Aerohive NETWORKS

datasheet

HiveOS 6.1

Network Operating System Routing Features

HiveOS Routing delivers non-stop networking, branch routing with VPNs and enterprise firewall security to remote and branch offices.

Aerohive HiveOS is the operating system that powers all Aerohive devices. HiveOS Routing delivers non-stop networking, routing with VPNs, and enterprise firewall security to remote and branch offices.

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 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

Secure Auto-configuration

Aerohive's industry-leading secure auto-configuration avoids truck rolls. Secure auto-configuration prevents unauthorized users from gaining access to the home device. The administrator can enable an option which will require users to enter a device registration code when deploying routers remotely before HiveManager will be allowed to manage them. Doing so prevents unauthorized users from intercepting routers and using the auto provisioning feature to gain access to the corporate network.

Layer 3 IPSec VPN

With device-based IPSec VPN, HiveOS Routing enables remote users to get access to corporate resources via any authenticated device without having to worry about installing or maintaining software on their equipment. Combined with the local intelligence, cloud security services, and mobile device management capabilities of the Aerohive solution, every remote user experiences headquarters-like security and productivity, regardless of their location.

Cloud Proxy

Cloud-based security services ensure that branch office communications are "clean" without burdening IT with operating additional security appliances at each site, and without having to worry about configuring web proxy information on every end user device. Since most of the traffic generated at branch or remote locations is destined for the Internet, Aerohive's patent-pending Cloud Proxy automatically diverts that traffic through a cloud-based web security service. This diversion vastly reduces bandwidth costs by eliminating the need to route branch, remote office or mobile-user traffic back to a central location for filtering.

Network Flow-based Stateful Firewall

HiveOS Routing uses an advanced Network Flow-based Firewall that enforces policy at the network level, allowing the Aerohive device to manage traffic via a combination of user identity and very granular mobile device management. A user is granted access to network resources based on both who they are and on the type of device that they are using. This provides an invaluable extra layer of differentiated security that can change as your users change devices.

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

Warranty and Support

Every Aerohive Networks device is backed by a limited lifetime hardware warranty. Extended product and technical support may be purchased separately and can include next day advanced replacement, 24x7 or 8x5 technical support, web and email support access, and software updates. For complete support terms go to www.aerohive.com/support.

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 roaming
- Cooperative RF control
- Aerohive Mobility Routing Protocol (AMRP) for mesh routing to Aerohive APs

Support for 3G/4G USB-based WAN connectivity on BR platforms

Layer 3 IPSec VPN

- Remote office IPSec-based VPN solution
- IPSec hardware acceleration supported
- Profile-based split tunneling with NAT support

SLA Compliance

- Client and AP Health—Monitors connection quality and automatically triggers and reports on actions to improve quality

Security

- Patent-pending Cloud Proxy functionality to provide content filtering services to branch locations
- Wireless privacy and authentication Wi-Fi CERTIFIED™ WPA™ and WPA2™, 802.11i, WEP, 802.1X, PSK
- Granular user profile-based management defines VLANs, QoS, mobility policies and security policies for each user that enters the network
- Time-of-day and day-of-week access control
- On-board stateful inspection firewall policy enforcement with session state sync with neighbors
- ALG support for SIP, DNS, TFTP, and FTP
- Destination-based MAC firewall support
- Trusted Platform Module (TPM) - Hardware-based key storage and encryption
- Encryption: AES-CCMP, TKIP, and RC4 (WEP only)
- Up to 16 SSIDs and networks for client segmentation
- Industry-leading secure auto-configuration that avoids truck rolls

Flexible Route-based Load Balancing and WAN Redundancy

- Active-Active USB 3G/4G and Etho WAN
- Policy-based routes with failover
- Flexible failover tunneling configuration

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
- RADIUS server with local database or RADIUS proxy
- Standard Interchange Protocol, version 2 (SIP2) support for validation of users against a Library Information Systems (LIS)
- MAC-based RADIUS authentication
- Dynamic Change of Authorization (RFC3576)
- Up to 100 associated clients per radio

Captive Web Portal

- Built-in customizable captive web portal for securing wired port access
- RADIUS support for captive web portal
- Microsoft Active Directory authentication for captive web portal

QoS for Voice, Video and Data at the Radio

- Powerful QoS features usually only found on high-end routers
- Stateful VoIP roaming and failover
- User profile-based queuing, scheduling and policing
- 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)
- Marking and policing – WMM® (802.11e) for wireless, 802.1p and/or DiffServ
- Wi-Fi CERTIFIED WMM

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
- 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

- Central Management
  - Management via HiveManager NMS
  - Management via HiveManager Online NMS
- Device Configuration
  - CLI via Telnet, SSHv2, or console
- Monitoring
  - SNMP v1, v2c, and syslog

Services

- DHCP Server
- DNS Proxy
- Cloud Proxy

High Availability

- Full client session synchronization
- AAA caching of credentials for remote office survivability
- Wireless virtual access console
- Track IP or Gateway automatically initiates failover to USB or Ethernet