Aerohive NETWORKS

White Paper

The Benefits of Cloud Networking

Enable cloud networking to lower IT costs & boost IT productivity

Table of Contents

Introduction

The pressure to reduce costs for organizations, in either the public or private sector, is constant. At the same time, organizations have to maintain or improve user productivity and efficiency in all their departments to stay competitive. This issue of improving business practices and infrastructure with limited resources is a seemingly pervasive problem in today's markets. Innovative technology is one area where companies can look to help lower expenses with potential efficiency gains.

Specifically with respect to technology, many companies are taking advantage of the cloud to help with reducing expenditures while simultaneously improving productivity.

Cloud Service Applications

These days, there is a lot of publicity around the "cloud" and how many companies, regardless of vertical, are utilizing cloud technologies. It's important to quickly define what the cloud is before getting into more details.

At its basic level, the term "cloud-computing service" refers to the delivery of software, infrastructure, or storage via the Internet in real-time with pervasive access to the material available anytime or anywhere by devices with Internet capability. As opposed to traditionally having computing resources in-house, cloud-computing services provide a huge upside and workload shift for IT departments. They no longer have to spend a significant portion of their budget on purchasing dedicated hardware to run business applications or designate physical space for the hardware appliances. In addition, the time spent on configuring, maintaining, and updating dedicated hardware is virtually eliminated. Cloud providers remove these burdens from in-house IT teams.

Cloud services can be up and running in significantly less time than traditional physical installations, and in general, they cost less. With a cloud service, you just open a browser, log in, customize the application, and start using it. For example, most of us already use some form of cloud technologies today such as Web-based email service from Gmail or file storage services such as Dropbox or iCloud. In addition, with the continuing rapid growth of BYOD (Bring Your Own Device), cloud services enable users with their own personal mobile devices to instantly access applications or personal data from anywhere and at any time.

At its core, there are six key characteristics of cloud services:

On-demand self-service
End-users can provision computing capabilities, such as server time and network storage, as needed automatically without requiring the involvement of IT staff.

Broad network access
Capabilities are available over the network and accessible through standard devices including laptops and mobile devices.

Resource pooling
Computing resources are pooled to serve multiple end-users with different physical and virtual resources (storage, CPUs, memory, network bandwidth, and virtual machines) that are dynamically assigned based on demand.

Elasticity
Capabilities can be rapidly provisioned, to quickly scale as needed.

Measured service
Resource use is automatically controlled and optimized through metering, and resource usage can be monitored, controlled, and reported to both the provider and end-user of the utilized service.

Multi-tenancy
Shared resources serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

Cloud Networking

Cloud networking is a vital segment of cloud services and represents a fundamental shift in how IT services are provided to users.

Historically, a company's own IT department acquired, deployed, and maintained networking applications such as network management software. New applications and evolving use-cases often required the purchase of additional hardware such as servers. This leads to not only more capital expenditures, but also to increased support time that must be devoted by IT personnel. IT departments are already stretched while managing one central location, and when trying to deploy and maintain networking equipment and applications in distributed sites, the costs and support time needed by IT are compounded even further.

Cloud networking introduces a new way to deploy, operate, and manage distributed enterprise networks. It delivers enterprise-class network capabilities via a cloud infrastructure that requires little or no capital investment in additional hardware appliances or IT resources.

Unlike traditional hardware-based legacy solutions, cloud networking automates highly complex tasks to make them extremely simple, enabling enterprises to deploy locations in minutes and operate distributed networks with services delivered via a cloud infrastructure, while providing unprecedented levels of centralized control and network visibility. Cloud services are usually subscription-based as well, reducing any upfront capital costs.

Public cloud networking and private cloud networking are two distinct services. Public cloud networking is when a cloud provider makes networking applications available to IT users over the Internet with little to no deployment needed within the company's IT infrastructure. Public cloud networking services are also offered on a pay-per-usage model. Private cloud networking services refer to a proprietary computing networking architecture that provides hosted services to a limited number of users behind a firewall. For example, a company's internal IT department using a private cloud infrastructure essentially hosts applications within their own private network and provides them to their own IT users.

