



## CONTRÔLEUR DE MOBILITÉ ARUBA MC-800

Le MC-800 est un contrôleur de mobilité Aruba haut de gamme pour réseaux locaux sans fil qui agrège jusqu'à 16 points d'accès, centralise le contrôle et assure la sécurité de déploiements sans fil. Le MC-800 est tout à fait adapté aux réseaux orientés utilisateurs, pour une connectivité mobile, un accès basé sur l'identité et des services de continuité des applications pour les déploiements sans fil de succursales/petites agences. Le MC-800 peut être facilement déployé sans perturber un réseau de succursale existant et faire l'objet d'une gestion centralisée à partir d'un siège social ou d'un centre de données à l'aide du système de gestion de mobilité Aruba. Grâce à des fonctions de convergence avancées, telles que le contrôle d'admission d'appel, la gestion RF (radiofréquences) de la voix et une qualité de service au niveau radio, le MC-800 assure des fonctionnalités de VoIP mobiles.



De plus, le MC-800 peut être déployé sous forme de passerelle de sécurité basée sur l'identité pour authentifier des utilisateurs avec et sans fil, appliquer des stratégies de contrôle d'accès basées sur des rôles et mettre en quarantaine les points d'accès non sécurisés pour empêcher leur accès au réseau d'entreprise. Les utilisateurs invités peuvent être pris en charge facilement et en toute sécurité grâce à un serveur de portail captif intégré et à des services de réseau avancés, tels que le délestage EAP et le serveur DHCP, qui assurent une continuité de service sur un réseau de succursale, y compris en cas de défaillance de la liaison WAN. Le MC-800 peut créer un environnement local sécurisé sans devoir rajouter d'équipements (réseau privé virtuel ou pare-feu) grâce à ses fonctionnalités intégrées de translation d'adresse (NAT) et de réseau privé virtuel de site à site, à la séparation des tunnels et à un pare-feu avec état conforme ICASA. La prise en charge de réseaux privés virtuels de site à site peut être intégrée à tous les principaux concentrateurs de réseaux privés virtuels en vue d'assurer une intégration transparente aux réseaux privés virtuels d'entreprise existants.

### CAPACITÉS ET PERFORMANCES DU CONTRÔLEUR

Points d'accès contrôlés	Jusqu'à 16
Utilisateurs	256
Adresses MAC	4,096
Interfaces IP pour réseaux locaux privés virtuels (VPN)	128
Ports Fast Ethernet (10/100)	8
Ports Gigabit Ethernet (10/100/1000 ou GBIC)	1
Sessions de pare-feu simultanées	64,000
Tunnels IPsec simultanés	256
Débit du pare-feu	1 Gbits/s
Débit chiffré (3DES et AES-CCM)	200 Mbits/s

### FONCTIONNALITÉS DE CONTRÔLE ET DE SÉCURITÉ

#### DES RÉSEAUX LOCAUX SANS FIL

- Sécurité 802.11i (certifiée WPA2 et WPA)
- Authentification 802.1X au niveau machine et/ou utilisateur
- Prise en charge d'EAP-PEAP, EAP-TLS et EAP-TTLS
- Cryptage centralisé AES-CCM, TKIP et WEP
- Mise en cache PMK 802.11i pour les applications à itinérance rapide
- Délestage EAP pour l'évolutivité et la pérennité des serveurs AAA
- Authentification 802.1X pour les points d'accès autonomes
- Authentification basée sur l'emplacement, l'identifiant SSID et l'adresse MAC
- Prise en charge de plusieurs identifiants SSID pour le fonctionnement de plusieurs réseaux locaux sans fil
- Sélection de serveurs RADIUS basée sur le SSID
- Contrôle et gestion des points d'accès sécurisés sur IPsec ou GRE
- Compatible CAPWAP avec possibilité de mise à niveau
- Mode « réseau local sans fil distribué » pour les déploiements des points d'accès à distance

