

Rethink Your Branch Network Strategy

Create More Flexible, More Productive Branch Networks



Table of Contents

- Introduction.....3
- The Challenge of Mission Critical Remote Workers4
- Where to Start: The model of a mission critical network.....5
- Square peg in a round hole.....6
- Branch on Demand™: Access Purpose Built for the Virtual Enterprise8
- Teleworker Environments11
- Branch Offices13

Introduction

Virtualization, cloud computing, and wireless technologies are fundamentally changing enterprise computing, providing revolutionary gains in productivity and cost savings. They are also driving a complete rethinking of enterprise networking architectural strategy. The well-documented impact of these disruptive technologies affect everything from server strategies to power requirements. However, one of the most affected areas—the enterprise network access layer—has been left out of the conversation.

Traditional enterprise network architectures establish “rules of thumb” for access technologies, setting a foundation for network design and allowing customization for specific needs. For example, the question “How many switch ports do I need on this floor?” used to easily be answered by counting desks and assigning three to four Ethernet ports per desk. The answer to “What network equipment and services do I put into each branch?” was easily determined by identifying number of people in the branch and the most affordable type of equipment to install.

Cloud computing, virtualization, and mobility have converged to fundamentally alter these base assumptions and force companies to rethink network access architectures, particularly their branch networking strategy. Cloud computing and powerful, smart mobile devices create an environment where one home-based employee can be performing a business-critical function—blurring the line defining the network edge. Often, branch offices and teleworker locations are where an enterprise's customers engage with their brand. Providing secure, robust information and functionality at the point of service can dramatically increase company performance and customer satisfaction. For these reasons, remote worker locations must also be controlled and secured as much as the corporate headquarters.

In today's virtual enterprise, access to corporate resources must be secure, reliable, and manageable, with consistently enforced policy while simultaneously allowing access from anywhere at any time. This is why access network strategies have become critical to business growth. If IT can empower every remote worker with the full capabilities available at headquarters, the business can differentiate itself and directly influence the company's bottom line.

In this paper, we will examine the requirements of providing and supporting a secure, robust, accessible remote network. Instead of returning to the costly, inflexible network architectures that have traditionally been deployed, we will show how enterprises can benefit from a cloud-enabled approach that pushes mission-critical security and functionality beyond the confines of the corporate headquarters; provides the flexibility and business agility needed to meet remote worker needs; and does not require “big iron” equipment to deliver but instead off-loads compute-intensive tasks to the cloud to redefine the economics of deploying remote networks.

The Challenge of Classic Branch Architectures

Traditionally, the network services delivered to branches and teleworkers were determined by the number of people in the branch or remote location. The “number of people” rule of thumb was created because the amount of equipment investment and administration increased as network service requirements increased. In other words, “the more people that work at a site, the more investment we can justify.”

Today however, secure, reliable network services are delivered based on the *functions performed* at each location. Smart, mobile clients, lightweight laptops, and cloud-based or hosted applications now enable critical functions to be performed anywhere, regardless of the number of employees. Providing IT services to branch locations represents an increasingly large piece of IT staff responsibilities – for management, security, and support of critical applications. However, if size justifies investment, no single location would qualify for support staffing or “big iron” equipment.

When many branches and teleworkers add up to big business, it is time to rethink classic branch architectures that limit your ability to deliver capabilities remotely. You cannot wait for the branch to grow to a size that justifies investment. Instead, *functions* at each location must drive network policy and service requirements.

Therefore, branch deployment must become more flexible, robust, cost-effective, and far easier to deploy and support. One option is to outsource branch capabilities management to a service provider. However, when there are hundreds of deployments as small as one teleworker, outsourcing can quickly become cost-prohibitive.

Where to Start: A Mission-critical Network Model

Rethinking the branch network strategy starts with creating a model for network services based on each location's functions performed and delivering services based on users' identities. Fortunately the work here is already done. The model for network services based on function already exists. Headquarters or main campus networks already provide full security policy based on user identity.

The main services you can expect from a headquarters network include:

- **Mobility/Wireless Control and Intelligence**
 - › Wi-Fi, survivability, resiliency
- **Routing and Networking**
 - › VPN, Ethernet, WAN backup
 - › Ethernet/Wired access
- **Address/L3 Service**
 - › IP address management, DNS, DHCP
- **Security and Authentication Services**
 - › Stateful firewall, authentication, Radius, 802.1x
 - › L4-7 protection (per corporate policy)
- **Identity-based Policy Enforcement**
 - › Mobile device access controls
 - › Quality of service
- **Management and Visibility**
 - › Client stats and connection health reports
 - › Wi-Fi information, client health, spectrum info, rogue AP
 - › VPN stats
 - › Compliance reporting
 - › Topology detail
 - › Problem remediation: remote packet capture, SLA compliance

This is simply a place to start. Every network is different, but this list represents many of the functionality requirements that headquarters networks meet in order to provide secure, reliable, wired and wireless access to support mission-critical applications. The question is how to deliver these services to remote locations, which requires that we understand the limitations of classic architectures in providing the above functionality.