State of Cloud Services Market

Cloud service utilization by companies is quickly becoming as ubiquitous as using mobile devices. Cloud services, including those focused on cloud networking, are increasingly becoming an essential part of an organization's service to its users, and this is only expected to grow. In November 2014, a Gartner survey revealed that software-as-a-service (SaaS) deployments are now mission-critical and production grade.[1] This is an affirmation that more businesses are comfortable with cloud deployments beyond the front office running sales force automation and email.

According to IDC's update on cloud IT spending, worldwide spending on public IT cloud services was more than $56 billion in 2014 and is expected to approach $127 billion in 2018. From 2013–2018, public IT cloud services will enjoy a compound annual growth rate of 22.8%, six times that of the IT industry overall, as companies accelerate their shift to the cloud services model for IT consumption.[2]

"The IT industry is in the midst of an important transformative period as companies invest in the technologies that will drive growth and innovation over the next two to three decades," said Frank Gens, senior vice president and chief analyst at IDC. "By the end of the decade, IDC expects at least 80% of the industry's growth, and enterprises' highest-value leverage of IT, will be driven by cloud services and the other 3rd Platform technologies." More importantly, IDC believes the cloud services market is now entering an "innovation stage" that will produce an explosion of new solutions and value creation on top of the cloud.

[1] Source: Gartner Survey, November 2014, http://www.gartner.com/newsroom/id/2923217
[2] Source: IDC, November 2014, http://www.idc.com/getdoc.jsp?containerId=prUS25219014

Fears & Concerns with Cloud Networking

Cloud networking is rapidly being adopted by IT groups within enterprises. However, there are always concerns that need to be addressed:

Security
Security concerns usually need to be addressed first when IT managers are considering any cloud networking service. Many IT managers are apprehensive about the ability to control access to their sensitive data that would reside in the cloud and cannot afford the data being compromised. Despite the macro trend of moving to the cloud, some IT managers may still be more comfortable with their data deployed and maintained on their own infrastructure.
This fear can easily be alleviated by cloud networking providers clearly stating the physical security specifications of their datacenters as well as other security certifications they have attained. Cloud networking providers must also assure their IT customers that only users designated by them (the client) will have the ability to access and edit company data.

Privacy
Another key concern of IT management is maintaining privacy of networking data in the cloud. IT departments need to be assured that data is not being monitored either internally by the cloud provider or by any outside hackers. For example, some cloud clients may worry that if they can log-in from any location to access data and applications, it's possible the IT client's privacy could be compromised. However, cloud networking providers adopt myriad ways to protect privacy including using comprehensive authentication techniques and encryption methods.

High Availability
The ability to ensure high availability of data in the cloud is another common fear of IT teams. This is especially important for cloud networking as a company's IT department must keep their end-users happy and make certain the company's output and productivity won't be affected by any downtime. IT users are looking for some form of guarantee from providers that their networking data will be up and accessible at all times. For example, a service level agreement (SLA) that states 99.99% necessitates uptime of the cloud service in order to put this fear to rest. Cloud networking providers must also clearly state their resiliency plans including redundancy and backup measures in place for the utmost availability of data.

Poor Application Performance
Another inhibitor of deploying cloud networking pertains to poor application performance concerns. Companies can't afford to have IT users become less productive while waiting for browsers or applications that rely on cloud technologies to load. It is essential for cloud networking providers to continuously monitor usage to make sure any applications being accessed by their IT clients are being delivered optimally and efficiently.

Compliance
Many IT departments have to face regulatory compliance measures such as HIPAA (Health Insurance Portability and Accountability Act), PCI DSS (Payment Card Industry Data Security Standard), or Sarbanes-Oxley in order for their companies to stay in business. Companies that have to comply with such measures may fear moving to the cloud. Cloud networking providers must be transparent in sharing details such as encryption methods being used, the capability of generating audit reports, or the locations of their datacenters to help organizations maintain compliance.

