



## ARUBA MMC-6000 MULTI-SERVICE MOBILITY CONTROLLER

Der Aruba MMC-6000 Multi-Service Mobility Controller ist ein voll ausgestatteter modularer Controller, der bis zu 2.048 mit einem Standort verbundene Access Points (APs) zusammenfassen kann. Er ermöglicht eine wirklich benutzerzentrierte Netzwerkerfahrung durch ortsunabhängigen identitätsorientierten Netzzugriff und Application Continuity Services. Der MMC-6000 ist entwickelt worden, um große Deployments auf skalierbare Weise zu unterstützen und kann problemlos als Overlay (Parallelbetrieb) implementiert werden, ohne Beeinträchtigungen im Betrieb des bestehenden kabelgebundenen Netzwerks. Fortschrittliche Voice over WLAN-Funktionen wie Call Admission Control (CAC), sprachdatenfähiges Funkmanagement und strikte Funk-QoS erlauben es dem MC-6000-Controller, mobile VoIP-Fähigkeiten bereitzustellen. Das Gerät kann entweder über ArubaOS oder über das Aruba Mobility Management-System verwaltet werden.



Der MC-6000-Controller kann darüber hinaus auch als benutzerzentriertes Sicherheitsgateway eingesetzt werden, um kabelgebundene und drahtlose Benutzer zu authentifizieren, rollenbasierte Richtlinien für die Zugriffssteuerung durchzusetzen sowie unsichere Endgeräte unter Quarantäne zu stellen und sie so daran zu hindern, auf das Unternehmensnetzwerk zuzugreifen. Gäste werden problemlos und sicher durch den integrierten Captive Portal-Server und fortschrittliche Netzwerkdienste unterstützt. Durch seine integrierten Site-to-Site-VPN- und NAT-Fähigkeiten, Split-Tunneling und eine ICSA-zertifizierte Stateful Firewall kann der MC-6000 eine sichere Netzwerkumgebung schaffen, ohne dafür zusätzliche VPN- oder Firewall-Geräte zu benötigen. Unterstützung für Site-to-Site-VPN kann in alle wichtigen VPN-Konzentratoren integriert werden, um eine nahtlose Integration in vorhandene unternehmenseigene VPNs zu gewährleisten.

### LEISTUNG UND KAPAZITÄT DES CONTROLLERS

CMit dem Standort verbundene APs	Bis zu 2.048
Remote APs	Bis zu 8.192
Benutzer	Bis zu 32.768
MAC-Adressen	Bis zu 256.000
VLAN IP-Schnittstellen	512
Fast Ethernet Ports (10/100)	Bis zu 72
Gigabit Ethernet Ports (GBIC oder SFP)	Bis zu 40
10 Gigabit Ethernet Ports (XFP)	Bis zu 8
Aktive Firewall-Sitzungen	Bis zu 2.097.200
Gleichzeitige IPsec-Tunnel	Bis zu 32.768
Durchsatz der Firewall	Bis zu 80 Gbit/s
Verschlüsselter Datendurchsatz (3DES)	Bis zu 32 Gbit/s
Verschlüsselter Datendurchsatz (AES-CCM)	Bis zu 16 Gbit/s

### SICHERHEITS- UND STEUERUNGSFUNKTIONEN FÜR DRAHTLOSNETZWERKE

- 802.11i-Sicherheit (WFA-zertifizierter WPA2 und WPA)
- 802.1X-Authentifizierung von Benutzer und Gerät
- Unterstützung von EAP-PEAP, EAP-TLS, EAP-TTLS
- Zentralisierte Verschlüsselung durch AES-CCM, TKIP und WEP
- 802.11i-PMK-Caching für Fast Roaming-Anwendungen
- EAP-Offload für Skalierbarkeit und Absicherung von AAA-Servern
- Zustandsabhängige 802.1X-Authentifizierung für eigenständige Access Points
- Authentifizierung basierend auf MAC-Adresse, SSID und Standort
- Multi-SSID-Unterstützung für den Betrieb mehrerer Drahtlosnetzwerke
- SSID-basierte Auswahl des RADIUS-Servers
- Sichere Steuerung und Administration der Access Points über IPsec oder GRE
- CAPWAP-kompatibel und aufrüstbar
- Distributed WLAN-Modus für Deployments von Remote Access Points
- Gleichzeitige Unterstützung von centralized und distributed WLAN-Lösungen

