

Branch on Demand

Extending and Securing Access Across the Organization



Extending Access to Corporate Resources Across the Organization

As organizations extend corporate capabilities to teleworkers and branch offices, the added infrastructure and complexity can greatly increase costs and the burden on network administrators. This extra infrastructure usually requires support and maintenance in locations that lack IT staff and is difficult to deploy, configure, and secure consistently—even by skilled

The Aerohive Branch on Demand™ solution makes it easy to deploy corporate capabilities to employees anywhere, while reducing operational costs. The key lies in a suite of features and functionality designed specifically for remote environments that simplify operations, enforce security policy, reduce costs, and operate virtually maintenance-free.

Fast, Easy Configuration and Deployment

Remote employees are often not tech-savvy, and branch offices usually lack onsite IT staff, so remote wireless solutions have to be straightforward to install and configure. The Aerohive Branch on Demand solution allows anyone to simply plug in an Aerohive branch router, wait a few minutes for provisioning to be completed, and immediately access necessary resources.

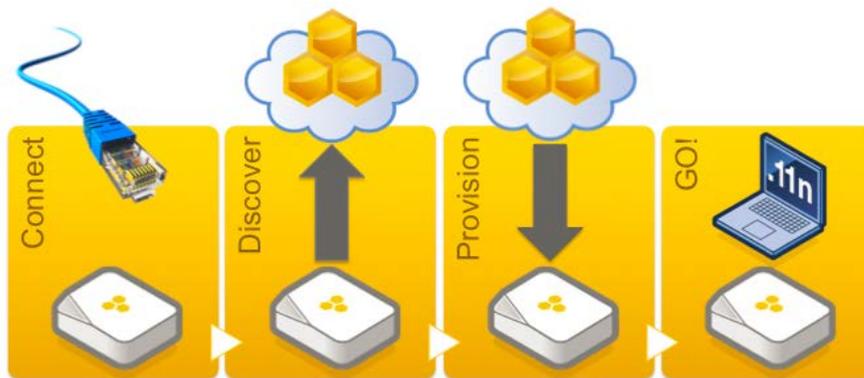


Figure 1: Zero Touch auto-provisioning removes any need for technicians onsite or truck rolls.

Aerohive eliminates the need for console cables, technical certification, or individual Secure Socket layer (SSL) virtual private network (VPN) clients to be installed on every connecting device.

Branch On Demand™

Aerohive's Branch on Demand™ solution redefines the economics, control, and performance of small branch and teleworker connectivity by leveraging our patent pending Cloud Services Platform to deliver a "Headquarters-like" network to every user regardless of location.

BR100/BR200

Branch Routers with built-in 802.11n



VPN Gateway

Virtual or Appliance



Cloud Services Platform

Integrated Cloud-based Services



Pre-configuration is unnecessary, because the highly intelligent Aerohive Cloud redirects every Aerohive device to its world-class HiveManager management platform, regardless of whether HiveManager resides in the Aerohive Cloud or on the local premises. Administrators simply:

- Create a configuration, which includes automatic IP address allocation (Figure 2)
- Provide parameters for branch routers to acquire the configuration
- Wait for remote users to plug in devices

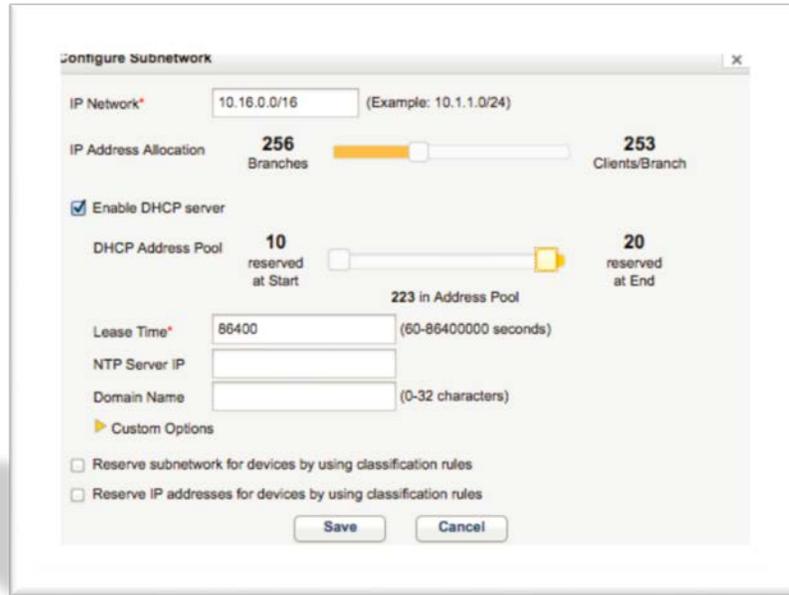


Figure 2: Automatic IP Address Management for the entire network of branch offices

Once a device comes online, HiveManager automatically pushes the configuration to it—and the remote site is up and running without requiring any administrator intervention.