Business Continuity
IT users also have concerns about recovering data from the cloud quickly in case of a man-made or a natural disaster. If they use cloud networking, IT needs to know how often backups happen (e.g., hourly or daily), where they happen, and how long data is archived from cloud networking providers, if at all. This fear can actually be mitigated as cloud networking would actually be an efficient means of backing up networking data. Instead of purchasing additional expensive networking gear in-house for backing up and storing data, a cloud networking provider delivering this capability would be more cost-effective.

Localization
Finally, IT departments may have concerns about using a cloud networking provider that may only reside in one region, like the United States. Often, if IT users reside in EMEA and/or APAC, they would like cloud networking services to reside in their local region. The rationale of having cloud networking localized could be due to local government rules or even comfort reasons of having a localized service. Most cloud networking providers understand this concern and have localized datacenters in the major regions of North America, EMEA, and APAC.

Over 10 years ago, there were fears about using online banking and how secure it truly was. People were concerned about paying bills online, moving funds among accounts, and even simply checking their statements online. But customers realized banks have it in their best interest to ensure they would feel safe using online services. Now, according to comScore, 1 in 4 Internet users access online banking sites globally. That represents over 423 million people[3]. Banks put in place strict security measures, ensure high availability of their service, and make sure their customers' account information is always backed up in case of any disruptions. Today, cloud networking providers are following similar procedures to help IT users stay comfortable with their service offerings.

Benefits Realized with Cloud Networking

While there are fears of using cloud technologies, the fact is that many networking applications are moving to the cloud and companies are beginning to understand the true benefits of cloud networking:

Lower Costs
According to the 2012 Cloud Networking Report by Dr. Jim Metzler, lower costs were identified as the primary driver for IT's interest in using SaaS-based services. With cloud networking, companies would have lower capital expenditures as opposed to purchasing all their own equipment and software. In addition, there is no worry about purchasing upgrades on hardware or software; the cloud networking provider takes care of this. Cloud networking is based on a pay-per-use model and payments will usually be monthly or yearly. Cloud networking is also considered a green solution since no rack space is used and results in lower utility costs.

Fast Deployment
Another major benefit of cloud networking is faster deployment as compared to purchasing and installing your own networking equipment. Many cloud networking applications such as network management can be turned on within a few days, hours, or even minutes depending on the provider. Using cloud networking lets IT users quickly utilize new applications without spending time installing and configuring networking equipment.

Productivity
By using cloud networking, the in-house IT staff can be off-loaded to focus on other tasks. IT doesn't have to worry about configuration or any maintenance updates associated with cloud networking service; this is fully taken care of by the cloud provider. IT's productivity will go up while any administration costs will go down.

Mobility
Since cloud networking applications are typically Web-based, IT users can access their networking-related data at any time and from anywhere using any device with Internet capability. IT users don't have to be tied to their desks. Along with the continuous growth of BYOD, IT users can take advantage of their personal mobile devices to access cloud networking applications and increase their productivity while they're on the road, roaming the office, or at home.

Instant Scalability
The ability to quickly add capacity is a huge benefit with cloud networking. Instead of IT procuring more networking hardware and/or software in-house for their additional end-users and waiting weeks or months to be up and running, cloud networking providers can quickly enable IT customers

[3] Source: comScore Data Mine, 2012, http://www.comscore.com/Insights/Data-Mine/1-in-4-Internet-Users-Access-Banking-Sites-Globally

to add more of their end-users or data instantly, sometimes within minutes.

Minimal Downtime
Updates related to cloud networking applications, as well as any networking infrastructure updates, are handled by the cloud provider. There is no need for the company's in-house IT department to worry about this and they don't have to bring the internal network down for updates. This is a tremendous advantage of using cloud networking since there is no downtime that could affect business.

