WHITE PAPER

Virtual Edge Solution

A New Opportunity for Managed and Cloud Service Providers

netsocket™

Contents

Introduction

Less than 10 years ago, the number of businesses implementing private cloud virtualization was almost non-existent. Today, more than 40 percent of enterprises have adopted or are evaluating virtualization in the data center as a competitive advantage for their distributed networking environments. Further fueling the adoption of virtualization is the rapid move toward Software-defined Networking (SDN) technology. SDN offers the promise of simplification, elasticity, and affordability so that networks can respond quickly and adjust dynamically to automated business policies and consumer demand, and network administrators and MSP service desk personnel can provide faster deployment of new applications and introduce new features and functionality without disrupting network operations.

"Netsocket has a really good understanding of the way applications are used in the branch and through the enterprise. Also, they have extensive routing capabilities bundled into the controller."

– Brad Casemore,
Research Director, IDC

According to industry experts, these technological influences are reshaping the network as a whole and upending the once previously well-defined network edge. As a result, enterprise and Small to Medium Sized (SMB) executives, as well as the service providers who support them, must rethink longstanding approaches to network growth and sustainability, particularly at the edge.

Network edge virtualization, unlike public and private clouds that are typically associated with the data center, has a distinctive set of network attributes. Located at the WAN interface of a distributed Small and Medium Size Business or a remote site in a larger enterprise, the network edge is typically bandwidth constrained; has less than 200 users or devices; and requires firewall, network address translation (NAT), and subnet functionality, as well as security/quality of service policies and network access control (NAC) features.

Analysts at IDC and Gartner believe that virtualization of the network edge, via well-architected SDN-based solutions, is inevitable and that this technology will completely replace purpose-built applications and legacy systems at the edge.

Netsocket agrees. This is why the company has devoted its considerable years of experience and expertise to the development of the Netsocket Virtual Network (NVN), a distributed virtualized SDN-based network composed of layered applications that deliver Wide Area Network (WAN) edge routing, as well as layer 2 and 3 switching, firewall and tunneling service. Among the solutions available using NVN components is the Virtual Edge solution, which can be deployed to multiple, distributed SMB sites and enterprise remote offices.

This whitepaper will identify the need for and benefits of network edge virtualization for enterprise and distributed SMB environments, as well as for the Managed Service Providers (MSPs) who support these complex, highly-distributed network ecosystems. It will also explain how a completely virtualized, SDN-based network edge solution can provide a cost-effective, flexible, and simple to use platform that enables businesses to easily grow their networks and deploy value-added services at their own pace.

The Challenge at the Network Edge

The ever increasing demands on legacy networks from 'big data', BYOD, layered security, efficient backup, and constant traffic with cloud-based resources have made traditional layered network design unsustainable over the long term. Over the last few years, the networking industry has responded to this challenge with SDN technology, solutions and products that represent a substantial step toward addressing the agility and cost issues characterized by legacy networks. Yet the network edge remains relatively uncharted territory with regard to SDN-based virtualization.

In essence, the same issues that once plagued customers at the data center edge continue to remain front and center at the network edge:

- traditional network products are too expensive and rigidly inflexible;
- maintenance and support costs are both high and too unpredictable;
- IT at the SMB level is not a core business competence; and
- all businesses, regardless of size, want to focus on their key business initiatives instead of worrying about the network.

Customers need a cloud-managed virtual network that is optimized for enterprise and SMB LAN/WAN deployment – one that provides the flexibility and scalability their business needs to meet existing and future network requirements.

RELIABLE, SECURE EDGE CONNECTIVITY FOR BRANCH AND REMOTE OFFICES

What customers want is a simple-to-install, cost-effective solution that provides secure, reliable edge connectivity for branch and remote offices. What they need is a cloud-managed virtual network that's optimized for enterprise and SMB LAN/WAN edge deployment and can:

- provide on-demand network scalability to meet existing and future business needs on a 'pay as you grow' basis;
- allow for immediate response to service requests for network configuration changes;
- enable 'whenever' access to needed business services, such as 4G WAN backup, security/UTM, session border control, voice services, and more; and
- facilitate predictable maintenance and support costs.

