nemertes RESEARCH
INDEPENDENCE INTEGRITY INSIGHT
issue paper

Business Benefits of Smarter Networks for Smarter Branches

By John Burke

CIO and Principal Research Analyst, Nemertes Research

Executive Summary

The next iteration of the WAN and the branch is an opportunity for IT to lay the groundwork for stepping into a more strategic role in the organization: to deliver a network consistently able to support successful business innovations and help drive good business outcomes. When IT can do that, it can become a trusted advisor to the business and a sought-after partner for business strategy development. The branch network must provide a good experience (with robust security) to any user as a part of any new initiative, whether facing staff, partners, or customers. So it needs intelligence, automation, and centralized, policy-driven control—and all at manageable (preferably lower) cost. IT leaders should: Explore an Internet-enabled branch strategy; design a WAN and branch stack with deeply automated, policy-based management of core services, including WAN optimization and security; seek to reduce the capital cost of the branch stack through integration of services into fewer boxes; and put branch-NFV and SDN for the WAN on the roadmap, with specific triggers for testing and stack redesign.

The Issue: The Agile Enterprise Needs Agile Networks For Agile Branches

IT is key to just about every new business initiative. When the organization pursues a new business opportunity—such as:

- Location-aware discounting for shoppers in a big-box retailer;
- Smart buildings that reduce office building operating costs through dynamic power management based on staff-location awareness;
- Seasonal mini-clinics to dispense flu shots and treat back-to-school illnesses.

IT infrastructure and services have to be ready to meet new needs, quickly. IT understands this, and knows it must *not* be a roadblock to innovation: Agile businesses require agile IT.

Agile businesses also require an agile branch strategy. Whether the next big thing is built around mobile devices, sensor-rich environments, or temporary branches, the branch network is key to service delivery. After all, most staff don't work (or shop!) at the data center—they are out in the branches. Many new business initiatives center on getting closer to clients and customers, digitally and physically. This makes branch strategy a key piece of the overall business plan.

Supporting branches is about more than basic connectivity—IT can't solve branch challenges just by throwing more bandwidth at them. Applications consume more bandwidth but are more sensitive to network quality, and users have less tolerance for performance hiccups. IT must build a smarter network better at managing traffic to meet demanding applications' needs and fulfill users' expectations. IT has to do so without increasing risk, by providing robust security in the branch. And, has to do all this in a supportable, sustainable, affordable way.

Agility Requires Simplicity, Intelligence

The enterprise needs to be free to add and drop branches whenever and wherever its current business strategy says to. For example, many organizations increase their number of physical locations by breaking up large expensive ones into smaller, cheaper ones, to reduce operating costs or to increase revenues through closer proximity to customers.

Most enterprises also continue to expand IT service portfolios. They offer new services out of their own data centers, and buy more cloud services. At the same time, employees in branch offices increasingly utilize multiple mobile devices, and connect them via the branch WLAN to internal and external services and to the wider Internet. This puts increased stress on branch WLANs, WAN links, the data center's Internet link, and any security infrastructure on that link. IT needs a branch network that can optimize performance for users on both computers and mobile devices, using either internally or externally sourced services.

So, IT needs to accommodate a dynamic pool of branches using more services from more devices—and do so without adding staff. So, the branch network must be easily, centrally managed. Ideally, IT would be able to:

- Connect each branch to the world by a single edge device offering multiple services, not a deep stack of devices;
- Use single-pane-of-glass monitoring, not different tools for different layers of function;
- Have deeply automated management.

Automation will increase both agility and security by making it easier and faster to bring new gear and new locations up on the network with instant, proper configuration. Policy-driven, centralized provisioning coupled with automated auditing improves security by ensuring proper configuration in the first place and by reducing or eliminating undocumented and unsanctioned divergence from standards.

Policy, Performance, and Security

In fact, policy takes two roles in the smart network, guiding both security and performance management. To make sure network resources best serve the operations and strategies of the business, policies should support performance requirements for services as well as enforce limitations. Policies should be centrally and singly defined to ensure consistency and to make policy maintenance a supportable, sustainable activity.

For either security or performance, policies ideally will allow the network to decide what to pass through and how to optimize it based on:

- User and application identity;
- The sensitivity and compliance requirements of the data being transmitted;
- User location and service source;
- Time of day, month, quarter, or year;
- User platform and connection method.

Thus, a truly intelligent branch network might prioritize traffic to all systems of record, internal or external, above most other traffic when the user is a company auditor and the time is within the last week of the fourth quarter. Or, it might block attempts to access the CRM, which contains sensitive data, via an unsecured mobile device, no matter whose it is.

