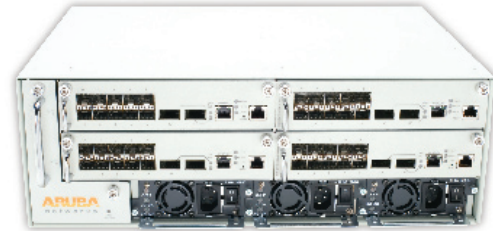




CONTRÔLEUR DE MOBILITÉ MULTISERVICE ARUBA MMC-6000

Le contrôleur de mobilité multiservice Aruba MMC-6000 est un contrôleur modulaire haut de gamme capable de regrouper jusqu'à 2 048 points d'accès connectés à un site. Le contrôleur MMC-6000 offre une expérience réseau véritablement centrée sur l'utilisateur et fournit une connectivité mobile, un accès basé sur l'identité ainsi que des services de continuité des applications. Le MMC-6000 est conçu pour prendre en charge des déploiements importants de manière évolutive. Il peut être facilement mis en œuvre en superposition sur le réseau câblé existant, sans le perturber. Grâce à des fonctionnalités avancées de type voix sur le réseau local sans fil comme le contrôle d'admission des appels, une gestion RF couplée à la voix et une qualité de service stricte sur le media radio, le contrôleur MMC-6000 est en mesure d'offrir des fonctions de VoIP mobile. Le MMC-6000 est géré via ArubaOS ou via le système de gestion de la mobilité d'Aruba.



En outre, ce contrôleur peut être déployé en tant que passerelle de sécurité centrée sur l'utilisateur afin d'authentifier les utilisateurs avec ou sans fil, d'appliquer les stratégies de contrôle d'accès basées sur les rôles et d'empêcher les équipements d'extrémité dangereux d'accéder au réseau d'entreprise. Les utilisateurs invités peuvent être pris en charge facilement et en toute sécurité grâce au serveur de portail captif intégré et à des services réseau avancés. Le MMC-6000 peut créer un environnement réseau sécurisé sans que la présence de nouveaux équipements (réseau privé virtuel/pare-feu) ne soit nécessaire, grâce à ses fonctionnalités intégrées de translation d'adresse réseau (NAT) et de réseau privé virtuel de site à site, à la séparation des tunnels et à un pare-feu dynamique certifié ICSA. La prise en charge de VPN site à site est interopérable avec tous les principaux concentrateurs VPN et ce, en vue d'assurer une intégration transparente aux réseaux privés virtuels d'entreprise existants.

CAPACITÉS ET PERFORMANCES DU CONTRÔLEUR

| | |
|--|--------------------|
| Points d'accès connectés à un site | Jusqu'à 2 048 |
| Points d'accès distants | Jusqu'à 8 192 |
| Utilisateurs | Jusqu'à 32 768 |
| Adresses MAC | Jusqu'à 256 000 |
| Interfaces IP pour réseaux locaux virtuels | 512 |
| Ports Fast Ethernet (10/100) | Jusqu'à 72 |
| Ports Gigabit Ethernet (GBIC ou SFP) | Jusqu'à 40 |
| 10 ports Gigabit Ethernet (XFP) | Jusqu'à 8 |
| Sessions de pare-feu actives | Jusqu'à 2 097 200 |
| Tunnels IPsec simultanés | Jusqu'à 32 768 |
| Débit du pare-feu | Jusqu'à 80 Gbits/s |
| Débit crypté (3DES) | Jusqu'à 32 Gbits/s |
| Débit crypté (AES-CCM) | Jusqu'à 16 Gbits/s |

- 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
- Authentification basée sur l'adresse MAC, la norme 802.1X et le portail captif
- Liaison des clés de cryptage, des noms d'utilisateur, des adresses IP, des adresses MAC pour créer de solides identités réseau
- Vérification de l'identité par paquet pour empêcher l'usurpation d'identité
- Évaluation de l'état des équipements d'extrémité, 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 cas de non disponibilité de serveur 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
- Inscription Web des invités avec Aruba GuestConnect™
- Règles de bon usage configurables pour l'accès des invités
- API XML pour intégrer le portail captif externe
- Option xSec pour le chiffrement et l'authentification des réseaux locaux câblés (authentification 802.1X, chiffrement AES-CBC 256 bits)

