



MSP Remote Device Support —a New Approach, a Better Technology

Are today's enabling technologies for remote device support meeting managed service providers (MSPs) expectations? We think not.

As enterprises continue to look to IT outsourcing as a means of increasing efficiency of network operations, the opportunity for managed service providers (MSPs) to increase market share grows accordingly. Additionally, MSPs are poised to take advantage of this market trend by not only growing their customer base, but by improving upon the services they currently offer, thereby fending off potential competitive threats.

As MSPs compete for business, they must adopt new enabling technologies to offer true value-added services. These technologies ultimately influence a potential customer's decision to outsource. MSPs must be able to demonstrate to potential customers that they can commit to a level of remote support service previously unachievable via standard remote access methods.

MSPs must demonstrate their ability to provide a full service outsource solution that extends beyond basic remote monitoring, and includes proactive issue discovery as well as rapid response to poor network performance or outages. Today, the majority of remote services are based on legacy transport mediums, such as; dialup, leased lines (frame relay or private), or VPN. Although each can be used to gain visibility into customer locations and can enable remote managed services, each has certain limitations:

- Monitor-only solutions typically require personnel dispatch for repair and maintenance resulting in delayed response.
- Reliance on third-party service providers for installation can result in delayed customer turn-up, delayed customer acceptance, and ultimately, lower customer take-rate.
- Bandwidth limitations can prohibit the ability to offer value-add remote services.
- Remote access equipment requires continued maintenance and provisioning.
- Revenue potential is impaired by the recurring cost of access lines per device at customer locations.
- Managed services are burdened with ongoing customer security concerns and new auditable compliance requirements.

According to industry studies from both Forrester Research and the Aberdeen Group, the managed services market is expected to grow by 30% this year (2007). Customer demand for higher asset uptime has driven MSPs to evaluate next-

generation tools that not only meet customer service level expectations, but also enable MSPs to offer differentiating services. However, there is an absence of available tools that provide both a remote monitoring and remediation solutions on the market. As a result, many MSPs choose to stay with their current connectivity methods or are forced to use multiple disparate tools which introduce complexity and cost to their services operations.

To adopt a newer technology, it must enable MSPs to achieve a greater level of operational efficiency. This increased operational efficiency must allow MSPs to differentiate their offerings against competitors and provide a better means for servicing customers. Therefore, any such technology has to prove beneficial to both MSPs and their customers by achieving the following:

- Creating visibility into customer locations with rapid installation and deployment, eliminating the need for dedicated access lines per device or site.
- Providing a simplistic implementation by avoiding disrupting customer networks, resources, and security requirements.
- Reducing operational costs by enabling remote repair and maintenance, thereby eliminating the need for truck rolls.
- Providing "always-on" available bandwidth to enable value-add services, to exceed customer required SLA levels.

With the maturity of the Internet, MSPs now have an instant, ubiquitous backbone infrastructure to address both multiple-site access limitations and recurring cost issues associated with dedicated lines (i.e. analog or leased lines). While the Internet alone does address multiple site access limitations, it does not address security requirements. In an attempt to comply with the security requirements of their customers, MSPs have historically tried using VPNs across the Internet to provide secure remote device support.

Although VPNs are a proven technology for network to network connections and allow MSPs to leverage the Internet as an IP-based transport solution, they only address the transport portion of a remote support strategy. All other factors involved in providing secure and controlled access remain. These factors include: address overlap, network address translation, access control, rules and policies, and event correlation.

These other factors must be properly addressed to achieve an acceptable level of security and service. To address these other factors in a VPN scenario requires coordination and highly-skilled expertise from both MSPs and customers. Also, additional equipment is needed by both parties on both sides of the connection, which requires constant updating.

Therefore, an optimal solution offered by MSPs must utilize a technology that removes the barriers between the MSP Network Operations Center (NOC) and the targeted device(s) at the customer sites. An optimal solution is one that utilizes a technology that creates a Virtual Service Infrastructure (VSI) which can seamlessly monitor and access customer equipment without jeopardizing the customer security.

In a Virtual Service Infrastructure, MSPs have the ability to utilize the Internet as a secure backbone infrastructure for network connectivity, logically extending the physical reach of an MSP's existing network beyond its NOC by expanding the footprint of its network. MSPs achieve this objective by removing geographical, physical and technical boundaries between the MSPs' NOCs and their customers' remote sites and devices. Leveraging the Internet in the VSI model, MSPs now have a ubiquitous and rapidly deployable network and a direct link to their customers' devices, thereby creating a secure virtual LAN that behaves as if specific customer devices are located at the NOC facility, regardless of where they actually geographically reside.

This virtual network expands beyond the MSP customer demarcation point. Customers are now able to eliminate all of the standard transport devices and tasks typically associated with standard VPN approaches. This includes all of the tasks involved in allowing an untrusted entity (i.e. the MSP) to gain access into the customer's trusted networks.

A virtual network dynamically applies all the visibility rules and policies required within the private network, thereby eliminating the chances of security breaches caused by human error during setup, and removal. In addition to eliminating these very complex steps, a VSI assures that the information being transported from a customer's device to the NOC is done so in a highly-secure and auditable method, assuring the MSP's adherence to its customer's internal policies, as well as compliance to new government regulations.

Technology that is in-tune with the VSI model can benefit both established and emerging MSPs that are looking for solutions that achieve an efficient Cap-ex and Op-ex method for supporting their customers SLAs.

Emerging MSPs now have an out-of-the-box method to attract and obtain new customers via the VSI's use of the Internet as the backbone infrastructure. It enables dynamic and secure policy-based control of access to customer sites. Further, due to its rapid deployment, it enables a quicker take-rate on evaluation, and it does so without reliance on local service providers for connectivity, or customer site network reconfiguration.

Established MSPs now have a migration path to IP-based managed services. The VSI can be used initially as a backup solution to their current architecture, and allow them to migrate their customers, with no impact to their customers' network. Further, as the VSI is agnostic to any Network Management Platform, MSPs' existing investment in their management platform is still fully optimized.

Independent of the MSPs' tenure, there is now a seamless method to meet the needs of their diverse customer base, both in terms of scale and service level requirements. This is true whether their offering is a monitor-only service level or a full turnkey offering, including device troubleshooting.

A VSI provides the means for MSP personnel to leverage their best of breed existing network support applications to achieve proactive support services with the bandwidth and security required between the Operations Center and the targeted customer network element(s). This is all performed on-demand without impacting

the customer's resources or corporate security, resulting in a lower total cost of ownership and improved customer satisfaction.