Given the virtualization technology trends and challenges described above, Netsocket believes that there is a significant opportunity to change the way in which networks are installed, deployed, and maintained at the network edge, making them radically more responsive to the constantly changing business needs of enterprises and distributed SMB environments.

Virtualized SDN for the Network Edge

Netsocket is at the forefront of delivering virtualized, Software-defined Networking to the edge. The Netsocket Virtual Network (NVN) is an advanced framework for network virtualization, with powerful automated orchestration capabilities for centralized design, management and deployment of software-based networks.

Composed of layered virtual system components, NVN delivers wide area network (WAN) edge routing, in addition to layer 2 and 3 switching, firewall, and tunneling services. All NVN software components operate in virtual machines on a low-cost, commodity X86 server platform. No application-specific hardware is required to operate any NVN software component.

The Netsocket Virtual Network Architecture

At its core, the NVN solution utilizes a three-tier SDN architecture that spans the application, controller, and infrastructure layers. Within these layers are virtualized system components – the vFlowController™, vFlowSwitch™, vNetCommander™, and vRemoteAgent – that can run on commodity x86 server platforms and provide a layered connection to the underlying network, enabling system administrators to more easily view and manage what is going on in the network.

The Netsocket Virtual Network delivers:

- Flexibility of configuration and management, enabling the adoption of automated orchestration and next generation management user interfaces and APIs;
- Seamless legacy network interoperability, achieved through intrinsic routing capability in the controller, allowing an ‘at-your-pace’ network migration path;
- Commoditization of switching functions, eliminating the need for any network hardware other than commodity layer 2 switches and off-the-shelf x86 servers; and
- Automated networking through NVN applications that are network configuration and operational state ‘aware,’ and capable of adaptively monitoring and controlling underlying network services.

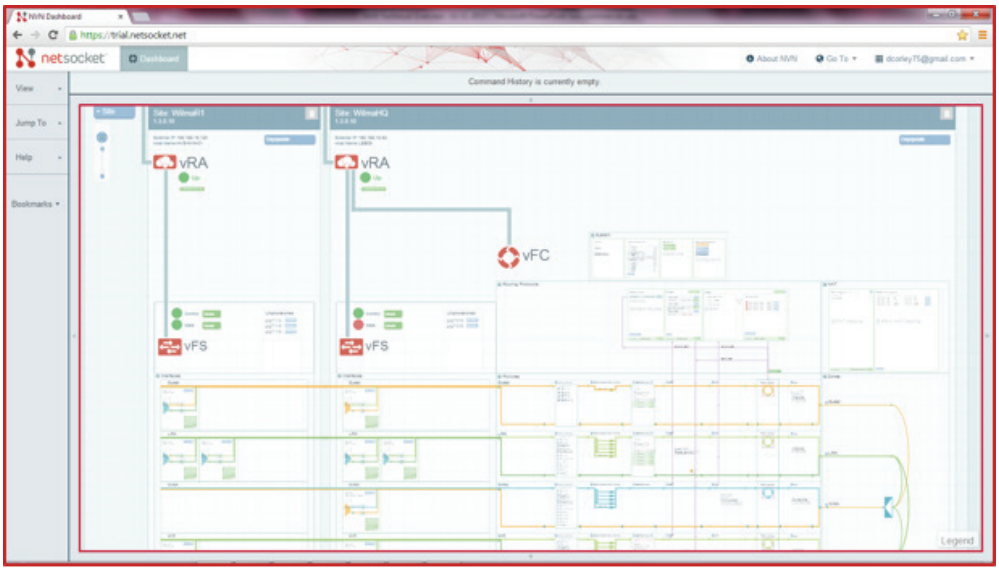
A Completely Virtualized Network Implementation

At its core, the NVN utilizes a three-tier architecture that spans the application, controller, and infrastructure layers. Within these layers are virtualized components – the vFlowController™, vFlowSwitch™, vNetCommander and vRemoteAgent – that can run on commodity x86 server platforms and provide a layered connection to the underlying network, enabling system administrators to more easily view what is going on in the network.