Centralized Management and Visibility

When you deploy thousands of remote devices, they have to be easy to manage, maintain, and monitor. Typical remote solutions require multiple consoles for managing remote connectivity, security, and troubleshooting. However, HiveManager provides a centralized interface that enables administrators to easily configure any number of Aerohive access points and branch office devices. An administrator can manage thousands of devices as easily as a single one. HiveManager provides everything from integrated IP Address Management to autoprovisioning and consistent policy deployment across all Aerohive devices.

With Aerohive Branch on Demand solutions, administrators have ultimate control over access to resources. They can define which users and devices can access a branch router, as well as provide access to specific local and remote resources for each connected user. The Aerohive branch routers support wired and wireless access with secure authentication, including 802.1X, captive web portal, and Aerohive Private Pre-Shared Key.

Administrators can configure customized access based on identity to apply firewall policies, VLAN assignments, tunnel permissions, and Quality of Service (QoS) to users or devices.

Optimized Application Performance

The Aerohive architecture distributes all data forwarding and control mechanisms out to the Aerohive APs or routers at no additional cost eliminating the cost of deploying additional equipment, such as a WLAN controller, at each site, and minimizing bottlenecks that can occur when such equipment is used across a WAN link. Network security and performance enhancement services, such as real-time packet prioritization, WLAN airtime fairness, and policy based QoS are also distributed to individual Aerohive devices to minimize latency.

Consistent Security and Compliance

Consistent, reliable security is a requirement for large-scale distributed networks. However, traditional enterprise branch routers and security licenses are too expensive for small offices or individual teleworkers, and a software client becomes cumbersome when multiple devices are required per user or if corporate voice connectivity and Quality of Service are needed.

Aerohive's patent-pending Private Pre-Shared Key (PSK) system generates and manages separate pre-shared keys for every WLAN client. This enables multiple users, each with a unique key, to access the same WLAN, providing one-to-one authentication and strong encryption. Clients cannot eavesdrop on each other in a Private PSK system, and network access can be revoked on a per-client basis.

Aerohive Branch on Demand solutions use a patented N-Way Cloud Proxy feature to provide enterprise-class security at an affordable price point. With Cloud Proxy, an administrator can use a cloud-based security service, such as Websense or Barracuda Online, and route all remote web traffic through the service before sending it to its final destination. HiveManager also delivers high visibility through extensive logs and compliance reports.

Unified Wired and Wireless Policy

Branch deployments need policy for users and all types of devices with the assurance of access regardless of access medium. With HiveManager, an administrator can create customized access policies, based on identity and device type, which in turn can assign firewall, tunneling, network, and queuing permissions to any user/device

regardless of the user's location or access medium. HiveManager also provides complete visibility for:

- Users and devices connected to any Aerohive network device
- Permissions assigned to each user/device
- Historical device reporting, even if it moves between wired and wireless access environments

Teleworker Environments

Teleworking continues to grow in popularity as enterprises use it to reduce capital and operations costs associated with offices, parking structures, and other facilities. Teleworking also helps organizations achieve their sustainability goals and provides a cost-effective benefit that helps recruit and retain top talent.

Successful teleworking deployments deliver consistent, persistent access to the same resources that workers would use at the corporate office. This includes voice, teleconferencing, secure Internet connectivity, and cloud-based services or applications, such as *salesforce.com*. The Aerohive Branch on Demand solution provides standards-based IP Security (IPsec) VPN functionality to access corporate resources, as well as patent-pending Aerohive Cloud Proxy (NWay Split Tunneling) to ensure the integrity of web traffic by integrating with cloud-based security vendors, such as Websense and Barracuda.

Aerohive has seamlessly integrated remote routing functionality into its industry-leading, cloud-enabled networking architecture to provide easy-to-manage, secure, and reliable connections to teleworkers.

