAP1 et MyAP2, doivent être définis sur le même mode et transmettre sur le même canal.

Pour notre exemple, supposons que nous utilisons le mode IEEE 802.11b et que nous diffusons sur le canal 6. (Nous choisirions le mode et le canal dans les menus déroulants de l'onglet Radio.)

5. Répétez maintenant les mêmes étapes pour MyAP2 :
 - Ouvrez les pages Web d'administration pour MyAP2 via l'adresse IP de MyAP2 dans une URL.
 - Accédez à l'onglet *WDS* sur les pages Web d'administration de MyAP2. (L'adresse MAC de MyAP2 s'affichera comme « adresse locale ».)
 - Configurez une interface WDS pour l'échange des données avec MyAP1, en commençant par l'adresse MAC de MyAP1.
 - Accédez aux paramètres radio pour MyAP2 pour vérifier que celle-ci utilise le même mode et diffuse sur le même canal que MyAP1. (Pour notre exemple, le mode est 802.11b et le canal est 6.)
 - Assurez-vous d'enregistrer les paramètres en cliquant sur **Update** (Mettre à jour).

20.4 Mise à jour des paramètres

Pour mettre à jour les paramètres WDS :

1. Accédez à l'onglet *WDS*.
2. Configurez les paramètres WDS selon les besoins.
3. Cliquez sur le bouton **Update** (Mettre à jour) pour appliquer les modifications.

21.1 Présentation des paramètres SNMP227
21.2 Accès aux paramètres SNMP228
21.3 Configuration des paramètres SNMP229
21.3.1 Configuration des alertes SNMP232
21.3.2 Mise à jour des paramètres SNMP233

Les sections suivantes décrivent la procédure à suivre pour configurer SNMP et les paramètres associés à l'API Enterprise-Manager de la passerelle sans fil 9160 G2 Wireless Gateway :

21.1 Présentation des paramètres SNMP

Simple Network Management Protocol (SNMP) définit une norme pour l'enregistrement, le stockage et le partage des informations sur les appareils réseau. SNMP facilite la gestion, le dépannage et l'entretien du réseau.

Les principaux composants d'un réseau géré par SNMP sont les appareils gérés, les agents SNMP et un système de gestion. Les agents stockent des données sur leurs appareils dans des bases de données MIB (Management Information Base) et renvoient ces données sur le gestionnaire SNMP Manager sur demande. Les appareils gérés peuvent être des nœuds de réseau tels que stations de base de point d'accès, routeurs, commutateurs, ponts, concentrateurs, serveurs ou imprimantes.

La passerelle sans fil 9160 G2 Wireless Gateway peut fonctionner comme un appareil géré par SNMP pour une intégration facile dans les systèmes de gestion de réseau sans fil tels que HP OpenView ou Devicescape Wireless Operations Center.

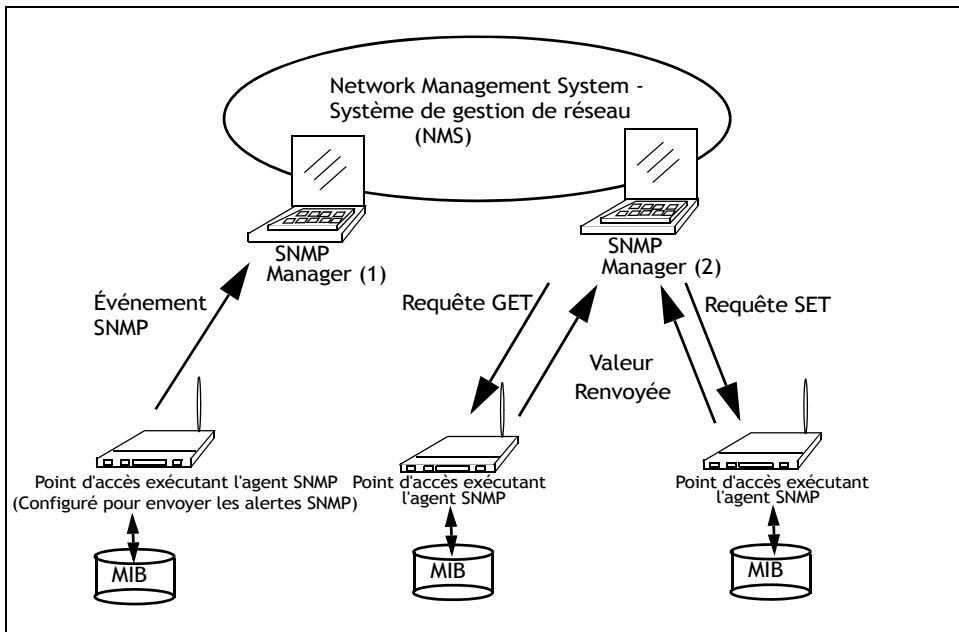
Les MIB sont des ensembles d'objets ou fichiers qui existent dans une base de données virtuelle sur un réseau. SNMP utilise un ensemble de commandes et des requêtes spécifiques pour obtenir des informations de la MIB.

La passerelle sans fil 9160 G2 Wireless Gateway prend en charge les MIB SNMP standard suivantes :

- Pont MIB 802.1d (RFC 1493).
- MIB SNMPv2 (RFC 3418).
- MIB IEEE Std 802.11 (base).
- MIB Groupe d'interfaces (RFC 2233).
- Deux MIB propriétaires (MIB sans fil et MIB système), basées sur la MIB IEEE 802.11k à venir. Elles fournissent des informations concernant la liste d'association client et le tableau de détection des points d'accès de la passerelle sans fil 9160 G2 Wireless Gateway, respectivement. La MIB système propriétaire contient des fonctionnalités de maintenance telles que le redémarrage du système ou la mise à niveau du firmware.

La passerelle sans fil 9160 G2 Wireless Gateway prend également en charge les alertes SNMP. La Figure 21.1 illustre la manière dont SNMP fonctionne sur un réseau.

Figure 21.1 SNMP exécuté sur un réseau



21.2 Accès aux paramètres SNMP

Pour configurer les paramètres SNMP, accédez à *Services > SNMP* (*Services > SNMP*) et mettez à jour les champs comme décrit ci-dessous.

Figure 21.2 Présentation des paramètres SNMP

Basic Settings	Modify SNMP Settings	
User Management		
Cluster	SNMP <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Access Points	Read-only community name (for permitted GETs) <input type="text" value="public"/>	
Sessions	Port number the SNMP agent will listen to <input type="text" value="161"/>	
Channel Management		
Wireless Neighborhood		
Security	Allow SNMP SET requests <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Status	Read-write community name (for permitted SETs) <input type="text" value="protected"/>	
Interfaces	Restrict the source of SNMP requests to only the designated hosts or subnets <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
Events	Hostname or subnet of Network Management System <input type="text" value="Valeur Renvoyée"/>	
Transmit/Receive		
Client Associations		
Neighboring Access Points		
Manage	Trap Destinations	
Ethernet Settings	Community name for traps <input type="text" value="trapcommunity"/>	
802.11 Settings	Enabled <input checked="" type="checkbox"/> Hostname <input type="text" value="one.traphost.com"/>	
802.11 Advanced Settings	<input checked="" type="checkbox"/> <input type="text" value="two.traphost.com"/>	
VWN	<input type="checkbox"/> <input type="text"/>	
WDS		
Guest Login		
MAC Filtering	<input type="button" value="Update"/>	
Load Balancing		
Services		
QoS		
Time		
SNMP		

21.3 Configuration des paramètres SNMP

Le démarrage/arrêt du contrôle des agents SNMP, la configuration du mot de passe de communauté, l'accès aux MIB et la configuration des destinations des alertes SNMP sont fournis via la passerelle sans fil 9160 G2 Wireless Gateway Psion Teklogix.

Tableau 21.1 Paramètres SNMP

Champ	Description
<i>SNMP Enabled/Disabled (SNMP activé/désactivé)</i>	<p>Vous pouvez choisir si vous souhaitez activer SNMP sur votre réseau ou non. Par défaut SNMP est désactivé.</p> <ul style="list-style-type: none">• Pour activer SNMP, cliquez sur Enabled (Activé).• Pour désactiver SNMP, cliquez sur Disabled (Désactivé). <p><i>Remarque : Si vous n'activez pas SNMP, tous les champs restants sur la page SNMP sont désactivés.</i></p>
<i>Read-only community name for permitted GETs (Nom de communauté en lecture seule pour les requêtes GET autorisées)</i>	<p>Entrez un nom de communauté en lecture seule.</p> <p>Le nom de communauté, comme défini dans SNMPv2c, sert de mécanisme d'authentification simple pour limiter les machines présentes sur le réseau qui peuvent demander des données à l'agent SNMP. Ce nom fonctionne comme un mot de passe et la requête est présumée authentique si l'expéditeur connaît le mot de passe.</p> <p>Le nom de communauté peut être dans n'importe quel format alphanumérique.</p>
<i>Port number the SNMP agent will listen to (Numéro de port écouté par l'agent SNMP)</i>	<p>Par défaut, un agent SNMP écoute uniquement les requêtes du port 161. Cependant, vous pouvez configurer cette option pour permettre à l'agent d'écouter les requêtes sur un autre port.</p> <p>Entrez le numéro du port sur lequel vous voulez que les agents SNMP écoutent les requêtes.</p>
<i>Allow SNMP SET Requests (Autoriser les requêtes SET SNMP)</i>	<p>Vous pouvez choisir d'autoriser ou non les requêtes SET SNMP.</p> <p>Activer les requêtes SET signifie que les machines présentes sur le réseau peuvent exécuter des requêtes SET vers l'agent configuré sur le point d'accès.</p> <p><i>Remarque : Les requêtes SET sont limitées à la MIB système propriétaire.</i></p> <ul style="list-style-type: none">• Pour activer les requêtes SET SNMP, cliquez sur Enabled (Activé).• Pour désactiver les requêtes SET SNMP, cliquez sur Disabled (Désactivé).
<i>Read-only community name for permitted SETs (Nom de communauté en lecture seule pour les requêtes SET autorisées)</i>	<p>Si vous avez activé les requêtes SET SNMP, vous pouvez définir un nom de communauté en lecture-écriture.</p> <p>Définir un nom de communauté est similaire à la définition d'un mot de passe. Seules les requêtes des machines qui s'identifient avec ce nom de communauté seront acceptées.</p> <p>Le nom de communauté peut être dans n'importe quel format alphanumérique.</p>

Tableau 21.1 Paramètres SNMP

Champ	Description
<i>Restrict the source of SNMP requests to only the designated hosts or subnets (Limiter la source des requêtes SNMP uniquement aux hôtes ou sous-réseaux désignés)</i>	<p>Vous pouvez limiter la source des requêtes SNMP autorisées.</p> <ul style="list-style-type: none"> Pour limiter la source des requêtes SNMP autorisées, cliquez sur Enabled (Activé). Pour autoriser n'importe quelle source à envoyer une requête SNMP, cliquez sur Disabled (Désactivé).
<i>Hostname or subnet of Network Management System (Nom d'hôte ou de sous-réseau du système de gestion de réseau)</i>	<p>Indiquez le nom d'hôte DNS ou le sous-réseau des machines qui peuvent exécuter des requêtes GET et SET sur les appareils gérés.</p> <p>Comme pour les noms de communauté, cette option offre un niveau de sécurité sur les paramètres SNMP. L'agent SNMP n'acceptera que les requêtes du nom d'hôte ou du sous-réseau spécifié ici.</p> <p>Pour spécifier un sous-réseau, entrez une ou plusieurs plages d'adresses de sous-réseau sous la forme <i>PlageAdresse/LongueurMasque</i>, <i>PlageAdresse</i> étant une adresse IP et <i>LongueurMasque</i>, le nombre de bits de masque. Les formats « AdresseRéseau/MasqueRéseau » et « AdresseRéseau/LongueurMasque » sont tous les deux pris en charge. Des hôtes individuels peuvent être utilisés, par exemple, une adresse IP ou un nom d'hôte. Par exemple, si vous entrez une plage de 192 . 168 . 1 . 0 /24, elle spécifie un sous-réseau avec l'adresse 192 . 168 . 1 . 0 et le masque de sous-réseau 255 . 255 . 255 . 0.</p> <p>La plage d'adresses est utilisée pour spécifier le sous-réseau du NMS désigné. Seules les machines dont les adresses IP sont comprises dans cette plage sont autorisées à exécuter des requêtes GET et SET sur l'appareil géré. Dans l'exemple ci-dessus, les machines avec des adresses entre 192 . 168 . 1 . 1 et 192 . 168 . 1 . 254 peuvent exécuter des commandes SNMP sur l'appareil. (L'adresse identifiée par le suffixe . 0 dans une plage de sous-réseau est toujours réservée à l'adresse de sous-réseau ; et l'adresse identifiée par . 255 dans la plage est toujours réservée à l'adresse de diffusion).</p> <p>Autre exemple, si vous entrez une plage de 10 . 10 . 1 . 128 /25, les machines avec des adresses IP entre 10 . 10 . 1 . 129 et 10 . 10 . 1 . 254 peuvent exécuter des requêtes SNMP sur des appareils gérés. Dans cet exemple, 10 . 10 . 1 . 128 correspond à l'adresse réseau et 10 . 10 . 1 . 255 à l'adresse de diffusion. 126 adresses seraient désignées.</p>

21.3.1 Configuration des alertes SNMP

Les alertes SNMP facilite la communication asynchrone de messages des appareils gérés par SNMP (comme la passerelle sans fil 9160 G2 Wireless Gateway) à des hôtes désignés. Si un système de gestion de réseau (NMS) est chargé de surveiller un grand nombre d'appareils sur un réseau, il n'est pas pratique d'interroger périodiquement chaque appareil du réseau. En activant des alertes d'événement SNMP sur le point d'accès, chaque appareil peut envoyer directement aux gestionnaires SNMP Manager ou à d'autres hôtes désignés sur le NMS des messages concernant certains événements réseau, tels que pannes d'interfaces réseau, échecs d'association ou d'authentification des clients avec le point d'accès, coupures d'alimentation système et modifications apportées à la topologie du réseau.

Les alertes SNMP économisent les ressources réseau en éliminant les requêtes SNMP redondantes. Elles aident aussi les gestionnaires SNMP Manager à dépanner leur réseau. Par exemple, si un gestionnaire SNMP Manager est responsable d'un grand réseau qui prend en charge de nombreux appareils, et que chaque appareil dispose d'un grand nombre d'objets, il est impossible de demander des informations à chaque objet sur tous les appareils. La solution optimale est que chaque agent sur l'appareil géré informe le gestionnaire des événements inhabituels. Cette opération s'effectue en envoyant une alerte de l'événement. Après avoir reçu les informations relatives à l'événement, le gestionnaire peut choisir l'action, le cas échéant, à suivre.

Tableau 21.2 Paramètres d'alertes SNMP

Champ	Description
<i>Community name for traps (Nom de communauté pour les alertes)</i>	Entrez la chaîne de communauté globale associée aux alertes SNMP. Les alertes envoyées à partir de l'appareil fournissent cette chaîne comme nom de communauté.
<i>Hostname (Nom d'hôte)</i>	Entrez le nom d'hôte DNS de l'ordinateur auquel vous souhaitez envoyer des alertes SNMP. Voici un exemple de nom d'hôte DNS : snmptests.teklogix.com Étant donné que les alertes SNMP sont envoyées aléatoirement depuis l'agent SNMP, il est judicieux de spécifier l'emplacement exact où les alertes doivent être envoyées. Assurez-vous de sélectionner la case Enabled (Activé) en regard du nom d'hôte adéquat.

21.3.2 Mise à jour des paramètres SNMP

Pour mettre à jour les paramètres SNMP :

1. Accédez à l'onglet *SNMP* (SNMP).
2. Configurez les paramètres SNMP selon les besoins.
3. Cliquez sur le bouton **Update** (Mettre à jour) pour appliquer les modifications.

LA 9160 G2 COMME STATION DE BASE **22**

22.1 Présentation	237
22.2 Protocoles radio	238
22.2.1 Protocole d'interrogation adaptative/de contention	238
22.3 Menus Narrow Band (Bande étroite)	239
22.3.1 Paramètres de configuration de radio à bande étroite.	239
22.3.1.1 Paramètres de radio RA1001A	241
22.3.2 Options de connectivité	242
22.3.3 Options de connectivité : mode station de base.	242
22.3.3.1 Paramètres de protocole d'interrogation	244
22.3.3.2 Paramètres radio	247
22.3.4 Options de connectivité : mode MRR	248
22.4 Menus de connectivité	248
22.4.1 Paramètres de configuration de station de base.	250
22.4.2 Paramètres de configuration des groupes MRR	251
22.4.2.1 RRM Groups (Groupes MRR).	253
22.4.2.2 Paramètres de protocole d'interrogation	254
22.4.2.3 Paramètres radio	256
22.4.2.4 Paramètres de groupe	257
22.4.2.5 Remote Radio Modules (Modules radio à distance (MRR))	258
22.4.3 Paramètres de configuration des fonctionnalités de liaison radio	258
22.4.3.1 Fonctionnalités de liaison radio	260
22.4.3.2 Automatic Radio Address (Adresse radio automatique)	261
22.4.3.3 Automatic Terminal Number (Numéro de terminal automatique)	262
22.4.4 Menu Hosts (Hôtes).	263
22.4.4.1 Configuration 9010	266

22.1 Présentation

La passerelle sans fil 9160 G2 Wireless Gateway peut fonctionner comme une station de base filaire ou sans fil, ou comme un module radio à distance (MRR), via une liaison radio et des protocoles propriétaires Psion Teklogix pour faciliter la communication avec les terminaux mobiles (reportez-vous à la section « Protocoles radio » à la page 238).

En tant que station de base filaire, la 9160 G2 peut communiquer avec les terminaux mobiles sans fil via un protocole d'interrogation adaptative/de contention (page 238), et elle est connectée au contrôleur réseau via un réseau.

En tant que station de base sans fil, la 9160 G2 communique avec la station de base filaire et les terminaux mobiles via WDS 802.11.

En tant que MRR, le fonctionnement et le délai de la liaison radio entre la 9160 G2 et les terminaux mobiles sont directement contrôlés par un contrôleur réseau qui utilise un protocole radio de timeplexing (reportez-vous à la section « Timeplexing et commutation cellulaire », ci-dessous). Elle est connectée au contrôleur réseau via un réseau.

Timeplexing et commutation cellulaire

Il existe deux méthodes de fonctionnement sur la liaison radio. La première méthode est appelée *commutation cellulaire*. Elle s'apparente aux systèmes de téléphonie cellulaire. Ici, chaque station de base utilise un canal radio différent. Les terminaux mobiles surveillent la liaison radio et basculent automatiquement sur le canal offrant la meilleure réception radio. Cette capacité de commutation cellulaire est transparente pour l'hôte.

La deuxième méthode est appelée *timeplexing*. Ici, toutes les bases module radio à distance (MRR) sur le site utilisent le même canal. Sur un réseau UDP/IP, un contrôleur réseau coordonne la séquence d'interrogation de sorte que les MRR ne transmettent pas simultanément. Cette capacité de timeplexing est transparente pour l'hôte. Le timeplexing est adapté aux sites avec des débits de transaction faibles.

La commutation cellulaire et le timeplexing peuvent être combinés dans un seul système Psion Teklogix : un site peut fonctionner sur deux ou plusieurs canaux, avec plusieurs bases regroupées par timeplexing utilisant chaque canal, et la commutation cellulaire entre canaux.

Dans tous ces cas, l'opérateur peut se déplacer librement sur le site sans perte de communication. Le système Psion Teklogix traite la commutation de canal et les transferts entre les bases sans alerter l'utilisateur.

Pour une utilisation comme station de base ou MRR, les paramètres des pages *Base Station Configuration* (Configuration de la station de base) dans l'écran *Configuration Main Menu* (Menu principal de configuration) doivent être définis de manière appropriée, comme décrit dans les sections suivantes.

En outre, les paramètres radio et d'hôte appropriés doivent être appliqués. Les paramètres radio se trouvent sur les pages *Radio* pour les radios *Narrow Band* (Bande étroite), comme indiqué dans la section Section 22.3.1. Les paramètres pour les hôtes sont décrits dans la section « Section 22.4.4 Menu Hosts (Hôtes) » à la page 263.



Remarque : Les principaux paramètres de la 9160 G2 doivent d'abord être configurés comme décrit dans le Chapitre 4 : « Étapes rapides de configuration et de lancement » et le Chapitre 5 : « Configuration des paramètres de base ». Pour plus de détails sur les protocoles RF, reportez-vous aux sections suivantes.

22.2 Protocoles radio

Les protocoles RF permettent aux terminaux mobiles de communiquer avec une station de base en partageant l'utilisation d'un canal radio de manière efficace. Les systèmes Psion Teklogix utilisent l'un des deux types de protocoles RF : le protocole d'interrogation adaptative/de contention de Psion Teklogix ou le protocole non propriétaire IEEE 802.11.

Lorsqu'elle est utilisée comme station de base ou comme MRR, la 9160 G2 utilise le protocole d'interrogation adaptative/de contention. La 9160 G2 prend en charge le fonctionnement simultané de la station de base et du point d'accès 802.11.

22.2.1 Protocole d'interrogation adaptative/de contention

Le protocole d'interrogation adaptative/de contention est toujours utilisé sur les systèmes radio à bande étroite avec des vitesses de transmission allant jusqu'à 19,2 Kbit/s, et peut également être utilisé sur les systèmes à étalement de spectre à des débits plus élevés.

Les terminaux mobiles fonctionnant avec ce protocole ne transmettent pas à moins de recevoir des interrogations de la 9160 G2. Les terminaux mobiles sont généralement interrogés en masse. Après chaque interrogation, les groupes de terminaux mobiles ont des fenêtres de réponse attribuées dans lesquelles ils peuvent répondre à l'interrogation. Si une « collision » se produit (si plus d'un terminal mobile tente de répondre dans une fenêtre particulière), la 9160 G2 qui procède à l'interrogation divise et réattribue automatiquement ce groupe jusqu'à ce que les terminaux mobiles puissent répondre sans collision.

Les fonctionnalités adaptatives de ce protocole permettent aux fenêtres de réponse d'être réglées de manière à s'adapter aux conditions de trafic RF élevées ou faibles, et pour empêcher les données d'être mises en file d'attente trop longtemps lorsqu'un terminal mobile spécifique a une salve de données à envoyer ou recevoir.

Les systèmes utilisant l'interrogation adaptative/de contention peuvent utiliser l'option cellulaire pour que les opérateurs puissent circuler sur le site tout en maintenant une communication ininterrompue lors du passage entre zones de couverture.

Si la base cellulaire n'est pas activée, un message « RESET : Press Enter (RÉINITIALISER : appuyez sur Entrée) » s'affiche sur l'écran du terminal mobile à chaque fois qu'un opérateur passe d'une zone de couverture de station de base à une autre.

22.3 Menus Narrow Band (Bande étroite)

22.3.1 Paramètres de configuration de radio à bande étroite

Lorsque vous sélectionnez le sous-menu *Radio* dans les options du menu *Narrow Band* (Bande étroite), la 9160 G2 affiche les *Narrow Band Radio Configuration Settings* (Paramètres de configuration radio à bande étroite) du mode de fonctionnement pour lequel la 9160 G2 est définie (station de base ou MRR). La page affichée vous permet de définir l'état de la 9160 G2, et de rétablir les paramètres de communication permanents de la carte radio RA1001.

Figure 22.1 Présentation des paramètres radio à bande étroite

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Narrow Band

Radio

Connectivity Options

Connectivity

Base Station

RRM Groups

View NarrowBand radio configuration settings

Radio Card: **Installed**

Radio Card Status: ☒ Enabled ☐ Disabled

Update

General Parameters:

Modulation: 2 Level

Baud Rate: 9600

Band Start: 450 MHz

Band Size: 20 MHz

Frequency Step: 12500 Hz

Channel Bandwidth: 25000 Hz

Collision Threshold: 1154ms

TX Delay, 4 Level: 11ms

Preamble, 2 Level: 10DEL,1SOH chars

Preamble, 4 Level: 6DEL,1SOH chars

Tuning Values:

Data Squelch: 62

Frequency Adjust: -100

Power: 88

Deviation, 4 Level: 66

Deviation, 2 Level: 44

Local Oscillator Adjust: 0

Demodulator Adjust: 181

TCXO Adjust: 122

Frequencies:

Channel	Rx	Tx
1	460000000 Hz	450000000 Hz
2	0 Hz	0 Hz
3	0 Hz	0 Hz
4	0 Hz	0 Hz
5	0 Hz	0 Hz
6	0 Hz	0 Hz
7	0 Hz	0 Hz
8	0 Hz	0 Hz
9	0 Hz	0 Hz
10	0 Hz	0 Hz
11	0 Hz	0 Hz
12	0 Hz	0 Hz
13	0 Hz	0 Hz
14	0 Hz	0 Hz
15	0 Hz	0 Hz
16	0 Hz	0 Hz
17	0 Hz	0 Hz
18	0 Hz	0 Hz
19	0 Hz	0 Hz
20	0 Hz	0 Hz

Radio Card Status (État de la carte radio)

Ce paramètre **active** ou **désactive** la radio à bande étroite. La carte peut être **désactivée** temporairement lorsque, à des fins de test, il est nécessaire qu'il n'y ait aucune interférence radio. Appuyez sur le bouton **Update** (Mettre à jour) pour appliquer la modification.

22.3.1.1 Paramètres de radio RA1001A

La page *Narrow Band Radio Configuration Settings* (Paramètres de configuration de radio à bande étroite) affiche les paramètres *General* (Général), *Frequencies* (Fréquences) et *Tuning Values* (Valeurs de réglage) de la radio à bande étroite RA1001A. Ces paramètres du fabricant ne sont pas configurables. Les paramètres s'affichent dans les figures ci-dessous.

Figure 22.2 Paramètres de radio RA1001A

General Parameters:
Modulation: 2 Level
Baud Rate: 9600
Band Start: 450 MHz
Band Size: 20 MHz
Frequency Step: 12500 Hz
Channel Bandwidth: 25000 Hz
Collision Threshold: 1154ms
TX Delay, 4 Level: 11ms
Preamble, 2 Level: 10DEL,1SOH chars
Preamble, 4 Level: 6DEL,1SOH chars

Figure 22.3 Valeurs de réglage de radio RA1001A

Tuning Values:
Data Squelch: 62
Frequency Adjust: -100
Power: 88
Deviation, 4 Level: 66
Deviation, 2 Level: 44
Local Oscillator Adjust: 0
Demodulator Adjust: 181
TCXO Adjust: 122

Figure 22.4 Fréquences radio RA1001A

Frequencies:		
Channel	Rx	Tx
1	460000000 Hz	450000000 Hz
2	0 Hz	0 Hz
3	0 Hz	0 Hz
4	0 Hz	0 Hz
5	0 Hz	0 Hz
6	0 Hz	0 Hz
7	0 Hz	0 Hz
8	0 Hz	0 Hz
9	0 Hz	0 Hz
10	0 Hz	0 Hz
11	0 Hz	0 Hz
12	0 Hz	0 Hz
13	0 Hz	0 Hz
14	0 Hz	0 Hz
15	0 Hz	0 Hz
16	0 Hz	0 Hz
17	0 Hz	0 Hz
18	0 Hz	0 Hz
19	0 Hz	0 Hz
20	0 Hz	0 Hz

22.3.2 Options de connectivité

Lorsque vous sélectionnez ce sous-menu, la page affichée vous permet de définir les différentes options de fonctionnement de la 9160 G2 en mode station de base ou MRR.

22.3.3 Options de connectivité : mode station de base

Lorsque vous accédez au sous-menu *Connectivity Options* (Options de connectivité) de la 9160 G2 définie dans le mode de fonctionnement de la station de base, les paramètres Polling Protocol (Protocole d'interrogation) et Radio s'affichent.

Figure 22.5 Présentation des paramètres de protocole d'interrogation et radio

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Narrow Band

Radio

Connectivity Options

Set Operating Mode and view Polling Protocol or RRM settings

Operating Mode:

Auto-Startup: ☒ Enabled ☐ Disabled

Shared Channel: ☐ Enabled ☒ Disabled

Polling Protocol Parameters:

Number of Poll Windows: (Range 2..4)

Size of Poll Windows: (Range 5..32)

Maximum Message Segment Size: (Range 32..116)

Number of Retries: (Range 1..7)

Collision Size: (Range 3..10)

Free Window Factor: (Range 0..7)

Message Mode Limit: (Range 0..7)

Callsign Period: (Range 0..60)

Callsign String: (Max 10 letters or digits)

Radio Parameters:

Sync Delay: (Range 3..45)

Remote Tx On: (Range 3..60)

Active Channel: (Range 1..20)

Operating Mode (Mode de fonctionnement)

Ce paramètre vous permet de définir le mode de fonctionnement de la 9160 G2 en tant que **Base Station** (Station de base) ou **RRM** (MRR).

Auto-Startup (Démarrage automatique)

Ce paramètre **active** l'interrogation immédiate lorsque la 9160 G2 redémarre. Si *Auto-Startup* (Démarrage automatique) est **désactivé**, la 9160 G2 attendra que l'interrogation soit initialisée à partir du contrôleur réseau.

Shared Channel (Canal partagé)

Shared Channel (Canal partagé) est utilisé uniquement en Hollande pour s'adapter aux exigences du gouvernement. Lorsque ce paramètre est **activé**, il impose des restrictions de minutage pour l'interrogation. 2 secondes d'interrogation sont suivies de 0,5 seconde de silence ; aucune interrogation n'a lieu.

De plus, si un autre opérateur est détecté sur le canal, la 9160 G2 cessera les transmissions radio sur ce canal jusqu'à ce que le chemin soit clair.

22.3.3.1 Paramètres de protocole d'interrogation

Polling Protocol Parameters:

Number of Poll Windows:	<input type="text" value="3"/>	(Range 2..4)
Size of Poll Windows:	<input type="text" value="8"/>	(Range 5..32)
Maximum Message Segment Size:	<input type="text" value="100"/>	(Range 32..116)
Number of Retries:	<input type="text" value="3"/>	(Range 1..7)
Collision Size:	<input type="text" value="6"/>	(Range 3..10)
Free Window Factor:	<input type="text" value="7"/>	(Range 0..7)
Message Mode Limit:	<input type="text" value="4"/>	(Range 0..7)
Callsign Period:	<input type="text" value="0"/>	(Range 0..60)
Callsign String:	<input type="text" value="Teklogix"/>	(Max 10 letters or digits)

Number of Poll Windows (Nombre de fenêtres d'interrogation)

Ce paramètre définit le nombre de fenêtres d'interrogation que la 9160 G2 va utiliser. La valeur attribuée à ce paramètre dépend du nombre de terminaux mobiles et du protocole de liaison radio utilisé. Le Tableau 22.1 indique comment la valeur attribuée au paramètre *Number of Poll Windows* (Nombre de fenêtres d'interrogation) est déterminé.

Tableau 22.1 Nombre de fenêtres d'interrogation - Protocole cellulaire

Nombre de terminaux mobiles	Nombre minimum de fenêtres
1-16	2
17-81	3
82-256	4

Size of Poll Windows (Taille des fenêtres d'interrogation)

La valeur attribuée à ce paramètre détermine le plus grand message pouvant être transmis entre la 9160 G2 et le terminal mobile dans une fenêtre d'interrogation normale. La taille de la fenêtre peut être réglée de manière à recevoir entre **5** et **32** caractères.

Les fenêtres plus grandes augmentent la période d'interrogation et peuvent augmenter le temps de réponse. Les fenêtres plus petites augmentent le nombre de messages et d'interrogations à messages longs, et peuvent également augmenter le temps de réponse.



Important : En mode « cellulaire », la valeur minimale de ce paramètre est **8**.

Maximum Message Segment Size (Taille maximale de segment du message)

Ce paramètre détermine le plus grand message unique qui peut être transmis à un terminal mobile en mode message ou *depuis* un terminal mobile en mode message long. Dans une station de base 9160 G2, la valeur saisie pour ce paramètre doit être supérieure ou égale à la valeur saisie dans le contrôleur réseau ou le mini-contrôleur 9160 G2. La portée de ce paramètre est comprise entre 32 et 116 caractères. (Les messages dépassant cette limite sont divisés en plusieurs paquets). La valeur par défaut est **100**.

Number of Retries (Nombre de tentatives)

Ce paramètre détermine combien de fois la 9160 G2 tente de renvoyer un message si une confirmation n'est pas reçue du terminal mobile. (Ces nouvelles tentatives n'ont pas nécessairement lieu dans des interrogations consécutives car les messages incomplets sont renvoyés au bas de la file d'attente des messages.) Une fois que toutes les tentatives ont échoué, le terminal mobile est déclaré « hors ligne ». La 9160 G2 ne transmet pas de messages au terminal mobile jusqu'à ce que le terminal mobile se déclare « en ligne ». Les valeurs autorisées vont de **1** à **7**.

Collision Size (Taille de collision)

Ce paramètre réduit la probabilité que des bruits aléatoires sur la liaison radio soient interprétés comme une collision entre terminaux mobiles. Le temps de réponse augmente lorsque la 9160 G2 résout des collisions inutilement.

Collision Size (Taille de la collision) définit une limite supérieure au nombre de caractères qui sont reçus avant la réception d'un message d'erreur (CRC, CD perdu, etc.). Si huit est la valeur de ce paramètre, huit caractères ou moins, suivis d'un message d'erreur s'affichant sur la liaison radio, sont considérés comme du bruit. S'il y a plus de huit caractères, ils sont considérés comme une collision. Les valeurs autorisées vont de **3** à **10**.

Free Window Factor (Facteur de fenêtre libre)

La valeur entrée dans ce paramètre détermine si le « mode fenêtre libre » sera utilisé. Dans le mode fenêtre libre, tous les terminaux mobiles auxquels aucune autre fenêtre n'est attribuée peuvent utiliser la fenêtre libre.

Entrer une valeur de **0** (zéro) dans ce paramètre **désactive** le mode fenêtre libre. Accroître la valeur de ce paramètre augmente la probabilité qu'un message soit transmis dans la fenêtre libre.

Message Mode Limit (Limite du mode message)

Ce paramètre définit la limite supérieure du nombre de messages qui doivent être placés dans la file d'attente pour transmission avant que l'interrogation de mode message ne démarre. Les valeurs autorisées vont de **0** à **7**, **0 désactivant** le mode message.



Remarque : Le nombre de terminaux mobiles et d'événements passés font également partie de l'algorithme qui détermine l'activation ou non du mode message.

Callsign Period (Période d'indicatif)

Un indicatif est régulièrement transmis sous la forme d'un signal sonore en code Morse. Ce paramètre indique l'intervalle en minutes entre transmissions d'indicatif. Les valeurs autorisées vont de **0** à **60**. Les organismes fédéraux, Industry Canada et la Federal Communications Commission des États-Unis, exigent que chaque système transmette son propre indicatif d'identification toutes les 15 minutes.

Dans les pays où un indicatif n'est pas requis, paramétrer cette valeur sur **0** empêche la transmission d'indicatif, ce qui permet des temporisations d'interrogation plus courtes sur les terminaux mobiles et une commutation de canaux plus rapide.

Callsign String (Chaîne d'indicatif)

La chaîne peut avoir un maximum de **10** caractères. Tous les caractères sont des chiffres ou des lettres. Le préfixe « DE » (depuis) est ajouté au début de l'indicatif transmis.

22.3.3.2 Paramètres radio

Radio Parameters:		
Sync Delay:	<input type="text" value="18"/>	(Range 3..45)
Remote Tx On:	<input type="text" value="4"/>	(Range 3..60)
Active Channel:	<input type="text" value="1"/>	(Range 1..20)

Sync Delay (Délai de synchronisation)



Important : *Le réglage d'usine de ce paramètre ne doit pas être modifié sans connaissance réelle du délai du protocole radio.*

Sync Delay (Délai de synchronisation) indique le délai entre l'heure de la transmission de la station de base et la première fenêtre de réponse, mesurée en temps de caractère. La valeur attribuée à ce paramètre doit être compatible avec les autres stations de base et terminaux mobiles du système. La radio RA1001 est disponible en modulation à deux ou quatre niveaux, offrant des débits en bauds de 4 800 bit/s et 9 600 bits/s, ou 9 600 bit/s et 19 200 bit/s, respectivement.

Le paramètre par défaut pour une radio à bande étroite avec une modulation à deux niveaux, fonctionnant à 9 600 bauds, est **23**.

Le paramètre par défaut pour une radio à bande étroite avec une modulation à quatre niveaux, fonctionnant à 19 200 bauds, est **31**.

Remote Txon (Txon à distance)

Remote Txon (Txon à distance) s'adapte au temps de mise en marche de la radio sur les terminaux mobiles (distants). Ce paramètre indique le nombre de caractères transmis à la radio avant que les données réelles soient émises. Ce paramètre étant basé sur le temps de caractère, le nombre dépend du débit en bauds de la liaison radio.

La valeur attribuée au paramètre *Remote Txon* (Txon à distance) doit être cohérente sur tous les terminaux mobiles et l'équipement de station de base. Les valeurs autorisées vont de **3** à **60**.



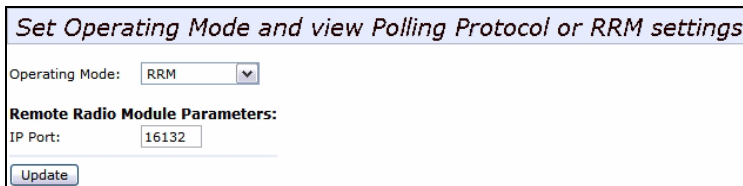
Important : *Le réglage d'usine de ce paramètre ne doit pas être modifié sans connaissance réelle du délai du protocole radio.*

Active Channel (Canal actif)

Ce paramètre détermine le canal radio de fonctionnement de la 9160 G2. Ainsi, le canal devient disponible pour la recherche de canal par les terminaux mobiles. Le canal sélectionné doit être l'un de ceux qui ont été configurés avec des fréquences, comme indiqué sur la page *Narrow Band Radio Configuration Settings* (Paramètres de configuration radio à bande étroite). Reportez-vous à la Figure 22.4 à la page 242 pour la liste des canaux et des fréquences associés.

22.3.4 Options de connectivité : mode MRR

Lorsque vous accédez au sous-menu *Connectivity Options* (Options de connectivité) pour une 9160 G2 esclave définie dans le mode de fonctionnement MRR, la 9160 G2 affiche les paramètres MRR.



The screenshot shows a configuration window titled "Set Operating Mode and view Polling Protocol or RRM settings". Inside, there is a section for "Operating Mode" with a dropdown menu currently showing "RRM". Below this is a section titled "Remote Radio Module Parameters:" which contains an "IP Port" field with the value "16132". At the bottom of the window is an "Update" button.

IP Port (Port IP)

Ce paramètre vous permet de saisir le numéro de port d'écoute de la 9160 G2 fonctionnant comme esclave MRR. Le numéro de port peut aller de **1024** à **32767**.



Important : Le numéro de port entré ici doit correspondre au numéro de port entré pour cette 9160 G2 dans la configuration MRR du contrôleur réseau.

22.4 Menus de connectivité

La passerelle sans fil 9160 G2 Wireless Gateway peut fonctionner comme une station de base ou un module radio à distance (MRR), ce qui facilite les communications entre les terminaux mobiles et les stations de base sans fil, et un contrôleur réseau (Psion Teklogix 9500 Communications Server ou passerelle sans fil 9160 G2 Wireless Gateway), via une gamme de plateformes hôte. Le contrôleur réseau peut également être un hôte exécutant un SDK Psion Teklogix (gestionnaire).

La 9160 G2 peut également servir de station de base esclave pour une autre 9160 G2 sur le réseau.

Figure 22.6 Configuration de station de base

Basic Settings	View Base Station configuration settings
User Management	
Cluster	Slave Base Stations:
Access Points	Number of configured Slave Base Stations: 0
Sessions	Base Station Number: 1 ▼
Channel Management	Status: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Wireless Neighborhood	Description: Unnamed Base Station
Security	IP Address: 0.0.0.0 Port: 16100
Status	Message Size: 100 (Range 32..116)
Interfaces	Auto-Startup: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Events	
Transmit/Receive	To Restore Default Configuration...
Client Associations	Click "Default" to re-load the default configuration values for this Base Station. Default
Neighboring Access Points	Update Cancel
Manage	
Ethernet Settings	
802.11 Settings	
802.11 Advanced Settings	
VWN	
WDS	
Guest Login	
MAC Filtering	
Load Balancing	
Services	
QoS	
Time	
SNMP	
Narrow Band	
Radio	
Connectivity Options	
Connectivity	
Base Station	

22.4.1 Paramètres de configuration de station de base

Les stations de base communiquent sur la liaison radio via des protocoles propriétaires Psion Teklogix. Les stations de base peuvent être connectées aux contrôleurs réseau à l'aide de réseaux TCP/IP via Ethernet. En tant que station de base communiquant avec les terminaux mobiles via une liaison radio, la 9160 G2 utilise le protocole d'interrogation adaptative/de contention RF (reportez-vous à la section *Protocoles radio* à la page 238 pour plus de détails sur ces protocoles).

La 9160 G2 contrôle le fonctionnement et la temporisation de la liaison radio. Chaque station de base utilise un canal radio différent, et les terminaux mobiles utilisent la commutation cellulaire pour circuler entre les stations.

Les options et paramètres des pages suivantes vous permettent de configurer la 9160 G2 comme station de base maître reliée à un maximum de 32 stations de base 9160 G2 esclaves via un réseau Ethernet. La 9160 G2 maître est connectée à un serveur 9500 Communications Server, ou à jusqu'à six hôtes exécutant le Kit de développement logiciel Psion Teklogix. L'option *Base Station* (Station de base) sous *Connectivity* (Connectivité) vous permet d'ajouter une nouvelle station de base esclave au système ou de modifier les paramètres sur une station de base esclave existante.

Appuyer sur le bouton **Update** (Mettre à jour) enregistre vos paramètres ; appuyer sur le bouton **Default** (Par défaut) charge à nouveau les valeurs de configuration par défaut pour cette station de base.

Number of Configured Slave Base Stations (Nombre de stations de base esclaves configurées)

Vous pouvez configurer jusqu'à **32** stations de base 9160 G2 esclaves.

Base Station Number (Numéro de station de base)

Ce paramètre indique le numéro attribué à la station de base. Choisir le **numéro de station** dans la liste déroulante affiche les paramètres qui peuvent être modifiés ou supprimés pour cet hôte. De nouvelles stations de base esclaves peuvent être ajoutées en sélectionnant un numéro libre et en configurant des paramètres pour celui-ci.

Status (État)

Ce paramètre **active** ou **désactive** cette station de base esclave.

Description

Le nom entré dans ce paramètre est utilisé comme un autre moyen d'identifier l'adresse IP d'une station de base esclave.

IP Address (Adresse IP)

Ce paramètre fournit l'adresse IP correspondante pour la station de base esclave.

L'adresse IP **doit être une valeur unique** pour que chaque station de base esclave puisse être identifiée sur le réseau.

La valeur acceptable est comprise entre **0.0.0.0** et **239.255.255.255**.

La valeur par défaut du port IP est **16100**.

Message Size (Taille du message)

Message Size (Taille du message) détermine le plus grand message unique qui peut être transmis à un terminal mobile. La portée de ce paramètre est comprise entre **32** et **380** caractères. (Les messages dépassant cette limite sont divisés en plusieurs paquets).

Pour les stations de base de protocole d'interrogation, la limite supérieure est **116**.

Auto-Startup (Démarrage automatique)

Lorsque ce paramètre est **activé**, les stations de base esclaves démarre l'interrogation lorsque la **9160 G2 maître** démarre. Lorsque *Auto-Startup* (Démarrage automatique) est **désactivé**, les stations de base ne démarrent pas l'interrogation avant de recevoir une commande *start polling* (démarre l'interrogation) de l'**hôte**.

22.4.2 Paramètres de configuration des groupes MRR

Alors que la 9160 G2 peut fonctionner comme un module radio à distance (MRR, reportez-vous à la section « Options de connectivité : mode MRR » à la page 248), elle peut également contrôler d'autres MRR. Pour qu'une 9160 G2 contrôle des MRR, des groupes MRR doivent être configurés. Une fois qu'un groupe MRR a été défini, entre un et quatre MRR peuvent être membres d'un groupe.

Tous les MRR d'un groupe fonctionnent sur le même canal radio. La 9160 G2 coordonne les transmissions de tous les MRR au sein d'un groupe (pour cette raison, la 9160 G2 qui contrôle est parfois appelée « maître de timeplexing »).

Figure 22.7 Présentation des paramètres de configuration des groupes MRR

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Narrow Band

Radio

Connectivity Options

Connectivity

Base Station

RRM Groups

View RRM Groups configuration settings

RRM Groups:

Number of Configured RRM Groups: 0

RRM Group Number: 1

Status: ☐ Enabled ☒ Disabled

Description: Unnamed RRM Group

Auto-Startup: ☒ Enabled ☐ Disabled

Shared Channel: ☐ Enabled ☒ Disabled

Polling Protocol Parameters:

Number of Poll Windows: 3 (Range 2..4)

Size of Poll Windows: 8 (Range 5..32)

Maximum Message Segment Size: 100 (Range 32..116)

Number of Retries: 3 (Range 1..7)

Collision Size: 6 (Range 3..10)

Free Window Factor: 0 (Range 0..7)

Message Mode Limit: 4 (Range 0..7)

Callsign Period: 0 (Range 0..60)

Callsign String: Teklogix (Max 10 letters or digits)

Radio Parameters:

Sync Delay: 22 (Range 3..45)

Remote Tx On: 13 (Range 3..60)

Active Channel: 1 (Range 1..20)

Group Parameters:

Combination 1: (Sequence of RRM indices)

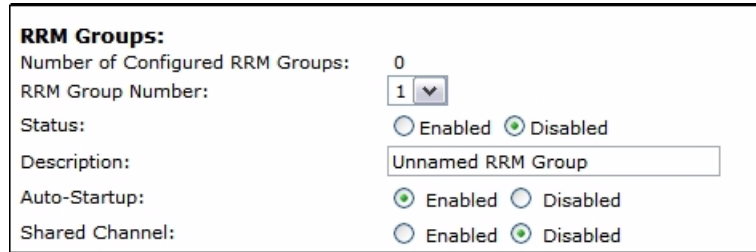
Combination 2: (Sequence of RRM indices)

Remote Radio Modules:

Enabled	Description	IP Address	Port
<input type="checkbox"/>	Unnamed RRM	0.0.0.0	16132
<input type="checkbox"/>	Unnamed RRM	0.0.0.0	16132
<input type="checkbox"/>	Unnamed RRM	0.0.0.0	16132
<input type="checkbox"/>	Unnamed RRM	0.0.0.0	16132

Update

22.4.2.1 RRM Groups (Groupes MRR)



RRM Groups:

Number of Configured RRM Groups: 0

RRM Group Number: 1

Status: ☒ Enabled ☐ Disabled

Description: Unnamed RRM Group

Auto-Startup: ☒ Enabled ☐ Disabled

Shared Channel: ☐ Enabled ☒ Disabled

Cette fenêtre permet à l'utilisateur de définir les options pour un nouveau groupe MRR. Chaque MRR doit être membre d'un groupe ; il peut y avoir plus d'un groupe MRR configuré dans la 9160 G2. Un groupe peut contenir entre un et quatre MRR.

Cet écran est très similaire à celui de la section « Options de connectivité : mode station de base » à la page 242, la différence étant que les paramètres configurés dans ces menus radio s'appliquent à la radio RA1001A résidente dans la 9160 G2, tandis que les paramètres configurés ici s'appliquent aux autres 9160 G2 distantes (les MRR).