NVN System Components.

vFlowController – Virtualized Routing, Firewall and Tunnel Functions

Residing at the controller layer, the vFlowController application can operate on any virtualized commodity x86 server platform, providing control for layer 3 packet flow. The vFlowController supports IPv4 and critical routing protocols (BGP, OSPF), stateless packet filtering, and includes intrinsic virtualized routing, firewall, and IPSec Virtual Private Network (VPN) tunnel functions to support critical enterprise needs. A primary advantage of the intrinsic nature of these features is their close coupling with flow control functions. This pairing delivers performance benefits above and beyond what can be delivered through an extrinsic common application-layer API, such as a traditional SDN northbound API.



vFlowSwitch – Virtualized Packet Forwarding

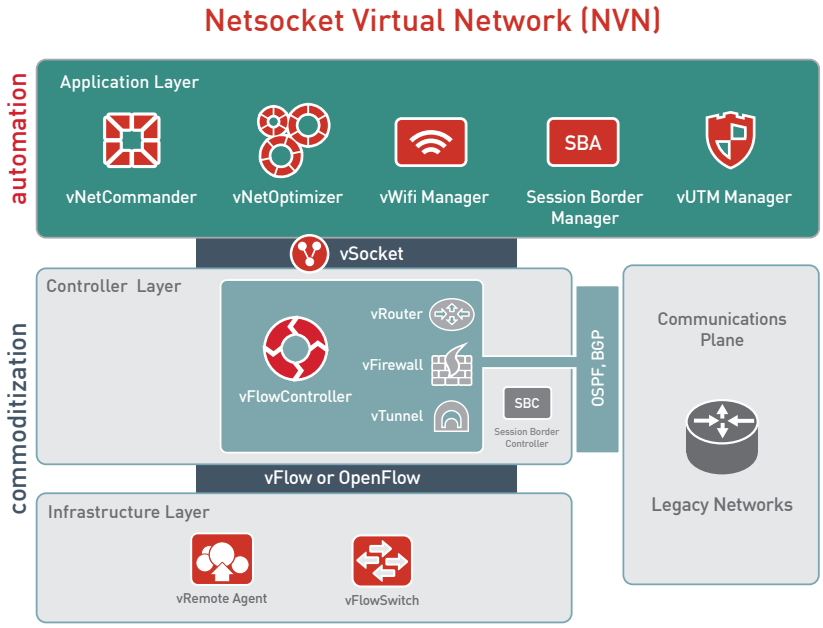
Within the infrastructure layer is the vFlowSwitch, a virtualized application that is responsible for layer 3 packet forwarding. Within a typical network deployment, the vFlowSwitch is hosted in a hypervisor virtual machine and is coupled to layer 2 virtual switches, a native component of the hypervisor environment. In the case of Microsoft's HyperV, that virtual layer 2 switch is their vSwitch. The vFlowSwitch configuration attributes are administered and configuration steps necessary to connect vFlowSwitch ports and vSwitch ports are automated via the vNetCommander application. One or more vFlowSwitch modules can be associated with a parent vFlowController, based on individual network requirements.

vNetCommander - Powerful, Unified Network Management

vNetCommander™ is the first Netsocket-built NVN application. vNetCommander enables system administrators to configure and install a complete Netsocket Virtual Network to a target platform in a matter of minutes. Within the application layer, it provides robust, unified network management and enables centralized administration of NVN components. Its elements include a web-based GUI and template-based installation, bulk-provisioning, and software upgrade orchestration functions. Day 2 configuration operations are simplified through the use of a GUI rather than multiple CLI commands. vNetCommander provides automated modification of router, switch and tunnel attributes, including quality-of-service (QoS) queue management, traffic filtering rate limiting, and routing protocol configuration. vNetCommander's workflow automation for installation, bulk provisioning and software upgrade orchestration represents a dramatic reduction in the time required to design, install and initially configure a highly-scalable routed network.