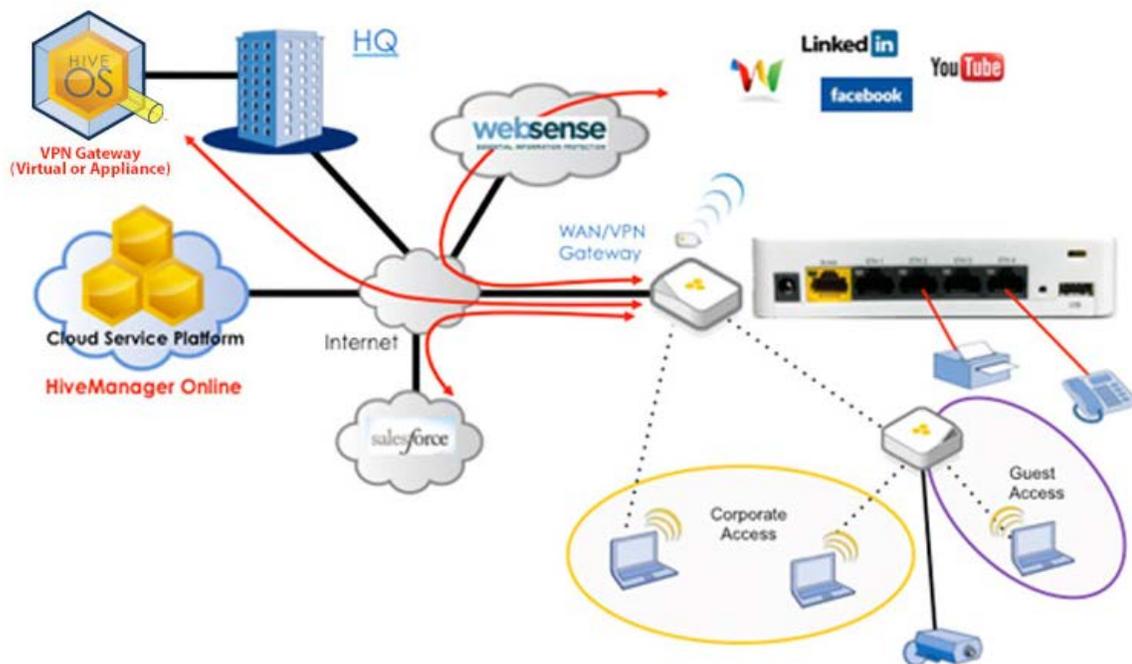


Figure 3: A typical installation of the Aerohive Branch on Demand teleworker solution

In this example, HiveManager provides easy configuration, monitoring, and troubleshooting for teleworker devices. The BR100 router discovers HiveManager using configured options or by querying the Aerohive Cloud for its assigned HiveManager, regardless of whether that HiveManager is in the cloud or on a customer premises. Aerohive also has a VPN concentration solution that can terminate IPsec tunnels from Aerohive branch routers. The solution is available as a single, rapidly deployable hardware appliance called VPN Gateway or as a software-based solution that runs on VMware-compliant equipment called VPN Gateway Virtual Appliance.

This teleworker scenario configures the BR100 branch router with multiple SSIDs. For example, one SSID is used for employee access using 802.1X and another SSID is for guest access using a pre-shared key. Four 10/100 Ethernet ports are also configurable to share a consistent VLAN with an SSID, or provide distinct access to the available networks, and can be protected using 802.1X, Captive Web Portal, or MAC authentication.

Traffic from authenticated employees can be routed across the VPN tunnel, as well as assigned to a priority QoS queue, separate from associated guest traffic. An administrator can configure the BR100 branch router to separate web traffic not destined for the VPN tunnel and send it through the Aerohive Cloud Proxy service to a remote security service. A wireless Service Level Agreement (SLA) can be configured to ensure that wireless access performance meets a sufficient standard for remote application access, and to automatically boost airtime for a user if the SLA is not met.

Branch Offices

Traditional branch-office VPN solutions generally add cost, complexity, and confusion to each location. Although branch offices represent about 20 percent of IT infrastructure, they often require 80 percent of IT's maintenance resources. Software solutions are less expensive, but quickly become unmanageable or inadequate when multiple devices or devices that cannot support VPN clients want to connect.

Through the cloud, the Branch on Demand solution simplifies provisioning, management, monitoring, and troubleshooting for branch office deployments, even without technical resources onsite. Enterprises can achieve significant CAPEX and OPEX savings while maintaining visibility into remote networks, meeting security objectives and compliance standards, and increasing productivity.

