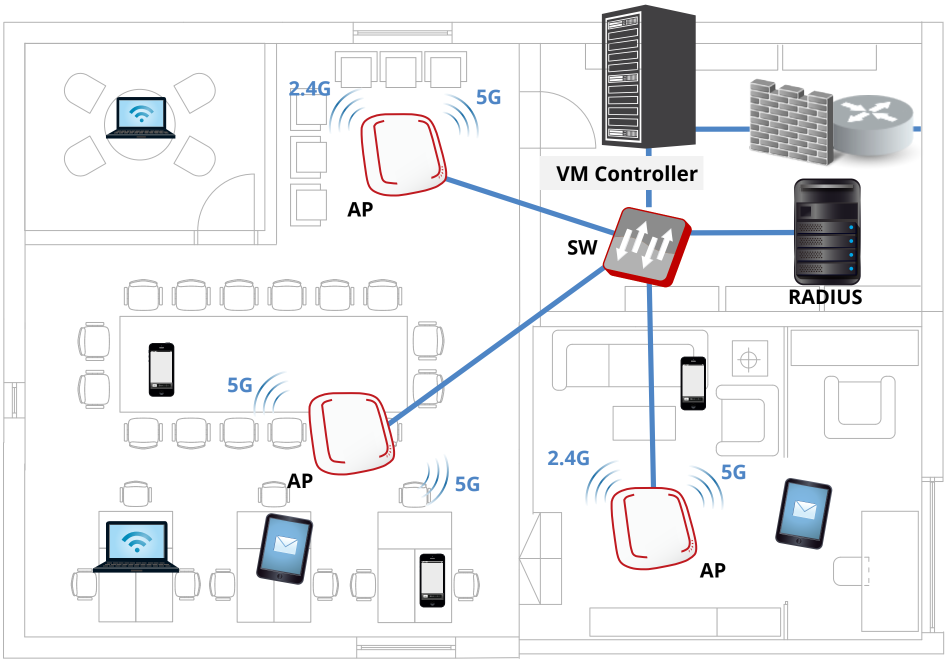
VM Controller

INTRODUCTION

The VM controller can allow to run any VMware enviornment. With AP management, user authentication, policy assignment, traffic shaping, firewall features, and much more all packaged into a single box, the VM Controller provides network administrators with a reliable, easy-to-use, and centralized management console for an entire organization's wireless network infrastructure.

The VM Controller can be deployed and configured easily by anyone, including non-wireless savvy users. For example, automated AP discovery prevents network administrators from having to go through the hassle of individually adding and configuring each access point. Access points as well as connected Wi-Fi devices can then be monitored and managed from a centralized point, with extensive logging & reporting features to assist in troubleshooting and maintenance.

As Wi-Fi enabled handheld devices such as smartphones and tablets become ever so prevalent in our daily lives, businesses and network operators alike are faced with a mind-boggling dilemma – how to simultaneously address the needs of BYOD (Bring Your Own Device), manage Wi-Fi users, and maintain network service quality for mission critical applications. The VM Controller is designed exactly with these requirements in mind, and with a total cost of ownership that satisfies even the most price conscious, organizations are guaranteed to receive an unmatched ROI on their wireless LAN infrastructure.



FEATURES

SECURITY

Security is often one of the most important concerns when it comes to enterprise wireless networks. From the most basic need of preventing network access by unauthorized users to performing rogue AP detection and enforcing network isolation, the Edgecore Controllers provide a complex set of features that prevent malicious activities in an organization's network.

For deployment flexibility, the Edgecore Controllers support user authentication via both the industry standard 802.1X as well as web-based captive portals. The highly customizable captive portals with integrated walled garden capability can be adapted to suit the needs of hotels, schools, and other public venues. For unregistered users without an account, guest access can be provided by simply entering an e-mail address, logging in with social media accounts, or purchasing a data plan through PayPal.

With various account generation methods, the Edgecore Controllers are able to identify users and track user activities, ensuring network security in public Wi-Fi.

The Edgecore Controllers also support remote access via VPN, which is crucial for travelling businessmen. At the same time, site-to-site VPN establishes secure connections between corporate headquarters and branch offices.

USER SECURITY	
Authentication Types	802.1X UAM (browser-based) IP or MAC-based
Authentication Servers	Local On-Demand Guest RADIUS LDAP NT Domain SIP POP3
Customizable Captive Portal	Yes
Customizable Wild Card Walled Garden	Yes
User Blacklisting	Yes
ACCOUNT GENERATION	
On-demand Account	SMS registration Purchase via PayPal Hotel PMS integration Selectable Billing Plans Account Ticket Printer
On-demand Account Flexibility	Customizable Billing Plans Account Credentials Access Codes Smart Login
Guest Wi-Fi Account	Limitation by duration and volume Configurable reactivation time E-mail registration and activation
Social Media Login	Yes
NETWORK SECURITY	
VPN	Remote Site-to-Site
Tunneling Protocols	IPSec PPTP
Network Isolation	Intra-VLAN or Port Inter-VLAN or Port
Rogue AP Detection	Yes
Certificates	Built-in Root CA

MOBILITY

The advent of the era of smartphones and tablets has opened a chasm between how the Internet is used and how organizations provide Internet connectivity. Wireless networks have transformed from a luxury to a necessity, in order to support devices that don't have legacy wired capability. Furthermore, additional features need to be provided in order to address the rapidly changing usage behavior.