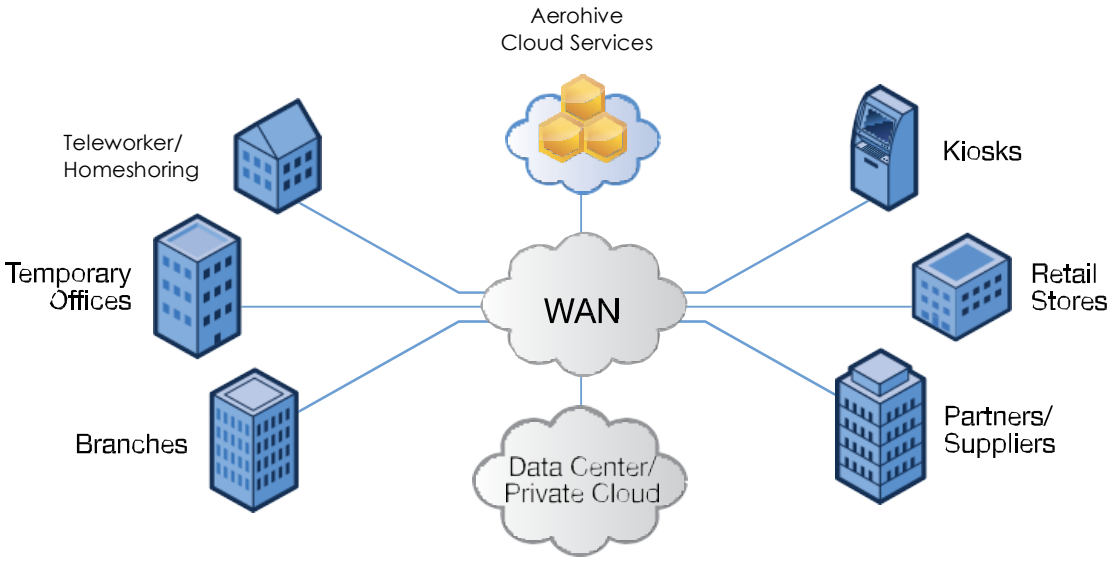
Great Security
Ironically, security, which is one of the greatest fears of using cloud networking, is actually a big advantage offered by cloud networking vendors. Most providers have stringent security policies for their cloud networking offerings. Encryption and authentication, data loss prevention, physical security of datacenters, firewall implementation, and malware protection are just a few of the security features commonly provided by cloud networking providers. Ultimately, they have it in their best interest to protect IT customers' data and ensure long-term loyalty.

Aerohive Networks' Cloud-Enabled Networking

Aerohive Networks is the pioneer of cloud networking technology and simplifies networking by reducing the cost and complexity of distributed enterprise deployments with cloud-enabled networking solutions.

Legacy networking deployments required the purchase of networking hardware such as switches, routers, or wireless access points, as well as the purchase of centralized controllers and licensing for network management at each location requiring a mobility infrastructure. Any additions or changes in the networking hardware, or additional end-users put strain on the existing infrastructure and on the IT staff to manage. Cloud-enabled networking removes these centralized controller burdens while lowering CAPEX and utility costs, providing instant-anywhere access via a Web browser, and delivering unlimited scalability.

The Aerohive Cloud Services Platform is a globally distributed, cloud-based infrastructure that is home to Aerohive-developed SaaS applications. The Aerohive cloud-based infrastructure delivers network management and mobility applications giving customers a single, unified and contextual view of the mobile-centric network edge. The Cloud Services Platform is hosted in secure SOC Type II compliant datacenters, with 24x7 monitoring, scheduled backups and disaster recovery capabilities. The result is robust cloud-enabled network solutions for Aerohive customers that are provisioned through Aerohive's own HiveManager Online and HiveManager NG SaaS.



Aerohive Key Cloud Capabilities

- SaaS applications provide flexible and economical network security and mobile device management capabilities, enabling organizations of any size to start small and grow incrementally
- Out-of-band applications allow capabilities to be deployed and managed even without a direct connection to the corporate data center
- Globally distributed Aerohive datacenters provide a 99.9% uptime SLA, backup services, and data privacy to ensure services and data are always safe
- Decentralized intelligence means your network doesn't change functionality if connection to the cloud is lost.

More technical details about can be found in Aerohive's Cloud Services Platform white paper.

Currently, Aerohive offers the following three cloud-enabled services for customers.