- Prise en charge simultanée, distribuée et centralisée des réseaux locaux sans fil

#### FONCTIONNALITÉS DE SÉCURITÉ BASÉE SUR L'IDENTITÉ

- Authentification des utilisateurs avec ou sans fil
- Gestion basée sur l'adresse MAC, la norme 802.1X et un portail captif
- Liaison des clés de chiffrement, des noms d'utilisateur, des adresses IP et des adresses MAC pour créer de solides identités réseau
- Vérification de l'identité pour empêcher l'usurpation d'identité
- Évaluation de la position des points d'accès, mise en quarantaine et application de mesures correctives
- Prise en charge de Microsoft NAP, Cisco NAC et Symantec SSE
- Prise en charge des serveurs AAA basés sur RADIUS et LDAP
- Base de données utilisateur interne en alternative à des serveurs AAA
- Autorisation basée sur des rôles pour éviter tout abus de privilège
- Solide application de stratégies avec inspection des paquets avec état
- Comptabilisation des sessions par utilisateur pour effectuer un audit d'usage
- Création des comptes invités avec Aruba GuestConnect™ sans HTTPS
- Règles de bon usage configurables pour l'accès des invités
- API XML pour intégrer un portail captif externe
- Option xSec pour le chiffrement et l'authentification des réseaux locaux câblés (authentification 802.1X, cryptage AES-CBC 256 bits)

#### FONCTIONNALITÉS DE CONVERGENCE

- Possibilité de Voix et données sur un seul identifiant SSID pour les périphériques faisant l'objet d'une convergence
- Qualité de service basée sur les flux avec Voice Flow Classification™
- Passerelles de couche application SIP, Spectralink SVP, Cisco SCCP et Vocera
- Mise en file d'attente prioritaire stricte pour la qualité de service au niveau radio

# CONTRÔLEUR DE MOBILITÉ ARUBA MC-800

- Support de 802.11e (WMM, U-APSD et T-SPEC)
- Contrôle de la qualité de service pour éviter les abus de privilèges sur le réseau via 802.11e
- Marquage Diffserv et prise en charge de 802.1p pour la qualité de service sur le réseau
- Détection des clients VoIP en ligne et hors ligne
- Contrôle d'admission d'appel VoIP à l'aide de VFC (Voice Flow Classification)
- Seuils de réservation des appels pour les appels VoIP mobiles
- Gestion RF de la voix pour assurer la qualité voix
- Prise en charge de l'itinérance rapide pour assurer la qualité voix mobile
- Gestion SIP et génération d'une tonalité de retour d'appel (RFC 3960)
- Limites de débit par utilisateur et par rôle (contrats pour la bande passante)

## FUNCTIONNALITÉS ADAPTIVE RADIO MANAGEMENT™ (ARM)

- Paramètres de puissance d'émission et de gestion des canaux automatiques pour les points d'accès contrôlés
- Gestion des flux destinés à l'utilisateur final et surveillance simultanée de la radio
- Couverture à restauration automatique basée sur des conditions RF dynamiques
- Options de déploiement dense pour optimiser la capacité
- Équilibrage de charge des points d'accès basé sur le nombre d'utilisateurs
- Équilibrage de charge des points d'accès basé sur l'utilisation de la bande passante
- Détection des interférences RF et des trous de couverture
- Prise en charge de 802.11h pour la détection et l'évitement
- Détection automatique de l'emplacement des balises RFID actives
- API d'emplacement XML intégrée pour les applications RFID