The Edgecore Controllers support a variety of mobility features that aim to make enterprise Wi-Fi both easier to use and simpler to manage. For example, by supporting fast roaming, users on mobile devices can be on-the-go without worrying about interrupted connections. It is also not uncommon to see a single user with multiple handheld devices - with the Edgecore Controller all of the devices can login to Wi-Fi using the same username and password. Finally, mobile-optimized captive portals and ticket-printed QR code automatic login are both easy methods for a user to get online from their mobile device.

DEVICE MOBILITY	
Fast Roaming Between Access Points	Yes
Cross Gateway Roaming	Yes
WISPr Smart Client	Yes
Mobile Device Recognition for Optimized Captive Portal	Yes
Multiple Device Logins Per Account	Yes
QR Code Automatic Login	Yes
Device Plug-and-Play	Yes
On-Demand Smart Login without Re-Authentication	Yes

MANAGEMENT

In a wireless LAN, the Edgecore Controller is the central point of management for network administrators, whether it is monitoring current online users or troubleshooting network connectivity issues. The management console of the Edgecore Controller is a browser-based GUI that is simple and intuitive to operate. From this interface, network administrators can configure traffic shaping profiles, track previous network usage, perform system backup and restore, and much more.

From the user management perspective, one of the core benefits of the Edgecore Controller is its ability to enforce different traffic profiles based on both the location (Service Zone) of the user and the time of access. For example, the profiles applied during work hours can be different from that of during after-work hours. From bandwidth limitations to specific routing rules, network administrators gain fine-grained control over Wi-Fi users.

For access points, the Edgecore Controller support automatic discovery and provisioning, eliminating many repetitive and cumbersome tasks often faced during initial network deployment. Centralized AP configuration and monitoring also greatly reduces maintenance overhead for IT staff.

SYSTEM MANAGEMENT	
Browser-Based Configuration	◆ Yes
Administrator Accounts	◆ Multiple tiered access privileges ◆ Monitor each admin’s current accessed page
System Time	◆ NTP synchronization ◆ Manually configured
System Backup & Restore	◆ Yes
SNMP	◆ Yes; v2c
Network Utilities	◆ Yes; built-in packet capture
AP MANAGEMENT	
Automatic AP Discovery	◆ Yes
Automatic AP Provisioning	◆ Yes; template-based
AP Configuration Backup & Restore	◆ Yes
AP Firmware Batch Upgrade	◆ Yes
Tunneled AP Management	◆ Yes; both L2 & L3 APs
AP Load Balancing	◆ Yes
Automatic AP Firmware Upgrade	◆ Yes
Automatic Periodically AP Backup	◆ Yes
SWITCH MANAGEMENT	
Automatic Switch Discovery	◆ Yes
Automatic Switch Provisioning	◆ Yes; template-based
Switch Configuration Backup & Restore	◆ Yes
Switch Power Scheduling	◆ Yes
USER MANAGEMENT	
User Policy Assignment	◆ Role-based ◆ Time & location dependent
Bandwidth Limitation	◆ User-based ◆ Group-based ◆ Bandwidth throttling
Traffic Classification / Remarking	◆ Yes; 802.1p / DSCP
Stateful Firewall	◆ Yes; each rule with individual enforcement schedules
Static Route Assignment	◆ Yes
Concurrent Session Limit	◆ Yes
IP Address Reassignment	◆ Allow clients to obtain different IP addresses after authentication

SERVICES

As wireless networks increasingly become the primary network used by organizations, it is crucial to take into consideration fundamental network services, such as DHCP, NAT, and routing. In addition to providing these functions, the Edgecore Controller also implements the concept of a "Service Zone", which essentially segments the controller into multiple virtual controllers, each with its own associated network services, user policies, authentication settings, etc.

On the reliability end, the Edgecore Controller supports WAN port failover, which helps businesses reduce the chance of network downtime and prevents lost productivity and revenue. Furthermore, load balancing between the WAN ports increases overall performance by alleviating congestion and distributing traffic between the two outgoing links.

Finally, the Edgecore Controller provides unique value-added capabilities, such as a direct integration with Micros Opera PMS that greatly simplifies the overhead of providing managed Wi-Fi in hotels.