HiveManager NG

HiveManager NG is Aerohive's next generation enterprise-class cloud-enabled network management solution. It sets a new standard for simplicity and flexibility in unified networking by combining streamlined configuration workflows, real-time client and event monitoring, simplified troubleshooting, versatile RF planner tools, and API integrations. HiveManager NG truly provides a platform for enabling a next-generation network focused on mobility. Some of the key benefits include:

Simplified Deployment
Simplified deployment workflow and seamless transition from demo to production

Centralized Configurations
Granular and streamlined device and network configuration

Centralized Policy Management

Context-aware user policies with granular and flexible control enable IT to deliver an optimized end-user experience

Dashboard

Dashboard with contextual filters and time range slider enables monitoring of network from assets, health status, data usage and security standpoints.

Monitor
Real-time and historical view of devices, clients, alarms, and events. Ability to take informed action immediately from the monitor interface

Troubleshooting
Help-desk optimized interface to triage client problems with actionable data for resolution to reduce escalation and provide better end-user experience

HiveManager Online

In legacy networking environments, often a dedicated hardware appliance was necessary to run network management software for monitoring and managing the networking equipment such as wireless access points. Network management typically requires IT to install and configure a hardware appliance. There's also the added task for IT to continuously manage and update the appliance on a regular basis. And this scenario is in just one location. Now imagine when organizations have many distributed locations and want to efficiently manage the network on a per location basis. This only

compounds the capital expenditures for numerous appliances and time needed for set up in each site. Many companies simply won't have the budget and IT resources to accomplish management across multiple locations.

To make IT department's life easier, Aerohive offers HiveManager Online Network Management Service. HiveManager Online is a cloud-based SaaS network management system for Aerohive network devices. HiveManager Online eliminates CAPEX associated with dedicated network management appliances and shifts expenses into a pay-as-you-go model. This reduces the initial costs of network management. There's no management appliance to deploy, manage, or take up any rack space per location. Since it's a cloud-based solution, it simplifies a company's ability to manage one or many locations. Network management can be done centrally by just one IT person and can easily be done via a Web browser from any location at any time.

HiveManager Online offers the same simple policy creation, firmware upgrades, and centralized monitoring options as the on-premise version of HiveManager, however, without the need to deploy another device in your network. HiveManager Online is hosted within

secure Tier IV SAS 70 Type II datacenters, with scheduled backups and disaster recovery capabilities. More details about Aerohive's backup and upgrade policies can be found in the Cloud Services Platform white paper.

ID Manager

Access for employee and guest devices is a common request that must be handled by any organization. There will always be employees, visitors and contractors who will need Internet access or access to corporate resources. As Wi-Fi continues to be the predominant method of access, employees and guests will want to be able to connect easily and quickly from any of their devices.

Each guest is unique and needs to be granted different levels of access depending on who they are. An infrequent guest may require basic Internet access, but a contractor will likely need to access the company's intranet site and its resources. On the other hand, employees require access to the secure company network with all associated functionality. Setting up capability for BYOD is not an easy task. In order to authenticate users, a RADIUS server and its associated software often are required to provide AAA management to devices requiring access. This requires additional equipment to be purchased, installed, and maintained. The set up for this can be cumbersome and requires dedicated IT staff at the location. Additionally, it can get quite expensive and complicated when a company has distributed locations.

Companies today need a simple, cost-effective, and easy-to-deploy solution that doesn't require dedicated equipment and IT experts at each location. The solution needs to be simple enough for non-technical employees and lobby personnel to use for setting up guest accounts without losing the robust security features. It also needs to be scalable, with the ability to be deployed instantly at any location when needed.

ID Manager is the first employee and enterprise guest management system to leverage the cloud to simplify and automate the deployment and maintenance of BYOD management. Aerohive simplifies BYOD management by combining industry-leading authentication integration with the Aerohive Cloud Services Platform to eliminate the need for any additional hardware or software to deliver a scalable, simple-to-administer enterprise BYOD management solution that streamlines the on-boarding of employees and visitors.