Number of Configured RRM Groups (Nombre de groupes MRR configurés)

Affiche le nombre de groupes MRR configurés dans cette 9160 G2.

RRM Group Number (Numéro de groupe MRR)

Ce paramètre indique le numéro attribué au groupe MRR. Choisir le **numéro de groupe MRR** dans la liste déroulante affiche les paramètres qui peuvent être modifiés ou supprimés pour ce groupe. De nouveaux groupes MRR peuvent être ajoutés en sélectionnant un numéro libre et en configurant des paramètres pour celui-ci.

Status (État)

Ce paramètre **active** ou **désactive** ce groupe MRR.

Description

Cette zone de texte permet à l'utilisateur d'entrer un nom pour le nouveau groupe MRR. La valeur est une chaîne de texte quelconque. La valeur par défaut est **Unnamed RRM Group** (Groupe MRR sans nom).

Auto-Startup (Démarrage automatique)

Lorsque ce paramètre est **activé**, la 9160 G2 établit la communication avec les MRR de ce groupe lors du démarrage, et elle démarre automatiquement l'interrogation. Lorsque *Auto-Startup* (Démarrage automatique) est **désactivé**, la 9160 G2 établit la communication avec les MRR de ce groupe lorsqu'elle démarre, mais ne démarre pas l'interrogation dans ce groupe MRR avant de recevoir une commande de démarrage d'interrogation de l'hôte. L'interrogation démarre si au moins un des MRR du groupe MRR fonctionne au démarrage de la 9160 G2.

Shared Channel (Canal partagé)

Si ce paramètre est **activé**, la 9160 G2 vérifie s'il existe un autre trafic sur le canal radio utilisé par ce groupe MRR avant l'interrogation.

Si ce paramètre est **désactivé**, la 9160 G2 suppose qu'elle a l'usage exclusif du canal radio MRR pour ce groupe et elle interroge sans vérifier le trafic radio.

Ce paramètre est obligatoire pour les systèmes installés aux Pays-Bas.

22.4.2.2 Paramètres de protocole d'interrogation



Avertissement : *Ces paramètres sont préconfigurés pour votre système, et ne doivent pas être modifiés sans une bonne connaissance de leur impact sur la liaison radio.*

Polling Protocol Parameters:		
Number of Poll Windows:	<input type="text" value="3"/>	(Range 2..4)
Size of Poll Windows:	<input type="text" value="8"/>	(Range 5..32)
Maximum Message Segment Size:	<input type="text" value="100"/>	(Range 32..116)
Number of Retries:	<input type="text" value="3"/>	(Range 1..7)
Collision Size:	<input type="text" value="6"/>	(Range 3..10)
Free Window Factor:	<input type="text" value="0"/>	(Range 0..7)
Message Mode Limit:	<input type="text" value="4"/>	(Range 0..7)
Callsign Period:	<input type="text" value="0"/>	(Range 0..60)
Callsign String:	<input type="text" value="Teklogix"/>	(Max 10 letters or digits)

Number of Poll Windows (Nombre de fenêtres d'interrogation)

Cette zone de texte permet à l'utilisateur de spécifier le nombre de fenêtres d'interrogation dans lesquelles le MRR écoute les réponses des terminaux mobiles après l'envoi d'une interrogation. Les valeurs autorisées vont de **2 à 4**. La valeur par défaut est **3**.

Size of Poll Windows (Taille des fenêtres d'interrogation)

Cette zone de texte permet à l'utilisateur de spécifier la taille des fenêtres d'interrogation Windows dans lesquelles les MRR de ce groupe MRR écoutent les réponses des terminaux mobiles. Les valeurs autorisées vont de **5 à 32**. La valeur par défaut est **8**.

Maximum Message Segment Size (Taille maximale de segment du message)

Cette zone de texte permet à l'utilisateur de spécifier la taille du plus grand segment de message, en octets, qui sera envoyé sur le réseau radio Psion Teklogix. Les messages plus gros sont divisés en plusieurs parties. Les valeurs autorisées vont de **32 à 116**. La valeur par défaut est **100**.

Number of Retries (Nombre de tentatives)

Cette zone de texte permet à l'utilisateur de définir le nombre de fois que le MRR retransmet un message à un terminal mobile, lorsqu'il ne reçoit pas d'accusé de réception du terminal mobile et avant de déclarer le terminal mobile hors ligne. Les valeurs autorisées vont de **1 à 7**. La valeur par défaut est **3**.

Collision Size (Taille de collision)

Cette zone de texte permet à l'utilisateur de spécifier le plus petit nombre de caractères de bruit reçus par le MRR, qui seront interprétés comme des transmissions d'interférences de l'équipement Psion Teklogix. Lorsque ce seuil est dépassé, le MRR commence la résolution de la collision. Les valeurs autorisées vont de **3 à 10**. La valeur par défaut est **6**.

Free Window Factor (Facteur de fenêtre libre)

Cette zone de texte permet à l'utilisateur de spécifier la probabilité pour le MRR d'inclure une fenêtre libre dans son interrogation, pendant laquelle un terminal mobile peut transmettre. Les valeurs autorisées vont de **0 à 7**. La valeur par défaut est **0**.

Message Mode Limit (Limite du mode message)

Cette zone de texte permet à l'utilisateur de spécifier la probabilité d'inclure une interrogation en mode message dans sa transmission d'interrogation. Les valeurs autorisées vont de **0 à 7**. La valeur par défaut est **4**.

Callsign Period (Période d'indicatif)

Cette zone de texte permet à l'utilisateur de spécifier la durée entre les transmissions de l'indicatif. Ce paramètre est exprimé en minutes. Une valeur de 0 (zéro) indique qu'aucun indicatif n'est transmis. Les valeurs autorisées vont de **0 à 60**. La valeur par défaut est **0**.

Callsign String (Chaîne d'indicatif)

Cette zone de texte permet à l'utilisateur de spécifier le texte à transmettre comme indicatif pour le MRR. Le texte est transmis en code Morse. La valeur par défaut est **Teklogix**.

22.4.2.3 Paramètres radio

Radio Parameters:		
Sync Delay:	<input type="text" value="22"/>	(Range 3..45)
Remote Tx On:	<input type="text" value="13"/>	(Range 3..60)
Active Channel:	<input type="text" value="1"/>	(Range 1..20)

Comme certains des paramètres radio sont les mêmes pour un groupe donné MRR en timeplexing, ils peuvent être configurés par l'utilisateur une fois sur la 9160 G2 ; la 9160 G2 les transmet ensuite aux MRR du groupe. Ces paramètres incluent le délai de synchronisation (*Sync Delay*), la transmission Txon à distance (*Remote Txon*) et le numéro de canal à utiliser (*Active Channel*).

Bien que la radio à bande étroite RA1001A dans chaque MRR du groupe soit configurée séparément, la 9160 G2 considère qu'ils sont configurés de manière identique. Pour s'en assurer, la 9160 G2 examine certains paramètres renvoyés par chacun des MRR. Ils incluent le débit radio en bauds et la transmission Txon.

Ces paramètres sont comparés aux valeurs renvoyées par d'autres MRR au sein du même groupe. Des messages d'erreur s'affichent si ces valeurs ne correspondent pas, mais la pire des valeurs est choisie pour être utilisée.



Avertissement : *Ces paramètres sont préconfigurés pour votre système et ne doivent pas être modifiés sans une bonne connaissance de leur impact sur la liaison radio.*

Sync Delay (Délai de synchronisation)

Cette zone de texte permet à l'utilisateur de spécifier le nombre de caractères de délai insérés entre la transmission du MRR et la première fenêtre de réponse. Les valeurs autorisées vont de **3 à 45**. La valeur par défaut est **22**.

Remote Txon (Txon à distance)

Cette zone de texte permet à l'utilisateur de spécifier le nombre de caractères de remplissage transmis par les radios de terminal mobile avant que les terminaux mobiles n'envoient les données du message. Les valeurs autorisées vont de **3 à 60**. La valeur par défaut est **13**.

Active Channel (Canal actif)

Cette zone de texte permet à l'utilisateur de spécifier le canal radio à utiliser par l'ensemble des MRR du groupe. Les valeurs autorisées vont de **1 à 20**. La valeur par défaut est **1**.

22.4.2.4 Paramètres de groupe

Group Parameters:	
Combination 1:	<input type="text"/> (Sequence of RRM indices)
Combination 2:	<input type="text"/> (Sequence of RRM indices)

Combination (Combinaison)

Ces zones de texte permettent à l'utilisateur de spécifier des sous-groupes MRR appelés *combinaisons*. Si les zones de couverture d'au moins deux des MRR de ce groupe ne se chevauchent pas, les MRR qui ne se chevauchent pas peuvent interroger en même temps. Cela améliore les temps de réponse du système et réduit la quantité de signalisation sur le réseau. Les MRR qui ne sont pas attribués aux combinaisons interrogent individuellement, après les interrogations en combinaison.

Par exemple, si le groupe MRR a 3 MRR et que les MRR 1 et 3 ne se chevauchent pas, les MRR 1 et 3 peuvent être placés dans un sous-groupe (*Combinaison 1*). Ils pourront ensuite interroger simultanément. MRR 2 peut être placé dans un autre sous-groupe (*Combinaison 2*). L'interrogation alterne entre les deux sous-groupes.

Pour configurer une combinaison, placez les numéros des MRR dans la zone de texte pour cette combinaison. Les nombres correspondent aux numéros des MRR nommés dans la liste des MRR du menu *Remote Radio Modules* (Modules radio à distance) (reportez-vous à la page 258). Par exemple, « 13 » dans la zone de texte de *Combinaison 1* place les MRR 1 et 3 dans ce sous-groupe.



Remarque : Lors de la configuration des combinaisons MRR, assurez-vous que les MRR configurés soient séquentiels, et qu'il n'y ait pas de chiffres manquants, ce qui peut se produire lorsque des MRR sont supprimés et ajoutés. Les combinaisons utilisent les MRR dans l'ordre dans lequel ils apparaissent dans la liste, pas l'ordre de leur numérotation.

22.4.2.5 Remote Radio Modules (Modules radio à distance (MRR))

Remote Radio Modules:				
	Enabled	Description	IP Address : Port	
1	<input checked="" type="checkbox"/>	Built-in	10.128.75.174	16132
2	<input type="checkbox"/>	Unnamed RRM	0.0.0.0	16132
3	<input type="checkbox"/>	Unnamed RRM	0.0.0.0	16132
4	<input type="checkbox"/>	Unnamed RRM	0.0.0.0	16132

Ce menu affiche les MRR qui composent ce groupe, y compris chaque description, adresse IP et numéro de port définis dans le sous-menu *Connectivity Options* (Options de connectivité) pour les 9160 G2 définies dans le mode de fonctionnement MRR (reportez-vous à la section « Options de connectivité : mode MRR » à la page 248). Chaque MRR peut être activé ou désactivé à partir de ce menu.

22.4.3 Paramètres de configuration des fonctionnalités de liaison radio

Dans la liste des options *Connectivity* (Connectivité), accéder à *Radio Link Features* (Fonctionnalités de liaison radio) permet d'ouvrir la page des paramètres de configuration pour les paramètres d'interrogation et cellulaires.

Figure 22.8 Présentation des paramètres de configuration des fonctionnalités de liaison radio

Basic Settings	View Radio Link Features configuration settings
User Management	
Cluster	
Access Points	
Sessions	
Channel Management	
Wireless Neighborhood	
Security	
Status	
Interfaces	
Events	
Transmit/Receive	
Client Associations	
Neighboring Access Points	
Manage	
Ethernet Settings	
802.11 Settings	
802.11 Advanced Settings	
VWN	
WDS	
Guest Login	
MAC Filtering	
Load Balancing	
Services	
QoS	
Time	
SNMP	
Narrow Band	
Radio	
Connectivity Options	
Connectivity	
Base Station	
RRM Groups	
Radio Link Features	

Radio Link Features:

Operate in Cellular Mode: ☒ Enabled ☐ Disabled

Poll ID: Range (0..255)

Polling Protocol Terminal Timeout: Range (1..240)

Percent Polling Protocol Terminal Timeout: Range (50..90)

Direct TCP Connections for TekTerm: ☐ Enabled ☒ Disabled

Direct TCP Check Duplicate Terminal Number: ☒ Enabled ☐ Disabled

Expiration period (in days) for Automatic Radio Address and Terminal Number: Range (2..365)

Automatic Radio Address

First Address: Last Address: Ranges (1..3840)

Automatic Terminal Number

Group	Ranges (1..1024)	Comments
1	<input type="text" value="0"/> ... <input type="text" value="0"/>	<input type="text"/>
2	<input type="text" value="0"/> ... <input type="text" value="0"/>	<input type="text"/>
3	<input type="text" value="0"/> ... <input type="text" value="0"/>	<input type="text"/>
4	<input type="text" value="0"/> ... <input type="text" value="0"/>	<input type="text"/>
5	<input type="text" value="0"/> ... <input type="text" value="0"/>	<input type="text"/>

22.4.3.1 Fonctionnalités de liaison radio

Radio Link Features:

Operate in Cellular Mode:

☒ Enabled ☐ Disabled

Poll ID:

35

Range (0..255)

Polling Protocol Terminal Timeout:

60

Range (1..240)

Percent Polling Protocol Terminal Timeout:

75

Range (50..90)

Direct TCP Connections for TekTerm:

☐ Enabled ☒ Disabled

Direct TCP Check Duplicate Terminal Number:

☒ Enabled ☐ Disabled

Expiration period (in days) for Automatic Radio Address and Terminal Number:

2

Range (2..365)

Operate in Cellular Mode (Fonctionner en mode cellulaire)

Pour fonctionner comme une station de base cellulaire, ce paramètre doit être **activé**.



Remarque : Le serveur 9500 Communications Server doit également être défini sur le mode cellulaire.

Poll ID (ID d'interrogation)

Dans le protocole d'interrogation adaptative/de contention pour les radios à bande étroite, *Poll ID* (ID d'interrogation) est utilisé pour attribuer une adresse unique à chaque station de base. Lorsque les terminaux mobiles passent d'une station de base à une autre, cette adresse est transmise par les stations de base aux terminaux mobiles, identifiant chaque 9160 G2 dans un système à plusieurs stations de base.

Polling Protocol Terminal Timeout (Délai terminal de protocole d'interrogation)

Ce paramètre détermine le temps en minutes pendant lequel un terminal mobile peut rester inactif avant que la 9160 G2 ne le déclare hors ligne. Avant que ce soit le cas, le terminal mobile sera déclaré hors ligne par le paramètre *Percent Polling Protocol Terminal Timeout* (Délai terminal de protocole d'interrogation en pourcentage) (voir ci-dessous).

Une fois que le terminal mobile est supprimé du système, il est nécessaire de le réinitialiser pour communiquer avec la 9160 G2. Ce paramètre réduit la surcharge de la liaison radio causée lorsque des terminaux mobiles qui ne communiquent pas sont pris en charge. Les valeurs autorisées vont de **1** à **240**.

Percent Polling Protocol Terminal Timeout (Délai terminal de protocole d'interrogation en pourcentage)

Ce paramètre détermine le temps pendant lequel un terminal mobile est autorisé à rester inactif avant que la 9160 G2 ne le déclare hors ligne. Ce délai est exprimé sous la forme d'un pourcentage du paramètre *Polling Protocol Terminal Timeout* (Délai terminal de protocole d'interrogation) (voir ci-dessus). Par exemple, si *Polling Protocol Terminal Timeout* (Délai terminal de protocole d'interrogation) est 60 et que ce paramètre est défini sur 75 %, le délai sera de $60 \text{ min} \times 75 \% = 45 \text{ minutes}$.

Un terminal mobile hors ligne est toujours considéré comme faisant partie du système. Les messages envoyés aux terminaux mobiles hors ligne sont mis en attente au niveau de la 9160 G2. Le terminal mobile reste hors ligne jusqu'à ce qu'il transmette un message en ligne. Les valeurs autorisées pour ce paramètre vont de **50 à 90**.

Direct TCP Connections for TekTerm (Connexions TCP directes pour TekTerm)

L'activation de ce paramètre permet au programme *TekTerm* résident des terminaux mobiles Psion Teklogix de se connecter directement à la 9160 G2, lorsqu'elle sert de station de base à un hôte via TCP/IP.

Direct TCP Check Duplicate Terminal Number (Vérification de doublons de numéro de terminal TCP direct)

Lorsque ce paramètre est activé, la 9160 G2 rejette les terminaux mobiles TCP directs qui tentent de se connecter via un numéro de terminal déjà utilisé par un autre terminal mobile. Lorsque ce paramètre est désactivé, le terminal mobile le plus récent à se connecter sera prioritaire sur les autres terminaux mobiles qui utilisent le même numéro de terminal.

22.4.3.2 Automatic Radio Address (Adresse radio automatique)

Automatic Radio Address		
First Address:	<input type="text" value="1024"/>	Last Address: <input type="text" value="2048"/>
Ranges (1..3840)		

Chaque terminal mobile Psion Teklogix utilisant la liaison radio dispose d'un numéro d'adresse radio unique, qui peut être attribué automatiquement par la 9160 G2 en activant ce paramètre.

Pour **activer** ce paramètre, les valeurs pour le premier et le dernier numéro d'adresse radio doivent être comprises entre **1** et **3840**. Les valeurs par défaut de la plage sont **1024 ... 2084**. Pour **désactiver** le paramètre, définissez les valeurs à **0**.



Remarques : Lorsque vous activez ce paramètre :

1. *Direct TCP Connections for TekTerm (Connexions TCP directes pour TekTerm) doit être désactivé (reportez-vous à la page 261).*
2. *Le paramètre Auto ID (ID automatique) du terminal mobile doit être activé pour que l'adresse radio soit attribuée automatiquement.*
3. *N'activez pas Auto Startup (Démarrage automatique) (reportez-vous à la page 319) sur les stations de base 9150 ou 9160 G2 exécutant 802.IQ avec des sessions utilisant Automatic Radio Address (Adresse radio automatique) et Automatic Terminal Number (Numéro de terminal automatique).*

Expiration Period (Période d'expiration)

Ce paramètre indique la durée, en jours, pendant laquelle une adresse radio ou un numéro de terminal particulier doit être inactif avant que la 9160 G2 ne déclare qu'il est « expiré ». Une adresse ou un numéro de terminal expiré peut être affecté à une autre radio ou session.



Remarque : Pour cette fonctionnalité, il est recommandé d'activer SNTP et de disposer d'un serveur SNTP disponible pour avoir des délais d'expiration précis.

22.4.3.3 Automatic Terminal Number (Numéro de terminal automatique)

Un numéro de terminal est attribué pour chaque session d'application créée dans un terminal mobile. Ce numéro permet d'identifier de manière unique toutes les transmissions vers et à partir de cette session.

Automatic Terminal Number			
Group	Ranges (1..1024)		Comments
1	<input type="text" value="0"/>	... <input type="text" value="0"/>	<input type="text"/>
2	<input type="text" value="0"/>	... <input type="text" value="0"/>	<input type="text"/>
3	<input type="text" value="0"/>	... <input type="text" value="0"/>	<input type="text"/>
4	<input type="text" value="0"/>	... <input type="text" value="0"/>	<input type="text"/>
5	<input type="text" value="0"/>	... <input type="text" value="0"/>	<input type="text"/>

Les numéros de terminal peuvent être attribués automatiquement aux sessions d'application. Le contrôleur fournit également un numéro de groupe à utiliser lors des sessions TESS et ANSI. Un maximum de cinq groupes de sessions de terminal peuvent être définis, et chaque groupe peut recevoir une plage de numéros de terminal différente pour l'attribution automatique. Ces plages ne peuvent pas se chevaucher entre groupes.

Ces groupes s'appliquent uniquement aux sessions TESS et ANSI. Dans le terminal mobile, les applications de terminal TES ou ANSI précisent le groupe auquel elles appartiennent, et elles utilisent la plage d'attribution de numéro de terminal automatique appartenant à ce groupe.

Tous les autres types de session appartiennent à une plage d'attribution de numéro de terminal automatique entre 1 et 3840 et n'utilisent pas le paramètre de « groupe ». Les émulations non ANSI et non TESS qui utilisent l'attribution de numéro de terminal automatique (par exemple, Remote Sockets) doivent une plage de terminaux définie à partir de 1, et cette plage doit être suffisamment grande pour recevoir tous les terminaux mobiles.

L'écran *Radio Link Features* (Fonctionnalités de liaison radio) fournit plusieurs paramètres pour chaque groupe Automatic Terminal Number (Numéro de terminal automatique) : une plage spécifiée par un numéro de terminal inférieur et un numéro de terminal supérieur, et un commentaire. Le commentaire est une chaîne de texte ASCII qui peut être utilisée pour décrire le groupe.



Remarques : Lors de l'activation du numéro de terminal automatique :

1. Direct TCP Connections for TekTerm (Connexions TCP directes pour TekTerm) doit être désactivé (reportez-vous à la page 261).
2. Le paramètre Auto Session (Session automatique) du terminal mobile doit être activé pour que le numéro de session du terminal soit attribué automatiquement.

22.4.4 Menu Hosts (Hôtes)

Lorsque la 9160 G2 sert de station de base, elle doit communiquer avec un « hôte » : un serveur 9500 Communications Server ou un ordinateur hôte utilisant un Kit de développement logiciel (SDK) Psion Teklogix. Par conséquent, chaque contrôleur de réseau maître, hôte SDK ou station de base maître qui communique avec la 9160 G2 doit être configurée comme un hôte. La page *Hosts* (Hôtes) des options *Connectivity* (Connectivité) affiche la description de l'hôte choisi dans la liste déroulante (voir la Figure 22.9 à la page 264).

La page de menu de cette option permet d'afficher les noms d'hôte présents sur le système. Six hôtes maximum peuvent être pris en charge. Une fois qu'un hôte a été configuré, sélectionner le **numéro d'hôte** de cet hôte répertorie les paramètres qui peuvent être modifiés ou supprimés.

Figure 22.9 Présentation des paramètres de configuration hôte de la station de base

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Narrow Band

Radio

Connectivity Options

Connectivity

Base Station

RRM Groups

Radio Link Features

Hosts

View the configuration settings for a Base Station's Host

Hosts:

Number of configured Hosts:0

Host Number:1

Status:☐ Enabled ☒ Disabled

Description:Unnamed Host

First Terminal:1

Last Terminal:32

9010 Configuration:

No Online/Offline:☐ Enabled ☒ Disabled

Monitor Poll:☐ Enabled ☒ Disabled

To Restore Default Configuration...

Click "Default" to re-load the default configuration values for this Host.

Default

Update

Cancel

Number Of Configured Hosts (Nombre d'hôtes configurés)

La page *Hosts* (Hôtes) des options *Connectivity* (Connectivité) affiche le nombre d'hôtes configurés sur le système. Six hôtes maximum peuvent être pris en charge.

Host Number (Numéro d'hôte)

Ce paramètre indique le numéro d'hôte attribué. Choisir le **numéro d'hôte** dans la liste déroulante affiche les paramètres qui peuvent être modifiés ou supprimés pour cet hôte. De nouveaux hôtes peuvent être ajoutés en sélectionnant un numéro libre et en configurant des paramètres pour celui-ci.

Le numéro d'hôte s'affiche également sur le terminal mobile RF lors du passage entre hôtes dans un environnement à plusieurs hôtes.

Status (État)

L'état doit être **Enabled** (Activé) pour que les terminaux mobiles communiquent avec cet hôte.

Description

Cette zone de texte vous permet de nommer le protocole utilisé par l'hôte. Les protocoles sont les méthodes par lesquelles les terminaux mobiles peuvent communiquer avec les ordinateurs hôtes sur différents supports physiques tels que les connexions Ethernet et liaison radio.

Lorsque la 9160 G2 sert de station de base, elle communique avec un hôte **9010/ TCP/IP** via une connexion réseau. Le protocole 9010 est un protocole propriétaire asynchrone développé par Psion Teklogix qui utilise les flux de données TESS (Teklogix Screen Subsystem) ou ANSI pour communiquer avec les terminaux mobiles. Pour plus d'informations, veuillez consulter le *manuel d'utilisation Psion Teklogix* pour : *9500 Communications Server, SDK, TESS* ou *ANSI*.

First Terminal/Last Terminal (Premier terminal/Dernier terminal)

Les valeurs entrées dans ces paramètres désignent le premier et le dernier terminal dans la plage de terminaux mobiles qui communiqueront avec l'hôte. Ces numéros de terminal sont configurés sur cet hôte particulier. Les numéros de terminal peuvent s'étendre sur une plage allant de **1** à **3840**.

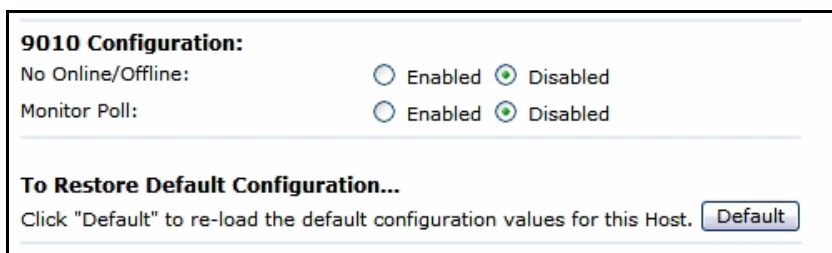
Restaurer la configuration par défaut

En bas de la page du menu Host (Hôte), vous pouvez cliquer sur **Default** (Par défaut) pour charger à nouveau les valeurs de configuration par défaut pour cet hôte.

Mise à jour des paramètres

À tout moment pendant la configuration de l'hôte, vous pouvez *mettre à jour* les paramètres ou *annuler* le processus en cliquant sur le bouton correspondant au bas de la page.

22.4.4.1 Configuration 9010



9010 Configuration:

No Online/Offline: ☐ Enabled ☒ Disabled

Monitor Poll: ☐ Enabled ☒ Disabled

To Restore Default Configuration...

Click "Default" to re-load the default configuration values for this Host.

No Online/Offline (Aucun En ligne/Hors ligne)

Si ce paramètre est **Enabled** (Activé), la station de base 9160 G2 **n'informe pas** le système hôte si l'état d'un terminal mobile passe d'en ligne à hors ligne. Si ce paramètre est **Disabled** (Désactivé), la 9160 G2 **informe** l'hôte de tout changement d'état du terminal mobile. La valeur par défaut de ce paramètre est **Disabled** (Désactivé).

Contrôle d'interrogation

Les hôtes envoient généralement des messages ou des interrogations nulles à la 9160 G2 dans un délai d'environ 40 secondes. Si le paramètre est **activé**, la station de base 9160 G2 contrôle les messages et les interrogations de cet hôte ; si elle ne reçoit un message ou une interrogation dans les 40 secondes, elle ferme la connexion. La valeur par défaut de ce paramètre est **Disabled** (Désactivé).

CONFIGURATION DU MINI-CONTRÔLEUR **23**

23.1 Présentation	269
23.2 Menu de configuration du mini-contrôleur	270
23.3 Menu Hosts (Hôtes)	270
23.4 Options du menu de l'hôte	274
23.4.1 Émulation 3274	274
23.4.1.1 Options d'émulation	274
23.4.1.2 Options TESS	275
23.4.1.3 Options de protocole Telnet	285
23.4.1.4 Configurations des touches de fonction	289
23.4.2 Émulation 5250	290
23.4.2.1 Options d'émulation	290
23.4.2.2 Options TESS	291
23.4.2.3 Options de protocole Telnet	301
23.4.2.4 Configurations des touches de fonction	305
23.4.3 Émulation ANSI	306
23.4.3.1 Options d'émulation	306
23.4.3.2 Options de protocole Telnet	310
23.4.3.3 Auto-Telnet/Auto-login (Telnet automatique/Connexion automatique)	312
23.4.3.4 Configurations des touches de fonction	316

23.1 Présentation

Le contrôleur réseau dans un système Psion Teklogix effectue un certain nombre de tâches importantes. L'une de ces tâches est l'*émulation* : la traduction des données entre le protocole de l'ordinateur hôte et le protocole utilisé par les terminaux mobiles Psion Teklogix.

Les données qui sont envoyées à partir d'un ordinateur hôte à un terminal mobile pour leur affichage, et renvoyées à l'hôte à la suite des opérations du terminal mobile, sont appelées flux de données. Les ordinateurs hôtes peuvent fournir des flux de données de différents types à leurs terminaux mobiles.

Les terminaux mobiles Psion Teklogix ne peuvent accepter directement que deux types de flux de données : *TESS* et *ANSI*. TESS (Teklogix Screen Subsystem) est le flux de données propriétaire utilisé par les terminaux mobiles Psion Teklogix. Les flux de données ANSI sont un type de flux de données standard utilisé par les terminaux mobiles ANSI filaires. Les autres types de flux de données fournis par l'hôte doivent être convertis en TESS ou ANSI avant que les terminaux mobiles Psion Teklogix puissent les utiliser. Cette conversion est réalisée par un logiciel d'émulation dans un contrôleur réseau.

La passerelle sans fil 9160 G2 Wireless Gateway est équipée de fonctionnalités d'émulation, lui permettant d'agir comme un mini-contrôleur. Lorsqu'une 9160 G2 est configurée comme un mini-contrôleur, les terminaux mobiles Psion Teklogix peuvent émuler un terminal mobile ANSI, 5250 ou 3274 via une 9160 G2 plutôt que par le biais d'un serveur de communications 9500.



Important : Les 9160 G2 agissant comme des mini-contrôleurs sont conçues pour des petits sites à faibles transactions. Un serveur de communications 9500 est nécessaire pour les systèmes qui prennent en charge plus de 50 terminaux mobiles.

En tant que mini-contrôleur, la passerelle sans fil 9160 G2 Wireless Gateway peut prendre en charge jusqu'à 32 stations de base en réseau et jusqu'à 50 terminaux mobiles.

Un mini-contrôleur 9160 G2 peut également gérer les configurations LAN sans fil.

Une 9160 G2 configurée comme un mini-contrôleur peut prendre en charge les émulations suivantes :

- Émulation 5250 avec TCP/IP via une connexion LAN Ethernet.
- Émulation 3274 avec TCP/IP via une connexion LAN Ethernet.
- Émulation ANSI avec TCP/IP via une connexion LAN Ethernet.



Remarque : Les principaux paramètres de la 9160 G2 doivent d'abord être définis comme décrit dans les chapitres précédents de ce manuel.

La 9160 G2 peut également être intégrée dans un système mapRF, via le protocole 802.IQv2 (pour plus de détails, reportez-vous à la section « Menu des fonctionnalités 802.IQ v2 » à la page 323).



Remarque : La fonctionnalité de mini-contrôleur n'est disponible qu'après avoir été déverrouillée via un mot de passe utilisé à l'invite de la console.

23.2 Menu de configuration du mini-contrôleur

Pour être utilisé comme mini-contrôleur, les paramètres des pages *Hosts* (Hôtes) doivent être définis de manière appropriée. Dans la liste des options de *Connectivity* (Connectivité), entrer *Hosts* (Hôtes) ouvre la page *Configuration Settings For A Base Station's Host* (Paramètres de configuration pour une station de base de l'ordinateur hôte). Pour plus d'informations sur la configuration des paramètres de protocole radio, reportez-vous à la section « Paramètres de configuration des fonctionnalités de liaison radio » à la page 258.

23.3 Menu Hosts (Hôtes)

La page de menu dans cette option permet d'afficher les noms d'hôte présents sur le système. Six hôtes maximum peuvent être pris en charge. Un « hôte » doit être configuré pour chaque hôte qui communique avec le mini-contrôleur 9160 G2. Une fois qu'un hôte a été configuré, sélectionner le **numéro d'hôte** de cet hôte répertorie les paramètres qui peuvent être modifiés ou supprimés.

Figure 23.1 Présentation des paramètres de configuration des hôtes

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Narrow Band

Radio

Connectivity Options

Connectivity

Base Station

RRM Groups

Radio Link Features

Hosts

802.1Q

Maintenance

Configuration

Upgrade

View the configuration settings for a Base Station's Host

?

When the 9160 acts as a Base Station, it must communicate with a "host" - a 9500 or 9400 network Controller, or a host computer using Psion Teklogix Software Development Kit (TSDK).

This page allows you to select the host names present on the system. Up to six hosts can be supported. A "host" must be configured for each master network controller, TSDK host, or master Base Station that communicates with the 9160.

Hosts:

Number of configured Hosts: 0

Host Number: 1

Status: ☐ Enabled ☒ Disabled

Description: Unnamed Host

First Terminal: 1

Last Terminal: 32

Emulation: 5250

5250 Emulation Options:

Write Error Code: Advisory text

Use International EBCDIC: ☐

Allow null character in fixed fields: ☐

TESS Options:

Field Underline Remapping: None

Alarm: ☐

Clear: ☐

Passthru: ☐

Procedures: ☐

Local: ☐

Host Print: ☐

Remote Print: ☐

Pages: 8 (Range 1..79)

Transmit Line: 0 (Range 0..24)

AIAG: 0 (Range 0..255)

Visible Match Character: 0 (Range 0..255)

Hidden Match character: 0 (Range 0..255)

Serial I/O: 0 (Range 0..255)

Print Line: 0 (Range 0..24)

Print Form Length: 0 (Range 0..24)

Barcode: 0 (Range 0..255)

Entry Line: 0 (Range 0..24)

Field Overhead: 5 (Range 0..80)

Command Region: 0, 0, 0, 0

Telnet Protocol Options:

Terminal Type: IBM-5251-11

Host Port: 23 (Range 1..32767)

Maximum Sessions per Terminal: 4 (Range 1..127)

First Local Terminal Port: 10000 (Range 1..32767)

Local IP Address to Bind: 0.0.0.0

First Terminal Listen Port: 0 (Range 0..32767)

Actively Negotiate with Host: ☐

Auto-telnet: DISABLE

Auto-telnet Host:

Auto-telnet without User Action: ☒

Enable Virtual Device Names: ☐

- Configure Device Names: Configure

- Device Name Prefix:

Function Key Mappings:

F1: F1 F14: F14 F27: F17

F2: F2 F15: F15 F28: F18

F3: F3 F16: CLEAR F29: UP

F4: F4 F17: PRINT F30: SESS

F5: F5 F18: HELP F31: ENTER

F6: F6 F19: F19 F32: ENTER

F7: F7 F20: F20 F33: ENTER

F8: F8 F21: F21 F34: ENTER

F9: F9 F22: F22 F35: ENTER

F10: F10 F23: F23 F36: ENTER

F11: F11 F24: F24 F37: ENTER

F12: F12 F25: DOWN F38: SELECTOR

F13: F13 F26: F16 F39: ENTER

To Restore Default Configuration...

Click "Default" to re-load the default configuration values for this Host. Default

Update Cancel

Number Of Configured Hosts (Nombre d'hôtes configurés)

La page *Hosts* (Hôtes) des options de *connectivité* affiche le nombre d'hôtes configurés sur le système. Six hôtes maximum peuvent être pris en charge.

Host Number (Numéro d'hôte)

Ce paramètre indique le numéro d'hôte affecté. Choisir le **numéro d'hôte** dans la liste déroulante affiche les paramètres qui peuvent être modifiés ou supprimés pour cet hôte. De nouveaux hôtes peuvent être ajoutés en sélectionnant un numéro libre et en configurant des paramètres pour celui-ci.

Le numéro d'hôte s'affiche également sur le terminal mobile RF lors du passage entre hôtes dans un environnement à plusieurs hôtes.

Status (État)

L'état doit être **Enabled** (Activé) pour que les terminaux mobiles communiquent avec cet hôte.

Description (Description)

Cette zone de texte vous permet de nommer le protocole utilisé par l'hôte. Les protocoles sont les méthodes par lesquelles les terminaux mobiles peuvent communiquer avec les ordinateurs hôtes sur différents supports physiques tels que les connexions Ethernet et par liaison radio.

Lorsque la 9160 G2 sert de station de base, elle communique avec un hôte **9010/ TCP/IP** via une connexion réseau. Le protocole 9010 est un protocole propriétaire asynchrone développé par Psion Teklogix qui utilise les flux de données TESS (Teklogix Screen Subsystem) ou ANSI pour communiquer avec les terminaux mobiles. Pour plus d'informations, veuillez consulter le *manuel d'utilisation Psion Teklogix* pour : *serveur de communications 9500, SDK, TESS* ou *ANSI*.

First Terminal/Last Terminal (Premier terminal/Dernier terminal)

Les valeurs entrées dans ces paramètres désignent le premier et le dernier terminal dans la gamme de terminaux mobiles qui communiquera avec l'hôte. Ces numéros de terminal sont configurés sur cet hôte particulier. Les numéros de terminal peuvent s'étendre sur une plage allant de **1** à **3840**.

Emulation (Émulation)

Ce menu déroulant fournit une liste des émulations hôte prises en charge par la passerelle sans fil 9160 G2 Wireless Gateway. En fonctionnant avec des terminaux mobiles et des stations de base Psion Teklogix, la 9160 G2 peut émuler des terminaux mobiles IBM 3278-2, 5251-11, et 5555-B01, ainsi que des terminaux mobiles ANSI.

Les protocoles sont les méthodes par lesquelles les terminaux mobiles peuvent communiquer avec les ordinateurs hôtes sur différents supports physiques tels que les connexions Ethernet et par liaison radio. La 9160 G2 prend en charge le protocole TCP/IP. Les émulations prises en charge sont les suivantes :

- 9010/ TCP/IP (pour plus de détails, voir ci-dessous).
- Émulation 3274 (voir pages 274 à 289 pour les paramètres de configuration).
- Émulation 5250 (voir pages 290 à 305 pour les paramètres de configuration).
- Émulation ANSI (voir pages 306 à 316 pour les paramètres de configuration).

Lorsque la passerelle sans fil 9160 G2 Wireless Gateway agit comme une station de base, elle utilise l'émulation 9010 (un protocole propriétaire asynchrone développé par Psion Teklogix) pour communiquer avec un serveur de communications 9500 ou un hôte via un kit de développement logiciel (SDK) de Psion Teklogix. Pour plus d'informations sur la configuration de la 9160 G2 comme station de base et émulation 9010, reportez-vous au Chapitre 22 : « La 9160 G2 comme station de base ».

Lorsque la passerelle sans fil 9160 G2 Wireless Gateway agit comme un mini-contrôleur, elle utilise les protocoles d'émulation 3274 et 5250 pour communiquer avec les hôtes IBM, ou le protocole d'émulation ANSI pour communiquer avec les terminaux mobiles ANSI.

Pour restaurer la configuration par défaut

En bas de la page du menu de l'hôte, vous pouvez cliquer sur **Default** (Par défaut) pour charger à nouveau les valeurs de configuration par défaut de cet hôte.

Mise à jour des paramètres

À tout moment pendant la configuration de l'hôte, vous pouvez *mettre à jour* les paramètres ou *annuler* le processus en cliquant sur le bouton correspondant au bas de la page.

23.4 Options du menu de l'hôte

Lorsque vous choisissez un *numéro d'hôte*, la 9160 G2 affiche les paramètres de configuration de cet hôte. Les émulations 5250, 3274 et ANSI disposent de quatre sous-menus : les *options d'émulation*, *options TESS*, *options de protocole Telnet* de l'hôte et les *configurations des touches de fonction* (pour une présentation de la page, reportez-vous à la Figure 23.1 à la page 271).

23.4.1 Émulation 3274

23.4.1.1 Options d'émulation

3274 Emulation Options:
Is Host Fujitsu: ☐
Use International EBCDIC: ☐
Allow null character in fixed fields: ☐

Avec une émulation IBM 3274 ou IBM 5250, le mini-contrôleur 9160 G2 convertit le flux de données depuis l'hôte en commandes TESS (Teklogix Screen Subsystem). Certains des paramètres dans cette page régissent la conversion des écrans de l'hôte pour TESS.

Is Host Fujitsu (L'hôte est-il Fujitsu)

Si ce paramètre est **activé**, le mini-contrôleur 9160 G2 attend des données de l'hôte qui contiennent des commandes natives, etc. , d'un hôte Fujitsu. L'activation de ce paramètre entraîne le remplacement des codes de formatage standard IBM (pour le démarrage de champ, la définition des tampons, etc.) par les codes utilisés par les ordinateurs hôtes Fujitsu.

Use International EBCDIC (Utiliser EBCDIC International)

Si ce paramètre est **activé**, le mini-contrôleur 9160 G2 utilise le jeu de caractères EBCDIC international, en échangeant les positions des caractères ! et].

Allow null character in fixed fields (Autoriser le caractère nul dans les champs fixes) :

Si ce paramètre est **activé**, le mini-contrôleur 9160 G2 autorise les caractères nuls dans les espaces des champs qui ont des attributs vidéo visuels tels que la vidéo inverse. La valeur par défaut pour l'émulation d'hôte 3274 est **désactivé**.

23.4.1.2 Options TESS

TESS Options:	
Alarm:	<input type="checkbox"/>
Clear:	<input type="checkbox"/>
Passthru:	<input type="checkbox"/>
Procedures:	<input type="checkbox"/>
Local:	<input type="checkbox"/>
Host Print:	<input type="checkbox"/>
Remote Print:	<input type="checkbox"/>
Pages:	<input type="text" value="8"/> (Range 1..79)
Transmit Line:	<input type="text" value="0"/> (Range 0..24)
AIAG:	<input type="text" value="0"/> (Range 0..255)
Visible Match Character:	<input type="text" value="0"/> (Range 0..255)
Hidden Match character:	<input type="text" value="0"/> (Range 0..255)
Serial I/O:	<input type="text" value="0"/> (Range 0..255)
Print Line:	<input type="text" value="0"/> (Range 0..24)
Print Form Length:	<input type="text" value="0"/> (Range 0..24)
Barcode:	<input type="text" value="0"/> (Range 0..255)
Entry Line:	<input type="text" value="0"/> (Range 0..24)
Field Overhead:	<input type="text" value="5"/> (Range 0..80)
Command Region:	<input type="text" value="0"/> , <input type="text" value="0"/> , <input type="text" value="0"/> , <input type="text" value="0"/>

Alarm (Alarme)

Lorsque ce paramètre est **activé**, les terminaux mobiles émettent un signal sonore lorsque le mot « ALARM » (ALARME) s'affiche sur l'écran de l'application à l'emplacement spécifié dans le paramètre *Command Region* (Région de commande) (voir page 284). Le mot « ALARM » doit être un champ *affichage uniquement*.



Remarque : Les paramètres Command Region (Région de commande) doivent être activés si vous souhaitez que ce paramètre fonctionne.

Clear (Effacer)

Si ce paramètre est **activé**, le mini-contrôleur 9160 G2 crée un champ de saisie *vide* pour un champ de saisie contenant des espaces.

Certaines applications hôtes dépendent des attributs vidéo des caractères affichés pour mettre en évidence des champs, en particulier les champs de saisie. Par exemple, l'écran d'application peut définir tous les champs de saisie avec la vidéo inverse et remplir le champ d'espaces. C'est efficace sur les terminaux mobiles qui prennent en charge la vidéo inverse, mais sur les terminaux mobiles où ce n'est pas le cas, peut rendre le champ invisible puisqu'il est constitué uniquement d'espaces.

Par défaut, tous les champs de saisie vides affichés sur le terminal mobile Psion Teklogix sont mis en évidence par le « caractère de saisie » sélectionné dans la configuration du terminal mobile.



Remarque : Cette opération est effectuée uniquement sur les écrans reçus de l'hôte. Les données envoyées à l'hôte ne sont pas affectées.

Passthru (Transfert)

Si ce paramètre est **activé**, la 9160 G2 permet à l'hôte d'envoyer les données directement au port série du terminal mobile RF. Il est le plus couramment utilisé pour l'impression.

Préparation des écrans de l'hôte au mode « Pass-through »

Le mot **PASSTHRU** (en lettres majuscules) doit apparaître sur la première ligne, à partir de la deuxième colonne, sur l'écran à envoyer via le port série du terminal mobile. Les données réelles à envoyer au terminal mobile peuvent commencer n'importe où en-dessous de la première ligne.

Avec les émulations 5250 ou 3274, des attributs occupent une position dans la mémoire tampon d'écran. Un attribut placé entre la colonne 2 et la fin du mot « PASSTHRU » décalera tous les caractères suivants d'une position vers la droite. Par conséquent, les attributs requis doivent occuper la colonne 1 de la première ligne (juste avant le mot « PASSTHRU »).

Exemple :

colonne : 1 2 3 4 5 6 7 8 9

Ligne 1 : @ P A S S T H R U @

Ligne 2 : @ P A R T : 1 2 3 4 5

où @ est un attribut.

Lorsque la 9160 G2 a fini de transmettre les données à l'imprimante du terminal mobile, elle envoie une touche **ENTRÉE** à l'hôte. L'hôte doit attendre la touche **ENTRÉE** avant d'envoyer d'autres écrans (y compris d'autres écrans PASSTHRU) à ce terminal mobile.



Remarque : Reportez-vous au manuel d'utilisation du terminal mobile approprié pour plus d'informations sur la configuration des paramètres sur le terminal mobile pour le mode « pass-through ».

Procédures (Procédures)

Si ce paramètre est **activé**, l'hôte peut envoyer des procédures TESS via la 9160 G2 aux terminaux mobiles. Une procédure TESS est un groupe de commandes TESS qui peuvent être exécutées par la commande TESS *execute procedure*.

Local (Local)

Si ce paramètre est **activé**, la 9160 G2 autorise l'hôte à fournir des pages à charger comme procédures TESS locales sur les terminaux mobiles.

Les procédures locales sont sélectionnées à partir d'un menu sur le terminal mobile. Les terminaux mobiles peuvent effectuer ces procédures lorsqu'ils sont hors ligne. Plus tard, lorsqu'ils sont en ligne, ils envoient les résultats de ces fonctions à l'hôte.



*Remarque : Le paramètre Procedures (Procédures) doit également être **activé** pour que Local (Local) fonctionne.*

Host Print (Impression hôte)

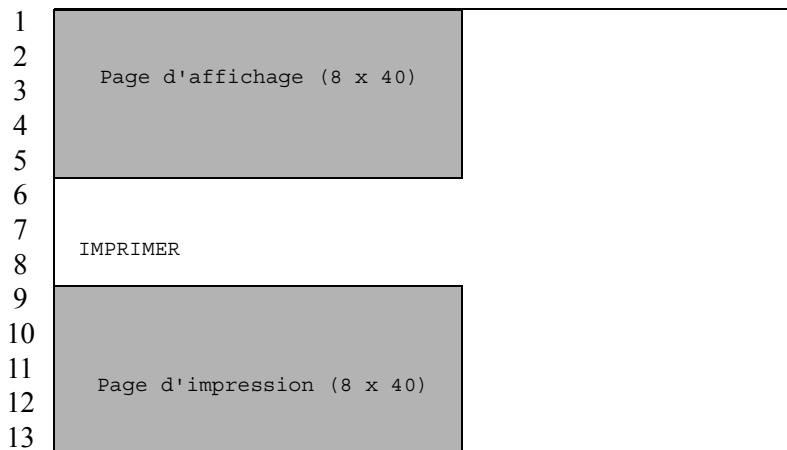
Lorsque ce paramètre est **activé**, l'hôte peut envoyer des données supplémentaires aux écrans du terminal mobile et demander au terminal mobile de les imprimer. Il s'agit de l'opposé de la fonctionnalité d'*impression locale* où le terminal mobile lance la demande d'impression.

