HiveOS 6.1

Network Operating System Wi-Fi Features

HiveOS Wi-Fi delivers non-stop, high-performance wireless service, application-aware enterprise firewall security, and mobile device management to every Wi-Fi device.

Aerohive HiveOS is the network operating system that powers all Aerohive devices. HiveOS Wi-Fi delivers non-stop, high-performance wireless service, application-aware enterprise firewall security, and mobile device management to every Wi-Fi device.

All Aerohive devices support the feature-rich HiveOS Cooperative Control architecture. HiveOS enables Aerohive devices to organize into groups, or "hives", which allows functionality like fast roaming, user-based access control and fully stateful application-aware firewall policies, as well as additional security and RF networking features—all without the need for a centralized or dedicated controller. This architecture has lower deployment and ownership costs with higher performance, reliability and scalability than any of the networking competitors in the market today.

Key Features and Benefits

Application Visibility and Control

HiveOS enables Aerohive Wi-Fi devices to have full context-based visibility and control of nearly 1000 layer 7 applications, including custom applications that may be in use on the network. By using the granular controls built into HiveOS, administrators can identify and prioritize applications important to specific users without having to create additional SSIDs or affect the entire network.

SLA Compliance Monitoring and Response

The SLA compliance solution brings determinism and visibility to the wireless network by enabling IT administrators to establish, monitor, and deliver reliable service to client devices. The SLA feature not only allows the ability to set a performance threshold for connected clients, but includes auto-remediation capabilities to re-allocate airtime to connected clients who do not meet the established SLA without any administrator intervention.

Increased Network Capacity with Airtime Management

Aerohive's Dynamic Airtime Scheduling enables faster clients, like 802.11n laptops, to get equal access to the airtime rather than allowing it to be monopolized by legacy or slow clients. In addition, Dynamic Airtime Scheduling can also track retries and manage upstream traffic to protect the network from misbehaving clients or users. Overall, Dynamic Airtime Scheduling can increase network capacity by up to ten times, just by keeping slow or legacy clients from dominating airtime.

Built-in Aerohive Spectrum Analysis

Spectrum Analysis is a critical tool for detecting interference from non-Wi-Fi radio devices such as Bluetooth, microwave ovens and cordless phones. In fact, detecting interference is so important to WLAN performance that Aerohive includes this capability with every access point shipped, with no additional hardware or licenses required. HiveOS uses spectrum analysis information to feed the Aerohive Channel Selection Protocol (ACSP) and boosts performance by avoiding interference from non-802.11 devices.

For more information visit www.aerohive.com/hiveOS.

Contact us today to learn how your organization can benefit from Aerohive networking solutions.

Aerohive Networks, Inc.
330 Gibraltar Drive
Sunnyvale, California 94089 USA
phone 408.510.6100
toll-free 866.918.9918
fax 408.510.6199
www.aerohive.com

Product Features

Cooperative Control
- Cooperative fast L2/L3 roaming
- Cooperative RF control
- Aerohive Mobility Routing Protocol (AMRP) for mesh routing
- Tunnel load balancing for L3 roaming

WIreless VPN
- Remote office IPSec-based VPN solution
- IPsec hardware acceleration supported
- Profile-based split tunneling with NAT support
- Supported across mesh
- RADIUS, DHCP, NTLM, LDAP and NTP can selectively go to local or remote network

SLA Compliance
- Client and AP Health – Monitor connection quality and automatically trigger and report on actions to improve quality
- Airtime Boost – Automatically increase airtime allocation to clients best able to use it to meet performance targets
- Load balancing – Direct clients to APs for improved connection quality

Security
- Trusted Platform Module (TPM)—Hardware-based key storage and encryption
- Wireless privacy and authentication Wi-Fi CERTIFIED™ WPA™ and WPA2™, 802.11i, WEP, 802.1X, PSK
- Dual-band, single-radio scanning
- Granular user profile-based management defines VLANs, QoS, mobility policies, and security policies for each user that enters the network
- Dynamic profile assignment based on device attributes
- Encryption: AES-CCMP, TKIP, and RC4 (WEP only)
- Time-of-day and day-of-week access control and SSID enablement
- On-board application-aware deep inspection firewall policy enforcement with session state sync with neighbors
- ALG support for SIP, DNS, TFTP, and FTP
- Destination-based MAC firewall support
- Up to 16 SSIDs per radio for network segmentation
- Tunneled guest networks
- Hive-wide client isolation
- WPA-TKIP vulnerability protection
- 802.11w management frame protection