vRemote Agent – Automation and Orchestration

The vRemoteAgent automates the local installation, initial provisioning and subsequent monitoring, fault isolation and configuration workflows at individual sites. It also orchestrates all local software upgrades initiated by the vNetCommander. Acting as the local agent of the cloud-based vNetCommander, vRemoteAgent facilitates communications between the vNetCommander and the site-hosted NVN elements (vFlowSwitch, vFlowController for control site, and hypervisor/operating system). It is hosted in a virtual machine of a hypervisor operating on each site's x86 platform. vRemoteAgent communicates bi-directionally with its parent vFlowController, its local vFlowSwitch, the local hypervisor/operating system and its parent vNetCommander. vRemoteAgent communicates with the local hypervisor/operating system through the Netsocket Virtualization Host Service application. vRemoteAgent is architected securely so that neither customer end users nor service desk operators have un-restricted access to the operating system or NVN components. Also, vRemoteAgent allows the creation of a secure remote diagnostics tunnel by which MSP service desk end users, using the vNetCommander GUI, can remotely manipulate a restricted set of hypervisor and operating system workflows.



NVN Distributed System Behavior

Controller Layer

Residing at the controller layer is the **vFlowController**, a virtual entity that provides centralized routing information for the NVN system. It is responsible for constructing routing and forwarding tables, as well as logic and packet handling policies via MSP service desk system configuration. The vFlowController then pushes this data to each vFlowSwitch module at every remote site. The vFlowController is hosted in a virtual machine on a hypervisor operating on an x86 server. There is one vFlowController per configured NVN routed network. Typically, the x86 platform on which the vFlowController is hosted is located at a central facility such as a corporate headquarters site or a data center.

Infrastructure Layer

Within the infrastructure layer, the **vFlowSwitch** acts as the data forwarding and handling element for the NVN system. The vFlowSwitch is hosted in a virtual machine on a hypervisor on an x86 server platform, and one vFlowSwitch is installed at each site. Within an NVN routed network there are one or more vFlowSwitch modules associated with each parent vFlowController.

The **vRemoteAgent** automates the local installation, initial provisioning and subsequent monitoring, fault isolation and configuration workflows at individual sites. Acting as the local agent of the cloud-based vNetCommander, the vRemoteAgent facilitates communications between the vNetCommander and the vFlowSwitch and vFlowController. The vRemoteAgent is hosted in a virtual machine of a hypervisor operating on each site's x86 platform.

"As one of the very first virtualized SDN solutions, we view Netsocket's NVN as a cost-efficient and performance efficient alternative to expensive proprietary routers and Layer 3 switches."

– SNS Research
October 2013

Application Layer

The solution management application for the NVN system is the **vNetCommander**. It is hosted in the cloud and operated by Netsocket as a service to the company's Managed Service Provider. MSP service desk personnel use vNetCommander as a tool to orchestrate, automate and simplify all lifecycle NVN management workflows, including fulfillment, installation, deployment, initial provisioning and day 2 operations. The vNetCommander software is multi-tenanted and supports a hierarchy of organizations, including their routed networks and distributed sites. Multiple levels of account management provide privileged access to the vNetCommander module's GUI and tools for use by MSP order fulfillment teams, systems integrators, MSP service desk teams, as well as the end customer.

vNetCommander automates software installation and initial provisioning so that installation workflow at a new site is near zero-touch. Initial provisioning and day 2 operational workflows are accomplished through the vNetCommander GUI via MSP service desk personnel. Under the hood, vNetCommander's orchestration and automation engine automates these day 2 workflows as well. Neither truck rolls nor knowledge of network Command Line Interface (CLI) are required for any lifecycle workflows. A view-only user account can be extended by MSP service desk personnel to end customers so that they can view the configuration state of their company's network.