Le texte qui est transmis à l'imprimante est formaté dans l'écran de l'application 24 x 80. Si l'hôte peut lancer l'opération d'impression, le texte est imprimé. La 9160 G2 identifie le texte supplémentaire comme une page d'impression par la présence du mot « PRINT » (IMPRIMER) (en lettres majuscules) commençant sur la 2e colonne de la ligne 13 sur l'écran 24 x 80. Le mot « PRINT » doit être défini comme du texte *affichage uniquement*.

La page d'impression est positionnée au-dessous de la page d'affichage du terminal mobile (voir la figure ci-dessous). La taille de la page d'impression est toujours identique à celle de la page d'affichage du terminal mobile (en supposant que, dans la configuration de l'ordinateur mobile, la longueur de la page est inférieure à 12 lignes).

Dans le cas où *Host Print* (Impression hôte) est **activé**, la 9160 G2 transmet la page d'impression au terminal mobile après avoir reçu l'écran d'application de l'hôte.

Figure 23.2 Écran d'application avec page d'impression



Remarques :

1. Contrairement à l'option Passthru (Transfert), lors de l'utilisation de l'impression hôte, aucune séquence d'échappement ne peut être envoyée à l'imprimante.
2. La prise en charge de l'impression doit être activée sur le terminal mobile en commandant l'impression dans le menu des fonctionnalités TESS ; reportez-vous au manuel d'utilisation du terminal mobile approprié pour plus d'informations.

Remote Print (Impression à distance)

Lorsque ce paramètre est **activé**, la 9160 G2 envoie la page d'impression à un terminal mobile lorsque celui-ci le demande (en utilisant la touche de fonction « F17 » du terminal mobile ou la touche « PRINT » sur les terminaux mobiles plus anciens). La 9160 G2 envoie la réponse de fonctionnalité à l'hôte.

Il s'agit de l'opposé de l'impression hôte où l'hôte lance la demande d'impression.



Remarque : La prise en charge de l'impression doit être activée sur le terminal mobile. Reportez-vous au manuel d'utilisation du terminal mobile approprié pour plus d'informations.

Pages (Pages)

Ce paramètre détermine le nombre d'écrans hôte (ou de pages) stockés au niveau du terminal mobile, avec un maximum de **79**.

La 9160 G2 réduit la quantité de données transmises aux terminaux mobiles en utilisant la capacité du terminal mobile à stocker une page de données pour chaque écran qu'il affiche. La 9160 G2 garde une image de chaque page stockée sur le terminal mobile. Après avoir reçu un écran d'application, la 9160 G2 tente d'associer l'écran à une page stockée. Si une page similaire est déjà dans la mémoire du terminal mobile, la 9160 G2 indique au terminal mobile d'afficher à nouveau sa copie de la page ; seules les modifications nécessaires sont envoyées à partir du contrôleur. Si aucune correspondance n'est trouvée, la page complète est envoyée au terminal mobile par liaison radio.



*Remarque : Il y a un paramètre correspondant sur le terminal mobile, et le nombre **réel** de pages enregistrées sera la **plus petite** des deux valeurs.*

Transmit Line (Ligne de transmission)

Lorsque cette fonctionnalité est **activée**, toutes les données modifiées au niveau du terminal mobile sont transmises automatiquement lorsque l'opérateur saisit des données dans un champ de *transmission à la saisie*.

La valeur dans cette zone de texte indique la ligne sur l'écran qui est désignée comme *ligne de transmission*. Le dernier champ de saisie au-dessus ou sur la ligne de transmission de l'écran sera identifié comme le champ de *transmission à la saisie*. Si des champs de saisie existent sur des lignes au-dessous de la ligne de transmission, aucun champ de saisie ne sera désigné comme champ de *transmission à la saisie*.

Une valeur de **0** (zéro) désactive cette fonctionnalité. Une valeur de **24** désigne le *dernier* champ de saisie sur chaque écran d'application comme champ de *transmission à la saisie*.

AIAG (AIAG)

Ce paramètre fournit la localisation et le remplissage automatiques de l'entrée depuis des lecteurs de code-barres. Lorsque les données d'un code-barres sont entrées dans un terminal mobile, le terminal mobile recherche sur la page en cours des champs « AIAG » qui peuvent accepter les données du code-barres. Les données préchargées dans le champ « AIAG » par le programme d'application déterminent si les données du code-barres sont acceptées.

Au niveau du mini-contrôleur 9160 G2, une valeur décimale de caractère ASCII entre **0** et **255** est définie pour correspondre à l'« identificateur de champ AIAG » défini au niveau de l'hôte. Une valeur de **0** (zéro) désactive cette fonctionnalité.

Le format des données préchargées est comme suit :

<mode> <préfixe AIAG(données)>

Le caractère de mode utilisé avec la commande permet des modes de fonctionnement différents pour répondre à diverses opérations d'application. L'opération de localisation et de remplissage automatiques s'applique uniquement aux données reçues d'un lecteur de code-barres. Les descriptions des modes et du préfixe AIAG sont indiquées dans le Tableau 23.1 à la page 280. Ces modes sont définis au niveau de l'hôte.

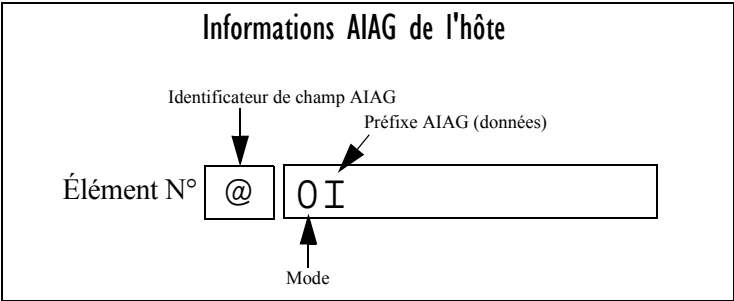
Tableau 23.1 Fonctions de mode et description du préfixe AIAG

Mode	Fonction
0	Affiche le préfixe, envoie le préfixe à l'hôte.
1	N'affiche pas le préfixe, envoie le préfixe à l'hôte.
2	Affiche le préfixe, n'envoie pas le préfixe à l'hôte.
3	N'affiche pas le préfixe, n'envoie pas le préfixe à l'hôte.
+4	Ajoutez 4 aux valeurs ci-dessus pour transmettre à l'hôte lorsque tous les champs AIAG avec 4 défini sont remplis. La fonction 0 est « activée » s'il y a des champs avec ce bit défini, et que tous les champs avec ce bit défini ont été remplis par l'opérateur.
+8	Ajoutez 8 aux valeurs ci-dessus pour autoriser le remplacement des données entrées précédemment.
+16	Ajoutez 16 aux valeurs ci-dessus pour indiquer la priorité de position du curseur pour la recherche et le remplissage.
Préfixe AIAG (données)	Le texte à faire correspondre dans le champ AIAG.

Exemple :

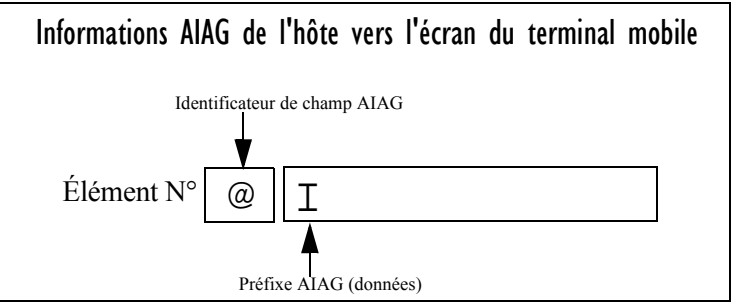
Les informations contenues dans l'exemple d'écran ci-dessous sont définies et envoyées à **partir de** l'hôte. Elles incluent l'« identificateur AIAG » (la balise identifiant s'il s'agit d'un champ AIAG), suivi du mode, dans ce cas Mode 0, puis, enfin, le « préfixe AIAG » - I.

Figure 23.3 Champ AIAG envoyé à partir de l'hôte



Lorsque les informations arrivent sur l'écran du terminal mobile, le champ AIAG approprié pour les informations numérisées est localisé via l'« identificateur AIAG ». Comme Mode 0 a été défini au niveau de l'hôte, le « préfixe AIAG » - I - s'affiche sur l'écran du terminal mobile, et lorsque cet écran est terminé, le préfixe est renvoyé à l'hôte.

Figure 23.4 Champ AIAG envoyé au terminal mobile



Caractère de correspondance visible

En insérant un caractère ASCII spécialement directement avant un champ de saisie, le programme d'application fait la distinction entre un « champ de correspondance » et un champ de saisie. Supposons, par exemple, qu'un crochet en chevron « > » est défini comme champ de correspondance visible.

Insérer « > » immédiatement avant le champ de saisie l'identifie comme un champ de correspondance, comme illustré ci-dessous.

N° de référence > _____

La plage possible pour ce paramètre, 0 à 255, représente les valeurs décimales des caractères ASCII. Une valeur de 0 (zéro) désactive cette fonctionnalité. La valeur décimale ASCII entrée sur la 9160 G2 doit coïncider avec la valeur définie par le programme d'application.

Pour utiliser la fonction *Visible Match* (Correspondance visible), l'ordinateur hôte précharge les données dans un champ de saisie correspondant. Les données sont visibles sur l'écran du terminal mobile. Les données préchargées envoyées à un terminal mobile peuvent être constituées de caractères exacts, de caractères correspondants spéciaux ou d'une combinaison des deux. Reportez-vous au Tableau 23.2 pour voir les caractères de correspondance reconnus par les terminaux mobiles Psion Teklogix.

Si une entrée ne correspond pas aux données préchargées, elle s'affiche, le terminal mobile émet un signal sonore et le curseur se déplace vers la première position dans le champ de correspondance. L'opérateur peut soit effectuer une autre entrée dans le champ de correspondance ou déplacer le curseur vers un nouveau champ. Lorsqu'une entrée (même si elle ne correspond pas aux données préchargées) est réalisée dans un champ de correspondance, elle est envoyée à l'hôte avec les données modifiées du terminal mobile lors de la prochaine transmission.

Tableau 23.2 Caractères de correspondance

Caractère	Description
#	Faire correspondre un chiffre.
&	Faire correspondre une lettre (majuscule ou minuscule).
^	Faire correspondre une lettre majuscule.
_	Faire correspondre une lettre minuscule.
/	Faire correspondre un caractère alphanumérique.
"	Faire correspondre une lettre, un chiffre ou un espace.
?	Faire correspondre un signe de ponctuation.
'	Faire correspondre n'importe quel caractère.
:	Faire correspondre toutes les positions des caractères du champ avec le caractère précédent.
;	Faire correspondre les caractères restants, mais pas nécessairement le reste du champ, avec le caractère précédent.

Exemple :

Supposons que vous souhaitiez précharger un champ d'entrée avec un numéro de référence. Si ce numéro de référence est connu, vous pouvez l'utiliser pour précharger le champ. Si plus de flexibilité est nécessaire, et que le numéro de référence commence toujours par deux caractères alphabétiques, suivis d'un trait d'union et de quatre chiffres, la chaîne de correspondance pour le champ serait : **&&-####** .

Caractère de correspondance masqué

Contrairement aux données d'un champ de « correspondance visible », les données préchargées dans un champ de « correspondance masqué » ne sont *pas* affichées sur le terminal mobile.



Remarque : Reportez-vous à la section « Caractère de correspondance visible » à la page 281 pour plus d'informations sur la correspondance de champ.

La plage possible pour ce paramètre, **0 à 255**, représente les valeurs décimales des caractères ASCII. Une valeur de **0** (zéro) désactive cette fonctionnalité. La valeur décimale ASCII entrée sur la 9160 G2 doit coïncider avec la valeur définie par le programme d'application.

Serial I/O (E/S série)

Les champs d'*entrée/sortie série* sont des entrées spéciales et des champs fixes qui acceptent l'entrée et la sortie vers un port série. Le programme d'application différencie ce champ comme étant d'*entrée/sortie série* en précédant le champ par un caractère spécial.

Si ce caractère précède un champ fixe, les données sont envoyées au port série du terminal mobile. S'il précède un champ de saisie, le champ accepte les données du port série du terminal mobile.

La plage possible pour ce paramètre, **0 à 255**, représente les valeurs décimales des caractères ASCII. Une valeur de **0** (zéro) désactive cette fonctionnalité.

Print Line (Ligne d'impression)

Ce paramètre vous permet de saisir le numéro de ligne de début de la page d'impression sur l'écran de l'application (voir aussi *Entry Line* (Ligne d'entrée)). Une valeur maximale de **24** déclenche l'impression de la page d'affichage ; une valeur de **0** (zéro) désactive cette fonctionnalité.

Print Form Length (Longueur de formulaire d'impression)

Ce paramètre définit la longueur du formulaire de l'imprimante en lignes. La plage est comprise entre **0** et **24**.

Barcode (Code-barres)

Les champs d'*entrée de code-barres uniquement* sont des champs d'entrée spéciaux qui n'acceptent que les entrées d'un lecteur de code-barres. Le programme d'application différencie un champ de saisie comme étant d'*entrée de code-barres uniquement* en précédant le champ par un caractère spécial.

La plage possible pour ce paramètre, **0** à **255**, représente les valeurs décimales des caractères ASCII. Une valeur de **0** (zéro) désactive cette fonctionnalité.

Entry Line (Ligne d'entrée)

Ce paramètre contient le numéro de la première ligne affiché s'il n'y a aucun champ de saisie dans la partie supérieure gauche de l'écran, et si un champ de saisie est au niveau de cette ligne ou au-dessous de cette ligne.

Le paramètre *Entry Line* (Ligne d'entrée) permet un décalage automatique dans l'écran hôte, de sorte que la zone affichée par le terminal mobile inclut un champ de saisie qui ne serait pas normalement disponible. Certains terminaux mobiles Psion Teklogix affichent uniquement le coin supérieur gauche de l'écran de l'application à cause de leur petite taille d'écran.

Field Overhead (Charge de champ)

Ce paramètre contient le nombre maximum de caractères autorisés entre deux champs *fixes* qui permet encore à la 9160 G2 de les réunir dans un seul champ.

Il arrive parfois que la 9160 G2 connecte deux champs fixes et les envoie ensuite comme un seul champ. Cela vous permet de réduire la charge de la liaison radio.

Par exemple, si deux champs avaient 4 caractères séparément et que ce paramètre était « 5 », ces champs seraient réunis en un seul.

Command Region (Région de commande)

Ce paramètre définit une région de l'écran hôte que la 9160 G2 examinera pour détecter la présence de commandes réservées.

Les quatre numéros dans les zones de texte *Command Region* (Région de commande) représentent les adresses rangée et colonne du coin supérieur gauche et du coin inférieur droit de la région de commande. La première zone de texte de chaque paire contient le numéro de rangée ; la deuxième contient le numéro de colonne. La plage des valeurs de rangée va de **0** à **24** ; celle des valeurs de colonne va de **0** à **80**.

Par exemple, pour définir les deux dernières lignes de l'écran hôte comme région de commande, saisissez les valeurs 23, 1 et 24, 80.

Actuellement, la seule commande prise en charge est *ALARM* (ALARME) (reportez-vous à la page 275 pour des informations détaillées sur cette commande). Lorsque le mot « ALARM » (ALARME) est placé n'importe où dans la région de commande, la passerelle 9160 G2 envoie une commande *bip* TESS au terminal mobile.

23.4.1.3 Options de protocole Telnet

Telnet Protocol Options:

Terminal Type:	IBM-3278-2	
Host Port:	23	(Range 1..32767)
Maximum Sessions per Terminal:	4	(Range 1..127)
First Local Terminal Port:	10000	(Range 1..32767)
Local IP Address to Bind:	0.0.0.0	
First Terminal Listen Port:	0	(Range 0..32767)
Actively Negotiate with Host:	<input type="checkbox"/>	
Configure LU Names:	<input type="checkbox"/>	Configure
LU Name Prefix:		
Send IAC Interrupt Process as a System Request:	<input type="checkbox"/>	
Send IAC Break as an Attention Key:	<input type="checkbox"/>	
Auto-telnet:	DISABLE	
Auto-telnet Host:		
Auto-telnet without User Action:	<input checked="" type="checkbox"/>	

Terminal Type (Type de terminal)

Ce paramètre vous permet de sélectionner le type de terminal mobile que la 9160 G2 va émuler pour cet hôte. Actuellement, les choix de terminal mobile pour l'*émulation 3274* sont **IBM 3278-2** et **IBM 3278-2-E**.

Host Port (Port hôte)

Ce paramètre vous permet de saisir une valeur de port hôte pour la connexion hôte d'*émulation 3274* sélectionnée. La valeur par défaut est **23**.

Maximum Sessions per Terminal (Nombre maximal de sessions par terminal)

Ce paramètre contient le nombre maximum de sessions Telnet qui sont autorisées à partir de chaque terminal mobile. La plage va de **1** à **127**, avec une valeur par défaut de **4**.

First Local Terminal Port (Premier port local de terminal)

Ce paramètre contient le numéro de port local à partir duquel le premier terminal mobile se connecte aux sessions Telnet sortantes. La valeur par défaut est **10000**.

Local IP Address to Bind (Adresse IP locale à relier)

Ce paramètre contient l'adresse IP de l'adaptateur réseau de la 9160 G2 à partir de laquelle le premier terminal mobile se connecte aux sessions Telnet sortantes.

First Terminal Listen Port (Premier port local d'écoute)

Ce paramètre indique le numéro du premier port auquel la 9160 G2 écoute les demandes de connexion Telnet aux terminaux mobiles. Pour **activer** ce paramètre, la valeur doit être au minimum de **1024**. Pour **désactiver** le port d'écoute, la valeur doit être **0**.

La valeur par défaut est **0** (désactivé).

Actively Negotiate with Host (Négocier activement avec l'hôte)

Lorsque ce paramètre est activé, la 9160 G2 commence les négociations avec l'hôte pendant la configuration de la connexion Telnet. Non recommandé pour la plupart des hôtes.

Configure LU Names (Configurer les noms de LU)

Telnet Terminal Naming

To remove an LU Name, click the "Remove" button. Ensure that you have selected at least one terminal. See the Help panel for more information.

<input type="checkbox"/> Edit	Terminal Number	LU Name
<input type="checkbox"/> [Edit]	1	ABC
<input type="checkbox"/> [Edit]	5	THING

Selected Terminals:

Add a Terminal...

To associate an LU Name with a Terminal, fill in the fields below and click "Add Name".

Terminal Number:

LU Name:

Un nom de LU est requis pour chaque terminal mobile configuré. Cette page vous permet d'attribuer des noms de LU (voir également *LU Name Prefix* (Préfixe de nom de LU) ci-dessous). Le nom de LU doit être unique et associé au numéro du terminal mobile. Un nom de LU peut contenir un maximum de 10 caractères alphanumériques ; les caractères minuscules sont convertis en majuscules à la saisie.

LU Name Prefix (Préfixe de nom de LU)

Si aucun nom de LU n'est spécifié pour un terminal mobile, la 9160 G2 ajoutera le numéro de terminal (cinq chiffres, avec des zéros non significatifs si nécessaire) au préfixe de LU pour créer le nom de LU complet.

Send IAC Interrupt Process as a System Request (Envoyer un traitement d'interruptions IAC comme une demande système)

Si ce paramètre est activé, la 9160 G2 envoie la demande de traitement d'interruptions IAC à l'hôte comme une demande système 3274.

Send IAC Break as an Attention Key (Envoyer une pause IAC comme touche Attention)

Si ce paramètre est activé, la 9160 G2 envoie la demande de traitement de pause IAC à l'hôte comme une touche Attention 3274.

Auto-Telnet (Telnet automatique)

Ce paramètre vous permet de désactiver ou d'activer la connexion automatique de sessions Telnet des terminaux mobiles sur cet hôte.

Les options fournies sont les suivantes : **Disable** (Désactiver) et **Auto-telnet** (Telnet automatique). La valeur par défaut est **Disable** (Désactiver).

Lorsque *Auto-telnet* (Telnet automatique) est **désactivé**, les sessions Telnet entre les terminaux mobiles et l'hôte doivent être lancées manuellement depuis les terminaux mobiles.

Lorsque *Auto-telnet* (Telnet automatique) est **activé**, la 9160 G2 ouvre une session Telnet depuis chaque terminal mobile dont le numéro de terminal est configuré sur cet hôte.

D'autres sessions Telnet peuvent être lancées depuis chaque terminal mobile vers l'hôte, mais ceci doit être fait manuellement.

Lorsque *Auto-telnet* (Telnet automatique) est **activé**, la 9160 G2 connectera automatiquement Telnet à l'hôte, à la fois au démarrage et lors de la fermeture de la session.



Remarque : Les sessions Telnet automatiques sont uniquement lancées pour les terminaux mobiles qui sont « en ligne » (sous tension et fonctionnant correctement sur le réseau RF Psion Teklogix).

Auto-telnet Host (Hôte Telnet automatique)

Ce paramètre contient le nom d'hôte ou l'adresse IP de l'hôte auquel la 9160 G2 connecte les sessions Telnet automatiques.



Remarque : Un nom d'hôte placé dans cette zone de texte doit être « résolu » par la 9160 G2 : la 9160 G2 doit pouvoir obtenir une adresse IP pour elle. Par exemple, le nom d'hôte peut correspondre à une entrée dans le tableau des hôtes 9160 G2, ou la 9160 G2 peut rechercher un serveur de nom de domaine.

Tout nom d'hôte qui peut être utilisé à l'invite TCP> du terminal mobile peut être utilisé ici.

Auto-telnet Without User Action (Telnet automatique sans intervention de l'utilisateur)

Si cette option est activée, le contrôleur ouvre immédiatement une connexion à l'hôte pour chaque terminal mobile qui est initialisé, sans que l'utilisateur n'appuie sur la touche [ENTRÉE].

23.4.1.4 Configurations des touches de fonction

Function Key Mappings:

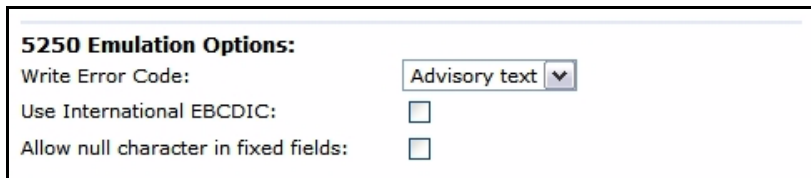
F1: <input type="text" value="F1"/>	F14: <input type="text" value="PA2"/>	F27: <input type="text" value="F13"/>
F2: <input type="text" value="F2"/>	F15: <input type="text" value="PA3"/>	F28: <input type="text" value="F14"/>
F3: <input type="text" value="F3"/>	F16: <input type="text" value="CLEAR"/>	F29: <input type="text" value="F15"/>
F4: <input type="text" value="F4"/>	F17: <input type="text" value="F17"/>	F30: <input type="text" value="SESS"/>
F5: <input type="text" value="F5"/>	F18: <input type="text" value="F18"/>	F31: <input type="text" value="F16"/>
F6: <input type="text" value="F6"/>	F19: <input type="text" value="F19"/>	F32: <input type="text" value="ENTER"/>
F7: <input type="text" value="F7"/>	F20: <input type="text" value="F20"/>	F33: <input type="text" value="ENTER"/>
F8: <input type="text" value="F8"/>	F21: <input type="text" value="F21"/>	F34: <input type="text" value="ENTER"/>
F9: <input type="text" value="F9"/>	F22: <input type="text" value="F22"/>	F35: <input type="text" value="ENTER"/>
F10: <input type="text" value="F10"/>	F23: <input type="text" value="F23"/>	F36: <input type="text" value="ENTER"/>
F11: <input type="text" value="F11"/>	F24: <input type="text" value="F24"/>	F37: <input type="text" value="ENTER"/>
F12: <input type="text" value="F12"/>	F25: <input type="text" value="SYSREQ"/>	F38: <input type="text" value="ENTER"/>
F13: <input type="text" value="PA1"/>	F26: <input type="text" value="ATTN"/>	F39: <input type="text" value="ENTER"/>

Function key n (Touche de fonction n)

Le paramètre *Function Key* (Touche de fonction) vous permet de sélectionner un code qui sera envoyé à l'hôte lorsque vous appuyez sur une touche de fonction sur le terminal mobile. Chaque touche de fonction peut être choisie dans la même gamme de codes possibles ; toutefois, chaque touche de fonction a un code différent par défaut. Les valeurs par défaut sont indiquées sur cette page.

23.4.2 Émulation 5250

23.4.2.1 Options d'émulation



5250 Emulation Options:

Write Error Code: Advisory text ▼

Use International EBCDIC: ☐

Allow null character in fixed fields: ☐

Avec une émulation IBM 5250 ou IBM 3274, le mini-contrôleur 9160 G2 convertit le flux de données depuis l'hôte en commandes TESS (Teklogix Screen Subsystem). Certains des paramètres dans cette page régissent la conversion des écrans de l'hôte pour TESS.

Write Error Code (Code erreur d'écriture)

Si *advisory text* (texte consultatif) est sélectionné ici, la 9160 G2 envoie des codes d'erreur à l'écran du terminal mobile sous forme de texte consultatif, inscrit au bas de l'écran. Si *screen text* (texte d'écran) est choisi, la 9160 G2 envoie les codes d'erreur sous forme de textes d'écran.

Use International EBCDIC (Utiliser EBCDIC International)

Si ce paramètre est **activé**, la 9160 G2 échange la position des caractères ! et] dans le tableau des caractères EBCDIC.

Allow null character in fixed fields (Autoriser le caractère nul dans les champs fixes) :

Si ce paramètre est **activé**, le mini-contrôleur 9160 G2 autorise les caractères nuls dans les espaces des champs qui ont des attributs vidéo visuels (tels que la vidéo inverse). La valeur par défaut pour l'émulation d'hôte 5250 est **activé**.

23.4.2.2 Options TESS

TESS Options:

Field Underline Remapping:	None	▼		
Alarm:	<input type="checkbox"/>			
Clear:	<input type="checkbox"/>			
Passthru:	<input type="checkbox"/>			
Procedures:	<input type="checkbox"/>			
Local:	<input type="checkbox"/>			
Host Print:	<input type="checkbox"/>			
Remote Print:	<input type="checkbox"/>			
Pages:	8	(Range 1..79)		
Transmit Line:	0	(Range 0..24)		
AIAG:	0	(Range 0..255)		
Visible Match Character:	0	(Range 0..255)		
Hidden Match character:	0	(Range 0..255)		
Serial I/O:	0	(Range 0..255)		
Print Line:	0	(Range 0..24)		
Print Form Length:	0	(Range 0..24)		
Barcode:	0	(Range 0..255)		
Entry Line:	0	(Range 0..24)		
Field Overhead:	5	(Range 0..80)		
Command Region:	0	, 0	, 0	, 0

Field Underline Remapping (Reconfiguration du soulignage de champ)

Vous avez la possibilité de modifier les attributs vidéo des caractères affichés afin de mettre en évidence les champs de saisie. Les options sont les suivantes : *None* (Aucun), *Blink* (Clignotement), *Bold* (Gras) et *Reverse* (Inverse).

Alarm (Alarme)

Lorsque ce paramètre est **activé**, les terminaux mobiles émettent un signal sonore lorsque le mot « ALARM » (ALARME) (en lettres majuscules) s'affiche sur l'écran de l'application à l'emplacement spécifié par le paramètre *Command Region* (Région de commande) (voir page 300). Le mot « ALARM » doit être un champ *affichage uniquement*.



*Remarque : Le paramètre Command Region (Région de commande) doit être **activé** si vous souhaitez que ce paramètre fonctionne.*

Clear (Effacer)

Si ce paramètre est **activé**, le mini-contrôleur 9160 G2 crée un champ de saisie *vide* pour un champ de saisie contenant des espaces.

Certaines applications hôtes dépendent des attributs vidéo des caractères affichés pour mettre en évidence des champs, en particulier les champs de saisie. Par exemple, l'écran d'application peut définir tous les champs de saisie avec la vidéo inverse et remplir le champ d'espaces. C'est efficace sur les terminaux mobiles qui prennent en charge la vidéo inverse, mais sur les terminaux mobiles où ce n'est pas le cas, il peut rendre le champ invisible puis qu'il est constitué uniquement d'espaces.

Par défaut, tous les champs de saisie vides affichés sur le terminal mobile Psion Teklogix sont mis en évidence par le « caractère de saisie » sélectionné dans la configuration du terminal mobile. La fonction *Clear* (Effacer) crée un champ de saisie vide à la place d'un champ de saisie rempli d'espaces.



Remarque : Cette opération est effectuée uniquement sur les écrans reçus de l'hôte. Les données envoyées à l'hôte ne sont pas affectées.

Passthru (Transfert)

Si ce paramètre est **activé**, la 9160 G2 permet à l'hôte d'envoyer les données directement au port série du terminal mobile RF. Il est le plus couramment utilisé pour l'impression.

Préparation des écrans de l'hôte au mode « Pass-through »

Le mot **PASSTHRU** (en lettres majuscules) doit apparaître sur la première ligne, à partir de la deuxième colonne, sur l'écran à envoyer via le port série du terminal mobile. Les données réelles à envoyer au terminal mobile peuvent commencer n'importe où en-dessous de la première ligne.

Avec les émulations 5250 ou 3274, des attributs occupent une position dans la mémoire tampon d'écran. Un attribut placé entre la colonne 2 et la fin du mot « PASSTHRU » décalera tous les caractères suivants d'une position vers la droite. Par conséquent, les attributs requis doivent occuper la colonne 1 de la première ligne (juste avant le mot « PASSTHRU »).

Exemple :

colonne : 1 2 3 4 5 6 7 8 9
Ligne 1 : @ P A S S T H R U @
Ligne 2 : @ P A R T : 1 2 3 4 5

où @ est un attribut.

Lorsque la 9160 G2 a fini de transmettre les données à l'imprimante du terminal mobile, elle envoie une touche « ENTRÉE » à l'hôte. L'hôte doit attendre la touche « ENTRÉE » avant d'envoyer d'autres écrans (y compris d'autres écrans « PASSTHRU ») à ce terminal mobile.



Remarque : Reportez-vous au manuel d'utilisation du terminal mobile approprié pour plus d'informations sur la configuration des paramètres sur le terminal mobile pour le mode « pass-through ».

Procédures (Procédures)

Si ce paramètre est **activé**, l'hôte peut envoyer des procédures TESS via la 9160 G2 aux terminaux mobiles. Une procédure TESS est un groupe de commandes TESS qui peuvent être exécutées par la commande TESS *execute procedure*.

Local (Local)

Si ce paramètre est **activé**, la 9160 G2 autorise l'hôte à fournir des pages à charger comme procédures TESS locales sur les terminaux mobiles.

Les procédures locales sont sélectionnées à partir d'un menu sur le terminal mobile. Les terminaux mobiles peuvent effectuer ces procédures lorsqu'ils sont hors ligne. Plus tard, lorsqu'ils sont en ligne, ils envoient les résultats de ces fonctions à l'hôte.



*Remarque : Le paramètre Procédures (Procédures) doit également être **activé** pour que Local (Local) fonctionne.*

Host Print (Impression hôte)

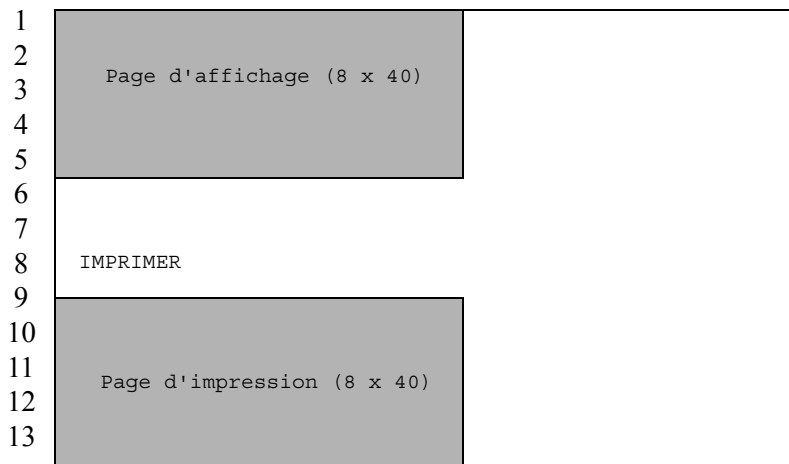
Lorsque ce paramètre est **activé**, l'hôte peut envoyer des données supplémentaires aux écrans du terminal mobile et demander au terminal mobile de les imprimer. Il s'agit de l'opposé de la fonctionnalité d'*impression locale* où le terminal mobile lance la demande d'impression.

Le texte qui est transmis à l'imprimante est formaté dans l'écran de l'application 24 x 80. Si l'hôte peut lancer l'opération d'impression, le texte est imprimé. La 9160 G2 identifie le texte supplémentaire comme une page d'impression par la présence du mot « PRINT » (IMPRIMER) (en lettres majuscules) commençant sur la 2e colonne de la ligne 13 sur l'écran 24 x 80. Le mot « PRINT » (IMPRIMER) doit être défini comme *texte affichage uniquement*.

La page d'impression est positionnée au-dessous de la page d'affichage du terminal mobile (voir la Figure 23.5 à la page 294). La taille de la page d'impression est toujours identique à celle de la page d'affichage du terminal mobile (en supposant que, dans la configuration de l'ordinateur mobile, la longueur de la page est inférieure à 12 lignes).

Dans le cas où *Host Print* (Impression hôte) est **activé**, la 9160 G2 transmet la page d'impression au terminal mobile après avoir reçu l'écran d'application de l'hôte.

Figure 23.5 Écran d'application avec page d'impression



Remarques :

1. Contrairement à l'option *Passthru* (Transfert), lors de l'utilisation de l'impression hôte, aucune séquence d'échappement ne peut être envoyée à l'imprimante.
2. La prise en charge de l'impression doit être activée sur le terminal mobile en commande d'impression dans le menu des fonctionnalités *TESS* ; reportez-vous au manuel d'utilisation du terminal mobile approprié pour plus d'informations.

Remote Print (Impression à distance)

Lorsque ce paramètre est **activé**, la 9160 G2 envoie la page d'impression à un terminal mobile lorsque celui-ci le demande (en utilisant la touche de fonction « F17 » du terminal mobile ou la touche « PRINT » sur les terminaux mobiles plus anciens). La 9160 G2 envoie la réponse de fonctionnalité à l'hôte.

Il s'agit de l'opposé de l'*impression hôte* où l'hôte lance la demande d'impression.



Remarque : La prise en charge de l'impression doit être activée au niveau du terminal mobile. Reportez-vous au manuel d'utilisation du terminal mobile approprié pour plus d'informations.

Pages (Pages)

Ce paramètre détermine le nombre d'écrans hôte (ou de pages) stockés au niveau du terminal mobile, avec un maximum de **79**.

La 9160 G2 réduit la quantité de données transmises aux terminaux mobiles en utilisant la capacité du terminal mobile à stocker une page de données pour chaque écran qu'il affiche. La 9160 G2 garde une image de chaque page stockée sur le terminal mobile. Après avoir reçu un écran d'application, la 9160 G2 tente d'associer l'écran à une page stockée.

Si une page similaire est déjà dans la mémoire du terminal mobile, la 9160 G2 indique au terminal mobile d'afficher à nouveau sa copie de la page ; seules les modifications nécessaires sont envoyées à partir du contrôleur. Si aucune correspondance n'est trouvée, la page complète est envoyée au terminal mobile par liaison radio.



*Remarque : Il y a un paramètre correspondant sur le terminal mobile, et le nombre **réel** de pages enregistrées sera la **plus petite** des deux valeurs.*

Transmit Line (Ligne de transmission)

Lorsque cette fonctionnalité est **activée**, toutes les données modifiées au niveau du terminal mobile sont transmises automatiquement lorsque l'opérateur saisit des données dans un champ de *transmission à la saisie*.

La valeur dans cette zone de texte indique la ligne sur l'écran qui est désignée comme *ligne de transmission*. Le dernier champ de saisie au-dessus ou sur la ligne de transmission de l'écran sera identifié comme le champ de *transmission à la saisie*. Si des champs de saisie existent sur des lignes au-dessous de la ligne de transmission, aucun champ de saisie ne sera désigné comme champ de *transmission à la saisie*.

Une valeur de **0** (zéro) désactive cette fonctionnalité. Une valeur de **24** désigne le *dernier* champ de saisie sur chaque écran d'application comme champ de *transmission à la saisie*.

AIAG (AIAG)

Ce paramètre fournit la localisation et le remplissage automatiques de l'entrée depuis des lecteurs de code-barres. Lorsque les données d'un code-barres sont entrées dans un terminal mobile, le terminal mobile recherche sur la page en cours des champs « AIAG » qui peuvent accepter les données du code-barres. Les données préchargées dans le champ « AIAG » par le programme d'application déterminent si les données du code-barres sont acceptées. Au niveau du mini-contrôleur 9160 G2, une valeur décimale de caractère ASCII entre **0** et **127** est définie pour correspondre à l'« identificateur de champ AIAG » défini au niveau de l'hôte. Une valeur de **0** (zéro) désactive cette fonctionnalité.

Le format des données préchargées est comme suit :

<mode> <préfixe AIAG (données)>

Le caractère de mode utilisé avec la commande permet des modes de fonctionnement différents pour répondre à diverses opérations d'application. L'opération de localisation et de remplissage automatiques s'applique uniquement aux données reçues d'un lecteur de code-barres. Les descriptions des modes et du préfixe AIAG sont indiquées dans le tableau ci-dessous. Ces modes sont définis au niveau de l'hôte.

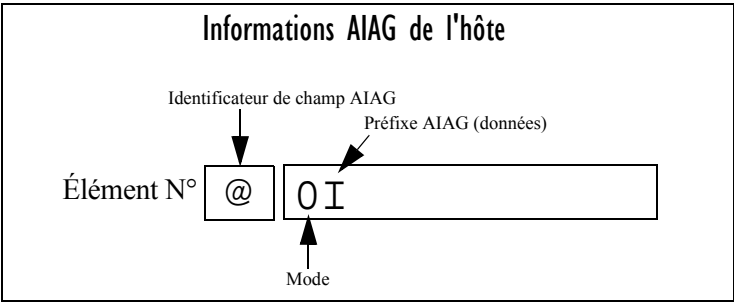
Tableau 23.3 Fonctions de mode et description du préfixe AIAG

Mode	Fonction
0	Affiche le préfixe, envoie le préfixe à l'hôte.
1	N'affiche pas le préfixe, envoie le préfixe à l'hôte.
2	Affiche le préfixe, n'envoie pas le préfixe à l'hôte.
3	N'affiche pas le préfixe, n'envoie pas le préfixe à l'hôte.
+4	Ajoutez 4 aux valeurs ci-dessus pour transmettre à l'hôte lorsque tous les champs AIAG avec 4 défini sont remplis. La fonction 0 est « activée » s'il y a des champs avec ce bit défini, et que tous les champs avec ce bit défini ont été remplis par l'opérateur.
+8	Ajoutez 8 aux valeurs ci-dessus pour autoriser le remplacement des données entrées précédemment.
+16	Ajoutez 16 aux valeurs ci-dessus pour indiquer la priorité de position du curseur pour la recherche et le remplissage.
Préfixe AIAG (données)	Le texte à faire correspondre dans le champ AIAG.

Exemple :

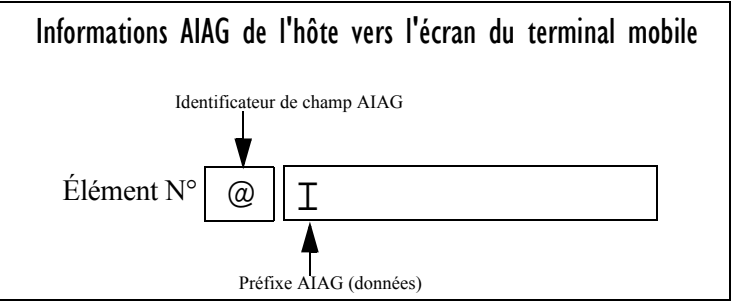
Les informations contenues dans l'exemple d'écran ci-dessous sont définies et envoyées à **partir de** l'hôte. Elles incluent l'« identificateur AIAG » (la balise identifiant s'il s'agit d'un champ AIAG), suivi du mode, dans ce cas Mode 0, puis, enfin, le « préfixe AIAG » - I.

Figure 23.6 Champ AIAG envoyé à partir de l'hôte



Lorsque les informations arrivent sur l'écran du terminal mobile, le champ AIAG approprié pour les informations numérisées est localisé via l'« identificateur AIAG ». Comme Mode 0 a été défini au niveau de l'hôte, le « préfixe AIAG » - I - s'affiche sur l'écran du terminal mobile, et lorsque cet écran est terminé, le préfixe est renvoyé à l'hôte.

Figure 23.7 Champ AIAG envoyé au terminal mobile



Caractère de correspondance visible

En insérant un caractère ASCII spécial directement avant un champ de saisie, le programme d'application fait la distinction entre un « champ de correspondance » et un champ de saisie. Supposons, par exemple, qu'un crochet en chevron « > » est défini comme champ de correspondance visible. Insérer « > » immédiatement avant le champ de saisie l'identifie comme un champ de correspondance, comme illustré ci-dessous.

N° de référence > _____

La plage possible pour ce paramètre, **0 à 255**, représente les valeurs décimales des caractères ASCII. Une valeur de **0** (zéro) désactive cette fonctionnalité. La valeur décimale ASCII entrée sur la 9160 G2 doit coïncider avec la valeur définie par le programme d'application.

Pour utiliser la fonction *Visible Match* (Correspondance visible), l'ordinateur hôte précharge les données dans un champ de saisie correspondant. Les données sont visibles sur l'écran du terminal mobile. Les données préchargées envoyées à un terminal mobile peuvent être constituées de caractères exacts, de caractères correspondants spéciaux ou d'une combinaison des deux. Reportez-vous au tableau ci-dessous pour voir les caractères de correspondance reconnus par les terminaux mobiles Psion Teklogix.

Si une entrée ne correspond pas aux données préchargées, elle s'affiche, le terminal mobile émet un signal sonore et le curseur se déplace vers la première position dans le champ de correspondance. L'opérateur peut soit effectuer une autre entrée dans le champ de correspondance ou déplacer le curseur vers un nouveau champ. Lorsqu'une entrée (même si elle ne correspond pas aux données préchargées) est réalisée dans un champ de correspondance, elle est envoyée à l'hôte avec les données modifiées du terminal mobile lors de la prochaine transmission.

Tableau 23.4 Caractères de correspondance

Caractère	Description
#	Faire correspondre un chiffre.
&	Faire correspondre une lettre (majuscule ou minuscule).
^	Faire correspondre une lettre majuscule.
_	Faire correspondre une lettre minuscule.
/	Faire correspondre un caractère alphanumérique.
"	Faire correspondre une lettre, un chiffre ou un espace.
?	Faire correspondre un signe de ponctuation.
'	Faire correspondre n'importe quel caractère.
:	Faire correspondre toutes les positions des caractères du champ avec le caractère précédent.
;	Faire correspondre les caractères restants, mais pas nécessairement le reste du champ, avec le caractère précédent.

Exemple :

Supposons que vous souhaitiez précharger un champ d'entrée avec un numéro de référence. Si ce numéro de référence est connu, vous pouvez l'utiliser pour précharger le champ. Si plus de flexibilité est nécessaire, et que le numéro de référence commence toujours par deux caractères alphabétiques, suivis d'un trait d'union et de quatre chiffres, la chaîne de correspondance pour le champ serait : **&&-####** .

Caractère de correspondance masqué

Contrairement aux données d'un champ de « correspondance visible », les données préchargées dans un champ de « correspondance masqué » ne sont *pas* affichées sur le terminal mobile.



Remarque : Reportez-vous à la section « Caractère de correspondance visible » à la page 297 pour plus d'informations sur la correspondance de champ.

La plage possible pour ce paramètre, **0 à 255**, représente les valeurs décimales des caractères ASCII. Une valeur de **0** (zéro) désactive cette fonctionnalité. La valeur décimale ASCII entrée sur la 9160 G2 doit coïncider avec la valeur définie par le programme d'application.

Serial I/O (E/S série)

Les champs d'*entrée/sortie série* sont des entrées spéciales et des champs fixes qui acceptent l'entrée et la sortie vers un port série. Le programme d'application différencie ce champ comme étant d'*entrée/sortie série* en précédant le champ par un caractère spécial.

Si ce caractère précède un champ fixe, les données sont envoyées au port série du terminal mobile. S'il précède un champ de saisie, le champ accepte les données du port série du terminal mobile.

La plage possible pour ce paramètre, **0 à 255**, représente les valeurs décimales des caractères ASCII. Une valeur de **0** (zéro) désactive cette fonctionnalité.

Print Line (Ligne d'impression)

Ce paramètre vous permet de saisir le numéro de ligne de début de la page d'impression sur l'écran de l'application (voir aussi *Entry Line* (Ligne d'entrée)). Une valeur maximale de **24** déclenche l'impression de la page d'affichage ; une valeur de **0** (zéro) désactive cette fonctionnalité.

Print Form Length (Longueur de formulaire d'impression)

Ce paramètre définit la longueur du formulaire de l'imprimante en lignes. La plage est comprise entre **0** et **24**.

Barcode (Code-barres)

Les champs d'*entrée de code-barres uniquement* sont des champs d'entrée spéciaux qui n'acceptent que les entrées d'un lecteur de code-barres. Le programme d'application différencie un champ de saisie comme étant d'*entrée de code-barres uniquement* en précédant le champ par un caractère spécial.

La plage possible pour ce paramètre, **0** à **255**, représente les valeurs décimales des caractères ASCII. Une valeur de **0** (zéro) désactive cette fonctionnalité.

Entry Line (Ligne d'entrée)

Ce paramètre contient le numéro de la première ligne affiché s'il n'y a aucun champ de saisie dans la partie supérieure gauche de l'écran, et si un champ de saisie est au niveau de cette ligne ou au-dessous de cette ligne.

Le paramètre *Entry Line* (Ligne d'entrée) permet un décalage automatique dans l'écran hôte, de sorte que la zone affichée par le terminal mobile inclut un champ de saisie qui ne serait pas normalement disponible. Certains terminaux mobiles Psion Teklogix affichent uniquement le coin supérieur gauche de l'écran de l'application à cause de leur petite taille d'écran.

Field Overhead (Charge de champ)

Ce paramètre contient le nombre maximum de caractères autorisés entre deux champs *fixes* qui permet encore à la 9160 G2 de les réunir dans un seul champ.

Il arrive parfois que la 9160 G2 connecte deux champs fixes et les envoie ensuite comme un seul champ. Cela vous permet de réduire la charge de la liaison radio.

Par exemple, si deux champs avaient 4 caractères séparément et que ce paramètre était « 5 », ces champs seraient réunis en un seul.

Command Region (Région de commande)

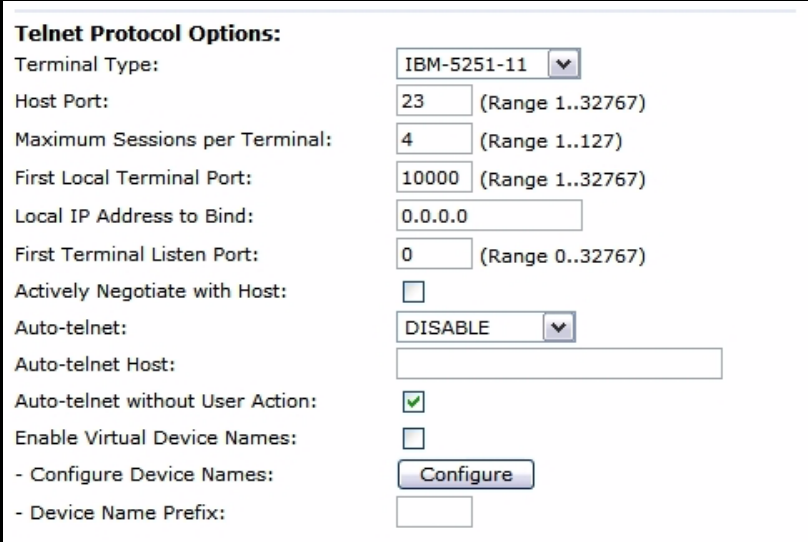
Ce paramètre définit une région de l'écran hôte que la 9160 G2 examinera pour détecter la présence de commandes réservées.