Square Peg, Round Hole

The primary challenges of delivering headquarters-like service to remote locations are cost and complexity. You need to deliver functionality to each location without either budget busting or creating a management nightmare with inconsistent policies being enforced. Traditional solutions are not suited to today's virtual enterprise for the following reasons.

SSL Virtual Private Networks (VPNs)



Figure 1: SSL VPNs are good for single clients but difficult for multi-device users

Secure Socket Layer (SSL) virtual private networks (VPNs) have been used to connect remote users, assuming that the remote user has a single laptop device. In this scenario, SSL VPNs were sufficient. Although they required the user to configure a client device and log in to the network separately from a standard computer startup login, SSL VPNs were adequate and inexpensive enough per laptop to do the job.

Today however, mission-critical work is being done by remote and branch workers who increasingly need multiple devices to access corporate resources. Analyst firm IDC predicts that this trend will quadruple the number of smart mobile devices in the

enterprise between 2009 and 2014 and cause the number of mobile devices to outsell devices with Ethernet ports starting in 2011¹. For IT administrators, this means:

- 2 or 3 devices per remote worker need to be managed and secured
- SSL VPN client software will proliferate across every device, if it is even available, because almost no voice over IP (VoIP) phones have this capability
- Each device must be configured to be able to log in to the network in order to use corporate resources
- Each device would have to be licensed to terminate the VPN tunnels

Even if these conditions are met, maintaining a consistent usage policy across all clients becomes even more difficult.

Consumer “Off-the-Shelf” Solutions

Another common scenarios for connecting remote users is to purchase less-expensive, consumer-grade equipment. These solutions offer a promising price point, often enable wired and wireless access, and can be relatively easy to set up. However, problems quickly outstrip any savings when this method is scaled to try and secure dozens of hundreds of remote locations.

First and foremost, the lack of centralized management and policy creation capabilities require IT administrators to effectively “touch” each location to make configuration changes. If a security enhancement becomes needed, the administrator would have to log in to each device and make the same exact change to all to maintain consistent security enforcement. For an enterprise trying to secure many branches and teleworkers, this drastically increases network operating costs.

Even with a consumer-grade solution, you still need expensive headend equipment to terminate VPN tunnels. The capital expenditure forces you to commit significant resources just to begin a branch office rollout.

In spite of these drawbacks, consumer solutions may be the default option if the enterprise chooses not to support remote sites with wired and wireless access. Ultimately,

¹ “Market Analysis Perspective (MAP) Enterprise Communications Infrastructure Market” IDC Nov 2010

the ultra-light branch or teleworker will most likely purchase their own consumer device for convenience and the IT department must assume responsibility for its security anyway.

Traditional Enterprise Solutions

Traditionally, the surest way to achieve the required end-user performance, security, manageability, and policy consistency was to deploy low-end routing solutions from large networking suppliers like Cisco or Juniper. These solutions provide VPN connectivity, centralized management, and enterprise-class policy enforcement. But again, these solutions are still based on classic network architectures that dictate available network services based on office size. Classic architectures also struggle to embed more functionality into smaller offices, which operates contrary to their design philosophies. The inevitable result is:

- **Too many devices:** To provide the requisite functionality for an office of less than 20 people, you would need at least four devices: a VPN router, a managed switch, a managed access point (AP), and a headend VPN concentrator/gateway.
- **Cost:** These VPN solutions begin at \$1000 per connection and limit the scalability of wireless capabilities. For example, if WAN connections are in closets, additional APs will likely be required.
- **Labor-intensive:** Traditional enterprise solutions require that the VPN router be either pre-staged with information on subnets, gateway IP addresses, passwords, and other parameter, or that a technician be mobilized to the site to complete the install.

When an end location is an office of 1 to 20 critical employees, and there are hundreds of locations, this solution quickly becomes prohibitively expensive and operationally complex.

Branch on Demand™: Access Purpose-built for the Virtual Enterprise

Aerohive Networks has pioneered a new class of Cloud-Enabled Networking solutions that resolve the issues associated with traditional branch office connectivity scenarios. Cloud-enabled networking solutions allow IT organizations to drastically simplify and reduce the costs of delivering mission-critical network services. When the network must deliver corporate CRM, ERP, supply chain management, and other critical applications

to one or dozens of employees anywhere, Aerohive greatly reduces the provisioning, management, security, and optimization requirements.

The Aerohive Branch on Demand solution is purpose-built to address the short-comings of classic branch office architectures. By using cloud services, Branch on Demand redefines the economics, control, and performance of small branch and teleworker connectivity. “Headquarters-like” connectivity is delivered through a suite of features designed specifically to 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. Aerohive eliminates the need for console cables, technical certification, or individual SSL VPN clients to be installed on every connecting device.