Captive Web Portal
- Built-in customizable captive web portal on APs for guest access
- Automatic multi-language support based on user browser
- External captive web portal support and walled garden allows for easy integration with 3rd party Captive Web Portal solutions
- RADIUS support for captive web portal
- Microsoft Active Directory authentication for captive web portal

Cooperative RF Management
- Cooperative channel selection, with DFS2 support
- Real-time display and analysis of received RF signals with signature-based detection of non-Wi-Fi devices
- Station (client) load balancing based on client count
- Cooperative transmit power level control

Location and Asset Tracking
- Built-in client location tracking with topology and heat maps
- Partnership with AeroScout to act as a sensor
- Partnership with Ekahau for location and asset tracking
- Tracks laptops and asset tags

Authentication
- 802.1X authentication for WEP, WPA, and WPA2
- Private PSK authentication allows for unique preshared keys (PSK) for each user within a single SSID
- Self-registration portal for dynamic PPSK creation and assignment
- RADIUS support with PEAP, EAP-TLS, TTLS, LEAP, and EAP-FAST
- LDAP authentication to directory servers, including OpenLDAP, Novell eDirectory, and Apple OpenDirectory
- Authentication to Microsoft® Active Directory™ with local credentials caching, also supports Global Catalog and multiple forests
- Multiple RADIUS server support (per AP, per SSID)
- RADIUS server with local database or proxy
- Standard Interchange Protocol, version 2 (SIP2) support for validation of users against a Library Information Systems (LIS)
- Support for Operator-Name RADIUS attribute
- MAC-based RADIUS authentication
- Dynamic Change of Authorization (RFC3576)
- User profile assignment based on any RADIUS attribute
- 100 associated clients per radio

QoS for Voice, Video and Data at the Radio
- Powerful QoS features usually only found on high-end systems
- Stateful VoIP roaming and failover
- User profile-based queuing, scheduling and policing
- Application prioritization and control for nearly 1000 layer 7 applications including custom applications
- QoS assignment per VLAN, user profile, service, and MAC address
- Protocol decoding and dynamic port detection for SIP calls
- Full queuing support with 8 queues – strict and weighted round robin queuing mechanisms
- Per VLAN, per user profile, per user, per service rate limiting
- VoIP call admission control (CAC) with 802.11e traffic specification (TSPEC)
- 802.11r fast roaming support with 802.11k radio measurement and 802.11v roaming management
- Marking and policing – WMM® (802.11e) for wireless, 802.1p and/or DiffServ
- Wi-Fi CERTIFIED WMM
- WMM power save (U-APSD)
- Support for Spectralink SVP protocol

Management
- Central management
  - Management via HiveManager
  - Management via HiveManager Online
- Device Configuration
  - CLI via Telnet, SSHv2, or console
- Virtual Console automatically sets up an SSID with CLI access allowing configuration of new APs without the need for serial or Ethernet cables
- Monitoring
  - SNMP v1, v2c, and syslog

Wireless IDS & IDP
- Built-in in-network rogue AP detection
- Integration with AirTight IDS & IDP solution
- Rogue AP mitigation
- Rogue client detection including ad hoc clients
- 2.4GHz and 5GHz scanning on single-radio devices
- Wireless compliance checking
- Sophisticated L2/L3 DoS protection with a wide range of L2/L3 attack signatures
- Port scan, IP spoofing, and IP address sweep protection provides added security, particularly for quarantine and guest networks
- Wide array of security actions including logging, blocking, disassociation and banning to enable the network to automatically respond to threats

Mesh
- Flexible radio configuration allows for simultaneous operation of mesh networking and client access functions
- Ethernet bridging support across mesh connections for a single device or workgroup
- Automatic neighbor detection and route determination
- Mesh traffic encrypted with AES
- L2 routing rather than Spanning Tree used for greater performance and less overhead
- Self-healing enabled by dynamic path selection

High Availability
- Full client session synchronization across APs
- Stateful failover of any AP even in the event of a wire failure
- AAA caching of credentials for remote office survivability
- Mesh failover in the event of wire or switch failure
- Dynamic mesh failover automatically changes access radio to backhaul radio in the event of a wire or switch failure
- Wireless virtual access console
- Track IP or Gateway automatically initiates failover or troubleshooting tools in the event of a failure

Services
- DHCP server and DHCP relay
- Client operating system detection by DHCP and HTTP User-Agent for policy assignment
- Bonjour Gateway to enable network-wide advertisement of Bonjour services
- Mobile Device Management enrollment support: require client device registration to receive network access