Les quatre numéros dans les zones de texte *Command Region* (Région de commande) représentent les adresses rangée et colonne du coin supérieur gauche et du coin inférieur droit de la région de commande. La première zone de texte de chaque paire contient le numéro de rangée ; la deuxième contient le numéro de colonne. La plage des valeurs de rangée va de **0** à **24** ; celle des valeurs de colonne va de **0** à **80**.

Par exemple, pour définir les deux dernières lignes de l'écran hôte comme région de commande, saisissez les valeurs 23, 1 et 24, 80.

Actuellement, la seule commande prise en charge est *ALARM* (ALARME) (reportez-vous à la page 291 pour des informations détaillées sur cette commande). Lorsque le mot « ALARM » (ALARME) est placé n'importe où dans la région de commande, la passerelle 9160 G2 envoie une commande *bip* TESS au terminal mobile.

23.4.2.3 Options de protocole Telnet



The screenshot shows a configuration window titled "Telnet Protocol Options:". It contains several settings for Telnet emulation:

- Terminal Type:** A dropdown menu set to "IBM-5251-11".
- Host Port:** A text box containing "23" with a range "(Range 1..32767)".
- Maximum Sessions per Terminal:** A text box containing "4" with a range "(Range 1..127)".
- First Local Terminal Port:** A text box containing "10000" with a range "(Range 1..32767)".
- Local IP Address to Bind:** A text box containing "0.0.0.0".
- First Terminal Listen Port:** A text box containing "0" with a range "(Range 0..32767)".
- Actively Negotiate with Host:** An unchecked checkbox.
- Auto-telnet:** A dropdown menu set to "DISABLE".
- Auto-telnet Host:** An empty text box.
- Auto-telnet without User Action:** A checked checkbox.
- Enable Virtual Device Names:** An unchecked checkbox.
- Configure Device Names:** A button labeled "Configure".
- Device Name Prefix:** An empty text box.

Terminal Type (Type de terminal)

Ce paramètre vous permet de sélectionner le type de terminal mobile que la 9160 G2 va émuler pour cet hôte. Actuellement, les choix de terminal mobile pour l'*émulation 5250* sont **IBM 5251-11**, **IBM 5555-B01** et **IBM 3179-2**.

Host Port (Port hôte)

Ce paramètre vous permet de saisir une valeur de port hôte pour la connexion hôte d'*émulation 5250* sélectionnée. La valeur par défaut est **23**.

Maximum Sessions per Terminal (Nombre maximal de sessions par terminal)

Ce paramètre contient le nombre maximum de sessions Telnet qui sont autorisées à partir de chaque terminal mobile. La plage va de **1** à **127**, avec une valeur par défaut de **4**.

First Local Terminal Port (Premier port local de terminal)

Ce paramètre contient le numéro de port local à partir duquel le premier terminal mobile se connecte aux sessions Telnet sortantes. La valeur par défaut est **10000**.

Local IP Address to Bind (Adresse IP locale à relier)

Ce paramètre contient l'adresse IP de l'adaptateur réseau depuis lequel le premier terminal mobile se connecte aux sessions telnet sortantes.

First Terminal Listen Port (Premier port local d'écoute)

Ce paramètre indique le numéro du premier port auquel la 9160 G2 écoute les demandes de connexion Telnet aux terminaux mobiles. Pour **activer** ce paramètre, la valeur doit être au minimum de **1024**. Pour **désactiver** le port d'écoute, la valeur doit être **0**.

La valeur par défaut est **0** (désactivé).

Actively Negotiate with Host (Négocier activement avec l'hôte)

Lorsque ce paramètre est activé, la 9160 G2 commence les négociations avec l'hôte pendant la configuration de la connexion Telnet. Non recommandé pour la plupart des hôtes.

Auto-Telnet (Telnet automatique)

Ce paramètre vous permet de désactiver ou d'activer la connexion automatique de sessions Telnet des terminaux mobiles sur cet hôte.

Les options fournies sont les suivantes : **Disable** (Désactiver) et **Auto-telnet** (Telnet automatique). La valeur par défaut est **Disable** (Désactiver).

Lorsque *Auto-telnet* (Telnet automatique) est **désactivé**, les sessions Telnet entre les terminaux mobiles et l'hôte doivent être lancées manuellement depuis les terminaux mobiles.

Lorsque *Auto-telnet* (Telnet automatique) est **activé**, la 9160 G2 ouvre une session Telnet depuis chaque terminal mobile dont le numéro de terminal est configuré sur cet hôte.

D'autres sessions Telnet peuvent être lancées depuis chaque terminal mobile vers l'hôte, mais ceci doit être fait manuellement.

Lorsque *Auto-telnet* (Telnet automatique) est **activé**, la 9160 G2 connectera automatiquement Telnet à l'hôte, à la fois au démarrage et lors de la fermeture de la session.



Remarque : Les sessions Telnet automatiques sont uniquement lancées pour les terminaux mobiles qui sont « en ligne » (sous tension et fonctionnant correctement sur le réseau RF Psion Teklogix).

Auto-telnet Host (Hôte Telnet automatique)

Ce paramètre contient le nom d'hôte ou l'adresse IP de l'hôte auquel la 9160 G2 connecte les sessions Telnet automatiques.



Remarque : Un nom d'hôte placé dans cette zone de texte doit être « résolu » par la 9160 G2 : la 9160 G2 doit pouvoir obtenir une adresse IP pour elle. Par exemple, le nom d'hôte peut correspondre à une entrée dans le tableau des hôtes 9160 G2, ou la 9160 G2 peut rechercher un serveur de nom de domaine. Tout nom d'hôte qui peut être utilisé à l'invite TCP> du terminal mobile peut être utilisé ici.

Auto-telnet Without User Action (Telnet automatique sans intervention de l'utilisateur)

Si cette option est activée, le contrôleur ouvre immédiatement une connexion à l'hôte pour chaque terminal mobile qui est initialisé, sans que l'utilisateur n'appuie sur la touche [ENTRÉE].

Enable Virtual Device Names (Activer les noms de terminal virtuel)

Si ce paramètre est activé, la 9160 G2 négocie avec l'hôte pour obtenir un nom de terminal virtuel pour la connexion Telnet.

Configure Device Names (Configurer les noms de terminal)

Telnet Terminal Naming

To remove an LU Name, click the "Remove" button. Ensure that you have selected at least one terminal. See the Help panel for more information.

<input type="checkbox"/> Edit	Terminal Number	LU Name
<input type="checkbox"/> [Edit]	1	ABC
<input type="checkbox"/> [Edit]	5	THING

Selected Terminals:

Add a Terminal...

To associate an LU Name with a Terminal, fill in the fields below and click "Add Name".

Terminal Number:

LU Name:

Un nom de LU est requis pour chaque terminal mobile configuré. Cette page vous permet d'attribuer des noms de LU (voir également *Device Name Prefix* (Préfixe de nom de terminal) ci-dessous). Le nom de LU doit être unique et associé au numéro du terminal mobile. Un nom de LU peut contenir un maximum de 10 caractères alphanumériques ; les caractères minuscules sont convertis en majuscules à la saisie.

Device Name Prefix (Préfixe de nom de terminal)

Si aucun nom de LU n'est spécifié pour un terminal mobile, la 9160 G2 ajoutera le numéro de terminal (cinq chiffres, avec des zéros non significatifs si nécessaire) au préfixe de LU pour créer le nom de LU complet.

23.4.2.4 Configurations des touches de fonction

Function Key Mappings:

F1:	F1	F14:	F14	F27:	F17
F2:	F2	F15:	F15	F28:	F18
F3:	F3	F16:	CLEAR	F29:	UP
F4:	F4	F17:	PRINT	F30:	SESS
F5:	F5	F18:	HELP	F31:	ENTER
F6:	F6	F19:	F19	F32:	ENTER
F7:	F7	F20:	F20	F33:	ENTER
F8:	F8	F21:	F21	F34:	ENTER
F9:	F9	F22:	F22	F35:	ENTER
F10:	F10	F23:	F23	F36:	ENTER
F11:	F11	F24:	F24	F37:	ENTER
F12:	F12	F25:	DOWN	F38:	SELECTOR
F13:	F13	F26:	F16	F39:	ENTER

Function key n (Touche de fonction n)

Le paramètre *Function Key* (Touche de fonction) vous permet de sélectionner un code qui sera envoyé à l'hôte lorsque vous appuyez sur une touche de fonction sur le terminal mobile. Chaque touche de fonction peut être choisie dans la même gamme de codes possibles ; toutefois, chaque touche de fonction a un code différent par défaut. Les valeurs par défaut sont indiquées sur cette page.

23.4.3 Émulation ANSI

23.4.3.1 Options d'émulation

ANSI Emulation Options:

Maximum Screen Size:	<input type="text" value="24"/>	rows	<input type="text" value="80"/>	columns
Host Timeout:	<input type="text" value="15"/>	(Range 0..255)		
Escape Timeout:	<input type="text" value="12"/>	(Range 0..255)		
Threshold:	<input type="text" value="200"/>	(Range 0..999)		
Echo:	<input checked="" type="checkbox"/>			
Function Key Remapping:	<input type="checkbox"/>			
Arrow Key Remapping:	<input type="checkbox"/>			
Page Saving:	<input checked="" type="checkbox"/>			
Page Saving consider Double Byte Characters:	<input type="checkbox"/>			
RLE:	<input type="checkbox"/>			
Convert 7 to 8 bits:	<input type="checkbox"/>			
Lower Character Set (GL):	<input type="text" value="ASCII"/>	<input type="button" value="v"/>		
Upper Character Set (GR):	<input type="text" value="ASCII"/>	<input type="button" value="v"/>		
Terminal Initialization Data:	<input type="text"/>			
Host Initialization Data:	<input type="text"/>			

Maximum Screen Size (Taille maximale de l'écran)

La *taille maximale de l'écran* vous permet de définir la taille d'écran maximale requise pour les terminaux mobiles, en rangées et en colonnes. Cette fonction garantit l'utilisation optimale de la mémoire lors de l'utilisation de l'option d'enregistrement de la page (reportez-vous à la section « Page Saving (Enregistrement de page) » à la page 308).

La plage va d'une définition minimum de **24 x 80** à une définition maximale de **60 x 132**. Le paramètre par défaut est **24 x 80**.

Host Timeout (Délai d'attente hôte)

Le *délai d'attente hôte* est l'intervalle (en *tics*, ou 60e de seconde) entre les requêtes de données reçues de l'hôte. La plage va de **0** à **255**, avec une valeur par défaut de **15**.

Lorsque ce délai s'est écoulé, si la 9160 G2 ne reçoit pas les caractères de l'hôte, elle suppose que l'hôte a fini de transmettre les données et attend la saisie utilisateur (en d'autres termes, elle suppose qu'un écran de données est complété).



Important : Le paramètre d'enregistrement de page (page 308) doit être activé pour modifier la valeur du délai d'attente hôte.

Escape Timeout (Délai d'échappement)

Le *délai d'échappement* est la durée (en *tics*, ou 60e de seconde) pendant laquelle la 9160 G2 garde un « ESC » reçu de l'hôte et considère que le prochain octet reçu fait partie d'une séquence d'échappement. La plage va de **0** à **255**, avec une valeur par défaut de **12**.

Lorsque ce délai s'est écoulé, l'hôte doit envoyer un autre caractère « ESC » pour démarrer une séquence d'échappement.



Remarque : C'est particulièrement important lorsqu'un ESC est à la fin d'un paquet de données.

Threshold (Seuil)

Le *seuil* est le nombre minimal d'octets de données de mise à jour pour l'écran du terminal mobile qui doivent être reçus de l'hôte avant que la 9160 G2 ne stocke l'écran comme une nouvelle « page enregistrée ». La plage va de **0** à **999**, avec une valeur par défaut de **200**.



Important : Le paramètre d'enregistrement de page (page 308) doit être activé pour modifier la valeur du seuil.

Echo (Écho)

Si ce paramètre est **activé**, la 9160 G2 utilise l'*écho « intelligent »*. Ce mode réduit la quantité de données envoyées au terminal mobile en diminuant le nombre de transmissions radio.

En général, lorsqu'une application de mode caractère est utilisée, chaque touche est envoyée à l'hôte en une seule transmission et le caractère est repris par l'hôte dans une nouvelle transmission. Lorsque l'*écho « intelligent »* est **activé**, la 9160 G2 n'envoie pas l'écho de l'hôte aux terminaux mobiles s'il correspond aux données envoyées depuis le terminal mobile. Ainsi, le nombre de transmissions radio est réduit.

Ce mode réduit également ou élimine le délai entre la saisie d'un caractère sur le clavier et l'affichage du caractère écho par l'hôte. Le nombre maximum de caractères en attente d'écho est **25**. Les caractères supplémentaires seront envoyés à l'hôte mais ne seront pas affichés.



Remarques :

1. Ce paramètre détermine aussi si une requête de paramètre ANSI est envoyée au terminal mobile.
2. L'écho « intelligent » doit également être activé sur le terminal mobile (reportez-vous au manuel d'utilisation du terminal mobile approprié).

Function Key Remapping (Reconfiguration des touches de fonction)

Si ce paramètre est **activé**, la 9160 G2 reconfigure les touches de fonction pour cette connexion hôte comme défini sur la page Function Key Remapping (Reconfiguration des touches de fonction) (page 316).

Arrow Key Remapping (Reconfiguration de flèche)

Si ce paramètre est **activé**, la 9160 G2 reconfigure les flèches pour cette connexion hôte comme défini sur la page Function Key Remapping (Reconfiguration des touches de fonction) (page 316).

Page Saving (Enregistrement de page)

Si ce paramètre est **activé**, la 9160 G2 utilise l'enregistrement de page, réduisant les données transmises au terminaux mobiles.

La 9160 G2 garde une image de chaque page stockée sur le terminal mobile. Après avoir reçu un écran d'application, la 9160 G2 tente d'associer l'écran à une page stockée. Si la page est déjà sur le terminal mobile, la 9160 G2 lui indique d'afficher à nouveau sa copie stockée de la page ; aucune donnée ne doit être envoyée par liaison radio pour cette page. Si la 9160 G2 ne trouve aucune correspondance pour la page, la page complète est envoyée au terminal mobile. Le réglage par défaut est **activé**.



Remarques : Lorsque l'enregistrement de page est activé, le nombre de pages enregistrées est celui qui est défini sur le terminal mobile. Reportez-vous au manuel d'utilisation du terminal mobile approprié pour plus d'informations.

Dans le cas d'utilisation d'ensembles de caractères à double octet, tels que le chinois ou le coréen, reportez-vous au paramètre Page Saving Consider Double Byte Character (Enregistrement de page tenant compte des caractères à double octet) ci-dessous.

Page Saving Consider Double Byte Character (Enregistrement de page tenant compte des caractères à double octet)

Lors de l'utilisation d'ensembles de caractères à double octet tels que le chinois ou le coréen, l'enregistrement de page (voir ci-dessus) écrase partiellement un caractère à double octet, ce qui risque de créer un seul octet de données d'écran non imprimable ou un nouveau caractère imprévu constitué de deux moitiés de caractères différents. Le terminal mobile peut également décaler les données sur l'écran pour tronquer les données incorrectes.

Lorsque *Page Saving Consider Double Byte Character* (Enregistrement de page tenant compte des caractères à double octet) est **activé**, l'enregistrement de page remplace chaque moitié de caractère à double octet orphelin par un espace pour éviter l'affichage de caractères modifiés et de données tronquées sur le terminal mobile. Le réglage par défaut est **désactivé**.



Remarque : Cette option ne devrait être utilisée que lors de l'utilisation d'ensembles de caractères à double octet.

RLE (RLE)

Si ce paramètre est **activé**, la 9160 G2 utilise le codage Run-Length Encoding (RLE) sur les données qu'elle envoie par liaison radio. *RLE* compresse les caractères répétés allant de l'hôte vers le terminal mobile. Si des caractères répétés sont trouvés dans le flux de données, le premier est envoyé, suivi par une courte séquence d'échappement (3 ou 4 caractères) qui indique au terminal mobile le nombre de fois que vous souhaitez répéter ce caractère. De cette manière, RLE compresse les données et diminue la quantité totale de trafic sur la liaison radio.

Convert 7 to 8 Bits (Convertir 7 bits en 8 bits)

Si ce paramètre est **activé**, la 9160 G2 convertit les séquences de commande 7 bits en équivalent 8 bits dans les flux de données ANSI vers les terminaux mobiles. Ceci remplace les séquences d'échappement à deux caractères par un seul caractère équivalent, compressant les données.

Lower Character Set (GL) (Ensemble de caractères minuscules)

Cette option doit être définie sur le même ensemble de caractères que celui sélectionné sur les terminaux mobiles. Ce paramètre est uniquement utilisé lorsque l'enregistrement de page est activé.

Upper Character Set (GR) (Ensemble de caractères majuscules)

Cette option doit être définie sur le même ensemble de caractères que celui sélectionné sur les terminaux mobiles. Ce paramètre est uniquement utilisé lorsque l'enregistrement de page est activé.

Terminal Initialization Data / Host Initialization Data (Données d'initialisation terminal / Données d'initialisation hôte)

Ces champs sont utilisés pour saisir des données qui seront envoyées depuis le contrôleur au terminal mobile ou depuis le contrôleur vers l'hôte chaque fois qu'un terminal mobile est réinitialisé. Par exemple, ils peuvent être utilisés pour demander une actualisation de l'hôte, ou pour réinitialiser les ensembles de caractères qui ont été définis sur le terminal mobile par l'hôte lors de la connexion.

Les données non imprimables peuvent être saisies sous forme hexadécimale (\xnn) ou octale (\nnn). Par exemple, le caractère d'échappement peut être saisi comme \x1b ou \033.

Ces paramètres peuvent aller jusqu'à 256 caractères. Si les champs sont vides, aucune donnée n'est envoyée.

23.4.3.2 Options de protocole Telnet

Telnet Protocol Options:

Terminal Type:

VT100

Host Port:

23

(Range 1..32767)

Maximum Sessions per Terminal:

4

(Range 1..127)

Close Host sessions on Terminal reset:

☐

First Local Terminal Port:

10000

(Range 1..32767)

Local IP Address to Bind:

0.0.0.0

First Terminal Listen Port:

0

(Range 0..32767)

TCP Session Request Key:

1

(Range 0..255)

Session Cycle Key:

2

(Range 0..255)

Last Active Session Key:

5

(Range 0..255)

Terminal Type (Type de terminal)

Ce paramètre indique le type de terminal mobile que la 9160 G2 va émuler. Les caractères saisis dans la zone de texte peuvent être toute chaîne ASCII acceptable pour l'hôte, avec un **maximum de 32** caractères. La valeur par défaut est **VT100**.

Host Port (Port hôte)

Ce paramètre indique la valeur du port de l'hôte pour la connexion hôte ANSI sélectionnée. La valeur par défaut est **23**.

Maximum Sessions per Terminal (Nombre maximal de sessions par terminal)

Ce paramètre contient le nombre maximum de sessions Telnet qui sont autorisées à partir de chaque terminal mobile. La plage va de **1** à **127**, avec une valeur par défaut de **4**.

Close Host Sessions on Terminal Reset (Fermer les sessions hôtes au redémarrage du terminal)

Lorsque ce paramètre est **activé**, et qu'un message de redémarrage de terminal est reçu, la session hôte pour ce numéro de terminal sera fermée. Le réglage par défaut est **désactivé**.

First Local Terminal Port (Premier port local de terminal)

Ce paramètre indique le numéro de port à partir duquel la 9160 G2 tente une connexion Telnet pour le premier terminal mobile. La valeur par défaut est **10000**. Les sessions Telnet supplémentaires sont affectées à des numéros de port plus élevés.

Local IP Address to Bind (Adresse IP locale à relier)

Ce paramètre indique l'adresse IP de l'interface 9160 G2 qui se connecte sur cet hôte. Il est utilisé avec les numéros de port local pour créer une prise unique pour chaque session de terminal.

First Terminal Listen Port (Premier port local d'écoute)

Ce paramètre indique le numéro du premier port auquel la 9160 G2 écoute les demandes de connexion Telnet aux terminaux mobiles. Pour **activer** ce paramètre, la valeur doit être au minimum de **1024**. Pour **désactiver** le port d'écoute, la valeur doit être **0**.

La valeur par défaut est **0** (désactivé).

TCP Session Request Key (Clé de demande de session TCP)

Ce paramètre contient le code de caractère décimal ASCII du caractère qui invite le terminal mobile à demander une nouvelle session de terminal ANSI. La plage va de **0** à **255**, avec une valeur par défaut de **1**.

Session Cycle Key (Clé de cycle de session)

Ce paramètre contient le code de caractère décimal ASCII du caractère qui invite le terminal mobile à afficher la prochaine session de terminal ANSI. La plage va de **0** à **255**, avec une valeur par défaut de **2**.

Last Active Session Key (Clé de dernière session active)

Ce paramètre contient le code de caractère décimal ASCII du caractère qui invite le terminal mobile à afficher la dernière session de terminal ANSI. La plage va de **0** à **255**, avec une valeur par défaut de **5**.

23.4.3.3 Auto-Telnet/Auto-login (Telnet automatique/Connexion automatique)

Auto-Telnet / Auto-Login:

Auto-telnet/login Enable:

DISABLE

Auto-telnet Host:

Auto-telnet Terminal Prompt:

Press ENTER to login.

Auto-login User ID:

Auto-login Password:

Auto-login User ID prompt:

gin:

Auto-login Password prompt:

word:

Auto-login failed login:

incorrect

Auto-telnet without User Action:

☐

Auto-telnet without User Action Timing Delay:

25 (Range 0..255)

Maximum of Auto-telnet Retries:

0 (Range 0..255)

Allow TCP Sessions:

☒

Auto-telnet/login Enable (Telnet automatique/Activation de session)

Ce paramètre vous permet de désactiver ou d'activer la connexion automatique de sessions Telnet des terminaux mobiles sur cet hôte. Vous avez le choix entre les options suivantes : **DISABLE (DÉSACTIVER)** ; **AUTO-TELNET (TELNET AUTOMATIQUE)** ; **AUTO-TELNET/LOGIN (TELNET AUTOMATIQUE/CONNEXION)**. La valeur par défaut est **DISABLE (DÉSACTIVER)**.

Lorsque *Auto-telnet* (Telnet automatique) est **désactivé**, les sessions Telnet entre les terminaux mobiles et l'hôte doivent être lancées manuellement depuis les terminaux mobiles.

Lorsque *Auto-telnet* (Telnet automatique) est **activé**, la 9160 G2 ouvre une session Telnet depuis chaque terminal mobile dont le numéro de terminal est configuré sur cet hôte. D'autres sessions Telnet peuvent être lancées depuis chaque terminal mobile vers l'hôte, mais ceci doit être fait manuellement.



Remarque : Les sessions Telnet automatiques sont uniquement lancées pour les terminaux mobiles qui sont « en ligne » (sous tension et fonctionnant correctement sur le réseau RF Psion Teklogix).

Lorsque *Auto-telnet* (Telnet automatique) et *Auto-Login* (Connexion automatique) sont **activés**, la 9160 G2 ouvre une session Telnet depuis chaque terminal mobile dont le numéro de terminal est configuré sur cet hôte. Elle connecte ensuite chaque session à l'hôte via l'ID utilisateur et le mot de passe fournis dans cette page.



Remarque : L'ID utilisateur et le mot de passe sont identiques pour toutes les sessions Auto-Telnet (Telnet automatique) automatiquement connectées à cet hôte.

Auto-telnet Host (Hôte Telnet automatique)

Ce paramètre contient le nom d'hôte ou l'adresse IP de l'hôte auquel la 9160 G2 connecte les sessions Telnet automatiques.



Remarque : Un nom d'hôte placé dans cette zone de texte doit être « résolu » par la 9160 G2 : la 9160 G2 doit pouvoir obtenir une adresse IP pour elle. Par exemple, le nom d'hôte peut correspondre à une entrée dans le tableau des hôtes 9160 G2, ou la 9160 G2 peut rechercher un serveur de nom de domaine.

Tout nom d'hôte qui peut être utilisé à l'invite TCP> du terminal mobile peut être utilisé ici.

Auto-telnet Terminal Prompt (Invite terminal Telnet automatique)

Ce paramètre contient le texte présenté à l'utilisateur pour demander une connexion. Les caractères peuvent être une chaîne ASCII ou une séquence d'échappement numérique présentée en chiffres octaux ou hexadécimaux.

Une séquence d'échappement octale prend l'une des formes suivantes : \0d, \Odd ou \0ddd, chaque d pouvant être un chiffre entre 0 et 7. Si ddd est plus grand que 256 décimal, la valeur de code du caractère représenté sera le reste du ddd/256 décimal.

Une séquence d'échappement hexadécimale prend l'une des formes suivante : \xh ou xhh, chaque h pouvant être n'importe quel chiffre entre 0 et 9, ou n'importe quelle valeur alpha entre a et f ou A et F.



Remarque : \0 est considéré comme un caractère, avec une valeur de code 0.

La valeur autorisée est un **maximum de 60** caractères sur la ligne. La valeur par défaut est aucun texte, il vous suffit d'appuyer sur <ENTRÉE> pour vous connecter.

Auto-login User ID (ID utilisateur de connexion automatique)

Ce paramètre contient l'ID utilisateur présenté par la 9160 G2 à l'hôte pour les sessions de connexion automatique. Les caractères peuvent être toute chaîne ASCII acceptable pour l'hôte, avec un **maximum de 32** caractères.

Auto-login Password (Mot de passe de connexion automatique)

Ce paramètre contient le mot de passe présenté par la 9160 G2 à l'hôte pour les sessions de connexion automatique. Les caractères peuvent être toute chaîne ASCII acceptable pour l'hôte, avec un **maximum de 32** caractères.

Auto-login User ID Prompt (Invite ID utilisateur de connexion automatique)

La passerelle 9160 G2 compare le texte dans cette zone au texte que lui présente l'hôte. Lorsqu'ils correspondent, la 9160 G2 suppose que l'hôte vient d'envoyer sa demande de nom d'utilisateur, puis elle envoie l'ID utilisateur spécifié dans le paramètre *Auto-Login User ID* (ID utilisateur de connexion automatique) à l'hôte. Les caractères peuvent être toute chaîne ASCII, avec un **maximum de 32** caractères. Le texte par défaut est **gin**:



Remarque : La chaîne de correspondance doit être aussi courte que possible, tout en étant suffisamment longue pour identifier de manière unique l'invite d'ID utilisateur. N'incluez pas de mots séparés par des espaces, car certains hôtes envoient des caractères autres que des caractères d'espace pour présenter un espace à l'écran.

Auto-login Password Prompt (Invite mot de passe de connexion automatique)

La passerelle 9160 G2 compare le texte dans cette zone au texte que lui présente l'hôte. Lorsqu'ils correspondent, la 9160 G2 suppose que l'hôte vient d'envoyer sa demande de mot de passe, puis elle envoie le mot de passe spécifié dans le paramètre *Auto-Login Password* (Mot de passe de connexion automatique) à l'hôte. Les caractères peuvent être toute chaîne ASCII, avec un **maximum de 32** caractères. Le texte par défaut est **word**:



Remarque : La chaîne de correspondance doit être aussi courte que possible, tout en étant suffisamment longue pour identifier de manière unique l'invite de mot de passe. N'incluez pas de mots séparés par des espaces, car certains hôtes envoient des caractères autres que des caractères d'espace pour présenter un espace à l'écran.

Auto-login Failed Login (Échec de la connexion automatique)

La passerelle 9160 G2 compare le texte dans cette zone au texte que lui présente l'hôte. Lorsqu'ils correspondent, la 9160 G2 suppose que l'hôte vient d'envoyer une chaîne informant le terminal mobile de l'échec d'une tentative de connexion. La 9160 G2 présente ensuite la *Auto-telnet Terminal Prompt* (Invite de terminal Telnet automatique) sur l'écran du terminal mobile pour demander à l'utilisateur de se connecter manuellement. Les caractères peuvent être toute chaîne ASCII, avec un **maximum de 32** caractères. Le texte par défaut est **incorrect**.



Remarque : La chaîne de correspondance doit être aussi courte que possible, tout en étant suffisamment longue pour identifier de manière unique l'invite d'échec de connexion. N'incluez pas de mots séparés par des espaces, car certains hôtes envoient des caractères autres que des caractères d'espace pour présenter un espace à l'écran.

Auto-telnet Without User Action (Telnet automatique sans intervention de l'utilisateur)

Si cette option est activée, le contrôleur ouvre immédiatement une connexion à l'hôte pour chaque terminal mobile qui est initialisé, sans que l'utilisateur n'appuie sur la touche [ENTRÉE]. Il est recommandé que si ce paramètre est sélectionné, la *Auto Telnet Terminal Prompt* (Invite de terminal Telnet automatique) est modifiée de sorte que l'utilisateur soit conseillé de patienter pendant que la connexion est établie.

Auto-telnet Without User Action Timing Delay (Telnet automatique sans délai d'action de l'utilisateur)

Lorsque cette option est activée, l'option *Auto-telnet Without User Action Timing Delay* (Telnet automatique sans délai d'action de l'utilisateur) peut être retardée d'un temps spécifié en millisecondes entre tentatives de connexion.

Maximum Of Auto-telnet Retries (Nombre maximal de connexions Telnet automatiques)

Le nombre de tentatives de connexion doit être effectué automatiquement avant d'abandonner.

Allow TCP Sessions (Autoriser les sessions TCP)

Lorsque ce paramètre est **activé**, la 9160 G2 permet à un utilisateur de terminal mobile de changer d'invite ou de session à l'invite (connexion automatique ou TCP). Si *Allow TCP Sessions* (Autoriser les sessions TCP) est **désactivé**, toutes les nouvelles sessions s'ouvrent comme des sessions de connexion automatique.

Faire une demande de session (normalement <CTRL> a sur le terminal mobile) peut être utilisé au niveau de l'invite pour modifier le type d'invite (si l'autre type d'invite est disponible).

Changer de session au niveau de l'invite est également possible (sur le terminal mobile : <CTRL> b [session suivante], ou <CTRL> e [dernière session]). Lors du changement de session à l'invite, l'état du terminal mobile (non connecté) sera correctement ajusté pour correspondre à celui de l'autre session.

Le réglage par défaut est **activé**.

23.4.3.4 Configurations des touches de fonction

Function Key Mappings:					
F1:	1b,4f,50,00,00,00,00,00	F11:	1b,5b,32,33,7e,00,00,00	F21:	1b,5b,31,7e,00,00,00,00
F2:	1b,4f,51,00,00,00,00,00	F12:	1b,5b,32,34,7e,00,00,00	F22:	1b,5b,32,7e,00,00,00,00
F3:	1b,4f,52,00,00,00,00,00	F13:	1b,5b,32,35,7e,00,00,00	F23:	1b,5b,33,7e,00,00,00,00
F4:	1b,4f,53,00,00,00,00,00	F14:	1b,5b,32,36,7e,00,00,00	F24:	1b,5b,34,7e,00,00,00,00
F5:	1b,5b,31,36,7e,00,00,00	F15:	1b,5b,32,38,7e,00,00,00	F25:	1b,5b,35,7e,00,00,00,00
F6:	1b,5b,31,37,7e,00,00,00	F16:	1b,5b,32,39,7e,00,00,00	F26:	1b,5b,36,7e,00,00,00,00
F7:	1b,5b,31,38,7e,00,00,00	F17:	1b,5b,33,31,7e,00,00,00	F27:	1b,5b,34,31,7e,00,00,00
F8:	1b,5b,31,39,7e,00,00,00	F18:	1b,5b,33,32,7e,00,00,00	F28:	1b,5b,34,32,7e,00,00,00
F9:	1b,5b,32,30,7e,00,00,00	F19:	1b,5b,33,33,7e,00,00,00	F29:	1b,5b,34,33,7e,00,00,00
F10:	1b,5b,32,31,7e,00,00,00	F20:	1b,5b,33,34,7e,00,00,00	F30:	1b,5b,34,34,7e,00,00,00
Up:	1b,5b,41,00,00,00,00,00	Down:	1b,5b,42,00,00,00,00,00	Right:	1b,5b,43,00,00,00,00,00
Left:	1b,5b,44,00,00,00,00,00				

Function key n (Touche de fonction n)

Le paramètre *Function Key* (Touche de fonction) vous permet de sélectionner un code qui sera envoyé à l'hôte lorsque vous appuyez sur une touche de fonction sur le terminal mobile. Chaque touche de fonction peut être choisie dans la même gamme de codes possibles ; toutefois, chaque touche de fonction a un code différent par défaut. Les valeurs par défaut sont indiquées sur l'écran ci-dessus.

24.1 Fonctionnalités 802.IQ	319
24.1.1 Fonctionnalités communes 802.IQ v1/v2.	319
24.1.2 Fonctionnalités 802.IQ v1	322
24.1.3 Menu des fonctionnalités 802.IQ v2	323
24.2 Mise à jour des paramètres 802.IQ	323

24.1 Fonctionnalités 802.IQ

802.IQ est un protocole 802.11 amélioré propriétaire Psion Teklogix qui permet aux terminaux mobiles de fonctionner dans un LAN sans fil sur un réseau qui prend simultanément en charge les protocoles TCP/IP et 802.IQ. Le protocole 802.IQ est disponible en deux versions : 802.IQ v1 et 802.IQ v2. La passerelle sans fil 9160 G2 Wireless Gateway peut prendre en charge les deux versions du protocole simultanément (les terminaux mobiles ne doivent en utiliser qu'un).

Le protocole 802.IQ v1 est un plan de routage LAN sans fil qui offre de meilleures performances dans un réseau sans fil 802.11 qu'il n'est possible avec un routage TCP/IP. Un terminal mobile peut communiquer avec le point d'accès 9160 G2 via protocole TCP/IP ou 802.IQ v1, ce qui rend un système à double opérabilité possible. Pour plus d'informations et les menus de configuration pour 802.IQv1, reportez-vous à la page 322.

Le protocole 802.IQ v2 est une version améliorée du protocole 802.IQ v1 qui transporte des paquets sur la couche UDP. Il fournit toutes les fonctionnalités 802.IQ v1, avec les fonctions supplémentaires de capacité de mise à niveau de logiciels sur RF, la possibilité d'ajouter des points d'accès tiers entre les contrôleurs et les terminaux mobiles et l'intégration au système mapRF si vous le souhaitez. Pour plus d'informations sur la manière de configurer un mini-contrôleur 802.IQ v2, reportez-vous à la page 323.

24.1.1 Fonctionnalités communes 802.IQ v1/v2



Important : *802.IQ doit uniquement être activée sur des 9160 G2 filaires.*

Ne configurez pas 802.QI sur des réseaux de pontage filaires 9160 G2 ; des balises 802.IQ seraient envoyées via la liaison WDS d'un réseau à l'autre (reportez-vous au Chapitre 20 : « Système de distribution sans fil (WDS) »).

Auto-Startup (Démarrage automatique)

Ce paramètre **active** 802.IQ immédiatement lorsque la 9160 G2 redémarre. Lorsque le 9160 G2 fonctionne comme station de base sous un contrôleur réseau ou un mini-contrôleur 9160 G2, ce paramètre doit être **désactivé**.

La valeur par défaut est **désactivé**.



Important : *Si Auto Startup (Démarrage automatique) est mal défini, les terminaux mobiles pourraient ne pas fonctionner correctement.*

Beacon Period (Période de balise)

Une balise 802.IQ est une diffusion envoyée à tous les terminaux mobiles compatibles 802.IQ. La balise permet aux terminaux mobiles de déterminer quand ils se sont déplacés entre les stations de base. Elle permet à un terminal mobile de déterminer si la station de base ou le contrôleur a été réinitialisé ou non et, si c'est le cas, comment récupérer les données. Si le contrôleur a été réinitialisé, le terminal mobile ferme toutes les sessions et est entièrement réinitialisé. Si la station de base a été réinitialisée, ou si le terminal mobile s'est déplacé vers une autre 9160 G2, une réinitialisation à chaud est effectuée (aucune donnée ne sera perdue).

Les valeurs autorisées du paramètre *Beacon Period* (Période de balise) vont de **1** à **20** secondes. La valeur par défaut est **2**.

Terminal Offline Timeout (Délai terminal hors ligne)

Ce paramètre définit la durée (en minutes) avant que la tâche 802.IQ de la 9160 G2 envoie un message hors ligne au maître cellulaire pour déclarer le terminal mobile hors ligne.

Les valeurs autorisées vont de **1** à **240**. La valeur par défaut est **5**.

Figure 24.1 Présentation des paramètres de configuration 802.IQ

Basic Settings	Modify 802.IQ settings
User Management	
Cluster	802.IQ v1/v2 Common Features:
Access Points	Auto-Startup: <input type="checkbox"/>
Sessions	Beacon Period: <input type="text" value="2"/> (Range 1..20)
Channel Management	Terminal Offline Timeout: <input type="text" value="5"/> (Range 1..240)
Wireless Neighborhood	
Security	802.IQ v1 Features:
Status	Enabled: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Interfaces	Initial RTT: <input type="text" value="1000"/> (Range 10..10000)
Events	Protocol Type ID: <input type="text" value="2457"/> (Range 1501..65535)
Transmit/Receive	Forward 802.IQ packets only: <input type="checkbox"/>
Client Associations	802.IQ v1 Beacon Interfaces:
Neighboring Access Points	Wired: <input type="checkbox"/>
	WLAN0: <input type="checkbox"/>
	WLAN1: <input type="checkbox"/>
	WDS0: <input type="checkbox"/>
	WDS1: <input type="checkbox"/>
	WDS2: <input type="checkbox"/>
	WDS3: <input type="checkbox"/>
Manage	
Ethernet Settings	802.IQ v2 Features:
802.11 Settings	Enabled: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
802.11 Advanced Settings	Beacon UDP port: <input type="text" value="8888"/> (Range 5001..65535)
VWN	<input type="button" value="Update"/>
WDS	
Guest Login	
MAC Filtering	
Load Balancing	
Services	
QoS	
Time	
SNMP	
Narrow Band	
Radio	
Connectivity Options	
Connectivity	
Base Station	
RRM Groups	
Radio Link Features	
Hosts	
802.IQ	

24.1.2 Fonctionnalités 802.IQ v1

Les menus *802.IQ v1 Features* (Fonctionnalités 802.IQ v1) sont accessibles depuis l'onglet *802.IQ* des options *Connectivity* (Connectivité) (reportez-vous à la Figure 24.1 à la page 321).

Enabled (Activé)

Ce paramètre active ou désactive la fonctionnalité 802.IQ v1. La valeur par défaut est **désactivé**.

Initial RTT (RTT initial)

Le paramètre *Initial RTT* (RTT initial) est utilisé pour vous aider à déterminer le temps écoulé, en millisecondes, entre une transmission de *point d'accès* et une *confirmation de terminal*. Le point d'accès adapte en permanence le temps de réponse acceptable, en calculant le temps écoulé moyen sur un nombre de transmissions pour chaque terminal mobile. Si une confirmation prend plus de temps que le temps de réponse moyen calculé, le point d'accès renvoie la transmission.

Comme les points d'accès ne peuvent pas calculer un temps de réponse *moyen* sans un certain nombre de transmissions, un point de départ ou « Initial Round Trip Time » (Temps de réponse initial) est nécessaire. Le point d'accès utilise le temps attribué au paramètre « Initial RTT » (RTT initial) comme valeur de départ des calculs de durée. Une fois que le point d'accès commence à émettre et recevoir des données depuis le terminal mobile et inversement, cette valeur est ajustée pour refléter le temps de réponse moyen entre les transmissions et les confirmations.

Les valeurs autorisées vont de **10** à **10000**. La valeur par défaut est **1000**.

Protocol Type ID (ID de type de protocole)

Ce paramètre identifie le type de protocole 802.IQ, afin d'éviter les conflits avec d'autres types de paquets générés par Ethernet qui utilisent le même type de protocole.

Les valeurs autorisées vont de **1536** à **65535**. La valeur par défaut est **2457**.



Important : La valeur par défaut de l'ID de type de protocole est rarement changée. Si le type de protocole est modifié, tous les terminaux mobiles doivent être modifiés en fonction.

Forward 802.IQ Packets Only (Transférer des paquets 802.IQ uniquement)

Lors du pontage de paquets entre les systèmes filaires et sans fil, ce paramètre permet à la 9160 G2 de filtrer automatiquement et de d'annuler tous les paquets non 802.IQ v1. Le paramètre par défaut est **désactivé**.

802.IQ v1 Beacon Interfaces (Interfaces de balise 802.IQ v1)

Choisissez l'interface sur laquelle les balises sont envoyées.

Les interfaces disponibles sont les suivantes : *Wired (filaire)*, *WLAN0*, *WLAN1*, *WDS0*, *WDS1*, *WDS2*, *WDS3*.

24.1.3 Menu des fonctionnalités 802.IQ v2

Les menus *802.IQ v2 Features* (Fonctionnalités 802.IQ v2) sont accessibles depuis l'onglet *802.IQ* des options *Connectivity* (Connectivité) (reportez-vous à la Figure 24.1 à la page 321).

Enabled (Activé)

Ce paramètre active ou désactive le protocole 802.IQv2.

La valeur par défaut est **désactivé**.

Beacon UDP Port (Port UDP de balise)

Ce paramètre identifie le port UDP pour les diffusions de balise. Si plus d'un contrôleur 802.IQ v2 est présent sur le réseau, le paramètre doit être modifié pour séparer les systèmes. Le paramètre doit également correspondre au paramètre correspondant sur le terminal mobile. La plage de valeurs va de **5001** à **65535**. La valeur par défaut est **8888**.

24.2 Mise à jour des paramètres 802.IQ

Pour mettre à jour les paramètres 802.IQ :

1. Accédez à la page *802.IQ Settings* (Paramètres 802.IQ).
2. Configurez les paramètres selon les besoins.
3. Cliquez sur le bouton **Update** (Mettre à jour) pour appliquer les modifications.

SERVEUR NETWORK TIME PROTOCOL (NTP) 25

25.1 Accès aux paramètres horaires	327
25.2 Activation ou désactivation d'un serveur NTP (Network Time Protocol)	328
25.3 Mise à jour des paramètres	329

Network Time Protocol (NTP) est un protocole Internet standard qui synchronise les horloges des ordinateurs sur votre réseau. Les serveurs NTP transmettent le *Temps universel coordonné (UTC)*, également appelé *Temps moyen de Greenwich* à leurs systèmes client. NTP envoie régulièrement des requêtes d'heure aux serveurs, utilisant l'horodatage renvoyé pour son horloge, y compris les ajustements au fuseau horaire. L'horodatage sera utilisé pour indiquer la date et l'heure de chaque événement dans les messages de journal. Reportez-vous à <http://www.ntp.org> pour plus d'informations générales sur NTP. Les sections suivantes décrivent la manière de configurer la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway pour utiliser un serveur NTP spécifié.

25.1 Accès aux paramètres horaires

Pour activer un serveur *NTP*, accédez à l'onglet *Services > Time* (Services > Heure) et mettez à jour les champs comme indiqué ci-dessous.

Figure 25.1 Paramètres horaires

Basic Settings	Modify how the access point discovers the time
User Management	Local Time: Mon Jun 18 18:41:53 UTC 2007
Cluster	Network Time Protocol (NTP): <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Access Points	NTP Server: <input type="text" value="pool.ntp.org"/>
Sessions	Time Zone: <input type="text" value="Custom"/> <input type="text" value="UTC"/> <input type="text" value="+0000"/>
Channel Management	<input type="button" value="Update"/>
Wireless Neighborhood	
Security	
Status	
Interfaces	
Events	
Transmit/Receive	
Client Associations	
Neighboring Access Points	
Manage	
Ethernet Settings	
802.11 Settings	
802.11 Advanced Settings	
VWN	
WDS	
Guest Login	
MAC Filtering	
Load Balancing	
Services	
QoS	
Time	

25.2 Activation ou désactivation d'un serveur NTP (Network Time Protocol)

Pour configurer votre point d'accès afin d'utiliser un serveur Network Time Protocol (**NTP**), vous devez d'abord **activer** l'utilisation de NTP, puis sélectionner le serveur NTP que vous souhaitez utiliser. (Pour annuler le service NTP sur le réseau, désactivez NTP sur le point d'accès.)

Tableau 25.1 Paramètres NTP

Champ	Description
<i>Local Time (Heure locale)</i>	L'heure locale actuelle s'affiche à chaque mise à jour.
<i>Network Time Protocol (NTP)</i>	<p>NTP fournit au point d'accès un moyen d'obtenir et de contrôler son heure à partir d'un serveur sur le réseau. L'utilisation d'un serveur NTP donne à votre point d'accès la capacité de fournir l'heure correcte de la journée dans les messages de journal et les informations de session.</p> <p>Pour plus d'informations sur NTP, reportez-vous à http://www.ntp.org.</p> <p>Choisissez d'activer ou de désactiver l'utilisation d'un serveur NTP (Network Time Protocol) :</p> <ul style="list-style-type: none">• Pour activer le serveur NTP, cliquez sur Enabled (Activé).• Pour désactiver le serveur NTP, cliquez sur Disabled (Désactivé).
<i>NTP Server (Serveur NTP)</i>	<p>Si NTP est activé, sélectionnez le serveur NTP que vous souhaitez utiliser.</p> <p>Vous pouvez spécifier le serveur NTP par nom d'hôte ou adresse IP, bien que l'utilisation de l'adresse IP ne soit pas recommandée car ces dernières peuvent changer plus facilement.</p>
<i>Time Zone (Fuseau horaire)</i>	<p>Une liste des fuseaux horaires (par exemple, « EST (-05:00) ») est présentée dans la liste déroulante, ainsi que le choix de définir votre propre valeur personnalisée. Si <i>Custom</i> (Personnalisé) est sélectionné, deux zones de texte apparaissent en regard de la zone de sélection, où vous pouvez entrer votre choix d'abréviation et de décalage horaire par rapport à l'heure UTC. Le décalage horaire personnalisé par rapport à l'heure UTC est donnée en heures et minutes à l'est d'UTC. Par exemple, -0800 correspond à huit heures à l'ouest d'UTC (c'est-à-dire Heure standard du Pacifique), tandis que +0930 correspond à neuf heures, trente minutes à l'est (c'est-à-dire Heure standard d'Australie centrale).</p> <p>Le réglage du passage à l'heure d'été n'est pas disponible.</p>

25.3 Mise à jour des paramètres

Pour mettre à jour les paramètres horaires :

1. Accédez à l'onglet *Time* (Heure).
2. Configurez les paramètres horaires selon les besoins.
3. Cliquez sur le bouton **Update** (Mettre à jour) pour appliquer les modifications.