NETWORK SERVICES	
Redundancy (High Availability)	◆ N+1 with automatic synchronization
Internet Protocols Supported	◆ IPv4 ◆ IPv6
DHCP Server / DHCP Relay	◆ Yes
Network Address Translation	◆ Yes
Built-in HTTP Proxy Server	◆ Yes
WAN Port Load Balancing	◆ Yes

Dynamic Routing	Yes
Local DNS Records	Yes
Hotel PMS Integration	Innkey PMS Oracle Hospitality OPERA IDS Next
Integrated Billing & Accounting System	Yes
Billing Quota Types	By duration By traffic volume

REPORTING

Whether it is real-time monitoring of network activity or tracking the usage of previous Wi-Fi users, network administrators need the appropriate tools at their disposal to increase efficiency and reduce workload. The Edgecore Controllers have an extensive set of logging and reporting features that allow network administrators to easily find any information related to the wireless network.

The built-in system dashboard provides a quick overview of the current system status, along with graphical reports of network traffic and system performance. In addition, there is a simple interface for viewing online devices and their associated detailed statistics, including but not limited to the roles they belong to, enforced network policies, and packets transferred.

Alongside network monitoring, the Edgecore Controller also performs detailed logging of all network activity. For example, the User HTTP Web Log allows network administrators to track users who visited malicious websites, while the DHCP Lease Log can assist in troubleshooting clients who cannot receive an IP address. Lastly, the Configuration Change Log shows administrators which settings have been modified in the past, in case there are configuration errors that need to be reverted.

SYSTEM & NETWORK STATUS	
System Dashboard	Yes
Graphical System Performance Reports	Yes
Traffic Volume Reports	Yes
System Process Monitor	Yes
Online Device Monitoring	Yes
Active Sessions List	Yes
Configurable SYSLOG Severity	Yes
SMTP (E-mail) Notifications	Yes
Multiple Concurrent E-mail Notification Receivers	Yes
NETWORK ACTIVITY LOGS	
System Log (SYSLOG)	Yes
CAPWAP Log	Yes
Configuration Change Log	Yes
RADIUS Server Log	Yes
User Events Log	Yes
User HTTP Web Log	Yes
Firewall Log	Yes
DHCP Server/Lease Log	Yes
PMS Interface Log	Yes
On-Demand Billing Report	Yes
AP Status E-mail Notification	Yes
AP Management Event Log	Yes
Logging to External FTP	Yes
Configurable Logs & Reporting Intervals	Yes

- (Captive Portal) of users with capacity to register at least 1000 customers.
- Registration and authentication through web portal
- The passwords of users registered for authentication through the web portal are stored in an encrypted form.
- Unauthenticated users can not access the same Vlan as the authenticated users. Apply flow rules independently for authenticated users and unauthenticated users.
- Pre-shared key authentication (PSK), each station that connects to the SSID providing the pre-shared key to access network resources, and the WPA2 protocol with 128-bit AES encryption algorithm should be used
- Authentication by IEEE 802.1X standard.
- Web Portal authentication, where connected to the network are redirected to a Web Portal where they must authenticate and then receive access policies.
- Authentication through social media accounts, and compatibility with at least Google and Facebook is mandatory;
- Implement the IEEE 802.1X protocol for wireless client authentication, with at least the following EAP methods: PEAP-MSCHAPv2 and EAP-TLS.
- Integration with Radius Server that supports the EAP methods cited.
- Enable the grouping of Access Points, in order to allow the management of each group individually, with creation of SSIDs, rules and Vlans for each group of Access Points.
- Support simultaneous connection of up to 1000 (thousand) wireless clients.
- The Centralized Management System may be directly and/or remotely connected to the Access Points managed by it, i.e., connected on different networks and interconnected by routing.
- Restricted access per user with the ability to create different access profiles where it is possible to determine the functionalities assigned to each profile, with at least one profile with permissions to create visiting users and a profile with permission to make any changes.
- Enable the creation of a new SSID, define authentication parameters, define the security policies associated with the SSID, define which Access Points will be propagating the SSID, without any need for individual access at each Access Point used.
- Identify and list neighboring radios and their SSID/BSSID that can be perceived by each AP.
- Monitor through the management software the performance of each Access Point, consolidating network operating information, containing at least: signal-to-noise ratio, interference, signal power, CPU performance, memory utilization, network interface utilization.
- In the event of inoperability of an access point, the wireless controller will automatically adjust the power of the adjacent Access Points in order to provide cover for the unassisted area.
- Roaming with session integrity.
- Open network management standards SNMPv2c and SNMPv3, including the generation of traps.
- Record events in internal and/or external log through the Contractor’s SYSLOG server.
- Automatically analyze and adjust access point power to eliminate coverage gaps and optimize network performance;
- Have a system for searching for customer information from the user’s IP address, MAC address and login, indicating which Access Point the user is logged into.
- Have reporting capacity for a previous period 12 months.
- Listing of wireless clients, indicating SSID, IP address, MAC address, time and date of login and associated Access Point;
- Listing of Access Points and the status of each Access Point in an individual manner, displaying information about the operation of radios, available wireless networks and currently authenticated customers.
- Available warranty choices up to 60 months
- Several licensing choices by online validation, including no term of use or any license expiration.