## FUNCTIONNALITÉS DE PROTECTION CONTRE LES INTRUSIONS PAR DES ÉQUIPEMENTS SANS FIL

- Intégration à l'infrastructure des réseaux locaux sans fil
- Fonctionnalités de surveillance simultanée ou dédiée de la radio
- Détection des points d'accès non autorisés et visualisation intégrée de leur emplacement
- Classification automatique des points d'accès non autorisés, brouilleurs et valides
- Confinement des points d'accès non autorisés par radio et par câble
- Détection et confinement adaptés aux réseaux locaux sans fil
- Détection des clients Windows en mode « bridge » et détection des ponts sans fil
- Protection contre les attaques entraînant un refus de service pour les points d'accès et les stations
- Détection et confinement des points d'accès autonomes mal configurés
- Surveillance des performances des points d'accès tiers et dépannage
- Création de signatures logicielles pour les nouvelles attaques des réseaux locaux sans fil
- Gestion de l'établissement de liaison EAP et analyse du numéro de séquence
- Détection d'usurpation d'identité de points d'accès valides
- Détection d'attaques (Airjack, saturation de trames et faux points d'accès)
- Détection d'absence de réponse, de diffusion en différé et de présence d'ASLEAP
- Détection d'analyse de réseau basé sur Netstumbler

## FUNCTIONNALITÉS DU PARE-FEU AVEC ÉTAT

- Inspection des paquets avec état liée à l'identité des utilisateurs ou aux ports
- Définition des stratégies en fonction de l'emplacement et de l'heure
- Reconnaissance des stations 802.11 dans le cadre de la mise en place de

- pare-feu pour réseaux locaux sans fil
- Application de stratégies par radio et constitution de listes noires
- Mise en miroir des sessions et journalisation par paquet pour l'analyse d'expertise
- Journaux détaillés sur le trafic du pare-feu pour effectuer un audit d'usage
- Pare-feu d'entreprise conforme ICASA 4.1
- Prise en charge des passerelles de couche application pour SIP, SCCP, RTSP, Vocera, FTP, TFTP et PPTP
- Translation d'adresse réseau (NAT) source et cible
- Matériel de traitement des flux dédié pour optimiser les performances
- Détection des attaques entraînant un refus de service (D.O.S.) et protection contre les attaques TCP et ICMP
- Réacheminement basé sur des stratégies dans des tunnels GRE pour le trafic des invités
- Interface de service externe pour intégrer les applications de sécurité tierces en ligne (antivirus, antispam et filtrage de contenu)
- Contrôle de l'intégrité et équilibrage de charge pour les services externes

## FUNCTIONNALITÉS DES SERVEURS POUR RÉSEAUX PRIVÉS VIRTUELS (VPN)

- Prise en charge des VPN de site à site dans les déploiements de succursale
- Interopérabilité de site à site avec des serveurs pour VPN tiers
- Émulation des serveurs pour VPN pour faciliter leur intégration dans le réseau local sans fil
- Arrêt des VPN L2TP/IPsec pour les clients de VPN Windows
- Arrêt des VPN XAUTH/IPsec pour les clients tiers
- Arrêt des VPN PPTP pour intégrer VPN hérités
- Prise en charge de serveurs RADIUS et LDAP pour assurer l'authentification des VPN
- Authentification PAP, CHAP, MS-CHAP et MS-CHAPv2
- Cryptage matériel pour DES, 3DES, AES et MPPE
- Tunnels xSec point à point sécurisés pour les VPN de couche 2

## FUNCTIONNALITÉS RESEAU ET SERVICES AVANCÉS

- Commutation de couche 2 et 3 par radio et par câble
- Regroupement des réseaux locaux virtuels pour faciliter les conceptions de réseau évolutives
- Mobilité des réseaux locaux virtuels pour assurer une itinérance de couche 2 transparente
- IP mobile proxy et DHCP proxy pour l'itinérance de couche 3
- Serveur DHCP et relais DHCP intégrés
- Redondance de contrôleur N+1 basée sur VRRP (couche 2)
- Redondance de contrôleur N+1 basée sur le dimensionnement des points d'accès (couche 3)
- Mode concentrateur d'accès câblé pour centraliser la sécurité
- Prise en charge d'Etherchannel pour la redondance des liaisons
- Protocole STP (Spanning Tree Protocol) 802.1d
- Support réseaux locaux virtuels 802.1Q