Netsocket's Virtual Edge Solution

Among the solutions available using the NVN software is the Netsocket Virtual Edge solution, a cloud-managed virtual network specifically optimized for enterprise and SMB LAN and WAN edge deployment. All NVN software components are virtualized and operate in virtual machines on a low-cost, commodity X86 server platform, so no application-specific hardware is required to operate any NVN software component.

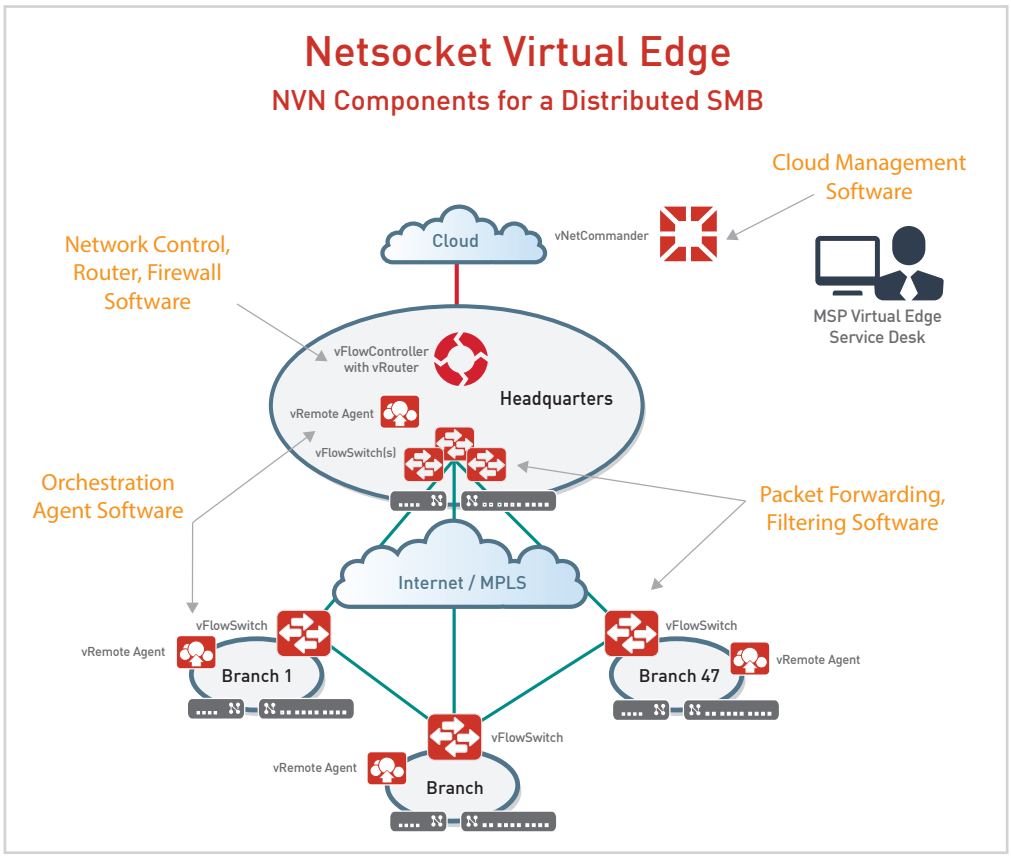
Netsocket defines the network edge as the point in an enterprise or distributed SMB customer's branch or remote office at which the local area network is "connected" to the wide area network. Further, the network edge:

- provides interconnection to the branch or remote office LAN;
- provides a connection point to the wide area WAN (typically the internet), as well as provides access to network resources at other branch, remote office or corporate sites.
- supports forwarding ingress traffic from WAN to the LAN;

- supports forwarding egress traffic from LAN to WAN; and
- supports forwarding traffic from one LAN subnet to another LAN subnet.

Powered by the Netsocket Virtual Network, the Virtual Edge solution enables end customers and service providers to rapidly deploy new managed services that emphasize the unique value of their own core IT services. Netsocket Virtual Edge capabilities can be installed in remote offices of distributed small to medium businesses and enterprise environments without the need for truck rolls or onsite network expertise for new and existing network moves, adds, changes.

