

HiveOS®

Aerohive's Secure, Adaptable, Software-Defined
LAN & WAN Network Operating System



AEROHIVE®
NETWORKS

HiveOS®

HiveOS delivers reliable, high-performance Wi-Fi with integrated SLA governance, application-aware enterprise firewall security, device management, containerization, granular QoS control, advanced spectrum intelligence, machine learning capabilities and much more.

Aerohive HiveOS is the network operating system that powers all Aerohive access points, based on a feature-rich 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. Cooperative Control and HiveOS leads the industry with reduced deployment and ownership costs while delivering higher performance, reliability and scalability than competing architectures.

Key Features

Software-Defined Radios (SDR) & Machine Learning

Software-Defined Radios (SDR) utilize machine learning algorithms to evaluate current and historical RF conditions and reduce radio contention by automatically disabling redundant 2.4GHz radios, or, on some APs, reprogramming the radios to operate in Dual 5GHz mode. This process dynamically optimizes network configuration over time to deliver optimal performance and increased network capacity in ever-changing environments.

Application Visibility and Control (AVC)

Full context-based visibility and control of over 1200+ layer 7 applications, including the option to define custom applications and network services. 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.

Increase Network Capacity with Airtime Management

Aerohive's Dynamic Airtime Scheduling enables faster clients, like 802.11ac devices, 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 10x, by preventing slow or legacy clients dominating airtime.

Zero-Wait DFS

Dynamic Frequency Selection (DFS) is a mechanism that enables devices to coexist on the same 5GHz frequency space used by radar systems. Unfortunately, if an AP detects radar, it must vacate that channel immediately and scan an adjacent channel for radar. This scanning process can take several minutes to complete. Once the AP classifies the new channel as available, only then will it switch over. Zero-Wait DFS speeds up the scanning process. The result – more efficient use of the 5GHz spectrum with minimum interruption and downtime, even when using DFS channels.

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 a reliable service to client devices. The SLA feature not only provides the ability to set a performance threshold for connected clients but includes auto-remediation capabilities to re-allocate airtime to clients that do not meet the established SLA.

Private Pre-Shared Key (PPSK)

Aerohive's 'Private' PSK technology provides easy on-boarding and unique network identity to devices, without security or complexity concerns. Due to compatibility issues with 802.1X, PPSK enables stronger security for IoT and Guests. Easily revoke access for a single device or individual, without affecting other users. Prevent key re-use with simultaneous connection limits and MAC-address binding. Thousands of keys can easily be managed and distributed via the cloud, mobile applications and self-registration.

Private Client Groups (PCG)

PPSK is further enhanced by Private Client Groups (PCG) which enable administrators to manage and control network services through virtualized containerization based on micro-location. Create mini-private networks for each and every user based on their PPSK – perfect for hospitality and student accommodation.

Built-in Spectrum Analysis and Intelligence

Spectrum Analysis is a critical tool for detecting interference from non-Wi-Fi radio devices such as Bluetooth, microwave ovens and cordless phones. Aerohive includes Spectrum Analysis with advanced signature detection in many of our access points, 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.

SD-LAN Cooperative Control Protocols

Aerohive Channel Selection Protocol (ACSP)

Responsible for Radio Resource Management (RRM) with dynamic channel and power adjustment based on RF conditions. ACSP minimizes co-channel and adjacent channel interference to provide optimized performance.

Aerohive Mobility Routing Protocol (AMRP)

Automatic neighbor discovery, negotiation of client state information between APs and dynamic backhaul-mesh in the event of a failure. AMRP enables fast/secure roaming while maintaining client session state.

Dynamic Network Extension Protocol (DNXP)

Dynamically establishes tunnels between APs in different subnets in order to provide seamless L3 roaming.

Identity-Based Network Extension Protocol (INXP)

Provides the ability to define a static tunnel which can be used to pass client traffic, based on identity. Typically used for guest-to-DMZ isolation.

Aerohive Network Extension Protocol (ANXP)

Responsible for Private Client Group (PCG) client tunneling between neighbor APs and an anchor AP. This enables a user retain access to their PCG network while roaming.

Product Specification

Cooperative Control & RF Management

- Cooperative fast L2/L3 roaming
- Cooperative channel selection, with DFS support
- RRM achieved using ACSP
- Dynamic tunnel load balancing for L3 roaming
- Real-time display and analysis of received RF signals with signature-based detection of non-Wi-Fi devices
- Wireless client load balancing
- Wireless client band steering
- Transmit Beamforming (implicit and explicit) *
- MU-MIMO*
- Cooperative transmit power level control
- 802.11h/Transmit Power Control (TPC) *
- Zero-Wait DFS support to dramatically reduce DFS scanning process time *
- Support for Software Defined Radios (SDR) with dynamic learning & selection algorithm - Automatically or manually enable Dual 5GHz to increase performance & capacity *

SLA Compliance

- Client and AP Health – Monitor connection quality plus reporting and auto-remediation
- Airtime Boost – Automatically increase airtime allocation to suitable clients to boost performance
- Load balancing – Direct clients to APs for improved connection quality and resource distribution