26.1 Accès aux paramètres de configuration du point d'accès	333
26.2 Réinitialisation de la configuration d'usine par défaut	334
26.3 Enregistrement de la configuration en cours dans un fichier de sauvegarde	334
26.4 Restauration de la configuration à partir d'un fichier enregistré précédemment . .	335
26.5 Redémarrage du point d'accès.	335
26.6 Mise à niveau du firmware	336
26.6.1 Mise à jour	337
26.6.2 Vérification de la mise à niveau du firmware.	337

Vous pouvez enregistrer une copie des paramètres actuels sur la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway dans un fichier de configuration de sauvegarde. Le fichier de sauvegarde peut être utilisé à une date ultérieure pour restaurer le point d'accès à la configuration précédemment enregistrée.

26.1 Accès aux paramètres de configuration du point d'accès

Pour gérer la configuration d'un point d'accès, accédez à l'onglet *Maintenance* > *Configuration* et utilisez l'interface comme décrit ci-dessous.

Figure 26.1 Présentation de la configuration du point d'accès

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Narrow Band

Radio

Connectivity Options

Connectivity

Base Station

RRM Groups

Radio Link Features

Hosts

802.1Q

Maintenance

Configuration

Manage this Access Point's Configuration

To Restore Factory Default Configuration ...

Click "Reset" to load the factory defaults in place of the current configuration for this AP.

[Reset](#)

To Save the Current Configuration to a Backup File ...

Click the link below to download a file containing the current configuration for this AP.

☐ Encrypt the configuration file

[download configuration](#)

To Restore the Configuration from a Previously Saved File ...

Enter the path and file name of the configuration backup file you want to use, or click "Browse" to open a dialog where you can locate and select the file. Then click "Restore" to load this file in place of the current configuration.

[Browse...](#)

[Restore](#)

To Reboot the Access Point ...

Click the "Reboot" button.

[Reboot](#)

26.2 Réinitialisation de la configuration d'usine par défaut

Si vous rencontrez des problèmes avec la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway et si vous avez essayé toutes les autres mesures de dépannage, utilisez la fonctionnalité *Reset Configuration* (Réinitialiser la configuration). Ceci restaurera les paramètres d'usine par défaut et effacera tous les paramètres, y compris un nouveau mot de passe ou des paramètres sans fil.

1. Cliquez sur l'onglet **Maintenance > Configuration**.
2. Cliquez sur le bouton **Reset** (Réinitialiser).

Les paramètres d'usine par défaut sont restaurés.



Remarque : Gardez à l'esprit que si vous ne réinitialisez pas la configuration depuis cette page, vous le faites uniquement pour ce point d'accès, pas pour d'autres points d'accès du cluster.

Pour plus d'informations sur les paramètres d'usine par défaut, reportez-vous à la section « Paramètres par défaut de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway » à la page 27.

26.3 Enregistrement de la configuration en cours dans un fichier de sauvegarde

Pour enregistrer une copie des paramètres actuels d'un point d'accès dans un fichier de configuration (format .cbk) :

1. Cliquez sur le lien **download configuration** (télécharger la configuration).
Une boîte de dialogue *File Download or Open* (Télécharger ou ouvrir le fichier) s'affiche.
2. Choisissez l'option *Save* (Enregistrer) dans cette première boîte de dialogue.
Un navigateur de fichiers s'affiche.
3. Utilisez le navigateur de fichiers pour accéder au répertoire dans lequel vous souhaitez enregistrer le fichier et cliquez sur **OK** pour enregistrer le fichier.

Vous pouvez conserver le nom de fichier par défaut (config.cbk) ou renommer le fichier de sauvegarde, mais assurez-vous d'enregistrer le fichier avec une extension .cbk.

26.4 Restauration de la configuration à partir d'un fichier enregistré précédemment

Pour restaurer la configuration sur un point d'accès aux paramètres précédemment enregistrés :

1. Sélectionnez le fichier de configuration de sauvegarde que vous souhaitez utiliser, en tapant le chemin d'accès complet et le nom du fichier dans le champ *Restore* (Restaurer) ou en cliquant sur **Browse** (Parcourir) et en sélectionnant le fichier.

(Seuls les fichiers qui ont été créés avec la fonctionnalité de sauvegarde .cbk peuvent être utilisés avec la fonction de restauration ; par exemple, config.cbk.)



Important : *Il est uniquement possible de restaurer le fichier de configuration sur une 9160 du même modèle que celle dont le fichier de configuration a été obtenu.*

Par exemple, une 9160 G2 modèle « 9160 Wireless Gateway » ne restaure pas un fichier de configuration enregistré à partir d'une 9160 G2 modèle « 9160 Wireless Gateway (Dual Radio) ».

2. Cliquez sur le bouton **Restore** (Restaurer).

Le point d'accès va redémarrer.



Remarque : *Lorsque vous cliquez sur **Restore** (Restaurer), le point d'accès redémarre. Une boîte de dialogue de confirmation « reboot » (redémarrer) et un message d'état « rebooting » (redémarrage en cours) s'affichent. Veuillez patienter pendant que le processus de redémarrage se termine (une ou deux minutes). Au bout d'un moment, essayez d'accéder aux pages Web d'administration comme indiqué dans l'étape suivante ; elles ne seront pas accessibles jusqu'à ce que le point d'accès ait redémarré.*

Lorsque le point d'accès a redémarré, accédez au pages Web d'administration en cliquant à nouveau sur l'un des onglets (si l'interface utilisateur est toujours affichée) ou en saisissant l'adresse IP du point d'accès dans votre navigateur. À présent, vous devriez voir les paramètres de configuration restaurés aux paramètres d'origine que vous avez récupérés dans le fichier de sauvegarde.

26.5 Redémarrage du point d'accès

À des fins de maintenance ou dans le cadre d'un dépannage, vous pouvez redémarrer la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway comme suit.

1. Cliquez sur l'onglet *Maintenance > Configuration*.
2. Cliquez sur le bouton **Restore** (Restaurer).

Le point d'accès va redémarrer.

26.6 Mise à niveau du firmware

Dès que de nouvelles versions du firmware de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway sont disponibles, vous pouvez mettre à niveau le firmware sur vos appareils pour bénéficier de nouvelles fonctionnalités et améliorations.



Important : *Ne procédez pas à une mise à niveau du firmware à partir d'un client sans fil qui est associé au point d'accès pour lequel vous effectuez la mise à niveau. Ceci entraînerait l'échec de la mise à niveau. En outre, tous les clients sans fil seront dissociés et aucune nouvelle association ne sera autorisée.*

Si vous êtes confronté à ce scénario, la solution consiste à utiliser un client filaire pour accéder au point d'accès :

- *Créez une connexion Ethernet filaire d'un PC au point d'accès.*
- *Affichez l'interface utilisateur d'administration.*

Répétez le processus de mise à niveau avec le client filaire.



Remarque : *Vous devez effectuer cette opération sur chaque point d'accès ; vous ne pouvez pas mettre à niveau le firmware automatiquement sur le cluster.*

Gardez à l'esprit que le succès de la mise à niveau du firmware restaure le point d'accès à la configuration d'usine par défaut. (Reportez-vous à la section « Paramètres par défaut de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway » à la page 27.)

Pour mettre à niveau le firmware sur un point d'accès particulier :

1. Accédez à *Maintenance > Upgrade* (Maintenance > Mise à niveau) dans les pages Web d'administration de ce point d'accès.

Upgrade firmware

Model

9160 Wireless Gateway NB (Dual Radio)

Platform

PTX9160G2

Firmware Version

E187k

New Firmware Image

Browse...

Please note:

Uploading the new firmware may take up to 20 seconds. Please do not refresh the page or navigate to another page while uploading the new firmware, or the firmware upload will be aborted. When the upload is complete, a page will be displayed indicating whether the new firmware was uploaded successfully. If successful, the upgrade will proceed automatically.

Upgrade

Les informations sur la version actuelle du firmware s'affichent et une option de mise à niveau d'une nouvelle image de firmware est proposée.

2. Si vous connaissez le chemin vers le nouveau fichier d'image de firmware, saisissez-la dans la zone de texte *New Firmware Image* (Nouvelle image de firmware). Sinon, cliquez sur le bouton **Browse** (Parcourir) et localisez le fichier image de firmware.



Remarque : Le fichier de mise à niveau du firmware fourni doit être au format : <NomdeFichier>.upgrade.tar

N'essayez pas d'utiliser des fichiers <NomdeFichier>.bin ou des fichiers d'autres formats pour la mise à niveau. Ils ne fonctionneront pas.

26.6.1 Mise à jour

1. Cliquez sur **Update** (Mettre à jour) pour appliquer la nouvelle image de firmware.
En cliquant sur Update (Mettre à jour) pour la mise à niveau du firmware, une fenêtre contextuelle de confirmation s'affiche, décrivant le processus de mise à niveau.
2. Cliquez sur **OK** pour confirmer la mise à niveau, et démarrez le processus.



Important : Le processus de mise à niveau du firmware commence une fois que vous cliquez sur Update (Mettre à jour), puis sur OK dans la fenêtre contextuelle de confirmation.

Le processus de mise à niveau peut prendre plusieurs minutes durant lesquelles le point d'accès ne sera pas disponible. N'éteignez pas le point d'accès pendant la mise à niveau. Une fois la mise à niveau terminée, le point d'accès peut redémarrer et reprendre un fonctionnement normal en utilisant les paramètres de configuration d'usine par défaut.

26.6.2 Vérification de la mise à niveau du firmware

Pour vérifier que la mise à niveau du firmware est terminée, vérifiez la version du firmware indiquée dans l'onglet *Upgrade* (Mise à niveau) (et également dans l'onglet *Basic Settings* (Paramètres de base)). Si la mise à niveau a réussi, le nom ou le numéro de la version mise à jour sera indiqué.

27.1 Description physique	341
27.2 Exigences en termes d'environnement	341
27.3 Exigences en termes d'alimentation CA	341
27.4 Exigences en termes d'alimentation Power Over Ethernet	342
27.5 Processeur et mémoire	342
27.6 Interfaces réseau.	342
27.7 Radios	342



Remarque : Les spécifications de performances sont nominales et susceptibles d'être modifiées sans préavis.

27.1 Description physique

Boîtier :	Couleur noir de jais, matériau mixte FR2000
Dimensions :	$\leq 30 \times 20 \times 12,5$ cm (11,8 x 7,9 x 4,9 po.)
Poids :	$\leq 2,25$ kg (5,0 lb) (sans les radios, antennes et options)

27.2 Exigences en termes d'environnement

Température de fonctionnement :	0 à 45 °C (32 à 113 °F)
Humidité relative de fonctionnement :	de 10 à 90 %
Température de stockage :	de 0 à 70 °C (32 à 158 °F)
Poussière et pluie :	IP42 ou supérieur
Vibrations :	EH0002 (vibrations d'expédition uniquement)
Fiabilité :	MTBF 25 000 heures (MIL-HDBK-217F)

27.3 Exigences en termes d'alimentation CA

Entrée universelle CA via un connecteur IEC320 standard. Désactive Power Over Ethernet (découverte 802.3af) lors de la connexion.

Tension d'entrée :	100 - 240 V CA nominal
Courant :	5,0 A maximum



Avertissement : *Un fil de mise à la terre, ne dépassant pas 3 m de longueur, doit être connecté entre la vis de mise à la terre (située sur le support à dégagement rapide) et un point de liaison de mise à la terre adapté sur toute 9160 G2 connectée à une antenne installée à l'extérieur.*

27.4 Exigences en termes d'alimentation Power Over Ethernet

Conforme à la norme IEEE 802.3af (désactivé lorsque l'alimentation secteur est connectée).

Tension d'entrée : 37 à 57 V CC.

Modules d'alimentation

intégrés : 2,5 W (en supposant $\eta = 0,8$ à l'intégralité de 12,5 watts depuis Ethernet)

Radios doubles 802.11b : 4 W

Carte logique principale : 6 W

27.5 Processeur et mémoire

Processeur Intel IXP420 à 266 MHz

8 Mo de ROM Flash

32 Mo de SDRAM

27.6 Interfaces réseau

Ethernet intégré : carte 10BaseT/100BaseT (10/100 Mbit/s) avec négociation automatique, semi-duplex et duplex intégral.
Le débit de données est automatiquement détecté.

27.7 Radios

Radio mini-carte PCI 802.11A/G sans antenne intégrée

Radio mini-carte PCI 802.11G sans antenne intégrée

Puissance de l'émetteur 100 mW pour les pays FCC ; 50 mW pour ETSI

Plage de fréquences de 2,4 à 2,5 GHz (802.11b/g) ; de 5,15 à 5,825 GHz (802.11a)

Débit de données 802.11b : 1, 2, 5,5, 11 Mo/s
802.11a/g : 6, 9, 12, 18, 24, 36, 48, 54 Mo/s

Nbre de canaux FCC : 11 (802.11b/g) et 12 (802.11a)
ETSI : 13 (802.11b/g) et 19 (802.11a)
Chine : 13 (802.11b/g) et 4 (802.11a)



Remarque : Les canaux 802.11a ne se chevauchent pas. Il existe des canaux sans chevauchement dans la bande de fréquence de 2,4 GHz.

RA1001A - Radio à bande étroite

Modulation à bande étroite propriétaire Psion Teklogix (FSK niveau 2/4)

Format de carte PC type III

Puissance d'émission 1 W ou 0,5 W

Plage de fréquences 403-422 MHz, 419-435 MHz, 435-451 MHz,
450-470 MHz, 464-480 MHz,
480-496 MHz, 496-512 MHz

Sensibilité Rx < -110 dBm à 19,2 kbit/s (FSK niveau 4)

Débits de données 4 800 bit/s, 9 600 bit/s, 19,2 kbit/s

ANNEXE A

BROCHAGES DE PORT ET DIAGRAMMES DES CÂBLES

A.1 Port de console

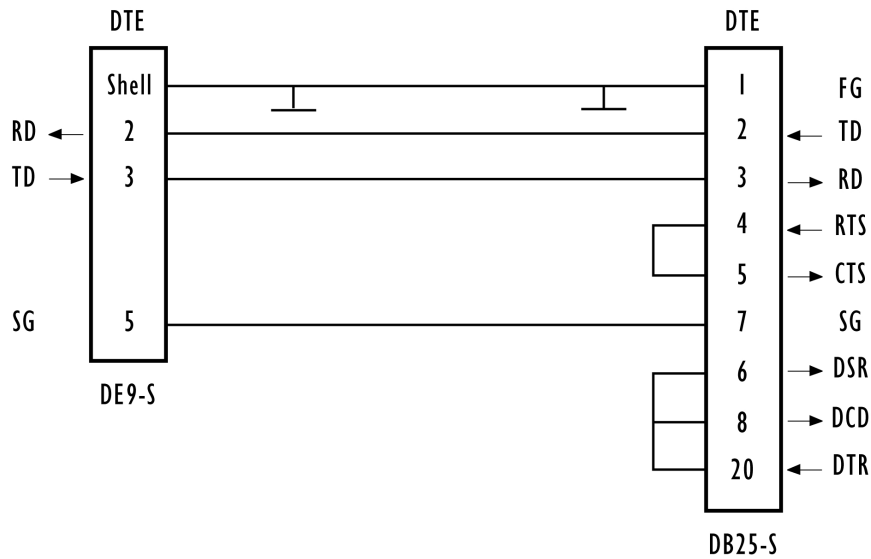
N° de broche	Nom	Fonction	Direction
3	TD	Transmit Data (Données de transmission)	Sortie
2	RD	Receive Data (Données de réception)	Entrée
5	SG	Signal Ground (Masse signal)	–
4*	DTR	Data Terminal Ready (Terminal de données prêt)	Sortie
7*	RTS	Request to Send (Demande d'envoi)	Sortie

* Toujours relevé

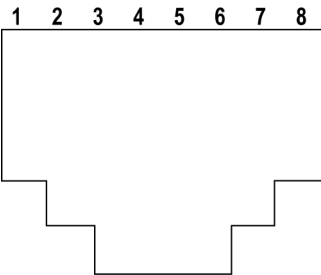
A.2 Descriptions des câbles série

N° de câble	Fonction	Connexion	Longueur standard
19387	9160 G2 à console	Directe	1,83 m (6 pieds)

Câble de port de console 19387



A.3 Brochages des connecteurs RJ-45 (Ethernet 10BaseT/100BaseT)



9160 G2 sur courant CA		9160 G2 sur Power over Ethernet*	
1	TD+	1	TD+
2	TD-	2	TD-
3	RD+	3	RD+
4	Non utilisé	4	
5	Non utilisé	5	
6	RD-	6	RD-
7	Non utilisé	7	
8	Non utilisé	8	
		* La 9160 G2 peut également accepter une alimentation de polarisation 48 VCC sur les paires de ligne de données (1,2) et (3,6) des systèmes fournissant Power over Ethernet.	



Remarque : Généralement, une connexion directe est nécessaire pour brancher une paire torsadée (10Base-T ou 100BaseT) au concentrateur.

ANNEXE B

PARAMÈTRES DE SÉCURITÉ SUR CLIENTS SANS FIL/SERVEUR RADIUS

B.1 Infrastructure réseau ; choix entre un serveur d'authentification intégré ou externe. . . .	8
B.1.1 Utilisation du serveur d'authentification intégré (EAP-PEAP)	8
B.1.2 Utilisation d'un serveur RADIUS externe avec des certificats EAP-TLS ou EAP-PEAP	8
B.2 Assurez-vous que le logiciel client sans fil est à jour.	9
B.3 Accès aux paramètres de sécurité client sans fil Microsoft Windows	9
B.4 Configuration d'un client pour accéder à un réseau non sécurisé (aucune sécurité) . . .	11
B.5 Configuration de la sécurité WEP statique sur un client.	12
B.6 Configuration de la sécurité IEEE 802.1x sur un client	15
B.6.1 Client IEEE 802.1x utilisant EAP/PEAP	15
B.6.2 Client IEEE 802.1x utilisant un certificat EAP/TLS	19
B.7 Configuration de la sécurité WPA/WPA2 Enterprise (RADIUS) sur un client	23
B.7.1 Client WPA/WPA2 Enterprise (RADIUS) utilisant EAP/PEAP	23
B.7.2 Client WPA/WPA2 Enterprise (RADIUS) utilisant un certificat EAP-TLS	27
B.8 Configuration de la sécurité WPA/WPA2 Personnel (PSK) sur un client.	31
B.9 Configuration d'un serveur RADIUS externe pour reconnaître la 9160 G2	34
B.10 Obtention d'un certificat TLS-EAP pour un client	38
B.11 Configuration du serveur RADIUS pour les balises VLAN	43
B.11.1 Configuration d'un serveur RADIUS	43

Généralement, les utilisateurs configurent la sécurité de leurs clients sans fil pour un accès à bon nombre de réseaux différents (points d'accès). La liste des « réseaux disponibles » change en fonction de l'emplacement du client et quels points d'accès sont en ligne et détectables dans cet emplacement.¹ Une fois qu'un point d'accès a été détecté par le client et que la sécurité est configurée pour lui, il reste dans la liste des réseaux du client, mais s'affiche comme accessible ou inaccessible en fonction de la situation. Pour chaque réseau (point d'accès) auquel vous souhaitez vous connecter, configurez les paramètres de sécurité sur le client pour correspondre au mode de sécurité utilisé par ce réseau.

Nous décrivons la configuration de la sécurité sur un client qui utilise un logiciel client Microsoft® Windows® pour la connectivité sans fil. Le logiciel client Windows est utilisé comme exemple en raison de sa disponibilité généralisée sur des ordinateurs et ordinateurs portables Windows. Ces procédures sont légèrement différentes si vous utilisez un logiciel différent sur le client (tel que Funk Odyssey®), mais les informations de configuration que vous devez fournir sont les mêmes.



Remarque : L'ordre recommandé pour procéder à la configuration de sécurité est (1) paramétrer la sécurité sur le point d'accès, et (2) configurer la sécurité de chacun des clients sans fil.

Nous pensons qu'au départ, vous vous connecterez à un point d'accès qui n'a aucune sécurité paramétrée (« None » (Aucun)) depuis un client sans fil non sécurisé. Avec cette connexion initiale, vous pouvez accéder aux pages Web d'administration sur du point d'accès et configurer un mode de sécurité (Security (Sécurité)).

*Lorsque vous configurez à nouveau le point d'accès avec un paramètre de sécurité et que vous cliquez sur **Update** (Mettre à jour), votre client sans fil sera dissocié et vous perdez la connectivité aux pages Web d'administration du point d'accès. Dans certains cas, vous devrez apporter des modifications supplémentaires aux paramètres de sécurité du point d'accès avant de configurer le client. Par conséquent, vous devez disposer d'une connexion Ethernet (filaire) de sauvegarde.*

Les sections suivantes expliquent comment configurer chacun des modes de sécurité pris en charge sur les clients sans fil d'un réseau desservi par la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway.

¹L'exception à cette règle sera le cas où le point d'accès est configuré pour interdire la diffusion de son nom de réseau. Dans ce cas, le SSID ne s'affichera pas dans la liste des réseaux disponibles sur le client. Au lieu de cela, le client doit avoir le nom exact du réseau configuré dans les propriétés de la connexion réseau avant de pouvoir se connecter.

B.1 Infrastructure réseau ; choix entre un serveur d'authentification intégré ou externe

Les configurations de sécurité réseau, y compris *PKI (Public Key Infrastructure)*, les serveurs *Remote Authentication Dial-In User Server (RADIUS)* et l'*autorité de certification (CA)*, peuvent varier fortement d'une entreprise à l'autre en termes de la manière dont elles fournissent *Authentication, Authorization, and Accounting (Authentification, autorisation et audit) (AAA)*. Au final, les spécificités de votre infrastructure déterminent comment les clients doivent configurer la sécurité pour accéder au réseau sans fil. Plutôt que d'essayer de prévoir et de couvrir les détails de chaque scénario possible, ce document fournit des consignes générales pour chaque type de configuration client pris en charge par la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway.

B.1.1 Utilisation du serveur d'authentification intégré (EAP-PEAP)

Si vous ne disposez pas d'un serveur RADIUS ou d'une infrastructure PKI et/ou que vous n'êtes pas familiarisé avec la plupart de ces concepts, nous vous recommandons fortement de configurer les passerelles sans fil Passerelle sans fil 9160 G2 Wireless Gateway avec une sécurité qui utilise le *serveur d'authentification intégré* du point d'accès. Cela signifie configurer le point d'accès pour utiliser le mode de sécurité IEEE 802.1x ou WPA/WPA2 Entreprise (RADIUS). (Le serveur d'authentification intégré utilise le protocole d'authentification EAP-PEAP.)

- Si la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway est configurée pour utiliser le mode IEEE 802.1x et le serveur d'authentification intégré, configurez les clients sans fil en suivant la procédure décrite dans la section « Client IEEE 802.1x utilisant EAP/PEAP » à la page B-15.
- Si la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway est configurée pour utiliser le mode WPA/WPA2 Entreprise (RADIUS) et le serveur d'authentification intégré, configurez les clients sans fil en suivant la procédure décrite dans la section « Client WPA/WPA2 Entreprise (RADIUS) utilisant EAP/PEAP » à la page B-23.

B.1.2 Utilisation d'un serveur RADIUS externe avec des certificats EAP-TLS ou EAP-PEAP

Nous supposons que si vous disposez d'un serveur RADIUS externe et d'une installation PKI/CA, vous saurez comment configurer les options de sécurité client adaptées à votre infrastructure de sécurité au-delà des suggestions fondamentales données ci-après. Les rubriques couvertes ici qui se rapportent plus particulièrement à la configuration de la sécurité client dans un environnement RADIUS - PKI sont les suivantes :

- « Client IEEE 802.1x utilisant un certificat EAP/TLS » à la page B-19.

- « Client WPA/WPA2 Enterprise (RADIUS) utilisant un certificat EAP-TLS » à la page B-27.
- « Configuration d'un serveur RADIUS externe pour reconnaître la 9160 G2 » à la page B-34.
- « Obtention d'un certificat TLS-EAP pour un client » à la page B-38.

Les détails de la procédure à suivre pour configurer un client EAP-PEAP avec un serveur RADIUS externe ne sont pas couverts dans ce document.

B.2 Assurez-vous que le logiciel client sans fil est à jour.

Avant de commencer, vous devez garder à l'esprit que les service packs, les correctifs, et les nouvelles versions de pilotes et d'autres technologies de prise en charge pour les clients sans fil sont générés à un rythme effréné. Ne pas avoir le bon pilote ou les bonnes mises à jour sur le client est un problème courant dans la configuration de la sécurité client. Par exemple, si vous configurez WPA sur le client, assurez-vous que vous disposez d'un pilote installé qui prenne en charge WPA, une technologie relativement nouvelle. Même de nombreuses cartes client actuellement disponibles ne sont pas fournies par l'usine avec les pilotes les plus récents.

B.3 Accès aux paramètres de sécurité client sans fil Microsoft Windows

Généralement, sous Windows XP, il y a deux manières d'accéder aux propriétés de sécurité d'un client sans fil :

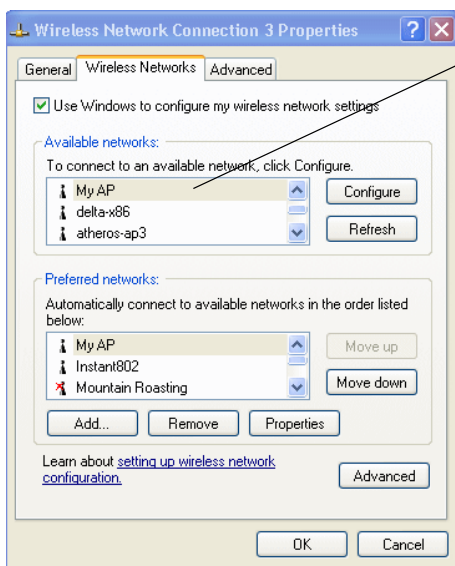
1. Depuis l'*icône de connexion sans fil* dans la barre des tâches Windows :
 - Cliquez avec le bouton droit de la souris sur l'icône de connexion sans fil dans votre barre des tâches Windows et sélectionnez **View available wireless networks** (Afficher les réseaux sans fil disponibles).
 - Sélectionnez le SSID du réseau auquel vous souhaitez vous connecter, puis cliquez sur **Advanced** (Avancé) pour afficher la boîte de dialogue *Wireless Network Connection Properties* (Propriétés de Connexion réseau sans fil).

OU

1. Depuis le menu *Start* (Démarrer) à l'extrémité gauche de la barre des tâches :
 - Dans le menu *Start* (Démarrer) de la barre des tâches, sélectionnez **Start, My Network Places** (Démarrer, Favoris réseau) pour afficher la fenêtre *Network Connections* (Favoris réseau).
 - Dans le menu *Network Tasks* (Gestion du réseau) à gauche, cliquez sur **View Network Connections** (Afficher les connexions réseau) pour afficher la fenêtre *Network Connections* (Connexions réseau).

- Sélectionnez la *connexion réseau sans fil* que vous souhaitez configurer, cliquez avec le bouton droit de la souris pour sélectionner **View available wireless networks** (Afficher les réseaux sans fil disponibles).
- Sélectionnez le SSID du réseau auquel vous souhaitez vous connecter, puis cliquez sur **Advanced** (Avancé) pour afficher la boîte de dialogue Wireless Network Connection Properties (Propriétés de Connexion réseau sans fil).

L'onglet *Wireless Networks* (Réseaux sans fil) (qui devrait automatiquement s'afficher) présente les *Available networks* (Réseaux disponibles) et *Preferred networks* (Réseaux préférés).



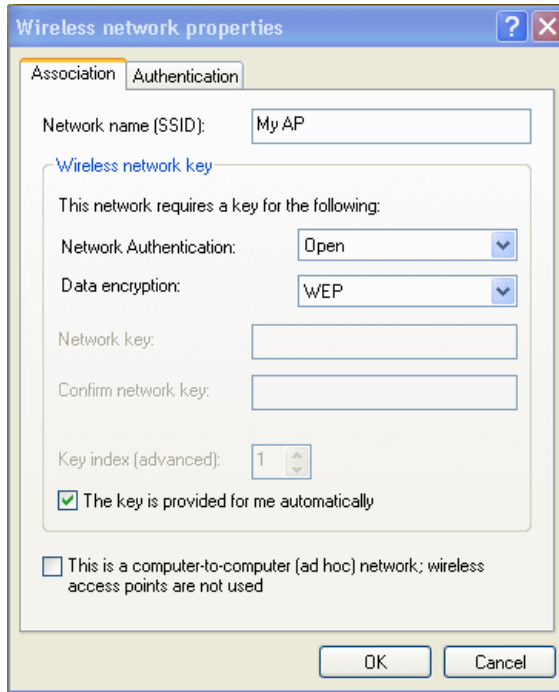
La liste des réseaux disponibles change en fonction de l'emplacement du client. Chaque réseau (ou point d'accès) qui est détecté par le client s'affiche dans cette liste. (« Refresh » (Actualiser) met à jour la liste avec les informations actuelles.)

Pour chaque réseau auquel vous souhaitez vous connecter, configurez les paramètres de sécurité sur le client pour correspondre au mode de sécurité utilisé par ce réseau.

Remarque : l'exception à cette règle sera le cas où le point d'accès est configuré pour interdire la diffusion de son nom de réseau, le nom ne sera pas affiché sur cette liste. Dans ce cas, vous devrez taper le nom exact du réseau pour pouvoir vous y connecter.

2. Dans la liste des *réseaux disponibles*, sélectionnez le SSID du réseau auquel vous souhaitez vous connecter, puis cliquez sur **Configure** (Configurer).

Ceci affiche la boîte de dialogue *Wireless Network Connection Properties* (Propriétés de Connexion réseau sans fil) avec les onglets *Association* et *Authentication* (Authentification) pour le réseau sélectionné.



Utilisez cette boîte de dialogue pour configurer tous les différents types de sécurité client décrits dans les sections suivantes. Assurez-vous que la boîte de dialogue *Wireless Network Properties* (Propriétés du réseau sans fil) dans lequel vous travaillez s'applique au nom de réseau (SSID) du réseau que vous souhaitez atteindre sur le client sans fil que vous êtes en train de configurer.

B.4 Configuration d'un client pour accéder à un réseau non sécurisé (aucune sécurité)

Si le point d'accès ou le réseau sans fil auquel vous souhaitez vous connecter est configuré sur « None » (Aucun), c'est à dire aucune sécurité, vous devez configurer le client en conséquence. Un client n'utilisant aucune sécurité de connexion est configuré avec *Network Authentication* (Authentification réseau) sur **Open** (Ouvret) sur ce réseau et *Data Encryption* (Cryptage des données) sur **Disabled** (Désactivé), comme décrit ci-dessous.

Si vous avez des paramètres de sécurité configurés sur un client pour les propriétés d'un réseau non sécurisé, les paramètres de sécurité peuvent en fait empêcher l'accès au réseau en raison de l'incompatibilité entre les configurations de sécurité du client et du point d'accès.

Pour configurer le client sans utiliser de sécurité, ouvrez la boîte de dialogue *Network Properties* (Propriétés du réseau) et configurez les paramètres suivants.

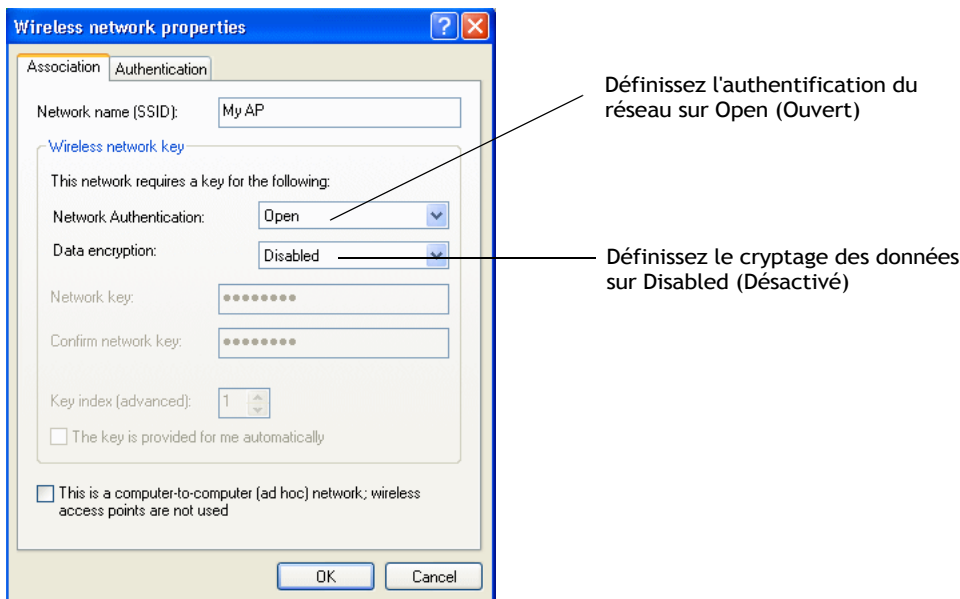


Tableau B.1 Paramètres d'association

<i>Network Authentication (Authentification réseau)</i>	Open (Ouvert)
<i>Data Encryption (Cryptage des données)</i>	Disabled (Désactive)

B.5 Configuration de la sécurité WEP statique sur un client

Wired Equivalent Privacy (WEP) statique crypte les données se déplaçant dans un réseau sans fil via une clé statique (non variante). L'algorithme de cryptage est un chiffrement de « flux » appelé RC4. Le point d'accès utilise une clé pour transmettre des données aux stations client. Chaque client doit utiliser cette même clé pour décrypter les données qu'il reçoit du point d'accès. Plusieurs clients peuvent utiliser des clés différentes pour transmettre des données au point d'accès. (Ou ils peuvent tous utiliser la même clé, mais c'est moins sécurisé, car cela signifie qu'une station peut décrypter les données envoyées par une autre.)

Si vous avez configuré la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway pour utiliser le mode de sécurité WEP statique. . .

. . . configurez la sécurité WEP sur chaque client comme suit.

Sélectionnez Open (Ouvert) ou Shared (Partagé)

Choisissez WEP comme mode de cryptage des données

Entrez la clé de réseau correspondant à la clé WEP sur le point d'accès dans la position définie sur l'index de clé de transfert (et tapez à nouveau pour confirmer)

Vous pouvez également définir un index de clé de transfert différent pour renvoyer des données du client au point d'accès

Désactivez l'option de clé automatique

Tableau B.2 Paramètres d'association

<i>Network Authentication</i> (Authentification réseau)	<p>Open (Ouvert) ou Shared (Partagé), en fonction de la manière dont vous avez configuré cette option sur le point d'accès.</p> <p><i>Remarque : Lorsque l'algorithme d'authentification du point d'accès est défini sur Both (Les deux), les clients définis sur Shared (Partagé) ou Open (Ouvert) peuvent s'associer au point d'accès. Les clients configurés pour utiliser WEP en mode Shared (Partagé) doivent disposer d'une clé WEP valide pour pouvoir s'associer au point d'accès. Les clients configurés pour utiliser WEP comme système Open (Ouvert) peuvent être associés au point d'accès, et ce, même sans clé WEP valide (mais une clé valide sera nécessaire pour afficher et échanger des données). Pour plus d'informations, reportez-vous à l'aide en ligne sur le point d'accès.</i></p>
<i>Data Encryption</i> (Cryptage des données)	WEP
<i>Network Key</i> (Clé réseau)	<p>Fournissez la clé WEP que vous avez saisie dans les <i>paramètres de sécurité</i> du point d'accès à l'index de clé de transfert.</p> <p>Par exemple, si l'index de clé de transfert du point d'accès est défini sur 1, pour la clé de réseau client, spécifiez la clé WEP que vous avez saisie comme clé WEP 1 sur le point d'accès.</p>
<i>Key Index</i> (Index de clé)	<p>Définissez l'index de clé pour indiquer laquelle des clés WEP spécifiées dans la page <i>Security</i> (Sécurité) du point d'accès sera utilisée pour le transfert de retour des données du client au point d'accès.</p> <p>Par exemple, vous pouvez définir cette option sur 1, 2, 3, ou 4 si vous avez les quatre clés WEP configurées sur le point d'accès.</p>
<i>The key is provided for me automatically</i> (La clé m'est fournie automatiquement)	Désactivez cette option (cliquez pour décocher la case).
<i>Enable IEEE 802.1x authentication for this network</i> (Activer l'authentification IEEE 802.1x pour ce réseau)	<p>Assurez-vous que l'authentification IEEE 802.1x est désactivée (la case doit être décochée).</p> <p>(Définir le mode de cryptage sur WEP devrait désactiver automatiquement l'authentification.)</p>

Tableau B.3 Paramètres d'authentification

<i>Enable IEEE 802.1x authentication for this network</i> (Activer l'authentification IEEE 802.1x pour ce réseau)	<p>Assurez-vous que l'authentification IEEE 802.1x est désactivée (la case doit être décochée).</p> <p>(Définir le mode de cryptage sur WEP devrait désactiver automatiquement l'authentification.)</p>
---	--

Cliquez sur **OK** dans la boîte de dialogue *Wireless Network Properties* (Propriétés du réseau sans fil) pour la fermer et enregistrer vos modifications.

Connexion au réseau sans fil avec un client WEP statique

Les clients WEP statique devraient maintenant pouvoir s'associer et s'authentifier au point d'accès. En tant que client, vous ne serez pas invité à entrer une clé WEP. La clé WEP configurée dans les paramètres de sécurité client est automatiquement utilisée lorsque vous vous connectez.

B.6 Configuration de la sécurité IEEE 802.1x sur un client

IEEE 802.1x est l'authentification basée sur le port de définition et l'infrastructure de gestion des clés standard. Les messages *EAP* (*Extensible Authentication Protocol*) sont envoyés sur un réseau sans fil IEEE 802.11 via un protocole appelé EAP Encapsulation Over LANs (EAPOL). IEEE 802.1x fournit des clés générées dynamiquement qui sont régulièrement actualisées. Un chiffrement de flux RC4 est utilisé pour crypter le corps de la trame et le contrôle de redondance cyclique (CRC) de chaque trame 802.11.

B.6.1 Client IEEE 802.1x utilisant EAP/PEAP

Le serveur d'authentification intégré sur la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway utilise Protected *Extensible Authentication Protocol* - Protocole d'authentification (*EAP*) protégé, appelé ici « EAP/PEAP ».

- Si vous utilisez le serveur d'authentification intégré avec le mode de sécurité « IEEE 802.1x » sur la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway, vous devez configurer les clients sans fil pour utiliser PEAP.
- En outre, vous avez peut-être un serveur RADIUS externe qui utilise EAP/PEAP. Si c'est le cas, vous devrez :
 1. Ajouter la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway à la liste des clients du serveur RADIUS.

ET

2. Configurer vos clients sans fil IEEE 802.1x pour utiliser PEAP.



Remarque : L'exemple suivant suppose que vous utilisiez le serveur d'authentification intégré fourni avec la passerelle sans fil 9160 G2 Wireless Gateway. Si vous configurez EAP/PEAP sur un client d'un point d'accès qui utilise un serveur RADIUS externe, le processus de configuration client sera différent de celui de l'exemple, notamment en matière de validation de certificats.

Si vous avez configuré la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway pour utiliser le mode de sécurité IEEE 802.1x. . .

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Modify Internal Network security settings

☒ Broadcast SSID ☐ Station Isolation

Mode: IEEE802.1x

☐ Use internal radius server

Radius IP: 10.128.14.14

Radius Key:

☐ Enable radius accounting

Update

. . . configurez ensuite la sécurité IEEE 802.1x avec l'authentification PEAP sur chaque client comme suit :

Wireless network properties

Association Authentication

Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: Open

Data encryption: WEP

Network key:

Confirm network key:

Key index (advanced): 1

☒ The key is provided for me automatically

☐ This is a computer-to-computer (ad hoc) network; wireless access points are not used

1 OK Cancel

Wireless network properties

Association Authentication

Select this option to provide authenticated network access for wireless Ethernet networks.

☒ Enable IEEE 802.1x authentication for this network.

EAP type: Protected EAP (PEAP)

Properties

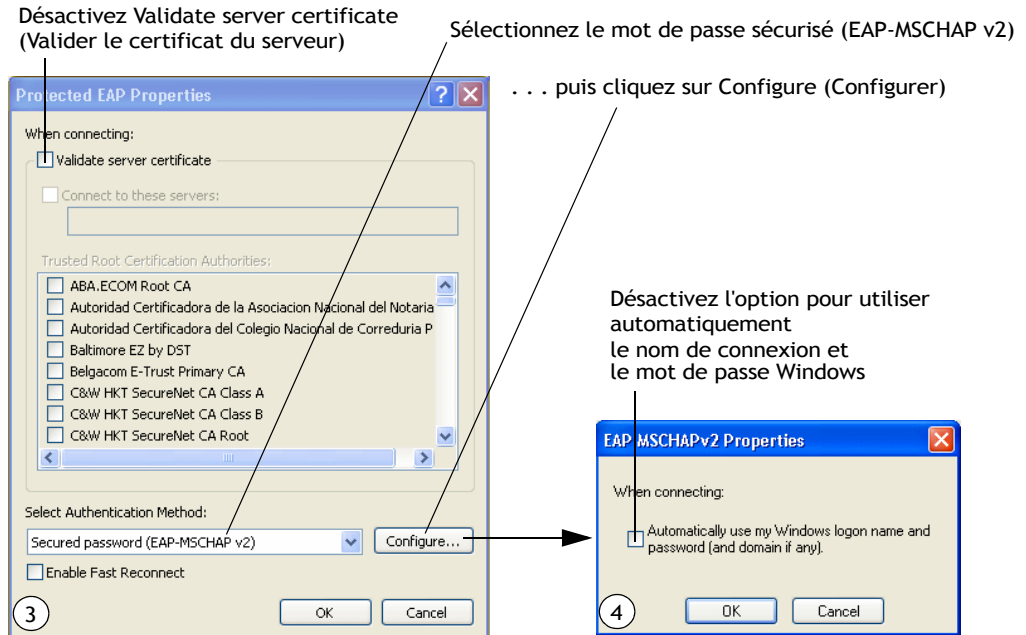
☐ Authenticate as computer when computer information is available

☐ Authenticate as guest when user or computer information is unavailable

2 OK Cancel

Annotations:

- Choisissez Open (Ouvert)
- Choisissez WEP comme mode de cryptage des données
- Activez (cochez) l'authentification IEEE 8021x
- Choisissez Protected EAP (PEAP) . . . ensuite, cliquez sur Properties (Propriétés)
- Activez l'option de clé automatique



1. Configurez les paramètres suivants dans l'onglet *Association* de la boîte de dialogue *Network Properties* (Propriétés du réseau).

Tableau B.4 Paramètres d'association

<i>Network Authentication</i> (Authentification réseau)	Open (Ouvert)
<i>Data Encryption</i> (Cryptage des données)	WEP <i>Remarque : Un chiffrement de flux RC4 est utilisé pour crypter le corps de la trame et le contrôle de redondance cyclique (CRC) de chaque trame IEEE 802.11. C'est le même algorithme de cryptage que celui qui est utilisé pour WEP statique. Par conséquent, la méthode de cryptage des données configurées sur le client pour ce mode est WEP.</i>
<i>This key is provided for me automatically</i> (Cette clé m'est fournie automatiquement)	Activez (cochez) cette option.

2. Configurez ce paramètre dans l'onglet *Authentication* (Authentification).

Tableau B.5 Paramètres d'authentification

<i>EAP Type (Type d'EAP)</i>	Choisissez Protected EAP (PEAP) .
------------------------------	--

3. Cliquez sur **Properties** (Propriétés) pour afficher la boîte de dialogue *Protected EAP Properties* (Propriétés EAP protégé) et configurez les paramètres suivants.

Tableau B.6 Paramètres des propriétés EAP protégé

<i>Validate server certificate</i> (Valider le certificat du serveur)	Désactivez cette option (cliquez pour décocher la case). <i>Remarque : Cet exemple suppose que vous utilisez le serveur d'authentification intégré au point d'accès. Si vous configurez EAP/PEAP sur un client d'un point d'accès qui utilise un serveur RADIUS externe, vous pourriez devoir utiliser la validation de certificat et choisir un certificat, en fonction de votre infrastructure.</i>
<i>Select Authentication Method</i> (Sélectionnez une méthode d'authentification)	Sélectionnez Secured password (EAP-MSCHAP v2) (Mot de passe sécurisé (EAP-MSCHAP v2)).

4. Cliquez sur **Configure** (Configurer) pour afficher la boîte de dialogue *EAP MSCHAP v2 Properties* (Propriétés MSCHAP v2 EAP).

Dans cette boîte de dialogue, **désactivez** (cliquez pour décocher) l'option *Automatically use my Windows logon name* (Utiliser automatiquement mon nom de connexion Windows). . . etc.

Cliquez sur **OK** dans toutes les boîtes de dialogue (en commençant par la boîte de dialogue *EAP MSCHAP v2 Properties* (Propriétés EAP MSCHAP v2)) pour fermer et enregistrer vos modifications.

Connexion au réseau sans fil avec un client PEAP IEEE 802.1x

Les clients PEAP IEEE 802.1x devraient maintenant pouvoir s'associer au point d'accès. Les utilisateurs du client seront invités à entrer un nom d'utilisateur et un mot de passe pour s'authentifier sur le réseau.

B.6.2 Client IEEE 802.1x utilisant un certificat EAP/TLS

Extensible Authentication Protocol (EAP) Transport Layer Security (TLS), ou EAP-TLS, est un protocole d'authentification qui prend en charge l'utilisation des cartes à puce et des certificats. Vous avez le possibilité d'utiliser EAP-TLS avec les modes WPA/WPA2 Enterprise (RADIUS) et IEEE 802.1x si vous disposez d'un serveur RADIUS externe sur le réseau pour le prendre en charge.



Remarque : Si vous souhaitez utiliser le mode IEEE 802.1x avec des certificats EAP-TLS pour l'authentification et l'autorisation de clients, vous devez disposer d'un serveur RADIUS externe et d'un serveur Public Key Authority Infrastructure (PKI), y compris une autorité de certification (CA), configurés sur votre réseau. Décrire ces configurations du serveur RADIUS, PKI, et CA ne fait pas partie des objectifs de ce document. Consultez la documentation relative à ces produits. Pour le logiciel PKI Windows Microsoft, vous trouverez quelques bons points de départ sur le Web :

« How to Install/Uninstall a Public Key Certificate Authority for Windows 2000 » (Comment installer/désinstaller une autorité de certification de clé publique pour Windows 2000) à l'adresse

<http://support.microsoft.com/default.aspx?scid=kb:en-us:231881>, et

« How to Configure a Certificate Server » (Comment configurer un serveur de certificats) à l'adresse

<http://support.microsoft.com/default.aspx?scid=kb:en-us:318710#3>.

Pour utiliser ce type de sécurité, vous devez procéder comme suit :

1. Ajoutez la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway à la liste des clients du serveur RADIUS. (Reportez-vous à la section « Configuration d'un serveur RADIUS externe pour reconnaître la 9160 G2 » à la page B-34.)
2. Configurez la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway pour utiliser votre serveur RADIUS (en fournissant l'adresse IP du serveur RADIUS dans le cadre des paramètres du mode de sécurité « IEEE 802.1x »).
3. Configurez les clients sans fil pour utiliser la sécurité IEEE 802.1x et « Smart Card or other Certificate » (Carte à puce ou autre certificat) comme décrit dans cette section.
4. Obtenez un certificat pour ce client comme indiqué dans la section « Obtention d'un certificat TLS-EAP pour un client » à la page B-38.

Si vous avez configuré la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway pour utiliser le mode de sécurité IEEE 802.1x avec un serveur RADIUS externe. . .