The Netsocket Virtual Edge solution consists of NVN software components described earlier in this paper – the vFlowController, vFlowSwitch, vNetCommander, and vRemoteAgent – as well as the Netsocket MicroCloud Server and MicroCloud Switch that are distributed across a distributed multi-site environment as shown in the diagram below.



MICROCLOUD SERVER

The MicroCloud Server is an x86 server that replaces a traditional costly router and server that would normally be deployed at a remote site's network edge. Powered through the NVN system, the MicroCloud Server requires no local configuration or management, and can scale to run additional applications as business needs demand. Each MicroCloud Sever hosts a hypervisor on which NVN and other applications are hosted in virtual machines.

Operating as a small form factor, multi-core x86 server appliance, the MicroCloud Server hosts the vFlowSwitch and vRemoteAgent on a hypervisor/OS at a remote site. Two MicroCloud Server platform types are offered to allow scalable performance and site service extensibility through hosting of additional virtualized applications. RAM, SSD and CPU capacity dictate the capacity of the three MicroCloud Server variants. At the site, the MicroCloud Server is connected to an optional hardware component – a low-cost, layer 2 VLAN "break-out" switch with VLAN/QoS support – the MicroCloud Switch.

Prior to delivery at the customer site, the MicroCloud Server is pre-installed by the MSP's system integrator with the operating system/hypervisor, the NVN software, and site-based credentials. Once delivered to the site, the MicroCloud Server is connected to the local area network (LAN) and the wide area network (WAN). The pre-installed NVN software automatically "calls home" to connect and authenticate to its parent vNetCommander using site-specific pre-loaded credentials. Immediately after authentication, the final steps of installation are carried out by the local vRemoteAgent and vNetCommander. The automation inherent in these steps removes the need for a truck roll by the MSP.

MICROCLOUD SWITCH

The MicroCloud Switch is a layer 2 breakout switch that provides the ability to "break-out" the trunked VLANs passing through the single gigabit Ethernet (GE) physical network port of the MicroCloud Server to multiple physical ports for connectivity to the site's LAN. The MicroCloud Switch provides eight to twenty-four low cost, layer 2 gigabit Ethernet ports with VLAN and QoS features. Automatically configured upon installation by the vNetCommander and vRemoteAgent, the switch ports are normally related to LAN subnets through VLAN IDs and can be cascaded to other external "access layer" layer 2 or layer 3 switches, providing local client device, server device and wireless access point connections. The vRemoteAgent orchestrates the automated configuration of VLANs on this layer 2 switch to individual layer 2 switch physical ports.

FAULT TOLERANCE AT THE NETWORK EDGE

During normal operations, should a vFlowController or its host platform/hypervisor fail, all of its subordinate vFlowSwitches will continue to forward packets and perform all packet handing. During the failure interval, no configuration changes to the vFlowController can be made. During this period, each vFlowSwitch will periodically poll its parent vFlowController

to determine if the vFlowController has been restored to service. When the vFlowSwitch detects that its parent vFlowController has been restored to service the vFlowSwitch and its virtual machine will be restarted. This restart process takes only a few seconds.

END-TO-END SOLUTION ORCHESTRATION – THE NVN ADVANTAGE

Following site activation, the primary tool used by MSP service desk personnel for day-to-day operations is the vNetCommander. The vNetCommander module's NVN Dashboard is the primary GUI by which a service desk operator can add new sites, make changes in configuration to existing sites, and diagnose and correct problems reported by customers. The dashboard includes a variety of tools to verify and visualize path connectivity, review interface traffic and QoS statistics, and archive running and startup network configurations. Context sensitive help is distributed throughout the dashboard and full diagnostics download is available for offline network evaluation. No specific expertise in router CLI interfaces is required for all of these operations. Operational tasks are provided through the intuitive visual interface.