All Aerohive devices run HiveOS, Aerohive's network operating system, and already provide industry-leading authentication services and integration with existing directory services such as RADIUS. ID Manager leverages this capability and uses RadSec to create

an authentication-specific private connection between the Aerohive devices and the Aerohive Cloud Services Platform. This allows for global security policies for employees and

for any guest. It allows employees to instantly authorize enterprise visitors, who are then policed by corporate use policy, anywhere in the world. Multiple secure guest profiles can be established and automatically applied to the visitor – from casual guests to fully secure temporary employees – ensuring that every guest has precisely the access you intend without requiring intervention from IT or helpdesk staff.

By leveraging the cloud, ID Manager can be deployed to any office with an Aerohive network, anywhere in the world - instantly. There is no additional hardware or software to buy since the cloud vastly simplifies the deployment and maintenance of BYOD management from one to many sites.

Branch on Demand

Organizations are not just limited to one location in many cases. They have distributed branch offices and teleworkers as well. Ensuring branch office employees and teleworkers have the ability to access corporate resources is critical for a company's distributed workforce to stay productive. However, to achieve true distributed corporate access, additional networking equipment is typically needed for branch offices and teleworkers. The added equipment inevitably leads to additional support and IT personnel needed to maintain the equipment. Remote users are often times not technically proficient to set up network access easily and on their own. Realistically, it just isn't feasible for companies to have dedicated support and resources available for each of their branch offices and teleworkers. What's needed is a solution that enables employees to simply plug in equipment, wait a few minutes for automated set up, and then immediately begin their access.

The Aerohive Branch on Demand solution makes it easy to deploy corporate capabilities to employees anywhere, while reducing operational costs. The solution is a complete branch office network solution, purpose-built for small branches and teleworkers, that combines the BR Series branch router platforms, HiveOS routing capabilities, and a Cloud VPN gateway which all can be run on Aerohive's Cloud Services Platform. Enterprises can provision branch office networks and teleworkers with just a few clicks.

Based on the HiveOS operating system, Aerohive branch routers require minimal intervention from the end-user. They simply plug the branch router in, and the device will leverage Aerohive's Cloud Services Platform to do the rest. The branch router will automatically find its HiveManager, download the corporate security policies, establish its VPN connection if necessary, and the office is up and running in minutes. There is no need to install complex VPN systems, download client software onto each user device, or train users on VPN use.

Further details on Aerohive cloud-enabled applications can be found here.

Summary

As described in this white paper, cloud networking has matured beyond an emerging technology and is being used by IT departments worldwide. IT users are running various networking apps in the cloud, like VoIP, network management, unified communications, virtual desktops, and more. Many organizations have devoted their IT spending now and in the future to take advantage of cloud networking as they realize the benefits it can bring.

IT departments see how cloud networking enables them to become more agile and save costs. Cloud networking will remain an area to help IT managers reduce capital expenses and off-load department resources to focus on other critical tasks. In addition, cloud networking goes hand-in-hand with the BYOD and pervasive mobility trend. As users in general continue to use their own personal mobile devices for corporate network access, IT users will also certainly use those devices to access any cloud networking applications as well.

Aerohive Networks recognizes the efficiencies of cloud networking and delivers a set of SaaS-based applications that reside on its Cloud Services Platform infrastructure. These applications currently include HiveManager Online, HiveManager NG, ID Manager, and Branch on Demand. Each of these applications leverages the scale, availability, and economies of the cloud to minimize in-house IT resource use, network provisioning complexity, and operational cost. Additionally, these applications help reduce an IT customer's capital expenditures by minimizing the amount of hardware and software equipment needed for one or more locations. Aerohive knows the world is moving to the cloud and will continue to provide exceptional cloud networking services to enterprises, branch offices, and teleworkers.

About Aerohive

Aerohive (NYSE: HIVE) enables our customers to simply and confidently connect to the information, applications, and insights they need to thrive. Our simple, scalable, and secure platform delivers mobility without limitations. For our tens of thousands of customers worldwide, every access point is a starting point. Aerohive was founded in 2006 and is headquartered in Sunnyvale, CA.

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
info@aerohive.com