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Modify Internal Network security settings

☒ Broadcast SSID
 ☐ Station Isolation

Mode: IEEE802.1x

☐ Use internal radius server

Radius IP: 10.128.14.14

Radius Key:

☒ Enable radius accounting

Update

. . . configurez ensuite la sécurité IEEE 802.1x avec l'authentification par certificat sur chaque client comme suit :

Choisissez Open (Ouvert)

Choisissez WEP comme mode de cryptage des données

Activez (cochez) l'authentification IEEE 8021x

Choisissez Smart Card/Certificate (Carte à puce/certificat)

. . . cliquez ensuite sur Properties (Propriétés)

Wireless network properties

Association

Authentication

Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: Open

Data encryption: WEP

Network key:

Confirm network key:

Key index (advanced): 1

☒ The key is provided for me automatically

☐ This is a computer-to-computer (ad hoc) network; wireless access points are not used

1

OK

Cancel

Activez l'option de clé automatique

Wireless network properties

Association

Authentication

Select this option to provide authenticated network access for wireless Ethernet networks.

☒ Enable IEEE 802.1x authentication for this network

EAP type: Smart Card or other Certificate

Properties

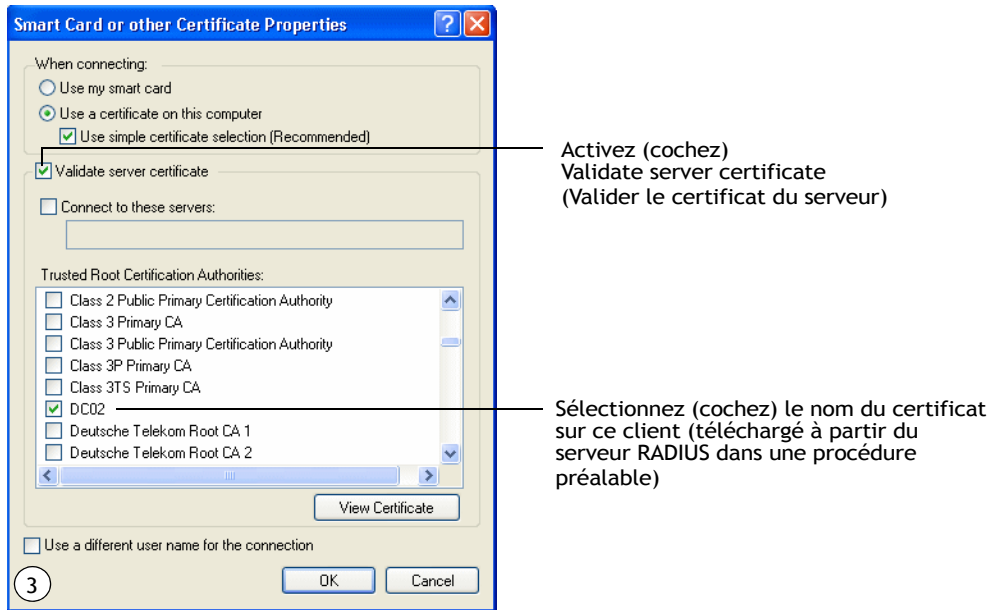
☐ Authenticate as computer when computer information is available

☐ Authenticate as guest when user or computer information is unavailable

2

OK

Cancel



1. Configurez les paramètres suivants dans l'onglet *Association* de la boîte de dialogue *Network Properties* (Propriétés du réseau).

Tableau B.7 Paramètres d'association

<i>Network Authentication</i> (Authentification réseau)	Open (Ouvert)
<i>Data Encryption</i> (Cryptage des données)	WEP <i>Remarque : Un chiffrement de flux RC4 est utilisé pour crypter le corps de la trame et le contrôle de redondance cyclique (CRC) de chaque trame IEEE 802.11. C'est le même algorithme de cryptage que celui qui est utilisé pour WEP statique. Par conséquent, la méthode de cryptage des données configurées sur le client pour ce mode est WEP.</i>
<i>This key is provided for me automatically</i> (Cette clé m'est fournie automatiquement)	Activez (cochez) cette option.

2. Configurez ces paramètres sur l'onglet *Authentication* (Authentification).

Tableau B.8 Paramètres d'authentification

Enable IEEE 802.1x authentication for this network (Activer l'authentification IEEE 802.1x pour ce réseau)	Activez (cochez) cette option.
EAP Type (Type d'EAP)	Choisissez Smart Card or other Certificate (Carte à puce ou autre certificat).

3. Cliquez sur **Propriétés** (Propriétés) pour ouvrir la boîte de dialogue *Smart Card or other Certificate Properties* (Propriétés Carte à puce ou autre certificat) et activez l'option **Validate server certificate** (Valider le certificat du serveur).

Tableau B.9 Paramètres Smart Card or other Certificate Properties (Propriétés Carte à puce ou autre certificat)

Validate server certificate (Valider le certificat du serveur)	Désactivez cette option (cliquez pour décocher la case).
Certificates (Certificats)	Dans la liste des certificats affichée, sélectionnez le certificat pour ce client.

Cliquez sur **OK** dans toutes les boîtes de dialogue pour fermer et enregistrer vos modifications.

4. Pour terminer la configuration du client, vous devez à présent obtenir un certificat du serveur RADIUS et l'installer sur ce client. Pour plus d'informations sur la procédure à suivre, reportez-vous à la section « Obtention d'un certificat TLS-EAP pour un client » à la page B-38.

Connexion au réseau sans fil avec un client IEEE 802.1x utilisant un certificat

Les clients IEEE 802.1x devraient désormais pouvoir se connecter au point d'accès en utilisant leurs certificats TLS. Le certificat que vous avez installé est utilisé lorsque vous vous connectez, de sorte que vous ne serez pas invité à entrer des informations de connexion. Le certificat est envoyé automatiquement au serveur RADIUS pour l'authentification et l'autorisation.

B.7 Configuration de la sécurité WPA/WPA2 Enterprise (RADIUS) sur un client

Wi-Fi Protected Access 2 (WPA2) avec *Remote Authentication Dial-In User Service (RADIUS)* est une mise en œuvre de la norme Wi-Fi Alliance IEEE 802.11h, qui comprend les mécanismes *Advanced Encryption Standard (AES)*, *Counter mode/CBC-MAC Protocol (CCMP)* et *Temporal Key Integrity Protocol (TKIP)*. Ce mode nécessite l'utilisation d'un serveur RADIUS pour authentifier les utilisateurs.

Ce mode de sécurité est rétrocompatible pour les clients sans fil qui ne prennent en charge que le **WPA** d'origine.

Lorsque vous configurez le mode de sécurité WPA/WPA2 Enterprise (RADIUS) sur le point d'accès, vous avez la possibilité de choisir d'utiliser le serveur d'authentification intégré ou un serveur RADIUS externe que vous fournissez.

Le serveur d'authentification intégré de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway prend en charge *Extensible Authentication Protocol - Protocole d'authentification (EAP) protégé (EAP)*, aussi appelé « EAP/PEAP », et *Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAP V2)*, qui fournit une authentification pour les connexions point à point (PPP) entre un ordinateur fonctionnant sous Windows et les appareils réseau tels que les points d'accès.

Ainsi, si vous configurez le réseau (point d'accès) pour utiliser le mode de sécurité et que vous choisissez le serveur d'authentification intégré, vous devez configurer les stations client pour utiliser WPA/WPA2 Enterprise (RADIUS) et EAP/PEAP.

Si vous configurez le réseau (point d'accès) pour utiliser ce mode de sécurité avec un serveur RADIUS externe, vous devez configurer les stations client pour utiliser WPA/WPA2 Enterprise (RADIUS) et le protocole de sécurité configuré sur votre serveur RADIUS.

B.7.1 Client WPA/WPA2 Enterprise (RADIUS) utilisant EAP/PEAP

Le serveur d'authentification intégré sur la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway utilise *Extensible Authentication Protocol - Protocole d'authentification (EAP) protégé*, appelé « EAP/PEAP ».

- Si vous utilisez le serveur d'authentification intégré avec le mode de sécurité « WPA/WPA2 Enterprise (RADIUS) » sur la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway, vous devez configurer les clients sans fil pour utiliser PEAP.
- En outre, vous avez peut-être un serveur RADIUS externe qui utilise EAP/PEAP. Si c'est le cas, vous devrez :
 1. Ajouter la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway à la liste des clients du serveur RADIUS.

- ET
2. Configurer vos clients sans fil « WPA/WPA2 Enterprise (RADIUS) » pour utiliser PEAP.



Remarque : L'exemple suivant suppose que vous utilisiez le serveur d'authentification intégré fourni avec la passerelle sans fil 9160 G2 Wireless Gateway. Si vous configurez EAP/PEAP sur un client d'un point d'accès qui utilise un serveur RADIUS externe, le processus de configuration client sera différent de celui de l'exemple, notamment en matière de validation de certificats.

Si vous avez configuré la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway pour utiliser le mode de sécurité WPA/WPA2 Enterprise (RADIUS) et utiliser le serveur d'authentification intégré ou un serveur RADIUS externe qui utilise EAP/PEAP. . .

Basic Settings	<h3>Modify Internal Network security settings</h3> <p><input checked="" type="checkbox"/> Broadcast SSID <input type="checkbox"/> Station Isolation</p> <p>Mode: WPA Enterprise ▼</p> <p>WPAVersions: <input checked="" type="checkbox"/> WPA <input checked="" type="checkbox"/> WPA2 <input type="checkbox"/> Enable pre-authentication</p> <p>Cipher Suites: <input checked="" type="checkbox"/> TKIP <input type="checkbox"/> CCMP (AES)</p> <div><input checked="" type="checkbox"/> Use internal radius server</div> <p>Radius IP: 10.128.14.14</p> <p>Radius Key: ••••••••</p> <div><input checked="" type="checkbox"/> Enable radius accounting</div> <p>Update</p>
User Management	
Cluster	
Access Points	
Sessions	
Channel Management	
Wireless Neighborhood	
Security	
Status	
Interfaces	
Events	
Transmit/Receive	
Client Associations	

... configurez d'abord les comptes d'utilisateur sur le point d'accès (rendez-vous dans l'onglet *User Management* (Gestion des utilisateurs))...

	Username	Real name	Status
<input type="checkbox"/> [Edit]	Darren	Darren Stevens	enabled
<input type="checkbox"/> [Edit]	Samantha	Samantha Stevens	enabled

Selected users:

[\[backup or restore the user database\]](#)

... configurez ensuite la sécurité WPA avec l'authentification PEAP sur chaque client comme suit.

Choisissez WPA

Sélectionnez TKIP ou AES comme mode de cryptage des données

Wireless network properties

Association | Authentication

Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: WPA

Data encryption: TKIP

Network key:

Confirm network key:

Key index (advanced): 1

☒ The key is provided for me automatically

☐ This is a computer-to-computer (ad hoc) network; wireless access points are not used

1 OK Cancel

Choisissez Protected EAP (PEAP)

... cliquez ensuite sur Propriétés (Propriétés)

Wireless network properties

Association | Authentication

Select this option to provide authenticated network access for wireless Ethernet networks.

☒ Enable IEEE 802.1x authentication for this network

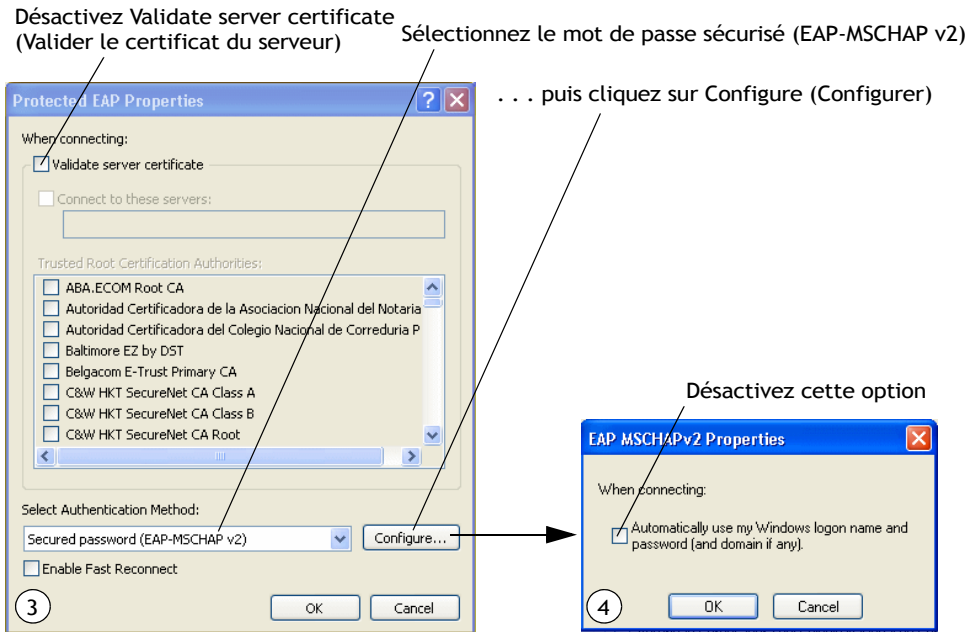
EAP type: Protected EAP (PEAP)

Properties

☐ Authenticate as computer when computer information is available

☐ Authenticate as guest when user or computer information is unavailable

2 OK Cancel



1. Configurez les paramètres suivants dans l'onglet *Association* et *Authentication* (Authentication) de la boîte de dialogue *Network Properties* (Propriétés du réseau).

Tableau B.10 Paramètres d'association

<i>Network Authentication</i> (Authentification réseau)	WPA
<i>Data Encryption</i> (Cryptage des données)	TKIP ou AES en fonction de la manière dont cette option est configurée sur le point d'accès. <i>Remarque :</i> Une fois que la suite de chiffrement sur le point d'accès est définie sur Both (Les deux), les clients TKIP avec une clé TKIP valide et les clients AES avec une clé valide CCMP (AES) peuvent s'associer au point d'accès. Pour plus d'informations, reportez-vous à l'aide en ligne sur le point d'accès.

2. Configurez ce paramètre dans l'onglet *Authentication* (Authentication).

Tableau B.11 Paramètres d'authentification

<i>EAP Type</i> (Type d'EAP)	Choisissez Protected EAP (PEAP) .
------------------------------	--

3. Cliquez sur **Propriétés** (Propriétés) pour afficher la boîte de dialogue *Protected EAP Properties* (Propriétés EAP protégé) et configurez les paramètres suivants.

Tableau B.12 Paramètres des propriétés EAP protégé

<i>Validate server certificate</i> (Valider le certificat du serveur)	Désactivez cette option (cliquez pour décocher la case). <i>Remarque :</i> Cet exemple suppose que vous utilisez le serveur d'authentification intégré au point d'accès. Si vous configurez EAP/PEAP sur un client d'un point d'accès qui utilise un serveur RADIUS externe, vous pourriez devoir utiliser la validation de certificat et choisir un certificat, en fonction de votre infrastructure.
<i>Select Authentication Method</i> (Sélectionnez une méthode d'authentification)	Sélectionnez Secured password (EAP-MSCHAP v2) (Mot de passe sécurisé (EAP-MSCHAP v2)).

4. Cliquez sur **Configure** (Configurer) pour afficher la boîte de dialogue *EAP MSCHAP v2 Properties* (Propriétés MSCHAP v2 EAP).

Dans cette boîte de dialogue, **désactivez** (cliquez pour décocher) l'option *Automatically use my Windows logon name* (Utiliser automatiquement mon nom de connexion Windows). . . etc., pour que dès que vous serez connecté, vous soyez invité à entrer votre nom d'utilisateur et mot de passe.

Cliquez sur **OK** dans toutes les boîtes de dialogue (en commençant par la boîte de dialogue *EAP MSCHAP v2 Properties* (Propriétés EAP MSCHAP v2)) pour fermer et enregistrer vos modifications.

Connexion au réseau sans fil avec un client PEAP WPA/WPA2 Enterprise (RADIUS)

Les clients PEAP « WPA/WPA2 Enterprise (RADIUS) » devraient maintenant pouvoir s'associer au point d'accès. Les utilisateurs du client seront invités à entrer un nom d'utilisateur et un mot de passe pour s'authentifier sur le réseau.

B.7.2 Client WPA/WPA2 Enterprise (RADIUS) utilisant un certificat EAP-TLS

Extensible Authentication Protocol (EAP) *Transport Layer Security* (TLS), ou EAP-TLS, est un protocole d'authentification qui prend en charge l'utilisation des cartes à puce et des certificats. Vous avez la possibilité d'utiliser EAP-TLS avec les modes WPA/WPA2 Enterprise (RADIUS) et IEEE 802.1x si vous disposez d'un serveur RADIUS externe sur le réseau pour le prendre en charge.



Remarque : Si vous souhaitez utiliser le mode IEEE 802.1x avec des certificats EAP-TLS pour l'authentification et l'autorisation de clients, vous devez disposer d'un serveur RADIUS externe et d'un serveur Public Key Authority Infrastructure (PKI), y compris une autorité de certification (CA), configurés sur votre réseau. Décrire ces configurations du serveur RADIUS, PKI, et CA ne fait pas partie des objectifs de ce document. Consultez la documentation relative à ces produits. Pour le logiciel PKI Windows Microsoft, vous trouverez quelques bons points de départ sur le Web :

« How to Install/Uninstall a Public Key Certificate Authority for Windows 2000 » (Comment installer/désinstaller une autorité de certification de clé publique pour Windows 2000) à l'adresse <http://support.microsoft.com/default.aspx?scid=kb:en-us:231881>, et

« How to Configure a Certificate Server » (Comment configurer un serveur de certificats) à l'adresse <http://support.microsoft.com/default.aspx?scid=kb:en-us:318710#3>.

Pour utiliser ce type de sécurité, vous devez procéder comme suit :

1. Ajoutez la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway à la liste des clients du serveur RADIUS. (Reportez-vous à la section « Configuration d'un serveur RADIUS externe pour reconnaître la 9160 G2 » à la page B-34.)
2. Configurez la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway pour utiliser votre serveur RADIUS (en fournissant l'adresse IP du serveur RADIUS dans le cadre des paramètres du mode de sécurité « WPA/WPA2 Enterprise [RADIUS] »).
3. Configurez les clients sans fil pour utiliser la sécurité WPA et « Smart Card or other Certificate » (Carte à puce ou autre certificat) comme décrit dans cette section.
4. Obtenez un certificat pour ce client comme indiqué dans la section « Obtention d'un certificat TLS-EAP pour un client » à la page B-38.

Si vous avez configuré la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway pour utiliser le mode de sécurité WPA/WPA2 Enterprise (RADIUS) avec un serveur RADIUS externe. . .

Modify Internal Network security settings

☒ Broadcast SSID ☐ Station Isolation

Mode: WPA Enterprise

WPA Versions: ☒ WPA ☒ WPA2

☐ Enable pre-authentication

Cipher Suites: ☒ TKIP ☐ CCMP (AES)

☐ Use internal radius server

Radius IP: 10.128.14.14

Radius Key:

☒ Enable radius accounting

Update

. . . configurez ensuite la sécurité WPA avec l'authentification par certificat sur chaque client comme suit.

Choisissez WPA

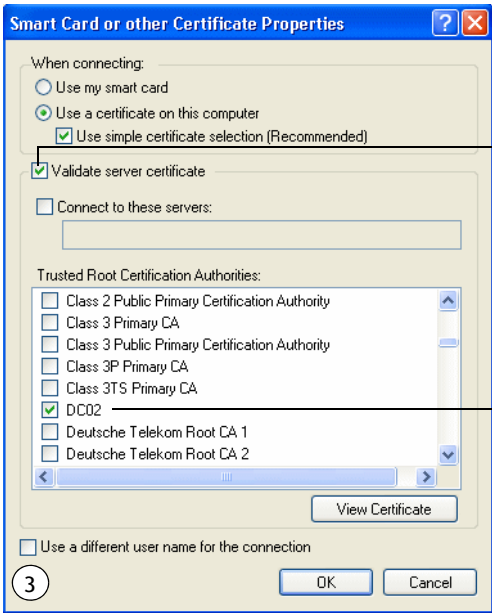
Sélectionnez TKIP ou AES comme mode de cryptage des données

Choisissez Smart Card or other Certificate (Carte à puce ou autre Certificat) et activez Authenticate as computer (Authentifier comme ordinateur) . . .

. . . ensuite, cliquez sur Propriétés (Propriétés)

1

2



Activez (cochez)
Validate server certificate
(Valider le certificat du serveur)

Sélectionnez (cochez) le nom du certificat
sur ce client (téléchargé à partir du
serveur RADIUS dans une procédure
préalable)

1. Configurez les paramètres suivants dans l'onglet *Association* de la boîte de dialogue *Network Properties* (Propriétés du réseau).

Tableau B.13 Paramètres d'association

<i>Network Authentication</i> (Authentification réseau)	WPA
<i>Data Encryption</i> (Cryptage des données)	TKIP ou AES en fonction de la manière dont cette option est configurée sur le point d'accès. <i>Remarque :</i> Une fois que la suite de chiffrement sur le point d'accès est définie sur « Both » (Les deux), les clients TKIP avec une clé TKIP valide et les clients AES avec une clé valide CCMP (AES) peuvent s'associer au point d'accès. Pour plus d'informations, reportez-vous à l'aide en ligne sur le point d'accès.

2. Configurez ces paramètres sur l'onglet *Authentication* (Authentification).

Tableau B.14 Paramètres d'authentification

<i>Enable IEEE 802.1x authentication for this network</i> (Activer l'authentification IEEE 802.1x pour ce réseau)	Activez (cochez) cette option.
<i>EAP Type</i> (Type d'EAP)	Choisissez Smart Card or other Certificate (Carte à puce ou autre certificat).

3. Cliquez sur **Propriétés** (Propriétés) pour ouvrir la boîte de dialogue *Smart Card or other Certificate Properties* (Propriétés Carte à puce ou autre certificat) et activez l'option **Validate server certificate** (Valider le certificat du serveur).

Tableau B.15 Paramètres Smart Card or other Certificate Properties (Propriétés Carte à puce ou autre certificat)

<i>Validate server certificate</i> (Valider le certificat du serveur)	Désactivez cette option (cliquez pour décocher la case).
<i>Certificates (Certificats)</i>	Dans la liste des certificats affichée, sélectionnez le certificat pour ce client.

- Cliquez sur **OK** dans toutes les boîtes de dialogue pour fermer et enregistrer vos modifications.
4. Pour terminer la configuration du client, vous devez à présent obtenir un certificat du serveur RADIUS et l'installer sur ce client. Pour plus d'informations sur la procédure à suivre, reportez-vous à la section « Obtention d'un certificat TLS-EAP pour un client » à la page B-38.

Connexion au réseau sans fil avec un client WPA utilisant un certificat

Les clients WPA devraient désormais pouvoir se connecter au point d'accès en utilisant leurs certificats TLS. Le certificat que vous avez installé est utilisé lorsque vous vous connectez, de sorte que vous ne serez pas invité à entrer des informations de connexion. Le certificat est envoyé automatiquement au serveur RADIUS pour l'authentification et l'autorisation.

B.8 Configuration de la sécurité WPA/WPA2 Personal (PSK) sur un client

Wi-Fi Protected Access (WPA) avec *Pre-Shared Key* (PSK) est un sous-ensemble de Wi-Fi Alliance IEEE 802.11i, qui comprend les mécanismes *Temporal Key Integrity Protocol* (TKIP), *Advanced Encryption Algorithm* (AES), et *Counter mode/CBC-MAC Protocol* (CCMP). PSK utilise une clé prépartagée pour effectuer une vérification initiale des informations d'identification du client.

Si vous avez configuré la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway pour utiliser le mode de sécurité WPA/WPA2 Personal (PSK). . .

The screenshot shows a web interface for configuring network security. On the left is a sidebar with a menu: Basic Settings, User Management, Cluster, Access Points, Sessions, Channel Management, Wireless Neighborhood, Security, and Status. The main area is titled 'Modify Internal Network security settings'. It contains several settings: 'Broadcast SSID' is checked, 'Station Isolation' is unchecked. The 'Mode' is set to 'WPA Personal' in a dropdown menu. Under 'WPA Versions', 'WPA' is checked and 'WPA2' is unchecked. Under 'Cipher Suites', 'TKIP' is checked and 'CCMP (AES)' is unchecked. A 'Key' field contains the text 'reoreore'. An 'Update' button is at the bottom right.

. . . configurez ensuite la sécurité WPA/WPA2 Personal (PSK) sur chaque client comme suit.

The screenshot shows a 'Wireless network properties' dialog box with the 'Authentication' tab selected. The 'Network name (SSID)' is 'My AP'. Under the 'Wireless network key' section, it says 'This network requires a key for the following:'. 'Network Authentication' is set to 'WPA-PSK' and 'Data encryption' is set to 'TKIP'. There are two fields for the 'Network key', both containing dots. The 'Key index (advanced)' is set to '1'. There are checkboxes for 'The key is provided for me automatically' and 'This is a computer-to-computer (ad hoc) network; wireless access points are not used'. 'OK' and 'Cancel' buttons are at the bottom.

Choisissez WPA-PSK.

Sélectionnez TKIP ou AES comme mode de cryptage des données.

Entrez la clé de réseau correspondant à celle spécifiée sur le point d'accès (et confirmez en tapant à nouveau).

Tableau B.16 Paramètres d'association

<i>Network Authentication</i> (Authentification réseau)	WPA-PSK
<i>Data Encryption</i> (Cryptage des données)	TKIP ou AES en fonction de la manière dont cette option est configurée sur le point d'accès. <i>Remarque :</i> Une fois que la suite de chiffrement sur le point d'accès est définie sur Both (Les deux), les clients TKIP avec une clé TKIP valide et les clients AES avec une clé valide CCMP (AES) peuvent s'associer au point d'accès. Pour plus d'informations, reportez-vous à l'aide en ligne sur le point d'accès.
<i>Network Key (Clé réseau)</i>	Fournissez la clé que vous avez saisie dans les paramètres de sécurité du point d'accès pour la suite de chiffrement que vous utilisez. Par exemple, si la clé sur le point d'accès est configurée pour utiliser une clé TKIP « 012345678 », un client TKIP indique cette même chaîne comme clé de réseau.
<i>The key is provided for me automatically</i> (La clé m'est fournie automatiquement)	Cette case doit être désactivée automatiquement en fonction d'autres paramètres.

Tableau B.17 Paramètres d'authentification

<i>Enable IEEE 802.1x authentication for this network</i> (Activer l'authentification IEEE 802.1x pour ce réseau)	Assurez-vous que l'authentification IEEE 802.1x est désactivée (décochée). (Définir le mode de cryptage sur WEP devrait désactiver automatiquement l'authentification.)
--	---

Cliquez sur **OK** dans la boîte de dialogue Wireless Network Properties (Propriétés du réseau sans fil) pour la fermer et enregistrer vos modifications.

Connexion au réseau sans fil avec un client WPA-PSK

Les clients WPA-PSK devraient maintenant pouvoir s'associer et s'authentifier au point d'accès. En tant que client, vous ne serez pas invité à entrer une clé. La clé TKIP ou AES configurée dans les paramètres de sécurité client est automatiquement utilisée lorsque vous vous connectez.

B.9 Configuration d'un serveur RADIUS externe pour reconnaître la 9160 G2

Un serveur *Remote Authentication Dial-In User Server* (RADIUS) externe qui s'exécute sur le réseau peut prendre en charge la distribution des cartes à puce/certificats EAP-TLS pour les clients d'une *infrastructure Public Key Infrastructure* (PKI), ainsi que la configuration et l'authentification du compte d'utilisateur EAP-PEAP. Par serveur RADIUS *externe*, nous voulons dire un serveur d'authentification externe au point d'accès lui-même. Il s'agit de faire la distinction entre le scénario dans lequel vous utilisez un serveur RADIUS du réseau et un autre dans lequel vous utilisez le *serveur d'authentification intégré* sur la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway.

Cette section donne un exemple de configuration d'un serveur RADIUS externe à des fins d'authentification et d'autorisation de certificats TLS-EAP des clients sans fil d'une certaine passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway configurée pour les modes de sécurité « WPA/WPA2 Enterprise (RADIUS) » ou « IEEE 802.1x ». Le but de cette section est de donner une idée de ce à quoi ressemble ce processus ; les procédures varient en fonction du serveur RADIUS que vous utilisez et la façon dont vous le configurez. Pour cet exemple, nous allons utiliser le service d'authentification par Internet (Internet Authentication Service) fourni avec le serveur Microsoft Windows 2003.



Remarque : Ce document n'explique pas comment configurer les utilisateurs avec privilèges d'administrateur sur le serveur RADIUS. Dans cet exemple, nous supposons que vous avez déjà des comptes d'utilisateur configurés sur le serveur RADIUS. Vous aurez besoin d'un nom d'utilisateur et d'un mot de passe serveur RADIUS pour cette procédure et la suivante, qui décrit comment obtenir et installer un certificat sur le client sans fil. Veuillez consulter la documentation de votre serveur RADIUS pour plus d'informations sur la configuration de comptes d'utilisateur.

Cette procédure indique la marche à suivre pour identifier votre passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway comme « client » sur le serveur RADIUS. Le serveur RADIUS peut alors gérer l'authentification et l'autorisation des clients sans fil pour le point d'accès. Cette procédure est requise *par point d'accès*. Si vous avez plus d'un point d'accès avec lesquels vous prévoyez d'utiliser un serveur RADIUS externe, vous devez suivre les étapes ci-dessous pour chacun de ces points d'accès.

Gardez à l'esprit que les informations que vous devez fournir au serveur RADIUS sur le point d'accès correspondent aux paramètres du point d'accès (*Security* [Sécurité]) et vice versa. Vous devez avoir déjà fourni l'adresse IP du serveur RADIUS au point d'accès ; pour les étapes qui suivent, vous devrez fournir l'adresse IP du point d'accès au serveur RADIUS. La clé RADIUS fournie sur le point d'accès est le « secret partagé » que vous devrez fournir au serveur RADIUS.

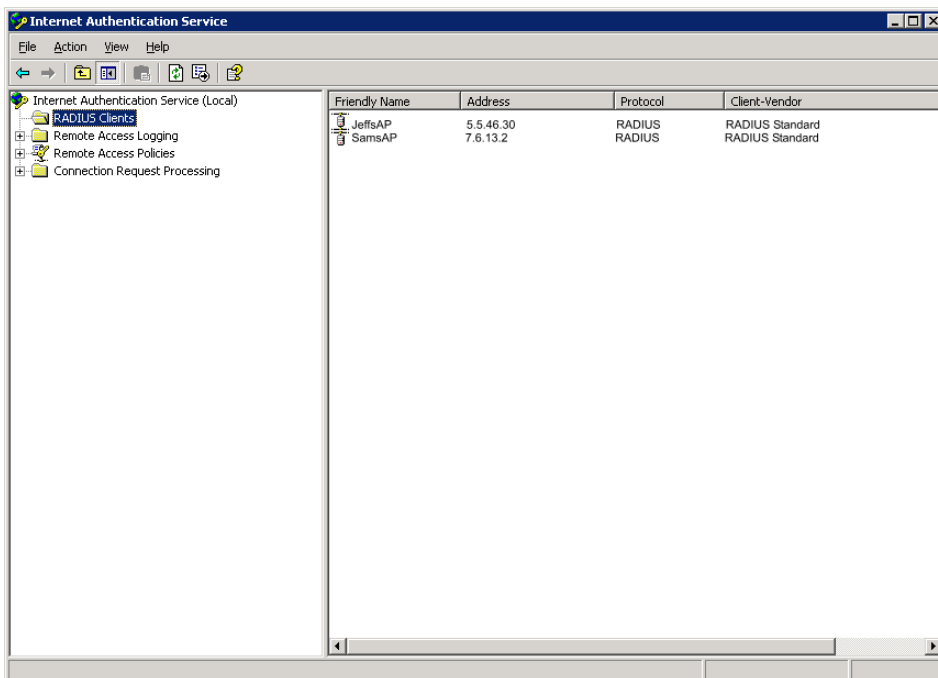
Annexe B : Paramètres de sécurité sur clients sans fil/serveur RADIUS
Configuration d'un serveur RADIUS externe pour reconnaître la 9160 G2

Basic Settings	<h3>Modify Internal Network security settings</h3> <p><input checked="" type="checkbox"/> Broadcast SSID <input type="checkbox"/> Station Isolation</p> <p>Mode: IEEE802.1x ▼</p> <div><input type="checkbox"/> Use internal radius server</div> <p>Radius IP: 10.128.14.14</p> <p>Radius Key: ●●●●●●●●</p> <p><input checked="" type="checkbox"/> Enable radius accounting</p> <p>Update</p>
User Management	
Cluster	
Access Points	
Sessions	
Channel Management	
Wireless Neighborhood	
Security	
Status	
Interfaces	

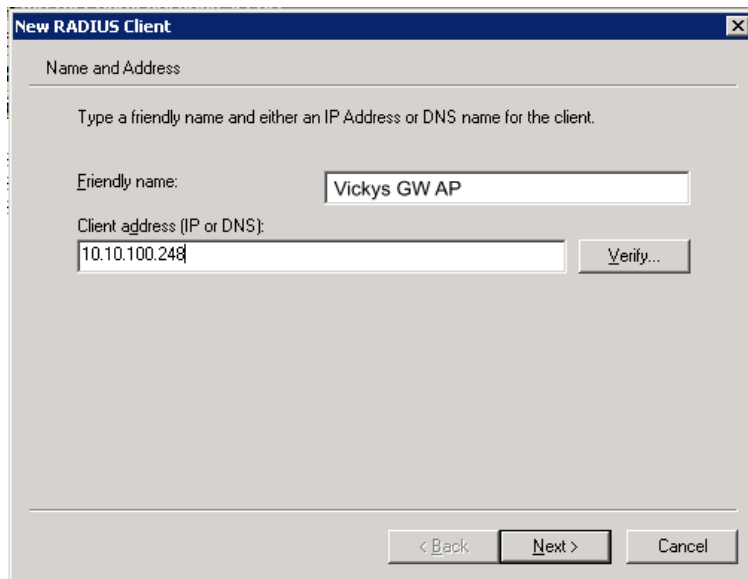


Remarque : Le serveur RADIUS est identifié par son adresse IP et les numéros de port UDP pour les différents services qu'il offre. Sur la version actuelle de la passerelle sans fil 9160 G2 Wireless Gateway, les ports UDP (User Datagram Protocol) du serveur RADIUS utilisés par le point d'accès ne sont pas configurables. (La passerelle sans fil 9160 G2 Wireless Gateway est codée en dur pour utiliser le port UDP 1812 du serveur RADIUS pour l'authentification et le port 1813 pour l'audit.)

1. Connectez-vous au système hébergeant votre serveur RADIUS et affichez le service d'authentification par Internet (Internet Authentication Service).

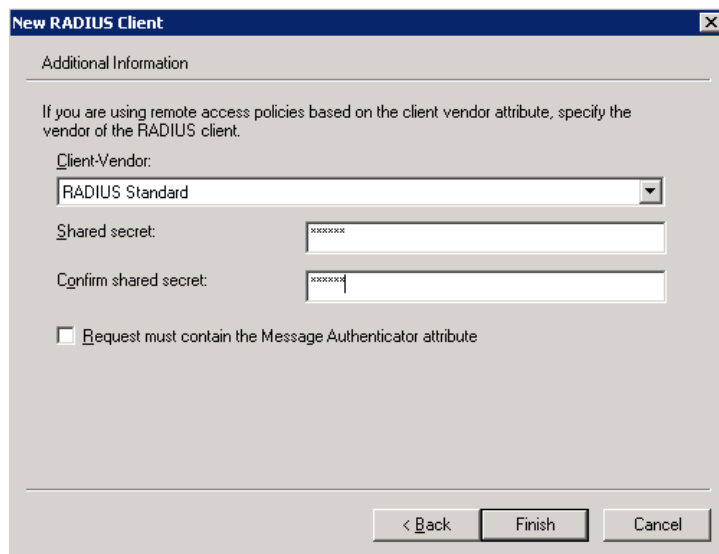


2. Dans le volet de gauche, cliquez avec le bouton droit de la souris sur le nœud **RADIUS Clients** (Clients RADIUS) et choisissez **New > Radius Client** (Nouveau > Client Radius) dans le menu contextuel.
3. Dans le premier écran de l'assistant *New RADIUS Client* (Nouveau client RADIUS), fournissez des informations sur la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway à laquelle vous souhaitez que vos clients se connectent :
 - Un nom logique (convivial) pour le point d'accès. (Vous pouvez utiliser le nom ou l'emplacement DNS.)
 - L'adresse IP pour le point d'accès. Cliquez sur **Next** (Suivant).



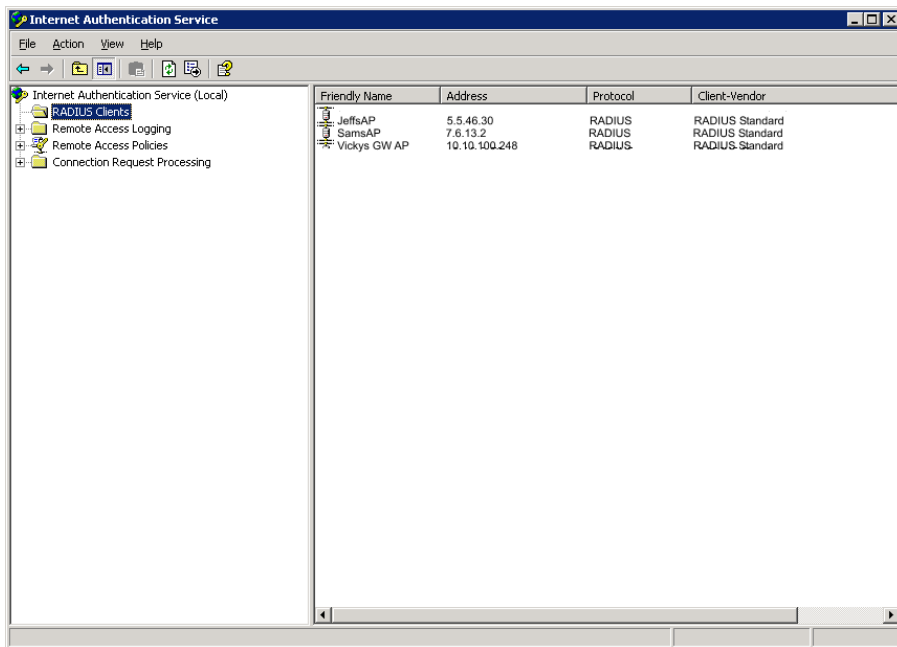
The dialog box is titled "New RADIUS Client". It has a tab labeled "Name and Address". Below the tab, there is a text area with the instruction: "Type a friendly name and either an IP Address or DNS name for the client." There are two input fields: "Friendly name:" with the text "Vickys GW AP" and "Client address (IP or DNS):" with the text "10.10.100.248". To the right of the second field is a button labeled "Verify...". At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

4. Pour *Shared secret* (Secret partagé), entrez la **clé RADIUS** que vous avez fournie au point d'accès (dans la page *Security* [Sécurité]). Saisissez de nouveau la clé pour confirmer.



The dialog box is titled "New RADIUS Client". It has a tab labeled "Additional Information". Below the tab, there is a text area with the instruction: "If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client." There is a dropdown menu labeled "Client-Vendor:" with the text "RADIUS Standard". Below this are two input fields for the "Shared secret:" and "Confirm shared secret:", both containing masked text (asterisks). At the bottom, there is a checkbox labeled "Request must contain the Message Authenticator attribute" which is currently unchecked. At the bottom of the dialog are three buttons: "< Back", "Finish", and "Cancel".

5. Cliquez sur **Finish** (Terminer). Le point d'accès est maintenant affiché comme client du serveur d'authentification.



B.10 Obtention d'un certificat TLS-EAP pour un client



Remarque : Si vous souhaitez utiliser le mode IEEE 802.1x avec des certificats EAP-TLS pour l'authentification et l'autorisation de clients, vous devez disposer d'un serveur RADIUS externe et d'un serveur Public Key Authority Infrastructure (PKI), y compris une autorité de certification (CA), configurés sur votre réseau. Décrire ces configurations du serveur RADIUS, PKI, et CA ne fait pas partie des objectifs de ce document. Consultez la documentation relative à ces produits. Pour le logiciel PKI Windows Microsoft, vous trouverez quelques bons points de départ sur le Web :

« How to Install/Uninstall a Public Key Certificate Authority for Windows 2000 » (Comment installer/désinstaller une autorité de certification de clé publique pour Windows 2000) à l'adresse <http://support.microsoft.com/default.aspx?scid=kb:en-us:231881>, et

« How to Configure a Certificate Server » (Comment configurer un serveur de certificats) à l'adresse <http://support.microsoft.com/default.aspx?scid=kb:en-us:318710#3>.

Les clients sans fil configurés pour utiliser les modes de sécurité « WPA/WPA2 Enterprise (RADIUS) » ou « IEEE 802.1x » avec un serveur RADIUS externe qui prend en charge les certificats TLS-EAP doivent obtenir un certificat TLS auprès du serveur RADIUS.

Il s'agit d'une étape initiale unique qui doit être effectuée sur chaque client qui utilise l'un de ces modes avec des certificats. Dans cette procédure, nous utilisons le serveur Microsoft Certificate Server comme exemple.

Pour obtenir un certificat pour un client, procédez comme suit.

1. Allez à l'URL suivante dans un navigateur Web :

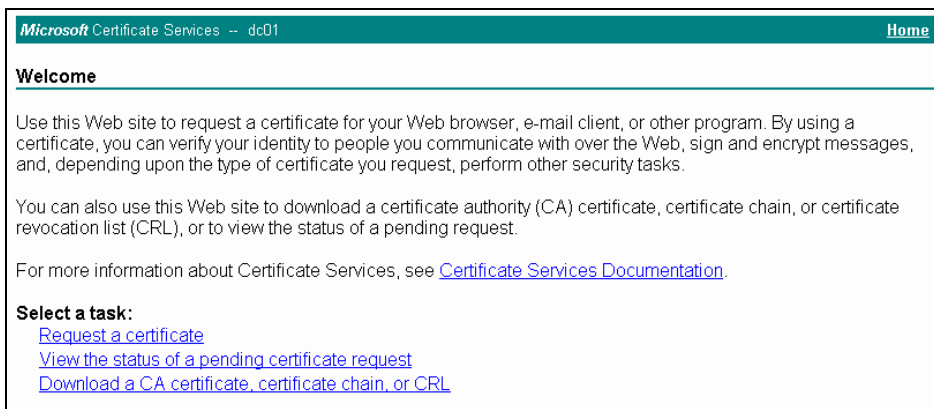
<https://AdresseIPduServeur/certsrv/>

AdresseIPduServeur étant l'adresse IP de votre serveur RADIUS externe, ou de l'*autorité de certification* (CA), selon la configuration de votre infrastructure.

2. Cliquez sur **Yes** (Oui) pour passer à la page Web sécurisée du serveur.



L'écran de bienvenue du serveur de certificats est affiché dans le navigateur.

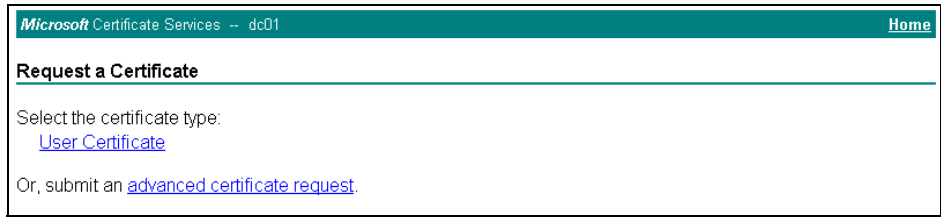


3. Cliquez sur **Request a certificate** (Demander un certificat) pour obtenir l'invite de connexion au serveur RADIUS.
4. Fournissez un **nom d'utilisateur** et un **mot de passe** valides pour accéder au serveur RADIUS.

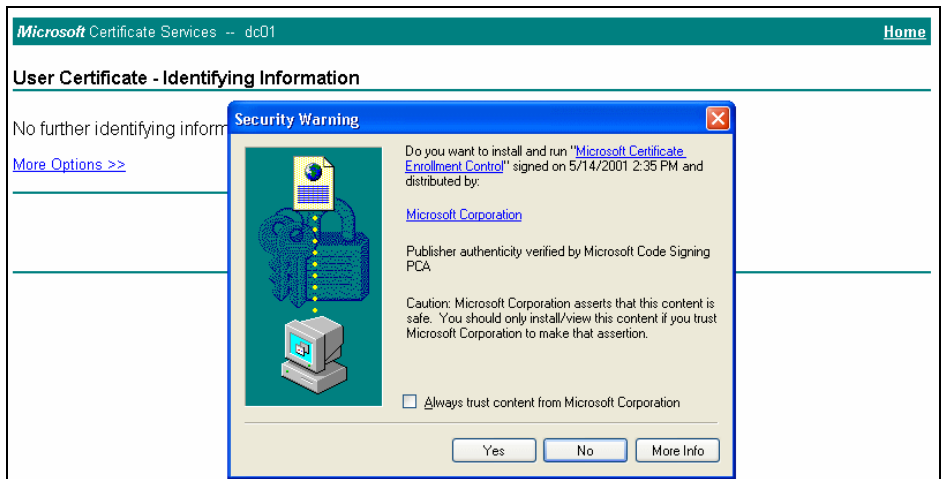


Remarque : Le nom d'utilisateur et le mot de passe que vous devez fournir ici permet d'accéder au serveur RADIUS, pour lequel vous avez déjà configuré des comptes d'utilisateur à ce stade. Ce document n'explique pas comment configurer des comptes d'utilisateur avec des privilèges d'administrateur sur le serveur RADIUS. Veuillez consulter la documentation de votre serveur RADIUS pour ces procédures.

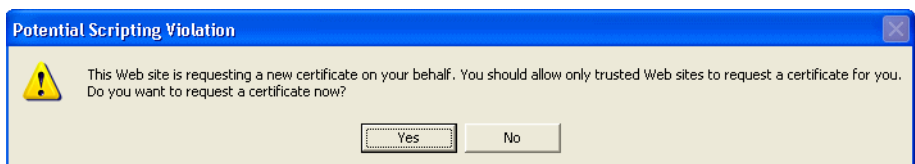
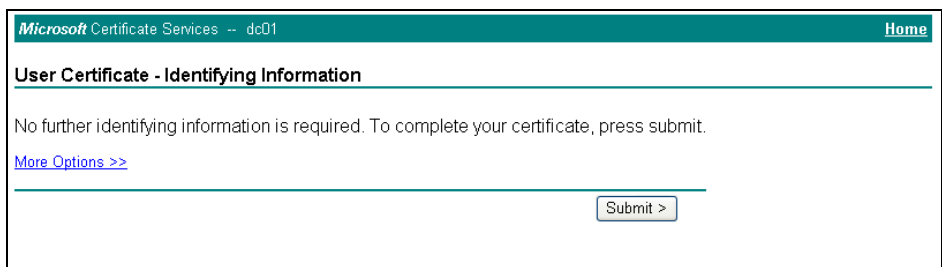
5. Cliquez sur **User Certificate** (Certificat utilisateur) dans la page suivante qui s'affiche.