Internet-Enabled Branches For Flexibility and Savings

Budgets are flat or down for most IT departments and for 60% of WANs. Everyone wants IT to spend less on day-to-day operations, to make more money available for the new and the strategic. So IT wants to reduce the costs of turning branches up, running them, and decommissioning them. This is driving rapidly growing interest in the Internet-enabled branch.

Internet-enabled branches come in two flavors: branches with direct Internet access supplementing dedicated WAN links, and branches with Internet links only. (Please see Figure 1.)

Direct-to-Internet branches represent an adaptation to a world in which:

- An increasing portion of the service portfolio—25% on average—is supplied via SaaS;
- All staff utilize partner, customer, and supplier Web systems;
- Internet links get steadily cheaper, faster, and more reliable.

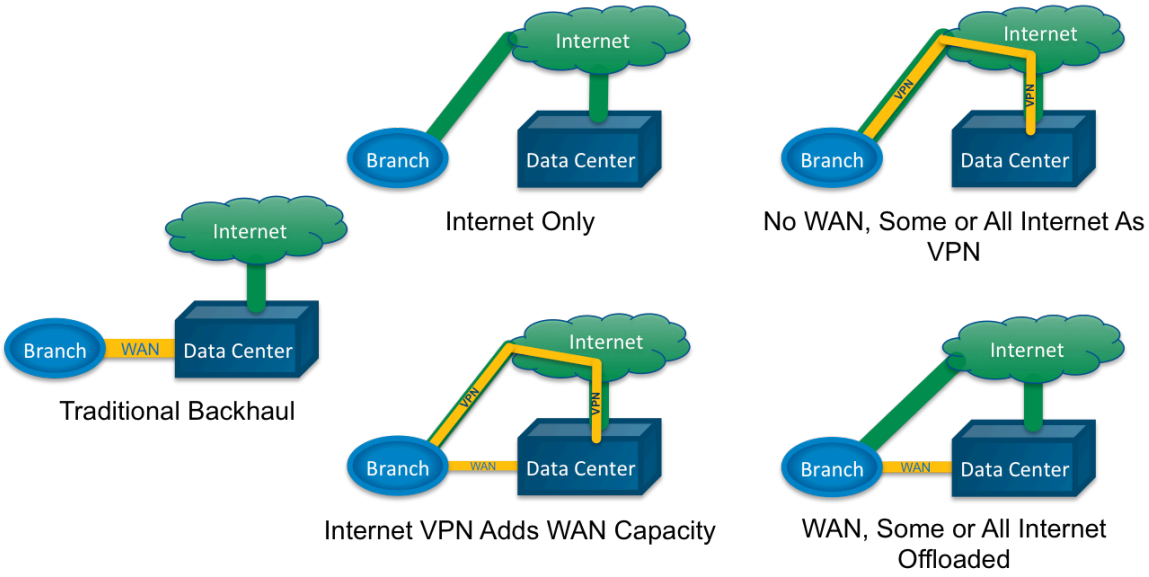

Figure 1: From Traditional WAN and Backhaul to Internet-Enabled Branches

Internet links can, minimally, be used to supplement WAN links. A site-to-site VPN across the Internet can take up low-priority and high-bandwidth traffic and offer redundancy to cover WAN outages. Beyond that, IT can offload some or all Internet-bound traffic from the branch directly to the Internet rather than backhauling it across high-cost WAN links. Either approach reduces WAN load, but the latter also frees up data center Internet bandwidth, and improves SaaS application performance.

Internet-only branches go further, using the same cheaper bandwidth for all branch communications. Connections come in three flavors: VPN-only, split pipe, and Internet only. VPN-only connections use the whole Internet link as an encrypted pipe back to a company data center. Split-pipe installations devote some bandwidth to a site-to-site VPN. Internet-only connections look to the data center like any other Internet site, and staff there use enterprise systems as if they were not on a company network.

Everyone Requires Performance With Security

Staff in branches has ever-greater reliance on IT services, and especially on network-sensitive applications such as unified communications, real-time collaboration tools, and VDI. More than 58% of organizations use VDI, for example; more than 74% have a UC initiative; 57% use social collaboration tools.

So network performance to the branch is crucial to staff getting their work done and having a good experience. This drives a need not just for rock solid reliability and high throughput but also for application intelligence. The intelligent network optimizes and prioritizes traffic for critical applications to ensure its behavior reflects organizational priorities and policies. Already, 56% of organizations deploy some application delivery optimization (ADO) tools, to deal with everything from bandwidth growth to streaming video.