Netsocket's Virtual Edge Solution

Summary Capabilities

System Capacity

- 100k customers per vNetCommander
- 10 sites per customer

Network Interfaces (per site)

- WAN — max 2 virtual interfaces, auto-failover, Ethernet (primary) or LTE/Ethernet (backup)
- LAN — max 7 virtual interfaces (subnets)
- Inter-site, full-esh AES-256 encrypted tunnels

Virtual Routing

- Protocols supported — static, BGP, OSPF
- Max throughput — 500k PPS, 1 Gbps
- Max route table entries — 5,000

Performance

- Max throughput — 500k PPS, 1 Gbps
- Max 200 users, 400 devices per site

Management

- Cloud-managed through vNetCommander
  - Hosted/operated by Netsocket
  - Used by MSP service desk personnel
- Zero-touch installation and provisioning— no truck rolls required
- Common Policy GUI — build once, push once to many sites, many virtual interfaces — no CLI skills required
- Policy attributes — filtering, QoS, DHCP, zoning
- Device/system monitoring — SNMP, email notification

Extensible Services

- Managed Routing — available now!
- Product plan:
  - Managed LAN edge
  - Managed WiFi
  - Managed Voice (SBC)
  - Managed Disaster Recover (backup/ restore/synch)

Virtual Edge Benefits

All NVN-powered Virtual Edge components run in virtual machines on a low-cost, commodity X86 server platform, so no application-specific hardware is required to operate any NVN software component. This provides a substantial benefit to end customers and the Managed Service Providers that operate their networks. It enables a three to one reduction in capital expenditures and a reduction of five to one in lifecycle operating expenditures, compared with traditional WAN edge routers, firewalls and layer 2/layer 3 switches. Because NVN software does not require Application-Specific Integrated Circuits (ASIC) or Field Programmable Gate Arrays (FPGA) to achieve WAN edge performance, the x86 computers on which NVN components are installed can host any application – further extending service revenue opportunities for MSPs.

In addition, the NVN system's powerful orchestration capability enables MSPs to remotely design and manage all aspects of the remote network, as well as to interconnect the network with third party add-on applications such as session border control, LTE WAN backup, voice services and more.

Netsocket's Virtual Edge Benefits for Customers and MSPs

The Virtual Edge solution is a cost-effective cloud-based networking edge offering that provides the flexibility businesses need	Managed Service Desk	**Dedicated Expert support to manage your company network so you can focus on your business needs**
	Zero-touch/Turnkey Networking	**No need to know anything about technology or networking to set up your services**
	Scalable for Operational Savings	**MSP can provide flexible provisioning for rapid deployment that can scale from small branches to larger distributed enterprises, allowing you to control operational costs**
	Extensible for Value-Add Services	**Expand your services over time—Virtual Edge can host new services such as automated backup, intrusion detection, session border control, and much more**

Summary

Virtualized SDN for the network edge is an inevitable quantum shift within the networking industry. Its full impact will continue to reshape enterprise and distributed SMB environments in the data center, at corporate offices, and at the network edge by providing unsurpassed cost and ease-of-use benefits.

Netsocket is the only vendor today to provide a completely virtualized software defined network edge solution that provides the flexibility that businesses need in order to scale capacity and deploy value-add services at their own pace.

About Netsocket

Netsocket is a technology leader in virtualized, software-defined networking. The company's flagship Netsocket Virtual Network (NVN) fulfills the promise of SDN today with powerful, robust automation applications running on a completely virtualized network infrastructure. NVN differs from current SDN offerings in that it is optimized to provide a Virtual Edge network for distributed enterprise branch offices/small to medium-sized businesses and the Service Providers who serve them. NVN delivers a new framework for network virtualization and advanced automation that transforms the network into a highly responsive business asset. To discover how Netsocket can virtualize your world, visit www.netsocket.com.

3701 W. Plano Pkwy, Suite 140, Plano TX 75075
Phone: +1 214.427.7300 Fax: +1 972.596.7943
info@netsocket.com
www.netsocket.com

www.netsocket.com