FONCTIONNALITÉS DE CONTRÔLE ET DE SÉCURITÉ DES RÉSEAUX LOCAUX SANS FIL

- Sécurité 802.11i (certifiée WPA WPA2 et WPA)
- Authentification 802.1X des ordinateurs et des utilisateurs
- Prise en charge d'EAP-PEAP, EAP-TLS et EAP-TTLS
- Chiffrement 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
- Interception et gestion de l'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 l'identifiant SSID
- Contrôle et gestion des points d'accès sécurisés sur IPsec ou GRE
- Compatible CAPWAP avec possibilité de mise à niveau

FONCTIONNALITÉS DE CONVERGENCE

- Voix et donnée 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™

CONTRÔLEUR DE MOBILITÉ MULTISERVICE ARUBA MMC-6000

- Passerelles de couche applicative SIP, Spectralink SVP, Cisco SCCP et Vocera
- Mise en file d'attente prioritaire stricte pour la qualité de service par radio
- Prise en charge de 802.11e (WMM, U-APSD et T-SPEC)
- Contrôle de la qualité de service pour éviter les abus 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
- Seuils de réservation des appels pour les appels VoIP mobiles
- Gestion RF tenant en compte l'état des conversations pour assurer la qualité vocale
- Prise en charge de l'itinérance rapide pour assurer la qualité vocale mobile
- Nouveau média 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)

FONCTIONNALITÉS ADAPTIVE RADIO MANAGEMENT™ (ARM)

- Paramétrage de puissance et de canaux automatique pour les points d'accès contrôlés
- Services simultanés de surveillance radio et de connectivité pour l'utilisateur final
- Recalcul dynamique de la couverture en cas de panne
- 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 radar
- Détection automatique de l'emplacement des balises RFID actives
- API d'emplacement XML intégrée pour les applications RFID

FONCTIONNALITÉS 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 sur la radio et sur le filaire
- Détection et confinement adaptés aux réseaux locaux sans fil
- Détection de clients Windows en mode pont et 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 d'attaque configurables pour les nouvelles attaques des réseaux locaux sans fil
- Analyse du numéro de séquence et vérification de l'intégrité de l'établissement de la liaison EAP
- Détection d'usurpation d'identité de points d'accès valides
- Détection d'attaques (Airjack, saturation de trames et faux points d'accès)
- Détection de l'utilisation d'ASLEAP, de trames de déauthentification et de réponses aux trames null probe.
- Détection d'analyse de réseau sans-fil basé sur l'utilisation de Netstumbler

FONCTIONNALITÉS DU PARE-FEU AVEC ÉTAT

- Inspection des paquets avec état liée à l'identité des utilisateurs ou aux ports
- Définition des politiques en fonction de l'emplacement et de l'heure
- Pare-feu prenant en compte l'état des stations 802.11
- Application de politiques par radio et constitution de listes noires de stations

- 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 ICSA 4.1
- Pare-feu gérant les couches applicatives SIP, SCCP, RTSP, Vocera, FTP, TFTP et PPTP
- Translation d'adresse réseau (NAT) source et cible
- Composants de traitement des flux dédiés pour optimiser les performances
- Détection et protection des attaques de type déni de service TCP et ICMP
- Réacheminement basé sur des politiques dans des tunnels GRE pour le trafic des invités
- API 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

FONCTIONNALITÉS DES SERVEURS POUR RÉSEAUX PRIVÉS VIRTUELS

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

FONCTIONNALITÉS RESEAU ET SERVICES AVANCÉS

- Commutation de niveaux 2 et 3
- Regroupement de VLANs pour faciliter les conceptions de réseau évolutives
- Mobilité des VLAN pour assurer une itinérance de niveau 2 transparente
- IP mobile proxy et DHCP proxy pour l'itinérance de niveau 3
- Serveur DHCP et relais DHCP intégrés
- Redondance de contrôleur N+1 basée sur VRRP (niveau 2)
- Redondance de contrôleur N+1 basée sur la configuration des points d'accès (niveau 3)
- Mode concentrateur d'accès filaire pour centraliser la sécurité
- Prise en charge d'Etherchannel pour la redondance des liaisons
- Protocole STP (Spanning Tree Protocol) 802.1d
- Gestion du protocole 802.1Q

FONCTIONNALITÉS DE GESTION BASÉES SUR LE CONTRÔLEUR

- Boîte à outils pour la planification RF et le déploiement des points d'accès
- Centralisation de la configuration des points d'accès et de la gestion des images
- 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 à l'échelle du système

FONCTIONNALITÉS D'ADMINISTRATION DU CONTRÔLEUR

- Accès via une interface utilisateur Web sur 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