### IDENTITÄTSORIENTIERTE SICHERHEITSFUNKTIONEN

- Authentifizierung kabelgebundener und drahtloser Benutzer
- Authentifizierung über Captive Portal, 802.1X und MAC-Adresse
- Verknüpfung von Benutzernamen, IP-Adresse, MAC-Adresse und Kodierungsschlüssel für die Erstellung effizienter und sicherer Netzwerkidentitäten
- Identitätsverifizierung pro Paket zur Verhinderung von Impersonation
- Bewertung, Quarantäne und Korrektur der Lage von Endgeräten
- Unterstützung von Microsoft NAP, Cisco NAC, Symantec SSE
- Unterstützung von RADIUS- und LDAP-basierten AAA-Servern
- Interne Benutzerdatenbank zur Ausfallsicherung der AAA-Server
- Rollenbasierte Authentifizierung zur Vermeidung überschüssiger Privilegien
- Sichere Durchsetzung von Richtlinien mit Stateful Packet Inspection
- Sitzungsprotokollierung pro Benutzer für Audits der Auslastung
- Webbasierte Zulassung von Gästen mit Aruba GuestConnect™
- Konfigurierbare allgemeine Nutzungsbedingungen für den Gastzugang
- XML-basierte API für die Integration externer Captive Portals
- xSec-Option für Authentifizierung und Verschlüsselung im kabelgebundenen Netzwerk (802.1X-Authentifizierung, 256-Bit AES-CBC-Verschlüsselung)

### KONVERGENZ

- Übertragung von Sprachdaten und normalen Daten in einem einzigen SSID für konvergente Geräte
- Auf dem Datenverkehr basierende QoS durch Voice Flow Classification™
- SIP, Spectralink SVP, Cisco SCCP und Vocera ALG
- Strenge Priorisierung für QoS über Funk
- 802.11e-Unterstützung – WMM, U-APSD und T-SPEC
- QoS-Richtlinien zur Verhinderung missbräuchlicher Verwendung des Netzwerks über 802.11e
- DiffServ-Markierung und 802.1p-Unterstützung für Netzwerk-QoS
- Erkennung des Auflegens/Abhebens des VoIP-Clients
- VoIP-Call Admission Control (CAC) über VFC

# ARUBA MMC-6000 MULTI-SERVICE MOBILITY CONTROLLER

- Grenzwerte für Anrufreservierung bei mobilen VoIP-Anrufen
- Sprachfähiges Funk-Management zur Gewährleistung der Sprachqualität
- Unterstützung von Fast Roaming zur Gewährleistung der mobilen Sprachqualität
- Frühzeitige Leitungs- und Klingelton-Generierung in SIP (RFC 3960)
- Begrenzung der Datenrate pro Benutzer und Rolle (Bandbreitenverträge)

## ADAPTIVE RADIO MANAGEMENT™ (ARM)

- Automatische Kanal- und Leistungseinstellung für gesteuerte Access Points
- Simultane Funküberwachung und Endbenutzerdienste
- Selbstregulierende Abdeckung, basierend auf dynamischen Funkbedingungen
- Optionen für engmaschiges Deployment zur Kapazitätsoptimierung
- Lastverteilung von Access Points auf Basis der Benutzeranzahl
- Lastverteilung von Access Points auf Basis der Bandbreitennutzung
- Erkennung von Funklöchern und Interferenzen
- 802.11h-Unterstützung für Radarerkennung und -umgehung
- Automatische Standorterkennung aktiver RFID-Markierungen
- Integrierte, XML-basierte Location API für RFID-Anwendungen

## WIRELESS INTRUSION PROTECTION

- Integration in die WLAN-Infrastruktur
- Simultane oder dedizierte Funküberwachung
- Erkennung nicht autorisierter Access Points und integrierte Anzeige der Standorte
- Automatische Einteilung der Access Points in die Kategorien „Nicht autorisiert“, „Interferierend“ und „Gültig“
- Eindämmung drahtloser und kabelgebundener nicht autorisierter Access Points
- Erkennung und Eindämmung von Ad-hoc-Drahtlosnetzwerken
- Erkennung von Client Bridging und Wireless Bridges unter Windows
- Schutz vor Denial of Service-Angriffen für Access Points und Stationen
- Erkennung und Eindämmung fehlerhaft konfigurierter eigenständiger Access Points
- Leistungsüberwachung der Access Points von Drittherstellern und Fehlerbehebung
- Flexible Erstellung von Angriffssignaturen für bislang unbekannte Angriffe auf das Drahtlosnetzwerk
- Analyse von EAP-Handshake und Sequenznummer
- Erkennung von betrügerischen Imitationen gültiger Access Points
- Erkennung von Angriffen wie Frame-Flooding, Fake AP und Airjack
- Erkennung von ASLEAP-, Death Broadcast- und Null Probe Response-Angriffen
- Netstumbler-basierte Erkennung von Network Probes