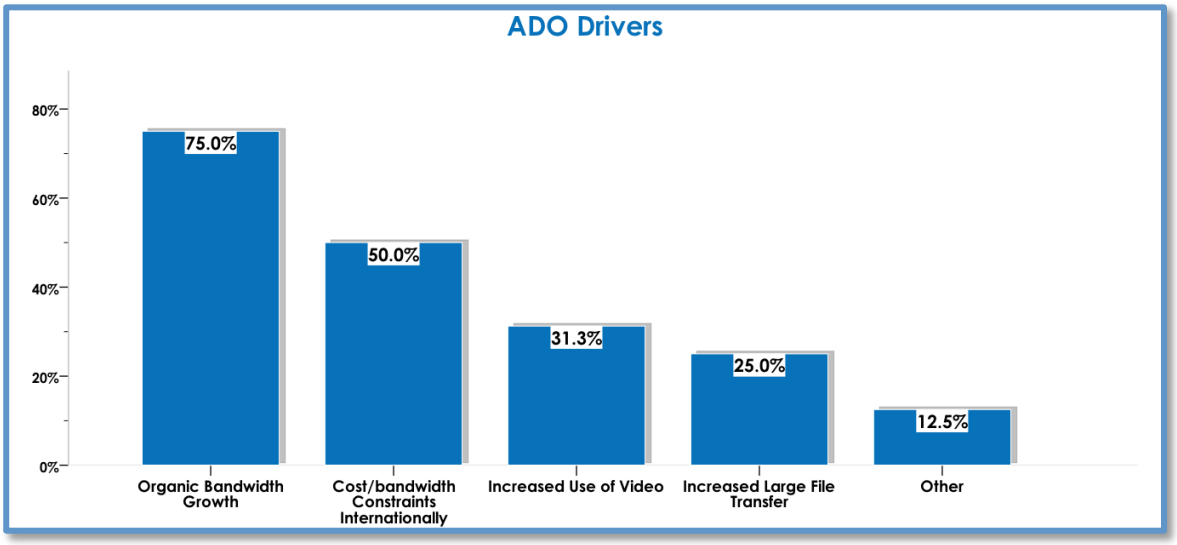

Figure 2: Why organizations optimize WAN traffic

Running at full speed doesn't mean running with scissors! Cost and agility drive adoption of direct-to-branch Internet, something a majority of companies now have for, on average, 52% of sites. In combination with mobility trends and the Internet of Things, direct-to-branch Internet expands the branch's security threat surface. So, branches need outward-facing edge security (firewall, etc.), and also inward-facing tools, e.g. network behavioral analysis and network access control.

New security measures threaten to reduce capital savings sought with the shift to Internet-enabled branches, but need not eliminate them. IT can minimize the impact if it can keep capital costs on new security low, e.g. through integration of security functions into existing hardware or carrier services. As importantly, it can keep operating costs down with centralized policy-based management and automation.

Software Defined Branch? SDN and NFV Exciting, But Still "Coming Soon"

The "branch in a box" dream is still alive in the enterprise: plug it in, turn it on, have a branch network ready to go. Software Defined Networking (SDN) and Network Functions Virtualization (NFV) may be the key. SDN separates the network control plane (which decides how to handle traffic) from its data plane (which acts on those decisions). SDN applications implement performance and security policies on any

network port, making the whole network more flexible and less expensive. NFV replaces specialized network hardware with virtual machines running on commodity hardware. Like SDN, it could make a single branch box flexible and repurposable.

However, SDN is still new. Most network vendors support it, but few applications exist, so very few enterprises have deployed SDN. Only 4% of companies will have deployed it at all by the end of 2014, fewer still to the branch. (Another 4% plan to deploy in 2015.) NFV is in its early days too, with standards still settling and few enterprise offerings. Nearly half of organizations don't even know what it is, and only about 15% plan to adopt it at some point.

Still, converting "the branch stack" into a set of virtualized functions running on cheap commodity hardware and/or a set of SDN applications would completely transform the branch network. IT should be monitoring and making plans for both SDN and NFV as part of the future branch network.

Conclusion and Recommendations

IT must use the next iteration of the WAN to lay the groundwork for an agile and flexible branch strategy in support of both business innovations and economic efficiency. This will help IT become a trusted advisor to the business and a sought-after partner in the formulation of business strategies. To be both nimbler and cheaper while guaranteeing good performance and sufficient security, the IT needs to incorporate more intelligence, automation, and centralized, policy driven control in a WAN augmented by branch Internet connectivity. IT leaders should:

- Explore an Internet-enabled branch strategy, replacing or augmenting WAN links with Internet VPN links and assessing direct-to-Internet models.
- Design a "smart branch" stack with the goal of deeply automated, policy-based management of the core services, including WAN optimization, Internet security, LAN and WLAN service and security, and performance and security monitoring.
- Seek to reduce the capital cost of the branch stack through integration of services into fewer boxes.
- Put branch-NFV and WAN SDN on the roadmap, with specific triggers (e.g. when a network vendor or managed service provider offers a reference architecture) for in-house testing and stack redesign.