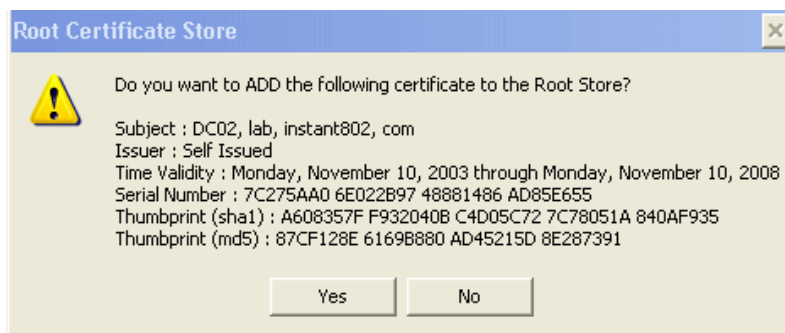
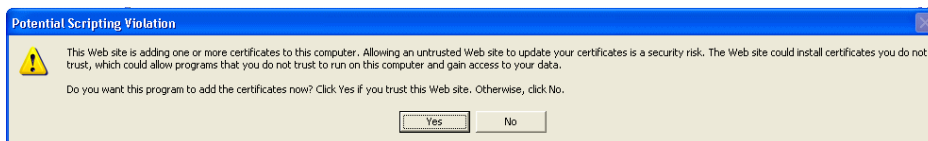
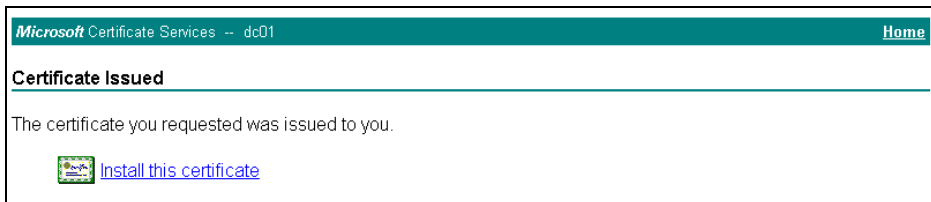
6. Cliquez sur **Yes** (Oui) dans la boîte de dialogue affichée pour installer le certificat.



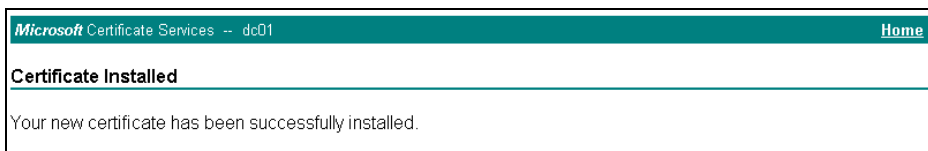
7. Cliquez sur **Submit** (Envoyer) pour terminer et sur **Yes** (Oui) pour confirmer l'envoi dans la fenêtre contextuelle.



8. Cliquez sur **Install this certificate** (Installer ce certificat) pour installer le certificat généré sur votre station client. (De même, cliquez sur **Yes (Oui)** dans la fenêtre contextuelle pour confirmer l'installation et ajouter le certificat à la racine.)



Un message de réussite s'affiche alors pour indiquer que le certificat est désormais installé sur le client.



B.11 Configuration du serveur RADIUS pour les balises VLAN

Un réseau local virtuel (VLAN) est un regroupement de ports sur un commutateur ou un regroupement de ports sur différents commutateurs. Les VLAN dynamiques vous permettent d'attribuer un utilisateur à un réseau VLAN et les commutateurs utilisent dynamiquement ces informations pour configurer le port automatiquement sur le commutateur.

La sélection du VLAN est généralement fondée sur l'identité de l'utilisateur. Le serveur RADIUS informe le NAS (le point d'accès par exemple) du réseau virtuel sélectionné dans le cadre de l'authentification. Cette configuration permet aux utilisateurs de VLAN dynamiques de se déplacer d'un site à un autre sans intervention et sans avoir à apporter des modifications aux commutateurs.

Dans le cas de la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway, si l'utilisateur a choisi d'utiliser un serveur RADIUS externe (configuré sur la page *Security* [Sécurité]), un serveur RADIUS externe essaiera d'authentifier l'utilisateur. Les informations d'authentification de l'utilisateur sont transmises à un serveur RADIUS. Si ces éléments sont valides, le NAS configure le port sur le VLAN indiqué par le serveur d'authentification RADIUS.

B.11.1 Configuration d'un serveur RADIUS

Un serveur RADIUS doit être configuré pour utiliser les attributs Tunnel dans les messages d'acceptation d'accès pour informer le point d'accès sur le VLAN sélectionné. Ces attributs sont définis dans RFC 2868 et leur utilisation pour le VLAN dynamique est spécifiée dans RFC 3580.

Dans le cas d'un serveur FreeRADIUS, les options suivantes peuvent être définies dans le fichier utilisateurs pour ajouter les attributs nécessaires.

```
example-user Auth-Type :=EAP, User-Password == « mot de passe »
```

```
Tunnel-Type = 13,
```

```
Tunnel-Medium-Type = 6,
```

```
Tunnel-Private-Group-ID = 7
```

Tunnel-Type et Tunnel-Medium-Type utilisent les mêmes valeurs pour toutes les stations. Tunnel-Private-Group-ID est l'ID VLAN sélectionné. Toutefois, il peut être différent pour chaque utilisateur.

ANNEXE C

DÉPANNAGE

C.1 Problèmes et solutions relatifs au système de distribution sans fil (WDS)	47
C.2 Rétablissement de cluster.	48
C.2.1 Redémarrer ou réinitialiser le point d'accès	48

Cette section fournit des informations sur la manière de résoudre les problèmes les plus courants que vous pourriez rencontrer au cours des mises à jour des configurations réseau sur les réseaux desservis par plusieurs points d'accès en cluster.

C.1 Problèmes et solutions relatifs au système de distribution sans fil (WDS)

Si vous rencontrez des difficultés pour la configuration d'une liaison WDS, assurez-vous d'avoir lu les notes et les mises en garde dans la section « Configuration des paramètres WDS » à la page 219. Ces notes sont réimprimées ici pour votre commodité. Les problèmes les plus courants rencontrés par les administrateurs lors des configurations WDS, c'est d'oublier de définir les deux points d'accès de la liaison sur le même canal radio et le même mode IEEE 802.11. Cette condition préalable, ainsi que d'autres, est répertoriée dans les remarques ci-dessous.



Remarques :

Lorsque vous utilisez WDS, assurez-vous de configurer les paramètres WDS sur les deux points d'accès participant à la liaison WDS.

Vous ne pouvez avoir qu'une seule liaison WDS entre toute paire de points d'accès. Autrement dit, une adresse MAC distante ne peut apparaître qu'une seule fois sur la page WDS pour un point d'accès particulier.

Les deux points d'accès qui participent à une liaison WDS doivent se trouver sur le même canal radio et utiliser le même mode IEEE 802.11. (Reportez-vous à la section « Configuration des paramètres radio » à la page 177 pour plus d'informations sur la configuration du mode et du canal radio.) Pour plus d'informations sur IEEE 802.11h, reportez-vous à la section « 802.11h Regulatory Domain Control (Contrôle du domaine réglementaire 802.11h) » à la page 155.

Assurez-vous que STP (Spanning Tree Protocol) est activé pour empêcher la redondance des chemins et les boucles avec les ponts WDS ou des combinaisons de connexions filaire (Ethernet) et de ponts WDS. Si STP est activé, vous pouvez utiliser WDS pour créer des liaisons de sauvegarde. Si STP est désactivé, gardez les règles suivantes à l'esprit :

- *Deux points d'accès ne peuvent être connectés que par un seul chemin ; un pont WDS (sans fil) ou une connexion Ethernet (filaire), mais pas les deux à la fois.*
- *Ne créez pas de liaisons de « sauvegarde ».*

- *Si vous pouvez tracer plus d'un chemin entre n'importe quelle paire de points d'accès, traversant n'importe quelle combinaison de liaisons Ethernet ou WDS, vous obtenez une boucle.*
- *Vous ne pouvez étendre ou ponter que le réseau interne ou invité, mais pas les deux.*

C.2 Rétablissement de cluster

Dans les cas où les points d'accès d'un cluster sont désynchronisés ou qu'un point d'accès ne peut pas rejoindre ou être supprimé d'un cluster, les méthodes suivantes pour rétablir le cluster sont recommandées.

C.2.1 Redémarrer ou réinitialiser le point d'accès

Ces méthodes de rétablissement sont indiquées dans l'ordre dans lequel vous devriez les essayer. Dans tous les cas, à l'exception du dernier (l'arrêt de mise en cluster), vous n'avez pas besoin de réinitialiser ou de redémarrer le point d'accès particulier dont la configuration n'est pas synchronisée avec les autres membres du cluster ou qui ne peut pas supprimer/rejoindre le cluster.

- Redémarrez physiquement le point d'accès via le cycle de mise sous tension (en appuyant sur le bouton de mise sous tension pour l'éteindre, puis le rallumer).
- Réinitialisez le point d'accès depuis son interface d'administration. Pour ce faire, accédez à <http://AdresseIPduPointdAccès>, accédez à **Reset Configuration** (Réinitialiser la configuration), puis cliquez sur le bouton **Reset** (Réinitialiser). (Les adresses IP des points d'accès sont sur la page Cluster > Access Points (Cluster > Points d'accès) pour n'importe quel membre du cluster.)

ANNEXE

D

GLOSSAIRE

0-9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

0-9

802

IEEE 802 (*IEEE Std. 802-2001*) est une famille de normes pour la communication poste à poste sur un **LAN**. Ces technologies utilisent un média partagé, avec diffusion d'informations pour une réception par toutes les stations. Les fonctionnalités de communications de base sont fournies par paquets. L'unité de base de transmission est une séquence d'octets de données (8 bits), qui peut avoir n'importe quelle longueur dans une plage qui dépend du type de **LAN**.

Sont inclus dans la famille 802 de normes **IEEE** les définitions de pont, la gestion et les protocoles de sécurité.

802.11

IEEE 802.11 (*IEEE Std. 802.11-1999*) est une spécification Medium Access Control (**MAC**) et de couche physique (**PHY**) pour la connectivité sans fil pour les stations fixes, portatives et itinérantes dans une zone locale. Elle utilise l'étalement de spectre à séquence directe (DSSS) dans la bande ISM 2,4 GHz et prend en charge des débits de données brutes de 1 et 2 Mbit/s. Elle a été officiellement adoptée en 1997, mais a été pratiquement remplacée par *802.11b*.

IEEE 802.11 est également utilisé généralement comme nom de référence pour la famille de normes **IEEE** pour les réseaux locaux sans fil.

802.11a

IEEE 802.11a (*IEEE Std. 802.11A-1999*) est une norme **PHY** qui spécifie le fonctionnement dans la bande U-NII 5 GHz via le multiplexage par répartition orthogonale de la fréquence (OFDM). Elle prend en charge les débits de données allant de 6 à 54 Mbit/s.

802.11a Turbo

IEEE 802.11a Turbo est une variante de la norme propriétaire **802.11a** d'*Atheros Communications*. Elle prend en charge les débits de transmission de données accélérés allant de 6 à 108 Mbit/s. Turbo Atheros 5 GHz est le mode IEEE 802.11a Turbo. Turbo Atheros 2,4 GHz est le mode IEEE 802.11g Turbo.

802.11b

IEEE 802.11b (*IEEE Std. 802.11b-1999*) est une amélioration de la première norme **802.11 PHY** permettant d'inclure des débits de données de 5,5 Mbit/s et 11 Mbit/s. Elle utilise l'étalement de spectre à séquence directe (DSSS) ou l'étalement de spectre par saut de fréquence (FHSS) dans la bande ISM 2,4 GHz ainsi que le Complementary Code Keying (CCK) pour fournir les débits de données les plus élevés. Elle prend en charge les débits de données allant de 1 à 11 Mbit/s.

802.11d

IEEE 802.11d définit des règles standard pour le fonctionnement des réseaux LAN sans fil IEEE 802.11 dans n'importe quel pays sans devoir procéder à une nouvelle configuration. Les exigences PHY telles que fournir des tableaux de saut de fréquence, des canaux acceptables et des niveaux de puissance pour chaque pays sont fournies. L'activation de la prise en charge de la norme IEEE 802.11d sur le point d'accès déclenche la diffusion par le point d'accès du pays dans lequel il fonctionne parmi ses balises. Les stations client utilisent ensuite ces informations. Cela est particulièrement important pour le fonctionnement des points d'accès dans les bandes IEEE 802.11a 5 GHz car l'utilisation de ces fréquences varie énormément d'un pays à l'autre.

802.11e

IEEE 802.11e est encore une norme **IEEE** provisoire (la version la plus récente est D5.0, juillet 2003). Un sous-ensemble actuellement disponible de la norme 802.11e est la norme *Wireless Multimedia Enhancements* (**WMM**).

IEEE 802.11e est une norme **IEEE** en développement d'améliorations **MAC** visant à prendre en charge **QoS**. Elle fournit un mécanisme pour déterminer la priorité du trafic dans **802.11**. Elle définit les modifications autorisées dans l'espace indépendant d'arbitrage (AIFS), une taille de fenêtre de contention minimale et maximale, et la longueur maximale (en μ sec) d'une salve de données.

802.11f

IEEE 802.11f (IEEE Std. 802.11f-2003) est une norme qui définit le protocole entre points d'accès (**IAPP**) pour les points d'accès (concentrateurs sans fil) dans un Extended Service Set (**ESS**). La norme définit comment les points d'accès communiquent les associations et les réassociations à leurs stations mobiles.

802.11g

IEEE 802.11g (IEEE Std. 802.11g 2003) est une extension de vitesse supérieure (jusqu'à 54 Mbit/s) de la norme **802.11bPHY**, tout en fonctionnant dans la bande 2,4 GHz. Elle utilise le multiplexage par répartition orthogonale de la fréquence (OFDM). Elle prend en charge les débits de données allant de 1 à 54 Mbit/s.

802.11h

IEEE 802.11h est une norme utilisée pour résoudre le problème des interférences qui existait dans la norme 802.11a. Les deux systèmes utilisés pour réduire les interférences dans 802.11h sont le contrôle de la puissance de transmission (TPC) et la sélection dynamique des fréquences (DFS). DFS détecte les autres points d'accès sur la même fréquence et les redirige vers un autre canal. TPC réduit la puissance de sortie de la fréquence de réseau du point d'accès, ce qui permet de réduire les risques d'interférence. Il s'agit d'une norme obligatoire en Europe, au Japon et aux États-Unis.

802.11i

IEEE 802.11i / WPA2 a été finalisé et ratifié en juin 2004.

IEEE 802.11i est une norme **IEEE** complète pour la sécurité dans un réseau local sans fil (**WLAN**) qui décrit **WI-FI Protected Access 2 (WPA2)**. Elle définit des améliorations sur la couche **MAC** pour contrer certaines des faiblesses de **WEP**. Elle intègre des techniques de cryptage plus fortes que le **WI-FI Protected Access (WPA)** d'origine, tel que l'Advanced Encryption Standard (**AES**).

Le **WPA** d'origine, qui peut être considéré comme un sous-ensemble de 802.11i, utilise **Temporal Key Integrity Protocol (TKIP)** pour le cryptage. WPA2 est rétrocompatible avec les produits qui prennent en charge le WPA d'origine.

802.11j

IEEE 802.11j normalise les puces qui peuvent utiliser les bandes radio 4,9 et 5 GHz conformément aux règles spécifiées par le gouvernement japonais pour ouvrir les deux bandes aux applications LAN sans fil internes, externes et mobiles. Ces règlements exigent que les entreprises règlent la largeur de ces canaux. IEEE 802.11j permet aux appareils sans fil d'accéder à des canaux précédemment indisponibles en tirant profit de nouvelles fréquences et de nouveaux modes de fonctionnement. C'est partiellement une tentative visant à atténuer l'encombrement sur les ondes, et cette norme a des relations tangentielles à la norme IEEE 802.11h.

802.11k

IEEE 802.11k est une norme **IEEE** en développement pour les réseaux sans fil (**WLAN**) qui permet la gestion automatique de la sélection du **Channel - Canal**, du **Roaming - Itinérance** client et de l'utilisation d'**Access Point - Point d'accès** (AP) du réseau. Les réseaux compatibles 802.11K équilibrent automatiquement la charge du trafic réseau sur les points d'accès pour améliorer les performances réseau et empêcher la sousutilisation ou surutilisation d'un point d'accès. 802.11K complètera finalement la norme **802.11e** de qualité de service (**QoS**) en assurant une qualité de service pour le multimédia sur une liaison sans fil.

802.1p

802.1p est une extension de la norme IEEE 802 responsable de la disposition QoS. L'objectif principal de 802.1p est de hiérarchiser le trafic réseau au niveau de la couche de liaison de données/MAC. 802.1p offre la possibilité de filtrer le trafic de multicast pour assurer qu'il n'augmente pas sur les réseaux commutés de couche 2. Il utilise des trames balises pour la hiérarchisation des priorités.

Afin d'être conformes à cette norme, les commutateurs de couche 2 doivent être capables de regrouper les paquets entrants LAN en plusieurs catégories de trafic.

802.1Q

IEEE 802.1Q est la norme **IEEE** pour les *réseaux locaux virtuels* (**VLAN**) spécifiques aux technologies sans fil. (Reportez-vous à <http://www.ieee802.org/1/pages/802.1Q.html>.)

La norme répond au problème de partage des grands réseaux en petites parties pour éviter que le trafic de données de diffusion et multicast consomme plus de bande passante que nécessaire. 802.11Q fournit également une meilleure sécurité entre les segments de réseaux internes. La spécification 802.1Q fournit une méthode standard d'insertion d'informations d'appartenance VLAN dans des trames Ethernet.

802.1x

IEEE 802.1x (IEEE Std. 802.1X-2001) est une norme de transfert des paquets **EAP** sur un réseau **802.11** sans fil via un protocole appelé *EAP Encapsulation Over LANs* (EAPOL). Elle établit un cadre qui prend en charge plusieurs méthodes d'authentification.

IEEE 802.1x authentifie les utilisateurs, pas les machines.

802.2

IEEE 802.2 (*IEEE Std. 802.2.1998*) définit la couche **LLC** pour la famille de normes **802**.

802.3

IEEE 802.3 (IEEE Std. 802.3-2002) définit la couche **MAC** pour les réseaux qui utilisent **CSMA/CA**. *Ethernet* est un exemple de ce type de réseau.

A

Access Point - Point d'accès

Lorsqu'un point d'accès est connecté à un réseau filaire et qu'il prend en charge un ensemble de stations sans fil, il est désigné comme un Basic Service Set (**BSS**). Un Extended Service Set (**ESS**) est créé en combinant au moins deux BSS.

Un *point d'accès* est le concentrateur de communication pour les appareils sur un **WLAN**, assurant une connexion ou un pont entre les appareils de réseau filaire et sans fil. Il prend en charge une *Wireless Networking Framework - Infrastructure de réseau sans fil* appelée *Infrastructure Mode - Mode infrastructure*.

Ad hoc Mode - Mode Ad-hoc

Le mode Ad-hoc est également appelé *mode « poste-à-poste »* ou Independent Basic Service Set (**IBSS**).

Le mode Ad-hoc est une **Wireless Networking Framework - Infrastructure de réseau sans fil** dans laquelle les stations communiquent directement les unes avec les autres. Il est utile pour établir un réseau rapidement dans des situations où une infrastructure formelle n'est pas nécessaire.

AES

Des informations complémentaires sont disponibles sur le [site Web de NIST](#).

L'*Advanced Encryption Standard* (AES) est une technique de cryptage de blocs de données 128 bits symétriques développée pour remplacer le cryptage DES. AES fonctionne sur plusieurs couches réseau simultanément.

Atheros XR (plage étendue)

Atheros Extended Range (XR) est une méthode propriétaire pour la mise en œuvre de trafic à faible débit sur des distances plus longues. Elle est conçue pour être transparente pour les clients et les points d'accès compatibles XR et conçue pour une interopérabilité avec la norme 802.11 en modes 802.11g et 802.11a. Il n'y a pas de prise en charge d'Atheros XR dans 802.11b, Atheros Turbo 5 GHz ou Atheros Dynamic Turbo 5 GHz.

B

Basic Rate Set - Ensemble de débits de base

L'*ensemble de débits de base* définit les débits de transmission obligatoires pour n'importe quelle station désirant rejoindre ce réseau sans fil. Toutes les stations doivent pouvoir recevoir des données aux débits indiqués dans cet ensemble.

Beacon - Balise

Les trames de balise fournissent le « pouls » d'un **WLAN**, en annonçant l'existence du réseau et en autorisant les stations à établir et à maintenir les communications dans un ordre donné. Une balise transmet les informations suivantes (dont une partie est optionnelle) :

- Le *Timestamp (horodatage)* est utilisé par les stations pour mettre à jour leur horloge à l'heure locale, permettant la synchronisation entre les stations associées.
- Le *Beacon interval (intervalle de balise)* définit l'intervalle de temps entre la transmission des trames de balise. Avant de passer en mode d'économie d'énergie, une station a besoin de l'intervalle de balise pour savoir à quel moment s'activer pour recevoir la balise.
- La *Capability information (information de capacité)* énumère les exigences pour les stations qui souhaitent rejoindre le **WLAN**. Par exemple, elle indique que toutes les stations doivent utiliser **WEP**.
- Le *Service Set Identifier (SSID)*.
- Le *Basic Rate Set - Ensemble de débits de base* est un bitmap qui répertorie les débits que le **WLAN** prend en charge.
- Les *Parameter Sets (ensembles de paramètres)* en option indiquent les fonctionnalités des méthodes de signalisation utilisées (par exemple, étalement de spectre par saut de fréquence, étalement de spectre à séquence directe, etc.).
- La *Traffic Indication Map (carte d'indication du trafic)* (TIM) en option identifie les stations utilisant le mode d'économie d'énergie qui ont des trames de données mises en file d'attente pour elles.

Bridge - Pont

Une connexion entre deux réseaux locaux (**LAN**) utilisant le même protocole, comme Ethernet ou **IEEE 802.1x**.

Broadcast - Diffusion

Certains modes de sécurité sans fil font la distinction entre la manière dont les trames de monodiffusion, multicast et de diffusion sont cryptées ou si elles sont cryptées.

Reportez-vous également à *Unicast - Monodiffusion* et *Multicast*.

Une *diffusion* envoie le même message en même temps à tout le monde. Dans les réseaux sans fil, la diffusion fait généralement référence à une interaction dans laquelle le point d'accès envoie le trafic de données sous forme de **Frame - Trame IEEE 802.1x** à toutes les stations client sur le réseau.

Broadcast Address - Adresse de diffusion

Reportez-vous à **IP Address - Adresse IP**.

BSS

Un *basic service set* (BSS) est une **Infrastructure Mode - Mode infrastructure Wireless Networking Framework - Infrastructure de réseau sans fil** avec un seul point d'accès. Reportez-vous également à Extended Service Set (**ESS**) et Independent Basic Service Set (**IBSS**).

BSSID

En **Infrastructure Mode - Mode infrastructure**, l'identificateur **BSSID** (*Basic Service Set Identifier*) est l'adresse **MAC** 48 bits de l'interface sans fil de l'**Access Point - Point d'accès**.

C

CCMP

AES-CCMP nécessite l'utilisation d'un coprocesseur matériel pour fonctionner.

Counter mode/CBC-MAC Protocol (CCMP) est une méthode de cryptage pour **802.11h** qui utilise **AES**. Elle utilise un mode de fonctionnement **CCM**, associant le mode Cipher Block Chaining Counter (CBC-CTR) et le code Cipher Block Chaining Message Authentication Code (CBC-MAC) pour le cryptage et l'intégrité des messages.

CGI

La *Common Gateway Interface* (CGI) est une norme pour exécuter les programmes externes à partir d'un serveur **HTTP**. Elle indique comment transmettre des arguments au programme d'exécution dans le cadre de la requête **HTTP**. Elle peut également définir un ensemble de variables d'environnement.

Un programme CGI est un moyen courant pour un serveur **HTTP** d'interagir dynamiquement avec les utilisateurs. Par exemple, une page HTML contenant un formulaire peut utiliser un programme CGI pour traiter les données de formulaire une fois qu'il a été validé.

Channel - Canal

Le *canal* définit la partie du spectre que la radio utilise pour émettre et recevoir. Chaque norme **802.11** offre un nombre de canaux, en fonction de la manière dont le spectre est mis sous licence nationale et transnationale par les autorités telles que la Federal Communications Commission (FCC), l'European Telecommunications Standards Institute (ETSI), la Korean Communications Commission, ou le Telecom Engineering Center (TELEC).

CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) est un protocole d'arbitrage/de contention réseau de faible niveau. Une station écoute le contenu multimédia et tente de transmettre une trame lorsque le canal est silencieux. Lorsqu'elle détecte que le canal est inactif, la station transmet le paquet. Si elle détecte que le canal est occupé, la station attend une durée aléatoire puis tente à nouveau d'accéder au contenu multimédia.

CSMA/CA est à la base de la Distributed Control Function (Fonction de contrôle distribué) (**DCF**) de la norme IEEE 802.11e. Reportez-vous également à **RTS** et **CTS**.

Le protocole CSMA/CA utilisé par les réseaux **802.11** est une variante du protocole CSMA/CD (utilisé par les réseaux **Ethernet**). Dans CSMA/CD, l'accent est mis sur la *détection* de collision tandis qu'avec CSMA/CA, l'accent est mis sur le *contournement* de collision.

CTS

Un message *Clear to Send* (*prêt à envoyer*) (CTS) est un signal envoyé par une station client **IEEE 802.11** en réponse à un message *Request to Send* (*demande d'envoi*) (**RTS**). Le message CTS indique que le canal est libre pour que l'expéditeur du message RTS lance le transfert de données. Les autres stations attendront pour ne pas encombrer les ondes. Ce message fait partie du protocole IEEE 802.11 **CSMA/CA**. (Reportez-vous également à **RTS**.)

D

DCF

La *Distribution Control Function* (*fonction de contrôle de distribution*) est un composant de la norme de technologie QoS (Qualité de service) d'IEEE 802.11e. La DCF coordonne l'accès au canal entre plusieurs stations sur un réseau sans fil en contrôlant des temps d'attente pour accéder aux canaux. Les temps d'attente sont déterminés par un minuteur d'interruption aléatoire, configurable en définissant des fenêtres de contention minimale et maximale. Reportez-vous également à **EDCF**.

DHCP

Le protocole *Dynamic Host Configuration Protocol* (*DHCP*) spécifie la manière dont un serveur central peut fournir dynamiquement des informations de configuration de réseau aux clients. Un serveur DHCP « offre » une « location » (pour une durée préconfigurée. Reportez-vous à **Lease Time - Durée de location**) au système client. Les informations fournies incluent les adresses IP du client, son masque réseau et l'adresse de ses serveurs *DNS* et *Gateway - Passerelle*.

DNS

Le *Domain Name Service* (DNS) est un service de requêtes d'usage général utilisé pour convertir des *noms complets* en adresses Internet. Un nom complet est composé du nom d'hôte d'un système, plus son nom de domaine. Par exemple, *www* est le nom d'hôte d'un serveur Web et *www.psionteklogix.com* est le nom complet de ce serveur. DNS convertit le nom de domaine *www.psionteklogix.com* en adresse IP, par exemple 66.93.138.219.

Un *nom de domaine* identifie une ou plusieurs adresses IP. Réciproquement, une adresse IP peut correspondre à plus d'un nom de domaine.

Un nom de domaine a un suffixe indiquant le *domaine de niveau supérieur* (TLD) auquel il appartient. Tous les pays possèdent leur propre domaine de niveau supérieur, par exemple .de pour l'Allemagne, .fr pour la France, .jp pour le Japon, .tw pour Taïwan, .uk pour le Royaume-Uni, .us pour les États-Unis, et ainsi de suite. Il existe également .com pour les entités commerciales, .edu pour les établissements scolaires, .net pour les opérateurs de réseau et .org pour d'autres organisations, ainsi que .gov pour le gouvernement des États-Unis et .mil pour ses services armés.

DOM

Le *Document Object Model* (DOM) est une interface qui permet aux programmes et aux scripts d'accéder et de mettre à jour dynamiquement le contenu, la structure et le style des documents. Le modèle DOM vous permet de modéliser les objets dans un document HTML ou XML (texte, liens, images, tableaux), en définissant les attributs de chaque objet et la manière dont il peut être manipulé.

Vous trouverez plus de détails sur le modèle DOM à la section W3C.

DTIM

Le message *Delivery Traffic Information Map* (DTIM) est un élément inclus dans certaines trames de *Beacon - Balise*. Il indique quelles stations client, actuellement en veille en mode faible puissance, ont des données mises en mémoire tampon sur le point d'accès (*Access Point - Point d'accès*) en attente d'enlèvement. Une partie du message DTIM indique la fréquence à laquelle la radio doit rechercher des données en mémoire tampon.

Dynamic IP Address - Adresse IP dynamique

Reportez-vous à *IP Address - Adresse IP*.

E

EAP

Le protocole *Extensible Authentication Protocol* (EAP) est un protocole d'authentification qui prend en charge plusieurs méthodes, comme les cartes de jeton, Kerberos, les mots de passe à usage unique, les certificats, l'authentification de clé publique, et les cartes à puce.

Les variations du protocole EAP incluent EAP Cisco Wireless (LEAP), Protected EAP (PEAP), EAP-TLS et EAP Tunnelled TLS (EAP-TTLS).

EDCF

Enhanced Distribution Control Function (fonction de contrôle de distribution améliorée) est une extension de *DCF*. EDCF, composant de la norme IEEE Wireless Multimedia (WMM) standard, fournit l'accès prioritaire aux supports sans fil.

ERP

Le protocole *Extended Rate Protocol (ERP)* fait référence au protocole utilisé par les stations **IEEE 802.11g** (débits de transmission de plus de 20 Mbit/s à 2,4 GHz) lorsqu'il est couplé à l'Orthogonal Frequency Division Multiplexing (multiplexage par répartition orthogonale de la fréquence) (OFDM). Intégré dans ERP et la norme **IEEE 802.11g**, on trouve un schéma d'interopérabilité effective des stations IEEE 802.11g avec des nœuds IEEE 802.11b sur le même canal.

Les anciens appareils IEEE 802.11b ne peuvent pas détecter les signaux ERP-OFDM utilisés par les stations IEEE 802.11g, et ceci peut entraîner des collisions entre des trames de données de stations IEEE 802.11b et IEEE 802.11g.

Reportez-vous également au protocole *CSMA/CA*.

S'il y a un mélange de nœuds 802.11b et 802.11g sur le même canal, les stations IEEE 802.11g le détectent via un indicateur ERP sur le point d'accès et activent une protection *Request to Send (RTS)* et *Clear to Send (CTS)* avant d'envoyer des données.

ESS

Un *Extended Service Set (ESS)* est une **Infrastructure Mode - Mode infrastructure Wireless Networking Framework - Infrastructure de réseau sans fil** avec plusieurs points d'accès, formant un seul sous-réseau qui peut prendre en charge plus de clients qu'un Basic Service Set (**BSS**). Chaque point d'accès prend en charge un certain nombre de stations sans fil, offrant une couverture sans fil plus large pour un grand espace, par exemple, un bureau.

Ethernet

Ethernet est une architecture de réseau local (**LAN**) prenant en charge des débits de transfert de données de 10 Mbit/s à 1 Gbit/s. La spécification Ethernet est à la base de la norme **IEEE802.3**, qui spécifie les couches physique et logicielle inférieure. Elle utilise la méthode d'accès *CSMA/CA* pour traiter les demandes simultanées.

Ethernet prend en charge les débits de données de 10 Mbit/s, *Fast Ethernet* prend en charge 100 Mbit/s et *Gigabit Ethernet* prend en charge 1 Gbit/s. Ses câbles sont classés comme « *XbaseY* », *X* étant le débit de transfert des données en Mbit/s et *Y* étant la catégorie du câblage. Le câble d'origine était *10Base5* (Thicknet ou « Câble jaune »). Il y a aussi *10Base2* (Cheapernet), *10baseT* (paire torsadée) et *100baseT* (Fast Ethernet). Ces deux derniers sont généralement fournis via un câblage *CAT5* avec des connecteurs *RJ-45*. Il y a également *1000Base-T* (Gigabit Ethernet).

F

Frame - Trame

Une *trame* se compose d'une partie discrète de données ainsi que de méta-informations descriptives fournies pour la transmission sur un réseau sans fil. Chaque trame inclut une adresse *MAC* source et destination, un champ de contrôle avec la version de protocole, le type de trame, le numéro de séquence de la trame, le corps de la trame (avec les informations devant être transmises) et la séquence de contrôle de trame pour la détection d'erreur. Une trame s'apparente à un *Packet - Paquet*, à la différence qu'un paquet fonctionne sur la couche réseau (couche 3 du modèle OSI) tandis qu'une trame fonctionne sur la couche Data-Link (couche 2 du modèle *OSI*).

G

Gateway - Passerelle

Avant qu'un hôte sur un *LAN* puisse accéder à Internet, il a besoin de connaître l'adresse de la *passerelle par défaut*.

Une *passerelle* est un nœud de réseau faisant office de point d'entrée vers un autre réseau. Une passerelle fournit également souvent un serveur proxy et un pare-feu. Elle est associée à un routeur, qui utilise les en-têtes et les tables de routage pour déterminer où les paquets sont envoyés, et à un commutateur ou pont, qui fournit le chemin d'entrée et de sortie de la passerelle pour le paquet.

H

HTML

Le langage *Hypertext Markup Language* (*HTML*) définit la structure d'un document sur le World Wide Web. Il utilise des balises et des attributs pour indiquer une mise en page pour le document.

Les documents HTML sont envoyés par le serveur au navigateur via *HTTP*. Reportez-vous également à *XML*.

Un document HTML commence par une balise <html> et se termine par une balise </html>. Un document formaté correctement contient également une section <head> ... </head>, qui contient les métadonnées servant à définir le document et une section <body> ... </body>, qui contient son contenu. Son langage de balisage est dérivé du *Standard Generalized Markup Language* (SGML).

HTTP

Le protocole *Hypertext Transfert Protocol* (*HTTP*) définit comment les messages sont formatés et transmis sur le World Wide Web. Un message HTTP se compose d'une **URL** et d'une commande (GET, HEAD, POST, etc.), une demande suivie d'une réponse.

HTTPS

Le protocole HTTPS (Secure Hyper Text Transfer Protocol) est la version sécurisée de HTTP, le protocole de communication du World Wide Web. HTTPS est intégré au navigateur. Si vous utilisez HTTPS, vous remarquerez une icône en forme de cadenas fermé dans l'angle inférieur de la page de votre navigateur.

Toutes les données envoyées via HTTPS sont cryptées, ce qui permet d'assurer une transaction sécurisée.

I

IAPP

Le protocole *Inter Access Point Protocol* (IAPP) est une norme **IEEE (802.11f)** qui définit les communications entre les points d'accès dans un « système de distribution ». Cela inclut l'échange d'informations sur les stations mobiles et la maintenance de tables de routage de ponts, plus la sécurisation des communications entre les points d'accès.

IBSS

Un *Independent Basic Service Set* (IBSS) est une **Ad hoc Mode - Mode Ad-hoc Wireless Networking Framework - Infrastructure de réseau sans fil** dans laquelle les stations communiquent directement les unes avec les autres.

IEEE

L'Institute of Electrical and Electronic Engineers (IEEE) est une organisation de normes internationales qui développe et établit des normes industrielles relatives à une large gamme de technologies, y compris la gamme 802 de normes sans fil et de mise en réseau. (Reportez-vous à *802*, *802.1x*, *802.11*, *802.11a*, *802.11b*, *802.11e*, *802.11f*, *802.11g* et *802.11h*.)

Pour plus d'informations sur les groupes de tâches et les normes IEEE, reportez-vous à <http://standards.ieee.org/>.

Infrastructure Mode - Mode infrastructure

Le *mode infrastructure* est une **Wireless Networking Framework - Infrastructure de réseau sans fil** sans fil dans laquelle les stations sans fil communiquent les unes avec les autres en passant au préalable par un **Access Point - Point d'accès**. Dans ce mode, les stations sans fil peuvent communiquer les unes avec les autres, ou avec des hôtes sur un réseau filaire. Le point d'accès est connecté à un réseau filaire et prend en charge un ensemble de stations sans fil.

Une infrastructure de mode infrastructure peut être fournie par un point d'accès unique (**BSS**) ou plusieurs points d'accès (**ESS**).

Intrusion Detection - Détection d'intrusion

Le *système de détection d'intrusion* (IDS) contrôle l'activité du réseau et signale les modèles suspects qui pourraient indiquer une attaque réseau ou système d'un individu tentant de s'introduire dans le système. Il signale les tentatives d'accès qui utilisent des protocoles non sécurisés non pris en charge ou inconnus.

IP

La version actuelle d'IP est *IPv4*. Une nouvelle version, appelée *IPv6* ou *IPng*, est en cours de développement. *IPv6* est une tentative de résolution du manque d'adresses IP.

L'*Internet Protocol* (protocole *Internet*) (IP) définit le format des paquets, également appelés datagrammes, ainsi que le schéma d'adressage. IP est un protocole de commutation de paquets sans connexion et de « meilleur effort ». Il fournit le routage, la fragmentation et le réassemblage des trames. Il est associé aux protocoles de niveau supérieur, tels que **TCP** ou **UDP**, pour établir la connexion virtuelle entre la destination et la source.

IP Address - Adresse IP

Il existe un nombre fini d'adresses IP qui peuvent exister. Par conséquent, un réseau local utilise généralement l'une des plages d'adresses désignées IANA pour une utilisation dans des réseaux privés. Ces plages d'adresses sont les suivantes :

10.0.0.0 à 10.255.255.255

172.16.0.0 à 172.31.255.255

192.168.0.0 à 192.168.255.255

Les systèmes sont définis par leur *adresse IP*, un numéro à quatre octets qui identifie de manière unique chaque hôte sur Internet. Il est généralement affiché sous la forme 192.168.2.254. C'est ce que l'on appelle la notation décimale à points.

Une adresse IP est divisée en deux parties : le préfixe réseau et un numéro d'hôte sur ce réseau. Un *Subnet Mask - Masque de sous-réseau* est utilisé pour définir les portions. Il existe deux numéros d'hôte spéciaux :

- La *Network Address - Adresse réseau* se compose d'un numéro d'hôte qui est « à zéro » (par exemple, 192.168.2.0).
- La *Broadcast Address - Adresse de diffusion* se compose d'un numéro d'hôte qui est « à un » (par exemple, 192.168.2.255).

Une *Dynamic IP Address - Adresse IP dynamique* est une adresse IP qui est automatiquement affectée à un hôte par un serveur *DHCP* ou un mécanisme similaire. Elle est appelée dynamique, car vous pourriez vous voir affecter une adresse IP différente à chaque fois que vous établissez une connexion.

Une *Static IP Address - Adresse IP statique* est une adresse IP qui est reliée à un hôte spécifique. Une adresse statique est généralement nécessaire pour n'importe quel hôte qui exécute un serveur, par exemple, un serveur Web.

IPSec

IP Security (IPSec) est un ensemble de protocoles qui prennent en charge l'échange sécurisé de paquets sur la couche *IP*. Il utilise des clés publiques partagées. Il existe deux modes de cryptage : Transport et Tunnel.

- Le mode *Transport* crypte uniquement la partie données (données utiles) de chaque paquet, mais conserve les en-têtes sans y apporter de modifications.
- Le mode *Tunnel* plus sécurisé crypte les en-têtes et les données utiles.

ISP - FAI

Un *fournisseur d'accès à Internet (Internet Service Provider)* (FAI) est une société qui fournit l'accès à Internet à des individus et des entreprises. Il peut fournir des services connexes tels que l'hébergement virtuel, le conseil en réseaux, la conception Web, etc.

J

Jitter - Gigue

La *gigue* est la différence entre la latence (ou retard) de transmission de paquets d'un nœud à un autre sur un réseau. Si les paquets ne sont pas transmis à une vitesse régulière (y compris *Latence*), la *QoS* pour certains types de données peut être affectée. Par exemple, les débits de transmission incohérents peuvent provoquer une distorsion de VoIP et de la diffusion de contenus multimédias. La *QoS* est conçue pour réduire l'instabilité ainsi que d'autres facteurs qui peuvent avoir un impact sur les performances réseau.

L

LAN

Un *réseau local* (Local Area Network) (LAN) est un réseau de communications couvrant une zone limitée, par exemple, les ordinateurs de votre réseau domestique ou quelques étages d'un bâtiment. Un LAN relie plusieurs ordinateurs et d'autres appareils réseau tels que stockage et imprimantes. *Ethernet* est la technologie la plus courante mettant en œuvre un réseau local (LAN).

Ethernet sans fil (*802.11*) est une autre technologie LAN très populaire (reportez-vous également à *WLAN*).

Latence

La *latence*, également appelée *délai*, est le temps nécessaire pour transmettre un *Packet - Paquet* de l'émetteur au récepteur. La latence peut se produire lorsque les données sont transmises entre le point d'accès et un client et inversement. Elle peut également avoir lieu lorsque les données sont transmises entre le point d'accès et Internet et inversement. La latence est causée par des facteurs de *réseau fixe* tels que le temps qu'il faut pour coder et décoder un paquet, et également par des facteurs de *réseau variable* tels qu'un réseau occupé ou saturé. Les fonctionnalités *QoS* sont conçues pour minimiser la latence pour le trafic réseau de haute priorité.

LDAP

Le protocole *Lightweight Directory Access Protocol (LDAP)* est un protocole d'accès de services d'annuaire en ligne. Il est utilisé pour fournir un mécanisme d'authentification. Il est basé sur la norme X.500, mais en moins complexe.

Lease Time - Durée de location

La *durée de location* indique la durée pendant laquelle le serveur **DHCP** donne à ses clients une **IP Address - Adresse IP** et d'autres informations requises. Lorsque la location expire, le client doit demander une nouvelle location. Si la location est définie sur une courte durée, vous pouvez mettre à jour vos informations de réseau et propager les informations fournies aux clients dans un délai opportun.

LLC

La couche *Logical Link Control (LLC)* contrôle la synchronisation des trames, le contrôle de flux et la vérification des erreurs. Il s'agit d'un protocole de niveau supérieur sur la couche **PHY**, fonctionnant conjointement avec la couche **MAC**.

M

MAC

Il utilise une adresse matérielle, appelée *adresse MAC*, qui identifie de façon unique chaque nœud d'un réseau. Tous les terminaux de réseau **IEEE 802** partagent un même format d'adresse MAC 48 bits, généralement affiché sous forme de chaîne de 12 chiffres hexadécimaux séparés par le caractère deux points, par exemple FE:CC:BA:09:87:65.

La couche *Media Access Control (MAC)* traite les paquets de données en déplacement entre **NIC** sur un canal partagé. Il s'agit d'un protocole de niveau supérieur sur la couche **PHY**. Il fournit un mécanisme d'arbitrage pour tenter d'empêcher les collisions de signaux.

MDI et MDI-X

Medium Dependent Interface (MDI) et *MDI crossover* (MDIX) sont des technologies de câblage à paires torsadées pour les ports Ethernet d'appareils matériels. Le câblage à paires torsadées et la détection automatique intégrés permettent la connexion entre des appareils similaires en utilisant un câble Ethernet standard. (Par exemple, si un point d'accès sans fil prend en charge MDI/MDIX, vous pouvez connecter un PC et ce point d'accès à l'aide d'un câble Ethernet plutôt que devoir utiliser un câble croisé).

MIB

MIB (Management Information Base) est une base de données virtuelle d'objets utilisés pour la gestion du réseau. Les agents *SNMP* ainsi que d'autres outils SNMP peuvent être utilisés pour contrôler tout appareil réseau défini dans la MIB.

MSCHAP V2

Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAP V2) fournit une fonction d'authentification pour les connexions *PPP* entre un ordinateur fonctionnant sous Windows et un *Access Point - Point d'accès* ou un autre appareil d'accès réseau.

MTU

La *taille maximale par unité transmise* (*Maximum Transmission Unit, MTU*) est la taille de paquet physique la plus grande, mesurée en octets, qu'un réseau peut transmettre. Tous les messages plus grands que la MTU sont fragmentés en paquets plus petits avant d'être envoyés.

Multicast

Certains modes de sécurité sans fil font la distinction entre la manière dont les trames de monodiffusion, multicast et de diffusion sont cryptées ou si elles sont cryptées.

Reportez-vous également à *Unicast - Monodiffusion* et *Broadcast - Diffusion*.

Un *multicast* envoie le même message à un groupe de destinataires. Envoyer un e-mail à une liste de diffusion est un exemple de multicast. Dans les réseaux sans fil, le multicast fait généralement référence à une interaction dans laquelle le point d'accès envoie le trafic de données sous forme de *Frame - Trame IEEE 802.1x* à un ensemble spécifique de stations client (adresses *MAC*) sur le réseau.

N

NAT

NAT sert trois buts principaux : elle offre une sécurité par obscurité en masquant les adresses IP internes, permet d'utiliser une large gamme d'adresses IP internes sans craindre de conflit avec les adresses utilisées par d'autres organisations, et autorise l'utilisation d'une seule connexion Internet.

Network Address Translation - Traduction d'adresse réseau (NAT) est une norme Internet qui masque les adresses IP internes en cours d'utilisation dans un **LAN**. Un serveur NAT exécuté sur une passerelle maintient un tableau de conversion qui cartographie toutes les adresses IP internes des requêtes sortantes à sa propre adresse et convertit toutes les requêtes entrantes sur le bon hôte interne.

Network Address - Adresse réseau

Reportez-vous à **IP Address - Adresse IP**.

NIC

Une *carte d'interface réseau* est un adaptateur ou une carte d'extension insérée dans un ordinateur pour fournir une connexion physique à un réseau. La plupart des cartes réseau sont conçues pour un type particulier de réseau, de protocole et de support, par exemple, **Ethernet** ou sans fil.

NTP

Le protocole *Network Time Protocol (NTP)* garantit la synchronisation des horloges système dans un réseau d'ordinateurs. Les serveurs NTP transmettent le *Temps universel coordonné* (UTC, également appelé *Temps moyen de Greenwich*) à leurs systèmes client. Un client NTP envoie régulièrement des requêtes d'heure aux serveurs, en utilisant l'horodateur renvoyé pour régler son horloge.

O

OSI

Le modèle de référence *Open Systems Interconnection* (OSI) est une infrastructure pour la conception de réseau. Le modèle OSI se compose de sept couches :

- La Couche 1, ou couche physique, identifie le support physique utilisée pour la communication entre les nœuds. Dans le cas des réseaux sans fil, le support physique est l'air, et les ondes de fréquence radio (RF) sont un composant de la couche physique.
- La Couche 2, ou couche Data-Link, définit comment les données à transmettre seront structurées et formatées, ainsi que des protocoles de faible niveau de communication et d'adressage. Par exemple, les protocoles tels que *CSMA/CA* et les composants tels que les adresses *MAC* et les *Frame - Trames* sont tous définis et traités comme une partie de la couche Data-Link.
- La Couche 3, ou couche réseau, définit la manière de déterminer le meilleur chemin pour faire transiter des informations par le réseau. Les *Packet - Paquets* et les *IP Address - Adresse IP* logiques fonctionnent sur la couche réseau.
- La Couche 4, ou couche de transport, définit les protocoles de connexion tels que *TCP* et *UDP*.
- La Couche 5, ou couche de session, définit les protocoles pour le lancement, la maintenance et la fin des communications et des transactions sur le réseau. Parmi les exemples courants de protocoles qui fonctionnent sur cette couche, on trouve NFS (Network File System) et SQL (Structured Query Language). Font également partie de cette couche les flux de communications comme monomode (l'appareil envoie des informations en vrac), mode semi-duplex (les appareils se relaient pour transmettre des informations en vrac), et mode duplex intégral (interactif, dans lequel les appareils transmettent et reçoivent simultanément).
- La Couche 6, ou couche de présentation, définit la manière dont les informations sont présentées à l'application. Elle comprend les méta-informations sur la manière de crypter/décrypter et compresser/décompresser les données. Les formats de fichiers JPEG et TIFF sont des exemples de protocoles de cette couche.
- La Couche 7, ou couche d'application, inclut des protocoles tels que Hypertext Transfer Protocol (*HTTP*), SMTP (Simple Mail Transfer Protocol) et FTP (File Transfer Protocol).