## STATEFUL FIREWALL

- An Benutzeridentität oder Ports gebundene Stateful Packet Inspection
- Definition von Richtlinien basierend auf Standort und Tageszeit
- 802.11-Station-Awareness zum Firewallschutz für das Drahtlosnetzwerk
- Durchsetzung von Funk-Richtlinien und Sperrung von Stationen
- Sitzungsspiegelung und Aufzeichnungen pro Paket für die forensische Analyse
- Detaillierte Aufzeichnungen über den Datenverkehr der Firewall für Audits der Nutzung
- Erfüllung der ICSA Corporate Firewall 4.1-Kriterien
- Application Layer Gateway (ALG)-Unterstützung für SIP, SCCP, RTSP, Vocera, FTP, TFTP, PPTP
- Network Address Translation (NAT) von Quelle und Ziel
- Dedizierte Hardware zur Verarbeitung des Datenverkehrs für maximale Leistung
- Erkennung von und Schutz vor Denial of Service-Angriffen über TCP und ICMP
- Auf Richtlinien basierende Weiterleitung des Datenverkehrs von Gästen in GRE-Tunnel

- Externe Serviceschnittstelle für die Integration von Sicherheitsdiensten von Drittherstellern für Inline-Anti-Virus- und -Anti-Spam-Anwendungen und Anwendungen zur Inhaltsfilterung
- Statusüberwachung und Lastverteilung externer Dienste

## VPN-SERVER

- Unterstützung von Site-to-Site-VPN für Deployments in Zweigstellen
- Site-to-Site-Kompatibilität mit VPN-Servern von Drittherstellern
- Emulation von VPN-Servern zur problemlosen Integration in Drahtlosnetzwerke
- VPN-Termination (L2TP/IPsec) für VPN-Clients unter Windows
- VPN-Termination (XAUTH/IPsec) für Clients von Drittherstellern
- VPN-Termination (PPTP) für die Integration alter VPN
- Unterstützung von RADIUS- und LDAP-Servern zur VPN-Authentifizierung
- Authentifizierung durch PAP, CHAP, MS-CHAP und MS-CHAPv2
- Hardwareverschlüsselung für DES, 3DES, AES, MPPE
- Sichere Punkt-zu-Punkt-xSec-Tunnel für L2-VPNs

## NETZWERKFUNKTIONEN UND ERWEITERTE DIENSTE

- L2- und L3-Switching über Funk und über Kabel
- VLAN-Pooling für einfache skalierbare Netzwerke
- VLAN-Mobilität für nahtloses L2-Roaming
- Mobile Proxy-IP und Proxy-DHCP für L3-Roaming
- Integrierte DHCP-Server und DHCP-Relais
- VRRP-basierte N+1-Controller-Redundanz (L2)
- Auf AP-Zuteilung basierende N+1-Controller-Redundanz (L3)
- Konzentrador-Modus für kabelgebundenen Zugriff für zentralisierte Sicherheit
- Etherchannel-Unterstützung für Verbindungsredundanz
- 802.1d-Spanning Tree Protocol (STP)
- 802.1Q-VLAN-Markierungen

## CONTROLLER-BASIERTE VERWALTUNGSFUNKTIONEN

- Toolkit für Funkplanung und AP-Deployment
- Zentralisierte Bereitstellung von Access Points und Image-Verwaltung
- Echtzeit-Visualisierung der Netzabdeckung mit Funk-Heatmaps
- Detaillierte Visualisierung der Statistiken zur optimalen Überwachung
- Ferngesteuerte Paketerfassung zur Fehlersuche im Funkbereich
- Kompatibilität mit den Analysetools Ethereal und AiroPeek
- Konfigurationsmanagement für mehrere Controller
- Visualisierung von Standorten und Aufspüren von Geräten
- Systemweite Aufzeichnung von Ereignissen und entsprechende Berichterstellung

## CONTROLLER-VERWALTUNG

- Webbasierter Zugriff auf die Benutzerschnittstelle über HTTP und HTTPS
- Schnellstart-Anzeigen für einfache Controller-Konfiguration
- CLI-Zugriff über SSH, Telnet und Konsolenports
- Rollenbasierte Zugriffssteuerung für eingeschränkten Administratorzugriff
- Authentifizierter Zugriff über RADIUS, LDAP oder interne Datenbanken
- SNMPv3- und SNMPv2-Unterstützung zur Controller-Überwachung
- Standard-MIBs und unternehmenseigene MIBs
- Detaillierte Nachrichtenaufzeichnungen mit syslog-Benachrichtigung

## STROMVERSORGUNG DES CONTROLLERS

PStromverbrauch Max. 466 Watt pro Netzteil

HW-PSU-200: Netzstromversorgung liefert 200 W  
Eingangsspannung 90–132 V~, 170–264 V~  
Eingangsfrequenz 47–63 Hz