QoS, Voice & Roaming

- QoS for Voice, Video and Data at the Radio
- Stateful VoIP roaming and failover
- User profile-based queuing, scheduling and policing
- Application prioritization and control for over 1200+ 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

QoS, Voice & Roaming (*Continued*)

- 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®
- Support for Spectralink SVP protocol
- Support for Lync, Skype and Skype for Business
- Hotspot 2.0 and PassPoint® Wi-Fi CERTIFIED™ *
- Voice Enterprise Wi-Fi CERTIFIED™ *

High Availability

- Full client session synchronization across APs
- AAA caching of credentials for remote office survivability
- Dynamic mesh failover automatically changes access radio to backhaul radio in the event of a wire or switch failure
- Wireless virtual access console – troubleshoot the AP locally without physically connecting
- Track IP or Gateway automatically initiates failover or troubleshooting tools in the event of a failure

Mesh

- Flexible radio configuration allows for simultaneous operation of mesh networking and client access
- Ethernet bridging support across mesh connections for 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

Security

- Trusted Platform Module (TPM) – Hardware-based key storage and encryption
- Wireless privacy and authentication Wi-Fi CERTIFIED™ WPA/WPA2 Personal and Enterprise, 802.11i, 802.1X, PSK
- Private Client Groups (PCG) enable the creation of 'private' networks using PPSK micro-location and micro-segmentation

Security (Continued)

- Granular user profile-based management defines VLANs, QoS, mobility policies and security policies for each network user
- 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 packet inspection (DPI) 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 for DMZ isolation
- Hive-wide client isolation
- WPA-TKIP vulnerability protection
- 802.11w management frame protection

Authentication

- 802.1X authentication for WPA and WPA2
- Private PSK (PPSK) authentication allows for unique pre-shared keys (PSK) for each user within a single SSID
- Up to 9999 local PPSKs per AP for AP230, AP250, AP245X, AP550, AP1130
- Up to 4096 local PPSKs per AP for AP122, AP122X, AP130, AP150W
- Self-registration portal for dynamic PPSK creation and assignment
- RADIUS client 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 credential caching. Also supports Global Catalog and multiple forests
- Multiple RADIUS server support (per AP SSID)
- RADIUS server with local database or proxy
- Standard Interchange Protocol, version 2 (SIP2) support for validation of users against a Library Information System (LIS)
- Support for Operator-Name RADIUS attribute
- MAC-based RADIUS authentication
- Dynamic Change of Authorization
- (RFC3576)
- User profile assignment based on any RADIUS attribute
- Up to 255 associated clients per radio for: AP130, AP230, AP245X, AP250, AP550, AP630, AP650, AP650X, AP1130
- Up to 100 associated clients per radio for: AP30, AP122, AP122X, AP150W

Wireless VPN

- Remote office IPsec-based VPN solution
- Profile-based split tunneling with NAT support
- Supported across mesh
- RADIUS, DHCP, NTLM, LDAP and NTP can selectively go to local or remote network
- Up to 127 GRE tunnels per AP
- Up to 128 L2 IPsec tunnels per AP (acting as L2 VPN server)
- Up to 1024 L2/L3 IPsec tunnels for VGVA

Captive Web Portal

- Built-in customizable captive web portal on APs
- Automatic multi-language support based on browser
- External captive web portal support, including Social Login, RADIUS authentication and walled garden configuration allows for easy integration with 3rd party
- Microsoft® Active Directory™ authentication

Wireless IDS & IPS

- Built-in in-network rogue AP detection & mitigation
- Rogue client detection including ad-hoc clients
- 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

Management

- Centralized management via HiveManager
- Device Configuration via CLI - Telnet, SSHv2 or console
- Virtual Console automatically sets up an SSID with CLI access allowing configuration of new APs
- Monitoring via SNMP (v1, v2c, v3) and syslog

Location and Asset Tracking

- Built-in location tracking with topology and heat maps
- Partnership with AeroScout to act as sensor
- Partnership with Ekahau for location and asset tracking
- Integrated iBeacon configuration

Services

- DHCP server and DHCP relay
- Client operating system detection by DHCP and HTTP User-Agent for policy assignment
- AP as a RADIUS server – up to 4 can be configured for redundancy. Optional RADIUS proxy for large deployments

IPv6-Ready

- Host-mode support for IPv6
- Interface IP address assignment via static configuration file entries or via SLAAC (RFC2462)
- DHCPv6 client for service auto configuration (RFC3315)
- DNS name resolution
- Multicast to unicast conversion
- IPv6 client address snooping and displaying
- Router Advertisement Guard
- DHCPv6 Shield
- RADIUS client for IPv6
- Support for Bonjour for IPv6 enabled clients
- Application Visibility and Control (AVC) (L7 inspection of IPv6 traffic)
- QoS for IPv6 enabled clients
- Firewall policies for IPv6 traffic
- Support for IPv6 devices to perform management functions through CLI or HiveManager
- Support for IPv6 versions of Ping, SSH, TFTP commands