CONTRÔLEUR DE MOBILITÉ MULTISERVICE ARUBA MMC-6000

- Accès authentifié via RADIUS, LDAP ou une base de données interne
- Prise en charge SNMPv3 et SNMPv2 pour assurer la surveillance du contrôleur
- MIB standards et privées
- Journaux de messages détaillés avec notification des événements syslog

OPTIONS D'ALIMENTATION DU CONTRÔLEUR

Consommation électrique 466 watts max. par bloc d'alimentation

HW-PSU-200 : les blocs d'alimentation CA fournissent une puissance de 200 W
Tension CA à l'entrée De 90 à 132 V CA, de 170 à 264 V CA
Fréquence à l'entrée CA De 47 à 63 Hz
Courant à l'entrée CA 5 A à 110 VCA

HW-PSU-400 : les blocs d'alimentation CA fournissent une puissance de 400 W
Tension CA à l'entrée 85-264 VCA, détection automatique
Fréquence à l'entrée CA De 47 à 63 Hz
Courant à l'entrée CA 5 A à 110 VCA

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 5,75½ (146 mm)
Largeur 17,4½ (444 mm)
Profondeur 12,5½ (317,5 mm)
Poids 30 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 |
|----------------------|---|
| 6000-BASE-2PSU-200 | Système de base Aruba MMC-6000 (Puissance standard) |
| 6000-BASE-2PSU-400 | Système de base Aruba MMC-6000 (Puissance SPOE) |
| SC-48-C1 | Carte de supervision I Aruba (prise en charge de 48 points d'accès) |
| SC-128-C1 | Carte de supervision I Aruba (prise en charge de 128 points d'accès) |
| SC-256-C2 | Carte de supervision II Aruba (prise en charge de 256 points d'accès) |
| M3mk1-128-G10X-10G2X | Module de mobilité multiservice Aruba Mark I 10 x 1000Base-X (SFP), 2 x 10Gbase-X (XFP), (Prise en charge points d'accès : 128) |
| M3mk1-G10X-10G2X | Module de mobilité multiservice Aruba Mark I 10 x 1000Base-X (SFP), 2 x 10Gbase-X (XFP), (aucune prise en charge de points d'accès) |
| LC-2G | Carte de lignes 2xGE Aruba |
| LC-2G24F | Carte de lignes 2xGE/24FE Aruba |

LC-2G24FP
LC-GBIC-T
LC-GBIC-SX
LC-GBIC-LX
SFP-TX
SFP-SX
SFP-LX
XFP-SR

XFP-LR

HW-CHAS

HW-PSU-200

HW-PSU-400

HW-FT

HW-SC-LC-BLANK

HW-PSU-BLANK

AK-5000-NA

HW-MNT-19

SPOE - Carte de lignes 2xGE/24 FE Aruba
Adaptateur d'interfaces GBIC Aruba - T
Adaptateur d'interfaces GBIC Aruba - SX
Adaptateur d'interface GBIC Aruba - LX
Aruba SFP - 1000Base-T, RJ45
Aruba SFP - 1000Base-SX, Connecteur LC
Aruba SFP - 1000Base-LX, Connecteur LC
Émetteur-récepteur XFP Aruba – émetteur-récepteur XFP en fibre optique 850 nm pouvant être branché en série (LC), portée : 300 m sur MMF
Émetteur-récepteur XFP Aruba – émetteur-récepteur XFP en fibre optique 1310 nm pouvant être branché en série (LC), portée : jusqu'à 10 km sur SMF
Gamme Aruba MMC-5000 et MMC-6000
4 fentes Châssis (plateau de ventilation exclus)
Alimentation des gammes Aruba MMC-5000 et MMC-6000 Alimentation : 200 Watts
Alimentation des gammes Aruba MMC-5000 et MMC-6000 Alimentation : 400 Watts
Plateau de ventilation de rechange des gammes Aruba MMC-5000 et MMC-6000 Plateau de ventilation de remplacement
Plateau de ventilation de rechange des gammes Aruba MMC-5000 et MMC-6000 Panneau d'obturation des fentes de la carte de supervision/lignes
Plateau de ventilation de rechange des gammes Aruba MMC-5000 et MMC-6000 Panneau d'obturation des fentes du bloc d'alimentation
Kit d'accessoires des gammes Aruba MMC-5000 et MMC-6000 (Guide d'installation matérielle et kit de montage en rack 19")
Plateau de ventilation de rechange des gammes Aruba MMC-5000 et MMC-6000 Kit de montage en rack de rechange des équipements 19" Kit

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

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