# ARUBA MMC-6000 MULTI-SERVICE MOBILITY CONTROLLER

Eingangsstromstärke	5 A bei 110 V~
HW-PSU-400: Netzstromversorgung liefert 400 W	
Eingangsspannung	85–264 V~, automatische Erkennung
Eingangsfrequenz	47–63 Hz
Eingangsstromstärke	5 A bei 110 V~

## BETRIEBSDATEN UND ABMESSUNGEN

Betriebstemperatur	0 bis 40 °C
Lagertemperatur	10 bis 70 °C
Luftfeuchtigkeit, nicht kondensierend	5 bis 95 %
Höhe	146 mm
Breite	444 mm
Tiefe	317,5 mm
Gewicht	~ 13,5 kg (ohne Verpackung)

## GARANTIE

Hardware	1 Jahr auf Teile/Einsatzfähigkeit*
Software	90 Tage*

## STANDARD- UND SICHERHEITS-KONFORMITÄT

FCC Teil 15 Class A CE  
 Industry Canada Class A  
 VCCI Class A (Japan)  
 EN55022 Class A (CISPR 22 Class A), EN61000-3  
 EN61000-4-2, EN61000-4-3, EN61000-4-4  
 EN61000-4-5, EN61000-4-6, EN61000-4-8  
 EN61000-4-11, EN55024, AS/NZS 3548  
 UL 60950, EN60950  
 CAN/CSA 22.2 Nr. 60950  
 CE-Zeichen, cTUVus, GS, CB, C-tick, Anatel, NOM, MIC, IQC

## BESTELLINFORMATIONEN

TEILENUMMER	BESCHREIBUNG
6000-BASE-2PSU-200	Aruba MMC-6000-Grundsystem (Standard-Stromversorgung)
6000-BASE-2PSU-400	Aruba MMC-6000-Grundsystem (SPOE- stromversorgung) SC-48-C1 Aruba Supervisor Card I (Unterstützung für 48 APs)
SC-128-C1	Aruba Supervisor Card I (Unterstützung für 128 APs)
SC-256-C2	Aruba Supervisor Card II (Unterstützung für 256 APs)
M3mk1-128-G10X-10G2X	Aruba Multi-Service Mobility-Modul Mark I, 10x 1000Base-X (SFP), 2x 10GBase-X (XFP), (Unterstützung für 128 APs)
M3mk1-G10X-10G2X	Aruba Multi-Service Mobility-Modul Mark I, 10x 1000Base-X (SFP), 2x 10GBase-X (XFP), (Unterstützung für 0 APs)
LC-2G	Aruba 2xGE Line Card
LC-2G24F	Aruba 2xGE/24FE Line Card

LC-2G24FP	Aruba 2xGE/24 FE Line Card SPOE
LC-GBIC-T	Aruba GBIC Interface Adapter – T
LC-GBIC-SX	Aruba GBIC Interface Adapter – SX
LC-GBIC-LX	Aruba GBIC Interface Adapter – LX
SFP-TX	Aruba SFP – 1000Base-T, RJ45
SFP-SX	Aruba SFP – 1000Base-SX, LC-Konnektor
SFP-LX	Aruba SFP – 1000Base-LX, LC-Konnektor
XFP-SR	Aruba XFP – 850 nm seriell steckbare XFP- Optik (LC), für Distanzen bis zu 300 m auf Multimode-Glasfaser
XFP-LR	Aruba XFP – 1310 nm seriell steckbare XFP- Optik (LC) für Distanzen bis zu 10 km auf Singlemode-Glasfaser
HW-CHAS	Aruba MMC-5000- & MMC-6000-Serie: Basis- 4-Slot-Gehäuse (ohne Lüfterplatte)
HW-PSU-200:	Aruba MMC-5000- & MMC-6000-Serie: Strom-versorgung – 200 Watt
HW-PSU-400:	Aruba MMC-5000- & MMC-6000-Serie: Strom-versorgung – 400 Watt
HW-FT	Aruba MMC-5000- & MMC-6000-Serie: Ersatz-Lüfterplatte
HW-SC-LC-BLANK	Aruba MMC-5000- & MMC-6000-Serie: Blindblech für den Steckplatz der Supervisor/ Line Card
HW-PSU-BLANK	Aruba MMC-5000- & MMC-6000-Serie: Blindblech für den Steckplatz des Netzteils
AK-5000-NA	Aruba MMC-5000- & MMC-6000-Zubehörset (HW-Installationsanleitung & Set zur Befesti- gung an 19 Zoll-Baugruppenträger)
HW-MNT-19	Aruba MMC-5000- & MMC-6000-Serie: Ersatz-Befestigungsset für 19 Zoll-Baugruppen-träger

Für weitere Informationen zu Konfiguration und Bestellung wen-  
den Sie sich bitte an einen Vertreter von Aruba Networks.

\* Erweiterungsmöglichkeit über einen Support-Vertrag



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

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