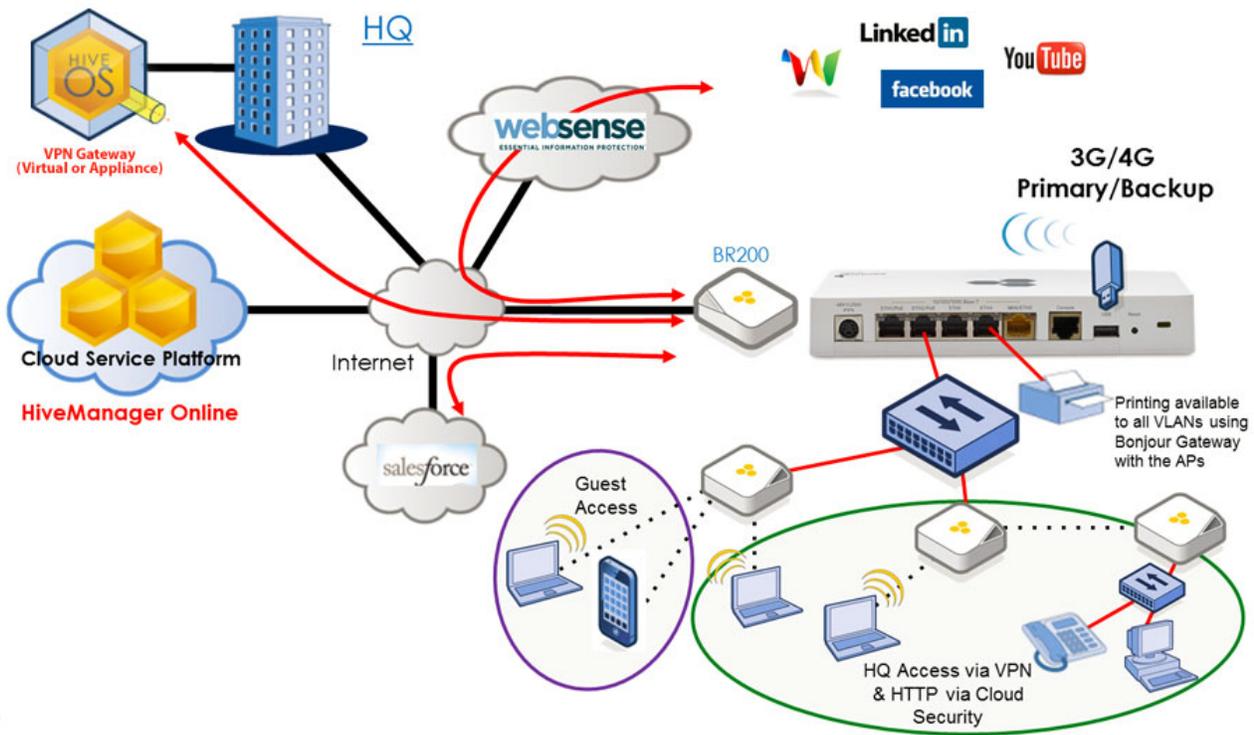


Figure 4: A typical Aerohive Branch on Demand branch office implementation

In branch deployments, reliable access to the central office, as well as secure Internet access for online applications and resources, is paramount. The Branch on Demand solution uses the Aerohive redirector to quickly and securely discover the HiveManager, regardless of whether HiveManager is online or at a customer premises.

Many branch offices, especially those subject to stringent compliance requirements like retail stores, will want to secure the Aerohive branch router in a wiring closet while still providing wireless access to the rest of the property. Aerohive makes it easy to extend wireless access by allowing an administrator to connect Aerohive APs through wireless mesh or wired Ethernet connections to branch routers. Administrators can configure APs to support multiple virtual LANS (VLANs) and user profiles, and can deploy a single policy to the entire location. This approach allows users to connect to any available AP and receive the correct permissions, based on their identity or device type.

User traffic can be routed across the VPN tunnel or to the Internet based on classic routing and firewall permissions. The Branch on Demand software also can separate “trusted” web traffic that should go directly to the Internet, and the Aerohive Cloud Proxy can allow an administrator to force all other web traffic to traverse an online security service.

Because all Aerohive devices support the same HiveOS network operating system, the BR100/BR200 integrate seamlessly with additional Aerohive access points and switches

in the network. Cooperative Control allows branch routers, access points, and switches to share user identity and device information across an entire hive of Aerohive products, and users will roam securely between devices and maintain permissions based on their identity and device type. Secure access for guests can be separated from corporate traffic and assigned to different network, quality of service (QoS), time-of-day access schedules, firewall policies, and web security settings, along with many other Aerohive features.

For More Information

Aerohive Branch on Demand solutions now make it easier and more cost-effective to implement wireless access to corporate resources everywhere—from the home office to branch offices and teleworkers. For more information about the Branch on Demand solution, visit <http://www.aerohive.com/solutions/applications/enterprise.html>.

About Aerohive

Aerohive was founded in 2006 and is headquartered in Sunnyvale, Calif. The company's investors include Kleiner Perkins Caufield & Byers, Lightspeed Venture Partners, Northern Light Venture Capital, New Enterprise Associates, Inc. (NEA) and Institutional Venture Partners (IVP). For more information, please visit www.aerohive.com, call us at 408-510-6100, follow us on Twitter @Aerohive, subscribe to our blog, join our community or become a fan on our Facebook page.



Corporate Headquarters

Aerohive Networks, Inc.
330 Gibraltar Drive
Sunnyvale, California 94089 USA
Phone: 408.510.6100
Toll Free: 1.866.918.9918
Fax: 408.510.6199
info@aerohive.com
www.aerohive.com

EMEA Headquarters

Aerohive Networks Europe LTD
Sequel House
The Hart
Surrey, UK GU9 7HW
+44 (0)1252 736590
Fax: +44 (0)1252711901