VIRTUAL MOBILITY CONTROLLERS

MC1500, MC3200, and MC4200 Virtual Controllers

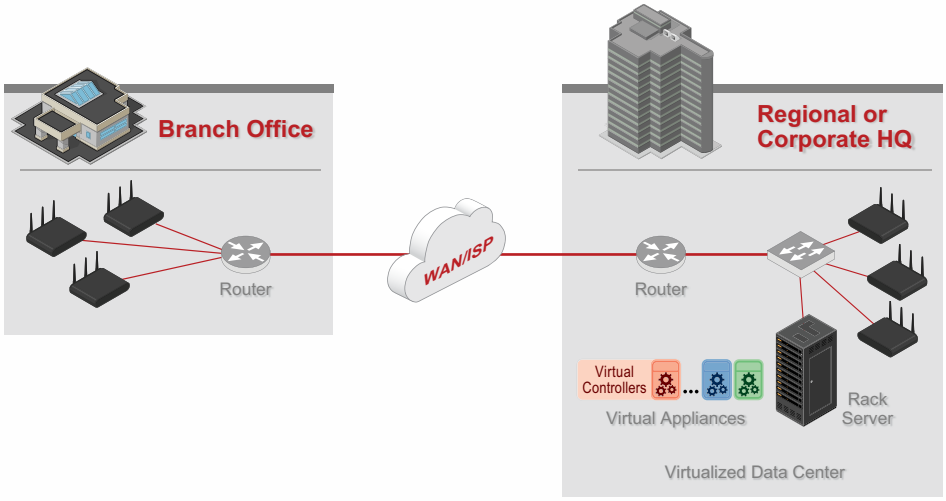
Regain the freedom of choice, flexible deployment, and the confidence of managed access in your distributed mobile enterprise

With Meru Virtual Mobility Controllers, you can leverage data-center virtualization and cloud computing to achieve operational and cost efficiencies—and greater choice in network deployment. These virtual controllers operate on x86 computing platforms in VMware environments, and they can reside alongside your other virtualized services.

These virtual appliances operate on low-profile rack servers and modular blade servers, letting you build a highly scalable controller with performance equivalent to purpose-built hardware appliances. They also let you leverage your current virtualization utilities to enhance resilience and application manageability. And you can deploy them in your virtualized data center or branch office, consolidating multiple services onto a common platform.

Benefits

- Run fewer servers and cut management costs by optimizing existing infrastructure and consolidating services
- Increase service availability by eliminating single points of failure
- Deploy additional instances more rapidly
- Expand hardware selection options and increase deployment flexibility
- Create an integrated, high-performing networking system by consolidating on a common platform
- Lower operating costs by standardizing on commodity hardware and operating systems
- Expedite product acquisition and streamline service deployment



For more information about the Virtual Mobility Controllers, visit **www.merunetworks.com**

VIRTUAL MOBILITY CONTROLLERS

TECHNICAL SPECIFICATIONS

APPLICATION SUPPORT AND OVER-THE-AIR QoS

SIP and H.323 Support
Dynamic out-of-the-box support for SIP and H.323v1 applications and codecs

QoS
Configurable dynamic QoS rules
Over-the-air resource reservation
Automatic, stateful flow detectors for SIP, H.323, Cisco SCCP, SpectraLink SVP, and Vocera
User-configurable static and dynamic QoS rules per application (user-defined) and per user (stations, users, and port numbers)
Call admissions control and call load balancing
WMM support

SECURITY

Authentication
Combination of captive portal, 802.1x, and open authentication
Advanced security using WPA2
802.1X with EAP-Transport Layer Security (EAP-TLS), Tunneled TLS (EAP-TTLS), Protected EAP (PEAP) MS-CHAPv2, Smartcard/Certificate, Lightweight EAP (LEAP), EAP-FAST and EAP-MD5, with mutual authentication and dynamic, per user, per session unicast and broadcast keys
Secure HTTPS with customizable captive portal utilizing RADIUS

Encryption Support
Static and dynamic 40-bit and 128-bit WEP keys, TKIP with MIC, AES, SSL, TLS

Security Policy
RADIUS-assisted, per user and per ESSID access control via MAC filtering
Multiple ESSID/BSSID, each with flexibility of separate and shared security policy

Rogue Detection and Suppression
All controllers have the intelligence to identify and classify rogue devices in 802.11n, 802.11a, and 802.11b/g

Security Firewall
Per user firewall with fine-grained policy management
System-configured or per user, RADIUS-configured firewall policy

MOBILITY

Zero-loss Handoffs
Infrastructure-controlled zero-loss handoff mechanism for standard Wi-Fi clients

Virtual Cell Load Balancing
Virtual Cell provides load balancing coordination for improved performance and WLAN resiliency upon AP failure

CENTRALIZED MANAGEMENT

Zero Configuration
Automatically selects power and channel settings
Access points automatically discover controllers and download configuration settings
Zero-touch, plug-and-play deployments

System Management
Centralized and remote management and software upgrades via System Director web-based GUI, SNMP, command-line interface (CLI) via serial port, SSH, Telnet, centrally managed via E(z)RF™ Network Manager
Centralized security policy for WLAN, multiple ESSIDs and VLANs with their own administrative/security policies

Intelligent RF Management
Coordination of access points with load-balancing for predictable performance
Centralized auto-discovery, auto-channel configuration, and auto-power selection for APs
Co-channel interference management

WIRED/WIRELESS SUPPORT

Wireless Compliance
IEEE 802.11 a/b/g/n, IEEE 802.11i support (AES, WEP, WPA, WPA2), IEEE 802.11e, WMM

Automatic Discovery & Configuration
All Meru access points

Wired/Switching
IEEE 802.1Q VLAN tagging, GRE tunneling and IEEE 802.1D Spanning Tree Protocol

Virtual controller part numbers—scale supported on platforms specified
MC1500-VE – up to 30 access points
MC3200-VE – up to 200 access points
MC4200-VE – up to 500 access points

Meru delivers an all-wireless network that fully supports the enterprise, delivering a consistent, interactive experience for all users. No matter what applications they are running. No matter how many other users are on the network.

Part Number	MC1500-VE	MC3200-VE	MC4200-VE
Use case	Small to mid-sized enterprises	Mid-size enterprises	Large enterprises
Scalability	Up to 30 access points and 500 clients	Up to 200 access points and 2,000 clients	Up to 500 access points and 5,000 clients
vCPUs	1	3	4
Memory	1GB	2GB	4GB
vNICs	2	2	4
Disk space	2GB	2GB	2GB
Redundancy	N+1 for controller instances of the same model	N+1 for controller instances of the same model	N+1 for controller instances of the same model
Virtual Platform	VMware ESX/ESXi 4.1	VMware ESX/ESXi 4.1	VMware ESX/ESXi 4.1

For more information about Meru Virtual Mobility Controllers, visit www.merunetworks.com or email your questions to: info@merunetworks.com

Meru Networks | Copyright © 2012 Meru Networks, Inc. All rights reserved worldwide. Meru Networks is a registered trademark of Meru Networks, Inc. All other trademarks, trade names, or service marks mentioned in this document are the property of their respective owners. 02.12 DS1017.US

Corporate Headquarters
894 Ross Drive, Sunnyvale, CA 94089
T +1 (408) 215-5300
F +1 (408) 215-5301
E info@merunetworks.com