## FUNCTIONNALITÉS DE GESTION BASÉES SUR LE CONTRÔLEUR

- Boîte à outils pour la planification RF et le déploiement des points d'accès
- Centralisation du dimensionnement des points d'accès et de la gestion des plans de couverture
- Visualisation en temps réel de la couverture avec des cartes dynamiques RF
- Visualisation de statistiques détaillées pour la surveillance
- Capture de paquets à distance pour le dépannage RF
- Interopérabilité avec les analyseurs Ethereal et Airopeek
- Gestion de la configuration de plusieurs contrôleurs
- Visualisation des emplacements et suivi des périphériques
- Collecte d'événement et génération de rapports

# CONTRÔLEUR DE MOBILITÉ ARUBA MC-800

## FONCTIONNALITÉS D'ADMINISTRATION DU CONTRÔLEUR

- Accès via une interface utilisateur Web HTTP et HTTPS
- Écrans de démarrage rapide pour faciliter la configuration du contrôleur
- Accès CLI à l'aide d'un port de console, SSH et Telnet
- Contrôle d'accès basé sur des rôles pour limiter l'accès administrateur
- Accès authentifié via RADIUS, LDAP ou une base de données interne
- Prise en charge SNMPv3 et SNMPv2 pour assurer la surveillance du contrôleur
- Bases d'information de gestion standard et bases d'information de gestion privées
- Journaux de messages détaillés avec notification des événements syslog

## SPÉCIFICATIONS DE L'ALIMENTATION DU CONTRÔLEUR

Consommation électrique	200 W, maximum
Tension CA	De 90 à 132 V CA, de 180 à 264 V CA
Fréquence CA	De 47 à 63 Hz

## SPÉCIFICATIONS DE FONCTIONNEMENT ET DIMENSIONS

Plage de température en fonctionnement	entre 0 et 40 °C
Plage de température en stockage	entre 10 et 70 °C
Humidité, sans condensation	De 5 à 95 %
Hauteur	1,75" (44,5 mm)
Largeur	17,4" (444 mm)
Profondeur	13" (330 mm)
Poids	10 lbs (sans emballage)

## GARANTIE

Matériel	1 an pièces/main d'œuvre*
Logiciels	90 jours*

## INDICATIONS DE CONFORMITÉ ET DE SÉCURITÉ

- FCC Partie 15 Classe A CE
- Industry Canada Classe A
- VCCI Classe A (Japon)
- EN 55022 Classe A (CISPR 22 Classe A), EN 61000-3
- EN 61000-4-2, EN 61000-4-3, EN 61000-4-4
- EN 61000-4-5, EN 61000-4-6, EN 61000-4-8
- EN 61000-4-11, EN 55024, AS/NZS 3548
- UL 60950, EN60950
- CAN/CSA 22.2 #60950
- Marque CE, cTUVus, GS, CB, C-tick, Anatel, NOM, MIC, IQC

## POUR COMMANDER

RÉFÉRENCE	DESCRIPTION
804-4-TX-AOS-STD	Contrôleur de mobilité A800-4 - SPOE, 1000Base-T GigE -4 points d'accès maximum
804-4-SX-AOS-STD	Contrôleur de mobilité A800-4 - SPOE, 1000Base-SX GigE -4 points d'accès maximum
800-16-TX-AOS-STD	Contrôleur de mobilité A800-16 - SPOE, 1000Base-T GigE -16 points d'accès maximum
800-16-SX-AOS-STD	Contrôleur de mobilité A800-16 - SPOE, 1000Base-SX GigE -16 points d'accès maximum

Pour plus d'informations sur la configuration et la commande de ce produit, contactez votre revendeur Aruba Networks.

\*Garantie prolongée avec contrat de prise en charge



[WWW.ARUBANETWORKS.COM](http://WWW.ARUBANETWORKS.COM)

1322 Crossman Avenue. Sunnyvale, CA 94089 | Tél. +1 408.227.4500 | Fax +1 408.227.4550