P

Packet - Paquet

Les données et les fichiers multimédias sont transmis entre les nœuds sur un réseau sous la forme de *paquets*. Les données et le contenu multimédia sont partagés et conditionnés dans des *paquets*. Un paquet comprend un petit bloc de contenu à envoyer, ainsi que ses adresses de destinataire et d'expéditeur. Les paquets sont transmis sur le réseau et inspectés par chaque nœud. Le nœud auquel il est adressé est le destinataire ultime.

Packet Loss - Perte de paquets

La *perte de paquets* décrit le pourcentage de paquets transmis sur le réseau qui n'a pas atteint sa destination. Une perte de paquets de 0 % indique qu'aucun des paquets n'a été perdu pendant la transmission. Les fonctionnalités *QoS* sont conçues pour minimiser la perte de paquets.

PHY

La couche physique (PHY) est la couche la plus basse dans le modèle de réseau (reportez-vous à *OSI*). La couche physique transmet le flux de bits (impulsions électriques, signal lumineux ou radio) sur le réseau au niveau électrique et mécanique. Elle fournit le moyen matériel d'envoyer et de recevoir des données sur un support, y compris la définition des câbles, les *NIC* et les aspects physiques.

Ethernet et la famille *802.11* sont des protocoles avec des composants de couche physique.

PID

Le *Process Identifier* (PID) est un nombre entier utilisé par Linux afin d'identifier de manière unique un processus. Un PID est renvoyé par l'appel système `fork()`. Il peut être utilisé par `wait()` ou `kill()` pour exécuter des actions sur le processus donné.

Port Forwarding - Transfert de port

Le *transfert de port* crée un « tunnel » via un pare-feu, ce qui permet aux utilisateurs Internet d'accéder à un service qui s'exécute sur l'un des ordinateurs de votre *LAN*, par exemple, un serveur Web, un serveur FTP ou SSH, ou d'autres services. Du point de vue de l'utilisateur extérieur, il semble que le service est en cours d'exécution sur le pare-feu.

PPP

Le *protocole point-à-point* est une norme de transmission des datagrammes de couche réseau (paquets **IP**) sur des liens point-à-point en série. Le protocole PPP est conçu pour fonctionner sur les connexions asynchrones et les systèmes synchrones orientés bits.

PPPoE

Le *protocole point-à-point sur Ethernet* (PPPoE) est une spécification pour la connexion des utilisateurs d'un **LAN** à Internet par l'intermédiaire d'un support haut débit commun, tel qu'une ligne de modem câble ou DSL unique.

PPtP

Le protocole *Point-à-point Tunnelling Protocol* (PPTP) est une technologie permettant la création d'un *réseau privé virtuel* (**VPN**) dans le *protocole point-à-point* (**PPP**). Ce protocole est utilisé pour garantir que les données transmises d'un nœud VPN à un autre soient sécurisées.

Proxy

Un *proxy* est un serveur situé entre une application client et un serveur réel. Il intercepte les requêtes et tente d'y répondre lui-même. S'il n'y parvient pas, elles sont transférées sur le véritable serveur. Les serveurs proxy ont deux buts principaux : améliorer les performances en étalant des requêtes sur plusieurs machines et filtrer les requêtes pour empêcher l'accès à certains serveurs ou services.

PSK

Pre-Shared Key - *Clé prépartagée* (PSK), reportez-vous à ***Shared Key* - Clé partagée**.

Public Key - Clé publique

Une *clé publique* est utilisée dans la cryptographie de clé publique pour crypter un message qui ne peut être décrypté qu'avec la clé privée ou secrète du destinataire. Le cryptage de clé publique est également appelé cryptage asymétrique, car il utilise deux clés, ou cryptage Diffie-Hellman. Reportez-vous également à ***Shared Key* - Clé partagée**.

Q

QoS

La norme **IEEE** pour la mise en œuvre QoS sur les réseaux sans fil est actuellement un projet du groupe de tâche **802.11e**. Un sous-ensemble de fonctionnalités **802.11e** est décrit dans la spécification **WMM**.

La qualité de service (QoS) définit les propriétés des performances d'un service réseau, y compris le débit garanti, les délais de transit et les files de priorité. QoS est conçue pour minimiser **Latence**, **Jitter - Gigue**, **Packet Loss - Perte de paquets** et l'encombrement réseau, et offre un moyen d'affecter une bande passante dédiée au trafic réseau de priorité élevée.

R

RADIUS

RADIUS (*Remote Authentication Dial-In User Service*) fournit un système d'authentification et d'audit. Il s'agit d'un mécanisme d'authentification courant pour de nombreux **ISP - FAI**.

RC4

Un chiffrement de flux symétrique fourni par *RSA Security*. Il s'agit d'un chiffrement de flux à taille de clé variable avec des opérations orientées octets. Il autorise des clés d'une longueur maximale de 2048 bits.

Roaming - Itinérance

En langage **IEEE 802.11**, les *clients itinérants* sont des stations client mobiles ou des appareils sur un réseau sans fil (**WLAN**) qui nécessitent l'utilisation de plus d'un **Access Point - Point d'accès** (AP) alors qu'ils entrent et sortent de différentes zones de service de station de base. **IEEE 802.11f** définit une norme selon laquelle les points d'accès peuvent communiquer des informations concernant les associations et dissociations clients dans la prise en charge de clients itinérants.

Router - Routeur

Un *routeur* est un appareil réseau qui transfère les paquets entre les réseaux. Il est connecté à au moins deux réseaux, souvent entre deux réseaux locaux (*LAN*) ou entre un *LAN* et un réseau étendu (*WAN*), par exemple, Internet. Les routeurs se trouvent au niveau des passerelles, des endroits où au moins deux réseaux se connectent.

Un routeur utilise le contenu des en-têtes et ses tables pour déterminer le meilleur chemin pour transférer un paquet. Il utilise des protocoles tels que le protocole ICMP (Internet Control Message Protocol), le protocole RIP (Routing Information Protocol), et le protocole PDRI (Internet Router Discovery Protocol) pour communiquer avec d'autres routeurs et configurer le meilleur routage entre deux hôtes. Le routeur exécute peu de filtrage des données qu'il transfère.

RSSI

RSSI (Received Signal Strength Indication, indicateur de niveau de signal reçu) est une valeur *802.1x* qui calcule la tension relative à la puissance du signal reçu. RSSI est une des façons différentes de mesurer et d'indiquer la puissance du signal de *fréquence radio* (RF). La puissance du signal peut également être mesurée en mW (milliwatts), dBms (décibels-milliwatts) et une valeur sous forme de pourcentage.

RTP

Real-Time Transport Protocol (RTP) est un protocole Internet pour la transmission de données en temps réel telles que les données audio et vidéo. Il ne garantit pas la livraison mais fournit des mécanismes de prise en charge pour l'envoi et la réception des applications afin d'activer les données réparties. RTP s'exécute généralement en plus du protocole *UDP*, mais peut également prendre en charge d'autres protocoles de transport.

RTS

Un message *Request to Send (demande d'envoi)* (RTS) est un signal envoyé par une station client au point d'accès, demandant l'autorisation d'envoyer un paquet de données et d'empêcher les autres stations client sans fil d'occuper les ondes radio. Ce message fait partie du protocole IEEE 802.11 *CSMA/CA*. (Reportez-vous également à *RTS Threshold - Seuil RTS* et *CTS*.)

RTS Threshold - Seuil RTS

Le *seuil RTS* spécifie la taille de paquet d'une demande d'envoi de transmission (**RTS**). Ceci permet de contrôler le flux de trafic au niveau du point d'accès et c'est particulièrement utile pour l'ajustement des performances sur un point d'accès avec un grand nombre de clients.

S

Shared Key - Clé partagée

Reportez-vous également à **Public Key - Clé publique**.

Une *clé partagée* est utilisée dans le cryptage conventionnel où une clé est utilisée à la fois pour le cryptage et le décryptage. C'est ce qu'on appelle également le cryptage à *clé secrète* ou *clé symétrique*.

SNMP

Le protocole *Simple Network Management Protocol* (SNMP) a été développé pour gérer et surveiller les nœuds sur un réseau. Il fait partie de la suite de protocoles **TCP/IP**.

SNMP se compose d'appareils gérés et de leurs agents, et d'un système de gestion. Les agents stockent des données sur leurs terminaux dans des *bases de données MIB* (*Management Information Base*) (**MIB**) et renvoient ces données sur le gestionnaire SNMP Manager sur demande.

SNMP Traps - Alertes SNMP

Les alertes SNMP permettent la communication asynchrone entre les appareils réseau et les agents gérés. Paramétrer des alertes SNMP économise les ressources réseau et élimine les requêtes SNMP redondantes.

SSID

Le *Service Set Identifier* (SSID) est une clé alphanumérique de trente-deux caractères qui identifie de façon unique un réseau local sans fil. Il est également appelé *nom de réseau*. Il n'y a aucune restriction sur les caractères qui peuvent être utilisés dans un SSID.

Static IP Address - Adresse IP statique

Reportez-vous à *IP Address - Adresse IP*.

STP

Le protocole *Spanning Tree Protocol* (STP) est un protocole de norme IEEE 802.1 (relatif à la gestion de réseau) pour les ponts *MAC* qui gèrent la redondance du circuit et empêchent la formation de boucles indésirables créées par plusieurs chemins actifs entre stations client dans le réseau. Les boucles se produisent lorsqu'il y a plusieurs routages entre les points d'accès. STP crée une arborescence qui couvre tous les commutateurs dans un réseau étendu, en faisant passer de force les chemins redondants à un état de veille ou de blocage. STP autorise un seul chemin actif à la fois entre deux appareils réseau (cela évite les boucles) mais établit des liens redondants comme sauvegarde au cas où le lien initial échouerait. Si les coûts STP changent, ou si un segment de réseau du STP est injoignable, l'algorithme STP reconfigure la topologie de l'arborescence et rétablit le lien en activant le chemin en veille. Sans STP, il est possible que les deux connexions soient simultanées en temps réel, ce qui pourrait créer une boucle infinie de trafic sur le réseau local.

Subnet Mask - Masque de sous-réseau

Un *masque de sous-réseau* est un nombre qui définit quelle partie d'une adresse IP correspond à l'adresse réseau et quelle partie correspond à une adresse hôte sur le réseau. Il est affiché sous forme de notation décimale à points (par exemple, un masque de 24 bits est affiché sous la forme 255.255.255.0) ou de numéro ajouté à l'adresse IP (par exemple, 192.168.2.0/24).

Le masque de sous-réseau permet à un routeur de déterminer rapidement si une adresse IP est locale ou doit être transmise par l'exécution d'une opération AND au niveau du bit sur le masque de sous-réseau et l'adresse IP. Par exemple, si l'adresse IP est 192.168.2.128 et que le masque réseau est 255.255.255.0, l'adresse réseau résultante est 192.168.2.0.

L'opérateur AND au niveau du bit compare deux bits et attribue 1 au résultat uniquement si les deux premiers bits sont 1. Le tableau suivant présente les détails du masque réseau :

Adresse IP	192.168.2.128	11000000 10101000 00000010 10000000
Masque réseau	255.255.255.0	11111111 11111111 11111111 00000000
Adresse réseau résultante	192.168.2.0	11000000 10101000 00000010 00000000

Supported Rate Set - Ensemble des débits pris en charge

L'*ensemble des débits pris en charge* définit les débits de transmission qui sont disponibles sur ce réseau sans fil. Toutes les stations doivent pouvoir recevoir des données aux débits indiqués dans cet ensemble. Toutes les stations doivent pouvoir recevoir des données aux débits indiqués dans l'*Basic Rate Set - Ensemble de débits de base*.

SVP

La priorité voix SpectraLink (SVP) est une approche QoS pour les déploiements Wi-Fi. SVP est une spécification ouverte qui est conforme à la norme IEEE 802.11b. SVP réduit le délai SVP et donne la priorité aux paquets voix sur les paquets de données sur le réseau local (LAN) sans fil, ce qui augmente la probabilité de meilleures performances réseau.

T

TCP

Le protocole *Transmission Control Protocol* (TCP) est une extension d'Internet Protocol (*IP*). Il ajoute une communication fiable (garantit la livraison des données), le contrôle du débit, le multiplexage (plus d'une connexion simultanée), et la transmission orientée connexion (nécessite que le destinataire d'un paquet accuse réception à l'expéditeur). Il garantit également que les paquets sont livrés dans l'ordre dans lequel ils ont été envoyés.

TCP/IP

Bien que *TCP* et *IP* soient deux protocoles spécifiques, le protocole TCP/IP est souvent utilisé pour désigner l'ensemble des protocoles basés sur eux, y compris ICMP, ARP, *UDP* et autres, ainsi que des applications s'exécutant sur ces protocoles, telles que Telnet, FTP, etc.

Internet et la plupart des réseaux locaux sont définis par un groupe de protocoles. Le plus important d'entre eux est le protocole *Transmission Control Protocol over Internet Protocol* (TCP/IP), le protocole standard de fait. TCP/IP a été développé à l'origine par la Defense Advanced Research Projects Agency (DARPA, également appelé ARPA, une agence du Ministère américain de la Défense).

TKIP

Le protocole *Temporal Key Integrity Protocol (TKIP)* fournit un vecteur d'initialisation 48 bits étendu, la construction et distribution de clé par paquets, un code Message Integrity Code (MIC, parfois appelé « Michael »), et un mécanisme de recomposition. Il utilise un chiffrement de flux **RC4** pour crypter le corps de la trame et le CRC de chaque trame **802.11** avant la transmission. Il s'agit d'un composant important des mécanismes de sécurité **WPA** et **802.11h**.

ToS

Les en-têtes de paquets **TCP/IP** incluent un champ *Type of Service (ToS)* de 3 à 5 bits défini par le développeur de l'application qui indique le type de service approprié pour les données dans le paquet. La façon dont les bits sont définis détermine si le paquet est en attente d'envoi avec des paramètres de délai minimal, débit maximal, faible coût ou « meilleur effort » moyens selon les exigences des données. Le champ ToS est utilisé par la passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway pour fournir un contrôle de configuration sur les files d'attente *qualité de service (QoS)* pour les données transmises du point d'accès vers les stations client.

U

UDP

Le protocole *User Datagram Protocol (UDP)* est un protocole de couche de transport offrant des services de datagrammes simples mais peu fiables. Il ajoute des informations d'adresse de port et une somme de contrôle à un paquet **IP**.

UDP ne garantit pas la livraison et n'exige pas une connexion. Le protocole est léger et efficace. Le traitement et la retransmission des erreurs doivent être effectués par le programme d'application.

Unicast - Monodiffusion

Certains modes de sécurité sans fil font la distinction entre la manière dont les trames de monodiffusion, multicast et de diffusion sont cryptées ou si elles sont cryptées.

Reportez-vous également à **Multicast** et **Broadcast - Diffusion**.

Une *monodiffusion* envoie un message à un seul récepteur spécifié. Dans les réseaux sans fil, monodiffusion fait généralement référence à une interaction dans laquelle le point d'accès envoie le trafic de données sous forme de **Frame - Trame IEEE 802.1x** directement à une adresse **MAC** de station client unique sur le réseau.

URL

Une *Uniform Resource Locator (URL)* est une norme de spécification de l'emplacement des objets sur Internet, par exemple un fichier ou un forum. Les URL sont largement utilisées dans les documents HTML pour spécifier la cible d'un lien hypertexte qui est souvent un autre document HTML (éventuellement stocké sur un autre ordinateur). La première partie de l'URL indique le protocole à utiliser et la seconde partie indique l'adresse IP ou le nom de domaine où cette ressource est située.

Par exemple, <ftp://ftp.devicescape.com/téléchargements/monfichier.tar.gz> indique un fichier qui doit être récupéré à l'aide du protocole FTP ; <http://www.devicescape.com/index.html> indique une page Web qui doit être extraite en utilisant le protocole **HTTP**.

UTC

Le Temps universel coordonné (UTC) est également appelé Temps moyen de Greenwich.

V

VLAN

Un *LAN virtuel* (VLAN) est un regroupement logique d'appareils sur un réseau, basé sur logiciel, qui leur permet d'agir comme s'ils étaient connectés à un réseau physique unique, bien que ce ne soit pas le cas. Les nœuds d'un VLAN partagent des ressources et une bande passante, et sont isolés sur ce réseau. La passerelle sans fil Passerelle sans fil 9160 G2 Wireless Gateway prend en charge la configuration d'un VLAN sans fil. Cette technologie est mise à profit sur le point d'accès pour la fonctionnalité de réseau invité « virtuel ».

VPN

Un *réseau privé virtuel* ou Virtual Private Network (VPN) est un réseau qui utilise Internet pour connecter ses nœuds. Il utilise le cryptage et d'autres mécanismes afin de garantir que seuls les utilisateurs autorisés accèdent à ses nœuds et que les données ne puissent pas être interceptées.

W

WAN

Internet est essentiellement un très grand WAN.

Un *réseau étendu* ou Wide Area Network (WAN) est un réseau de communications qui couvre une zone géographique relativement importante, s'étendant sur des distances supérieures à un kilomètre. Les WAN sont souvent connectés via des réseaux publics, tels que le système téléphonique. Ils peuvent également être connectés via des lignes louées ou des satellites.

WDS

Un *système de diffusion sans fil* ou Wireless Distribution System (WDS) permet la création d'une infrastructure entièrement sans fil. En général, un **Access Point - Point d'accès** est connecté à un **LAN** filaire. WDS permet aux points d'accès d'être connectés au réseau sans fil. Les points d'accès peuvent fonctionner comme relais ou ponts sans fil.

WEP

Wired Equivalent Privacy (WEP) est un protocole de cryptage pour les réseaux sans fil **802.11**. Toutes les stations et les points d'accès sans fil sur le réseau sont configurés avec une **Shared Key - Clé partagée** statique de 64 bits (clé secrète 40 bits + vecteur d'initialisation (IV) 24 bits) ou 128 bits (clé secrète 104 bits + IV 24 bits) pour le cryptage des données. Il utilise un chiffrement de flux **RC4** pour crypter le corps de la trame et le CRC de chaque trame **802.11** avant la transmission.

WI-FI

Un test et une certification d'interopérabilité pour les produits **WLAN** basés sur la norme **IEEE802.11** préconisée par Wi-Fi Alliance, une entreprise à but non lucratif.

WINS

Le *Windows Internet Naming Service* (WINS) est un processus de serveur de résolution des noms de domaine des ordinateurs fonctionnant sous Windows en adresses IP. Il fournit des informations qui permettent à ces systèmes de parcourir des réseaux distants en utilisant le *voisinage réseau*.

Wireless Networking Framework - Infrastructure de réseau sans fil

Il existe deux façons d'organiser un réseau sans fil :

- Les stations communiquent directement les unes avec les autres dans un réseau *Ad hoc Mode - Mode Ad-hoc*, également appelé Independent Basic Service Set (*IBSS*).
- Les stations communiquent via un *Access Point - Point d'accès* dans un réseau *Infrastructure Mode - Mode infrastructure*. Un point d'accès unique crée un ensemble de services de base (*BSS*) d'infrastructure, tandis que plusieurs points d'accès sont organisés dans un ensemble de services étendu (*ESS*).

WLAN

Le *réseau local sans fil* ou Wireless Local Area Network (WLAN) est un *LAN* qui utilise des ondes radio à haute fréquence plutôt que des câbles pour communiquer entre ses nœuds.

WMM

Wireless Multimedia (WMM) est une norme de technologie *IEEE* conçue pour améliorer la qualité des applications audio, vidéo et multimédia sur un réseau sans fil. Les deux points d'accès et les clients sans fil (ordinateurs portables, produits d'électronique grand public) peuvent être compatibles WMM. Les fonctionnalités WMM sont basées sur un sous-ensemble du projet de spécification *WLAN IEEE 802.11e*. Les produits sans fil qui sont construits à la norme et qui passent une série de tests de qualité peuvent recevoir le label « Wi-Fi Certified for WMM » (Certifié Wi-Fi pour WMM) pour garantir l'interopérabilité avec d'autres produits similaires. Pour plus d'informations, reportez-vous à la page WMM sur le site Web de Wi-Fi Alliance : <http://www.wi-fi.org/OpenSection/wmm.asp>.

WPA

Wi-Fi Protected Access (WPA) est une version *Wi-Fi* Alliance du projet de norme *IEEE 802.11h*. Il fournit un cryptage des données plus sophistiqué que *WEP* et également une authentification de l'utilisateur. WPA comprend les mécanismes *TKIP* et *802.1x*.

WPA2

La version Personal ne nécessite pas *IEEE 802.1x* ou *EAP*. Elle utilise un mot de passe de *clé prépartagée (PSK)* pour générer les clés nécessaires pour l'authentification.

Le **WPA** d'origine utilise Temporal Key Integrity Protocol (**TKIP**) pour le cryptage des données. WPA2 est rétrocompatible avec les produits qui prennent en charge le **WPA** d'origine.

Wi-Fi Protected Access (WPA2) est une norme de sécurité améliorée, décrite dans **IEEE 802.11h**, qui utilise Advanced Encryption Standard (**AES**) pour le cryptage des données.

WPA2, comme le **WPA** d'origine, prend en charge une version *Enterprise* et *Personal*. La version Enterprise nécessite l'utilisation de fonctionnalités de sécurité IEEE **802.1x** et une authentification *Extensible Authentication Protocol* (**EAP**) avec un serveur **RADIUS**.

WRAP

Le protocole d'authentification sans fil robuste ou *Wireless Robust Authentication Protocol* (WRAP) est une méthode de cryptage pour **802.11h** qui utilise **AES**, mais un autre mode de cryptage (**OCB**) pour le cryptage et l'intégrité.

X

XML

Le langage de balisage extensible ou *Extensible Markup Language* (XML) est une spécification développée par le **W3C**. XML est un format texte simple et souple dérivé du langage *Standard Generalized Markup Language* (SGML), conçu spécialement pour la publication électronique.

A

- Accès invité, Paramètres Ethernet 144
- access point
 - monitoring 125
- Activation et désactivation de la persistance, journaux des événements 129
- Activer les noms de terminal virtuel,**
 - Protocole Telnet 5250* 303
- administrateur
 - mot de passe
 - sur les paramètres de base 51
 - plateforme 31
- Adresse IP (station de base) 251
- Adresse IP locale à relier**
 - Protocole Telnet ANSI 311
 - Protocole Telnet 3274* 286
 - Protocole Telnet 5250* 302
- adresses IP
 - présentation des stratégies informatiques pour les points d'accès auto-gérés 33
 - 9160 G2 21
- adresses IP
 - accès 64
 - visualisation des points d'accès 57, 89
 - visualisation des points d'accès 65
- AIAG**
 - Émulation 3274* 279
 - Émulation 5250* 296
- Alarme**
 - Émulation 3274* 275
 - Émulation 5250* 291
- alimentation
 - configuration requise 18, 342
 - connexions 40
- ANSI, connexion de terminaux 23
- antenne directionnelle 19
- antenne omnidirectionnelle 19
- appareils externes 20
- associated wireless clients 136
- Aucun en ligne/Hors ligne,**
 - émulation 9010/ TCP/IP 266

authentification pour les modes de sécurité 98

Autoriser

Sessions TCP, Telnet ANSI 315

Autoriser le caractère nul

Émulation 3274 274

Émulation 5250 290

B

Balise

Interfaces, 802.IQv1 323

Période

802.IQ 320

Port UDP 802.IQv2 323

balises 802.1p 202

barre de progression pour synchronisation automatique de cluster 61

boucles, WDS 217

brochage *See port brochage*

C

cables

console port No. 19387 B-2

serial descriptions B-1

câbles

coaxial 20

canal, configuration radio 177

Canal actif

groupe MRR 257

paramètres RA1001A 248

Canal partagé

groupe MRR 254

Canal partagé, station de base 244

Caractère de correspondance masqué

Émulation 3274 283

Émulation 5250 299

Caractère de correspondance visible

Émulation 3274 281

Émulation 5250 297

cellulaire

base 238, 260

commutation 237

certificat
 obtenir un certificat TLS EAP pour le client C-38
 sécurité pour le client WPA/WPA2 Enterprise (RADIUS) C-27
 sécurité pour le IEEE 802.1x C-19

Charge de champ
Émulation 3274 284
Émulation 5250 300

Clé de cycle de session, Protocole Telnet ANSI 311

Clé de demande de session TCP, Protocole Telnet ANSI 311

Clé de dernière session active, Protocole Telnet ANSI 312

client
 associations 136
 contrôle d'intégrité de la liaison 136
 plateforme 32
 sécurité C-5
 session, définition 66
 sessions 65
 Voir aussi *stations* 177

cluster
 ajout d'un point d'accès 63
 arrêt de la mise en cluster 64
 définition 58
 dépannage D-48
 format 58
 formation 60
 gestion des canaux 77
 présentation 58
 sécurité 61
 synchronisation automatique 61
 taille et appartenance 61
 types de points d'accès pris en charge 58
 voisins 87, 89

Code-barres
Émulation 3274 284
Émulation 5250 300

Code erreur d'écriture, Émulation 5250 290

Collision
Taille
 groupe MRR 255
Taille
 radio à bande étroite 245

Combinaison, Groupe MRR 257

configuration
 mini-contrôleur 267–316
 configuration 9010 266
 configuration antenne requise 19, 20
 configuration de station de base 266
 configuration par défaut, restauration 266, 273

Configurer les noms de LU
Protocole Telnet 3274 287

Configurer les noms de terminal
Protocole Telnet 3274 304

conformité Wi-Fi 10

connectors
 RJ-45 B-3

connexion
 console 23
 Ethernet 21
 terminal à affichage vidéo 23
 terminaux compatibles ANSI 23

Connexion automatique, Telnet ANSI
 échec de la connexion 314
 ID utilisateur 314
 Mot de passe 314

Connexion automatique, Telnet ANSI
 Telnet automatique/Activation de session 312

Connexions TCP directes pour TekTerm, Fonctionnalités Radio Link 261

console
 connexion à 23
 port
 brochages B-1
 câble. 19387 B-2

Contrôle d'interrogation, émulation
 9010 / TCP/IP 266

conventions de texte 7

Convertir 7 bits en 8 bits
Émulation ANSI 309

couleurs et style de l'interface utilisateur 52

cryptage dans différents modes de sécurité 98

D

DCF
 en relation avec QoS 200
 minuteur d'interruption aléatoire 201
 débit de données, série 23
 DEC VT220, connexion 23

Délai d'échappement, *Émulation ANSI* 307

Délai de synchronisation
groupe MRR 256
radio à bande étroite 247

Délai de terminal de protocole d'interrogation en pourcentage,
Fonctionnalités Radio Link 261

Délai de terminal de protocole d'interrogation Fonctionnalités Radio Link 260

Démarrage automatique
(station de base) 251
groupe MRR 254
802.IQ 319

Démarrage automatique, mode station de base 243

démarrage du réseau 52

dépannage des problèmes de démarrage 44

Depth, Event Logs 130

DHCP, présentation en relation aux points d'accès auto-gérés 33

Données d'initialisation hôte Délai,
Émulation ANSI 310

Données d'initialisation terminal Délai,
Émulation ANSI 310

DSCP
balise 202
Priorité 204

E

EAP-PEAP
configuration sur un client IEEE 802.1x C-15
configuration sur un client WPA/WPA2 Enterprise (RADIUS) C-23

Effacer
Émulation 3274 275
Émulation 5250 292

emplacement, description 63

émulation 9010 266

émulations
ANSI 306–316
présentation 269
3274/Telnet 274, 289
5250 290–305
9010 / TCP/IP 266

Enregistrement de page
Émulation ANSI 308

Enregistrement de page tenant compte des caractères à double octet,
Émulation ANSI 308

Ensemble de caractères majuscules (GR),
Émulation ANSI 309

Ensemble de caractères minuscules (GL),
Émulation ANSI 309

Envoyer une pause IAC comme touche Attention, *Protocole Telnet* 3274 288

Envoyer un traitement d'interruptions IAC comme une demande système 287

équilibrage de la charge, configuration 191

espaces indépendants en relation avec QoS 200

Est hôte Fujitsu
Émulation 3274 274

Ethernet
cartes adaptateur 342
connexions 21, 40
connexions 21
fibre optique 100Base-FX 22
indicateur d'état LED 23
longueurs de câble 22
paramètres 141, 167
station de base 250
10BaseT
brochage B-3
10BaseT 21
100BaseT 21
brochage B-3

Ethernet 10BaseT 21

Ethernet 100BaseT 21

événements
journal 128
monitoring 128

exigences en termes d'environnement 17
humidité relative de fonctionnement 341
présentation 17
température de fonctionnement 341
température de stockage 341

exigences en termes de maintenance 18

Extended Service Set avec pontage WDS 215

É**Écho, Émulation ANSI** 307**Émulation**

configuration du mini-contrôleur 273

Émulation ANSI 306

Émulation 5250 290–305

État de la carte radio

menu de configuration radio à bande

étroite 240

Événements 128

F**Fermer les sessions hôtes au redémarrage du terminal**

Protocole Telnet ANSI 311

files d'attente, configuration de QoS 205

filtrage MAC, configuration 186

Firefox 24

Fonctionnalités Radio Link, paramètres de

configuration 258–263

fonctionnement

humidité relative 341

température 341

Fonctionnement en mode cellulaire,

fonctionnalités Radio Link 260

Fuseau horaire 328

G

gestion des canaux de points d'accès en

cluster

accès 79

affectations de canal proposées 83

affichage/paramétrage de verrouillage
82

exemple 80

paramètres avancés 84

présentation 79

gestion des clés, sécurité 98

Gravité, journaux des événements 130

Groupe MRR

Canal actif 257

Canal partagé 254

Chaîne d'indicatif 256

Combinaison 257

Délai de synchronisation 256

Démarrage automatique 254

Facteur de fenêtre libre 255

Limite du mode Message 255

Modules radio à distance 258

Nombre de fenêtres d'interrogation 254

Nombre de nouvelles tentatives 255

Numéro de groupe MRR 253

Paramètres du protocole**d'interrogation** 254

Période d'indicatif 256

Taille de collision 255

Taille des fenêtres d'interrogation 255

Taille maximale de segment de**message** 255

Txon à distance 257

Groupes MRR paramètres de

configuration 251

H**HÔTES**

configuration du mini-contrôleur 270

heure, configuration du point d'accès pour

utilisation d'un serveur NTP 328

homologations *xvi*homologations de sécurité électrique *xvi***Hôte****Délai, Émulation ANSI** 306**Impression***Émulation* 3274 277*Émulation* 5250 293**Port***Protocole Telnet ANSI* 310*Protocole Telnet* 3274 285*Protocole Telnet* 5250 301

Hôte de relais de journal pour les messages

du noyau, journaux des événements

131

Hôtes (configuration de station de base)

263–266

Hôte Telnet automatique*Protocole Telnet* 3274 288*Protocole Telnet* 5250 303**I**

icônes de l'interface utilisateur 52

ID d'interrogation Fonctionnalités Radio

Link 260

IEEE 802.1x

mode de sécurité

configuration 114

utilisation 100

IEEE 802.11

mode radio, configuration 177

IEEE 802.11a
 configuration 177
 IEEE 802.11b
 configuration 177
 IEEE 802.11g
 configuration 177
 IEEE 802.1x
 mode de sécurité
 configuration client C-15
 IEEE 802.11
 ensemble de débits, configuration 177
Impression à distance
 Émulation 3274 278
 Émulation 5250 295
 indicateurs d'état (LED) 23
Indicatif
 Chaîne
 groupe MRR 256
 Chaîne, radio à bande étroite 246
 Période
 groupe MRR 256
 Période, radio à bande étroite 246
 informations d'émission/réception 134
 Informations sur les émissions, Canada xv
 installation
 antennes 21
 câble d'alimentation 21
 exigences en termes d'environnement 341
 exigences en termes d'environnement 17
 LAN 21
 sécurité xvii
 installations LAN 21
 interface invité
 configuration 162
 explication 161
 présentation des fonctionnalités 12
 VLAN 162
 interfaces, réseau 342
 interfaces réseau 342
 Internet Explorer 24
 intervalle de balise, configuration 177
 isolation de station 106

L

LED 23

Libre

Facteur de fenêtre

groupe MRR 255

Facteur de fenêtre, radio à bande étroite 246

Ligne d'entrée

Émulation 3274 284

Émulation 5250 300

Ligne d'impression

Émulation 3274 283

Émulation 5250 299

Ligne de transmission

Émulation 3274 279

Émulation 5250 295

Local

Émulation 3274 277

Émulation 5250 293

Longueur de formulaire d'impression

Émulation 3274 284

Émulation 5250 299

M

mapRF

802.IQv2 319

Maximum

Sessions par terminal

Protocole Telnet ANSI 311

Protocole Telnet 3274 286

Protocole Telnet 5250 301

Taille d'écran, *Émulation ANSI* 306

Taille de segment de message

groupe MRR 255

Taille de segment de message, radio à bande étroite 245

mémoire 342

MENU HÔTE

mini-contrôleur 274

Menus de connectivité 263, 266

Message

Limite de mode, radio à bande étroite 246

Limite du mode

groupe MRR 255

Taille (station de base) 251

messages en ligne/hors ligne 266

MIB (Management Information Base) 227

MIB Voir *MIB (Management Information Base)* 227

Microsoft Internet Explorer 24

mini-contrôleur

- configuration 267–316
- émulations 269
- réseaux 269
- Mise à niveau du firmware 9
- mise à niveau logicielle
 - 802.IQv2 319
- mise en réseau, présentation des fonctionnalités 13
- mode de diffusion Turbo, non recommandé 8, 175
- Mode de fonctionnement**, station de base 243
- mode de sécurité en texte brut
 - configuration 108
 - utilisation 99
- mode de sécurité WEP
 - configuration 109
 - utilisation 99
- mode de sécurité WEP statique
 - configuration 109
 - sur liens WDS 217
 - utilisation 99
- mode de sécurité WPA Entreprise
 - configuration 119
 - utilisation 103
- mode de sécurité WPA Personal
 - configuration 117
 - utilisation 102
- Mode MRR 248
- modes Turbo Atheros 8, 175
- module SFP *Voir SFP* 22
- Modules radio à distance**, Groupe MRR 258
- mot de passe
 - paramètres réseau pour un administrateur 51
 - sur les paramètres de base 51

N

- navigateur Web 24
- Négociateur activement avec l'hôte**
 - Protocole Telnet* 3274 286
 - Protocole Telnet* 5250 302
- niveaux de modulation, radio à bande étroite 247

Nombre de

- Fenêtres d'interrogation**
 - groupe MRR 254

- Fenêtres d'interrogation**, radio à bande étroite 244

Tentatives

- groupe MRR 255

Nombre de

- tentatives, radio à bande étroite 245

Nombre maximal de connexions Telnet automatiques

- Protocole Telnet ANSI* 315

- Nom d'hôte DNS, Paramètres Ethernet 144

- normes 10

- Numéro d'hôte, configuration de station de base 265, 272

Numéro de terminal automatique,

- Fonctionnalités Radio Link 262, 263

- Numéro de terminal de vérification de présence de doublons TCP directs**,
Fonctionnalités Radio Link 261

O

Options de connectivité

- mode MRR 248

- mode station de base mode 242

P

Pages

- Émulation* 3274 278

- Émulation* 5250 295

- pages Web d'administration de connexion 42

paramètres

- modification avec un navigateur Web 24

- Paramètres 802.11 (Page Paramètres sans fil) 153, 158

- Paramètres avancés 802.11 (Page Paramètres radio) 175, 182

- paramètres de base, affichage 43

- Paramètres de groupe**, Groupe MRR 257

- Paramètres de l'interface interne,

- Paramètres Ethernet 147

- Paramètres de l'interface invité, Paramètres Ethernet 150

Paramètres du protocole d'interrogation

- Groupe MRR 254

- RA1001A 244

- paramètres filaires 141, 167

- Paramètres généraux**, radio à bande étroite 242

- Paramètres horaires 327
- paramètres par défaut, pour la passerelle
 - sans fil 9160 G2 Wireless Gateway 27
- paramètres par défaut décrits 27
- Paramètres radio**
 - Groupe MRR 256
 - RA1001A 247
- Paramètres radio RA1001A** 241
- Passthru**
 - Émulation* 3274 276
 - Émulation* 5250 292
- PEAP
 - configuration sur un client IEEE 802.1x C-15
 - configuration sur un client WPA/WPA2 Enterprise (RADIUS) C-23
- Période d'expiration**, Fonctionnalités
 - Radio Link 262
- période DTIM, configuration 177
- physique
 - description 341
 - spécifications 341
- Plage d'affectation de l'adresse radio automatique**, Fonctionnalités Radio
 - Link 261
- plage de terminaux, menu *Hôtes* 272
- plage de terminaux, menu *Hôtes* (émulation 9010) 265
- plain-text security mode
 - configuration client C-11
- plateforme
 - configuration administrateur requise 31
 - configuration client requise 32
- plateformes prises en charge
 - administrateur 31
 - client 32
- point d'accès
 - équilibre de la charge 187
 - filtrage MAC 183
 - gestion des utilisateurs 69
 - mise en cluster 58
 - paramètres Ethernet (filaires) 141
 - paramètres sans fil 151
 - pontage WDS 213
 - QoS 195
 - radio 173
 - réseau invité 159
 - sécurité 95
- points d'accès indésirables 136
- points d'accès voisins 136
- ponts, WDS 215
- Port**
 - paramètres RA1001A 248
 - portail captif 163
 - port fibre optique 100Base-FX 22
 - port fibre optique Ethernet 22
- ports
 - brochage
 - connecteur RJ-45 (10BaseT) B-3
 - brochages
 - console port B-1
 - emplacement 20
 - matériel 39
- Préfixe de nom de LU**
 - Protocole Telnet* 3274 287
- Préfixe de nom de terminal**
 - Protocole Telnet* 5250 304
- Premier port d'écoute de terminal**
 - Protocole Telnet ANSI* 311
 - Protocole Telnet* 3274 286
 - Protocole Telnet* 5250 302
- Premier port local de terminal**
- Port**
 - Protocole Telnet* 5250 302
 - Protocole Telnet ANSI* 311
 - Protocole Telnet* 3274 286
- Premier terminal** 265, 272
- présentation des fonctionnalités 10
- présentation des fonctionnalités d'orchestration 12
- prise en charge des normes IEEE 802.11 10
- Procédures**
 - Émulation* 3274 277
 - Émulation* 5250 293
- processeur 342
- Protocole**
 - ID type**, 802.IQv1 322
- protocole
 - interrogation adaptative/de contention 238
 - radio
 - commutation cellulaire 237
 - interrogation adaptative/de contention 238
 - timeplexing 237
 - protocole d'interrogation adaptative/de contention 238

puissance de transmission, configuration 177

Q

QoS *Voir qualité de service* 195

Qualité de service 195

R

raccordements du matériel 40

radio

activation ou désactivation 177

bande étroite RA1001A 343

canal géré de points d'accès en cluster 77

configuration d'un point d'accès pour une ou deux radios 177

configuration des paramètres 177

configuration installée 9

Délai de terminal de protocole d'interrogation en pourcentage 261

Délai de terminal de protocole d'interrogation 260

ensembles de débits 177

ID d'interrogation 260

indicateurs d'état LED 23

installation et antennes 18

intervalle de balise 177

mode de diffusion Turbo, non recommandé 8, 175

mode IEEE 802.11 177

nombre maximal de stations 177

Numéro de terminal automatique 262, 263

Période d'expiration 262

période DTIM 177

Plage d'affectation de l'adresse radio automatique 261

protocoles (interrogation adaptative, IEEE 802.11) 238

puissance de transmission 177

radio 802.11A/G 342

radio 802.11G 342

seuil de fragmentation 177

seuil RTS 177

spécifications 342

SuperAG 177

radio 802.11A/G 342

radio 802.11g 342

radio à bande étroite

modulation niveau 2 247

modulation niveau 4 247

Options de connectivité, Mode MRR 248

Options de connectivité, Mode station de base 242

paramètres de configuration 239, 248

Paramètres du protocole d'interrogation 244

Paramètres radio 247

Port paramètre 248

radio à bande étroite RA1001A

configuration 239

spécifications 343

radio à bande étroite Canal actif paramètre 248

Reconfiguration de flèche Délai, *Émulation ANSI* 308

Reconfiguration des touches de fonction *Délai, Émulation ANSI* 308

Reconfiguration du soulignage de champ *Émulation 5250* 291

Région de commande

Émulation 3274 284

Émulation 5250 300

RJ-45 brochages connecteur (10BaseT Ethernet) B-3

RLE, *Émulation ANSI* 309

ROM Flash 342

RTT initial, 802.1Qv1 322

S

salve de paquet

en relation avec QoS 202

sans fil

paramètres 151

présentation des fonctionnalités des points d'accès 7

voisinage 87

sauvegarde

base de données des comptes utilisateur 75

liens, WDS 217

SDRAM 342

sécurité

avantages et inconvénients des différents modes 97

certificats sur le client C-38

comparaison des modes 98

configuration 95–124

- configuration du point d'accès 105
 - configuration sur clients sans fil C-5
 - homologations xvi
 - IEEE 802.1x 114
 - instructions xvii
 - présentation des fonctionnalités 11
 - réseau invité 108
 - serveur d'authentification C-34
 - texte brut (configuration pour rien) 108
 - WEP statique 109
 - WPA/WPA2 Enterprise (RADIUS) 119
 - WPA/WPA2 Personal (PSK) 117
 - sécurité réseau invité 108
 - série
 - débit de données 23
 - E/S série**
 - Émulation 3274 283
 - Émulation 5250 299
 - indicateur d'état LED 23
 - serveur d'authentification
 - pour le mode de sécurité IEEE 802.1x 114
 - pour le mode de sécurité
 - WPA Enterprise 119
 - serveur de communications 9500, mode cellulaire 260
 - serveur NTP
 - configuration du point d'accès pour utilisation 328
 - Serveur RADIUS
 - voir aussi *serveur d'authentification*
 - Serveur RADIUS
 - configuration pour reconnaître les points d'accès C-34
 - Sessions 65
 - Seuil**
 - Émulation ANSI 307
 - seuil de fragmentation, configuration 177
 - seuil RTS, configuration 177
 - Simple Network Management Protocol (SNMP) 227
 - SNMP Voir *Simple Network Management Protocol* 227
 - spécifications
 - physique 341
 - radio 802.11A/G 342
 - radio 802.11G 342
 - radio à bande étroite RA1001A 343
 - spécifications Power Over Ethernet 342
 - SSID de diffusion 106
 - station de base
 - Adresse IP 251
 - Aucun en ligne/Hors ligne, hôte 9010 / TCP/IP 266
 - Canal partagé 244
 - configuration 235
 - configuration 263–266
 - Contrôle d'interrogation, hôte 9010 / TCP/IP 266
 - Démarrage automatique** 243, 251
 - Dernier terminal**, hôte 9010 / TCP/IP 265
 - Dernier terminal** hôte 272
 - Hôtes 263–266
 - hôte 9010 / TCP/IP 265, 272
 - Menus de connectivité 248, 263–266
 - menus radio à bande étroite 239–248
 - Mode de fonctionnement 243
 - Nom 251
 - Numéro d'hôte 265, 272
 - Numéro de station de base 250
 - Premier terminal 272
 - Premier terminal, hôte 9010 / TCP/IP 265
 - présentation 237
 - Taille du message 251
 - stations
 - configuration maximum autorisée 177
 - Voir aussi *client*
 - surveillance de session
 - accès 65
 - actualisation des informations 68
 - à propos de 65
 - visualisation des informations de session 67
 - surveillance intégrité de la liaison 136
 - synchronisation de cluster 61
- ## T
- Taille des fenêtres d'interrogation**
 - groupe MRR 255
 - radio à bande étroite 245
 - TekTerm, Fonctionnalités Radio Link 261
 - Telnet automatique**
 - Protocole Telnet 3274 288
 - Protocole Telnet 5250 302
 - Telnet automatique**, Telnet ANSI
 - Hôte 313

- Invite terminal 313
- Telnet automatique/Activation de session 312
- Telnet automatique sans délai d'action de l'utilisateur**
 - Protocole Telnet ANSI* 315
- Telnet automatique sans intervention de l'utilisateur**
 - Protocole Telnet ANSI* 315
 - Protocole Telnet 3274* 288
 - Protocole Telnet 5250* 303
- temps d'attente pour synchronisation automatique de cluster 61
- tension, entrée 18, 342
- tension d'entrée (alimentation requise) 18, 342
- tentatives, nombre de 245
- Terminal**
 - Délai hors ligne**
 - 802.IQ 320
 - Type**
 - Protocole Telnet ANSI* 310
 - Protocole Telnet 3274* 285
 - Protocole Telnet 5250* 301
- terminal
 - connexion d'un affichage vidéo 23
- terminal à affichage vidéo, connexion 23
- timeplexing 237
- TLS-EAP
 - configuration sur le client IEEE 802.1x C-19
 - configuration sur le client WPA/WPA2 Enterprise (RADIUS) C-27
 - obtention du certificat pour le client C-38
- ToS en relation avec QoS 198
- Touche de fonction n**
 - écrans de configuration des touches de fonction*
 - ANSI 316
 - 3274 289
 - 5250 305
- Transférer des paquets 802.IQ uniquement**, 802.IQ 323
- Txon à distance**
 - groupe MRR 257
 - radio à bande étroite 247
 - Type de service *Voir ToS* 198

U

- utilisateur
 - authentification
 - configuration sur le client WPA/WPA2 Enterprise (RADIUS) C-23
 - comptes
 - pour serveur d'authentification intégré 69
 - sauvegarde et restauration 75
 - configuration sur le client IEEE 802.1x C-15
- Utiliser EBCDIC international**
 - Émulation 3274* 274
 - Émulation 5250* 290

V

- VLAN
 - pour interface interne et invité 162
 - Priorité 204
- Voice over IP
 - service amélioré avec QoS 195
- voisin 89
- VWN (Virtual Wireless Networks), Paramètres Ethernet 146

W

- WDS
 - configuration 219
 - exemple 222
 - explication 215
 - règles 220
- WEP mode de sécurité
 - configuration client C-12
- WPA/WPA2 Enterprise (RADIUS), mode sécurité, configuration client C-23
- WPA/WPA2 Personal (PSK) mode sécurité, configuration client C-31
- 10BaseT Ethernet B-3
- 100BaseT Ethernet B-3
- 3274/Telnet 274
 - Protocole* 287
- 3274/Telnet 289
- 802.IQ
 - Délai Terminal hors ligne** 320
 - Démarrage automatique** 319
 - Période de balise** 320

- présentation du protocole 319
- 802.IQv1
 - description 319
 - ID type de protocole** 322
 - Interfaces balise 323
 - menu **Fonctionnalités** 323
 - RTT initial** 322
 - Transférer des paquets 802.IQ
 - uniquement 323
- 802.IQv2
 - Balise port UDP 323
 - description 319
 - menu **Fonctionnalités** 323
- 9010 / TCP/IP, configuration de station de base 265, 272