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
- Provide parameters for branch routers to acquire the configuration
- Wait for remote users to plug in devices

Once a device comes online, HiveManager automatically pushes the configuration to it. The branch or teleworker is up and running without requiring 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 APs and branch office devices. An administrator can manage thousands of devices as easily as one. HiveManager provides everything from integrated IP Address Management, to auto-provisioning and consistent policy deployment across all Aerohive devices.

Deployment Flexibility

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 BR100 branch router supports:

- Up to eight Service Set Identifiers (SSIDs) for wireless deployments
- 16 distinct virtual LANs (VLANs) shared across wired and wireless interfaces
- Authentication such as 802.1X, captive web portal, and Aerohive Private Pre-Shared Key to distinguish users

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.

Consistent Security and Compliance

Consistent, reliable security is a requirement for large-scale distributed networks. However, dedicated branch routers and security licenses are too expensive for small offices or individual teleworkers, and a software client does not always provide sufficient coverage, especially when corporate voice connectivity is needed.

Aerohive Branch on Demand solutions use a patented N-Way Cloud Proxy feature to provide enterprise-class security at a telecommuter 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. In fact, Robert Half International found that of 1400 CFOs surveyed about the popularity of teleworking in their corporations, 46 percent said that teleworking is second only to salary as the best way to attract top talent and 33 percent said it is the top draw!

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 (N-Way 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.

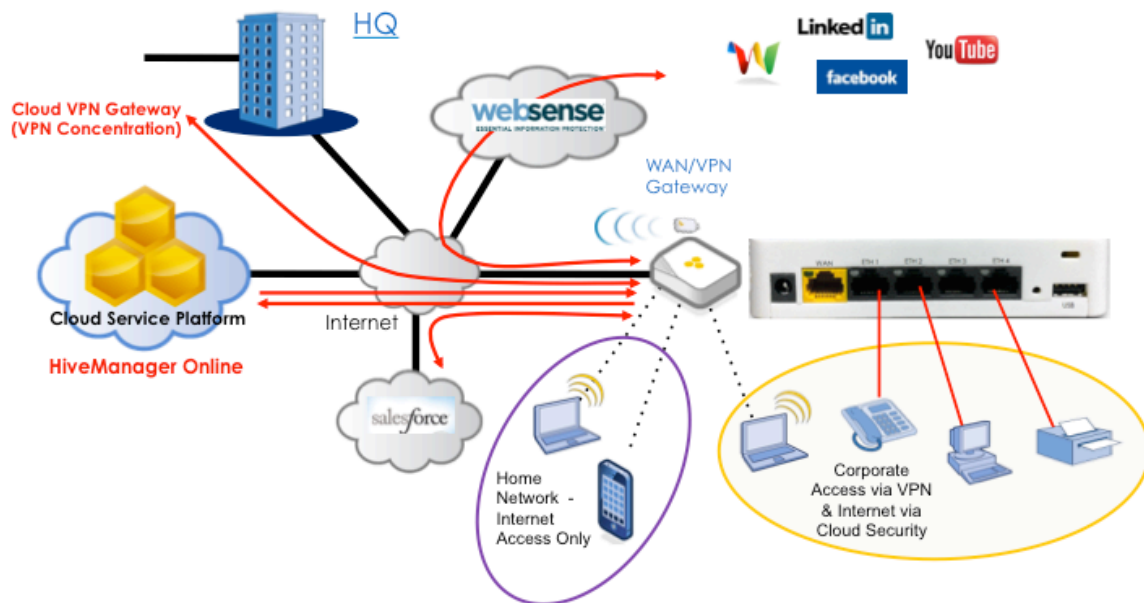


Figure 2 A typical installation of the Aerohive Branch on Demand teleworker solution

In this example, HiveManager provides easy configuration, monitoring, and troubleshooting for teleworker devices. The BR100 branch 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 has also introduced the Cloud VPN Gateway, a VMware-based appliance that terminates IPsec tunnels from Aerohive branch router devices. The Cloud VPN Gateway can scale based on the hardware dedicated to the VMware server and does not rely on HiveManager for connectivity.

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 LAN ports are also configurable to share a VLAN with a wireless SSID, as well as be protected by a Captive Web Portal.

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

BR100 branch router. Then they can configure the APs to support multiple VLANs and user profiles and deploy a single policy to the entire location. This approach allows users to connect to any available access point 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 Aerohive Mobility Routing Protocol (AMRP), a user can easily and securely roam between connected access points and the branch router as needed. Secure access for guests can be separated from corporate traffic and subjected to different network, 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 wired and 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 www.aerohive.com/solutions/applications/enterprise.html.

About Aerohive

Aerohive Networks reduces the cost and complexity of today's networks with cloud-enabled, distributed Wi-Fi and routing solutions for enterprises and medium sized companies including branch offices and teleworkers. Aerohive's award-winning cooperative control Wi-Fi architecture, public or private cloud-enabled network management, routing and VPN solutions eliminate costly controllers and single points of failure. This gives its customers mission critical reliability with granular security and policy enforcement and the ability to start small and expand without limitations. 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 and New Enterprise Associates, Inc. (NEA).



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

WP1101912