White Paper

New Enterprise Branch Networking Architectures

Understanding the market requirements, fundamental changes, and the need to adapt

By Dan Conde, ESG Senior Analyst

January 2018

This ESG White Paper was commissioned by Cisco Systems and is distributed under license from ESG.

Contents

Introduction

This paper examines the current challenges with branch networking architectures due to changing business requirements and recommends ways to understand those requirements and architect a new branch network around them.

The Evolving Branch Networking Situation

Todays' branch networking architectures were designed around long-held conventions about remote offices that are starting to change. The idea that most traffic went from remote offices to the data center reflects the now outmoded application deployment model, which was based on the fact that earlier applications were client-server-based. Even as apps were rearchitected to use a web browser as the client, the web server still resided in the data center since it was not based on a public SaaS model. Therefore, Internet traffic was backhauled through the data center first, and that was acceptable at the time. Since traffic traveled through the data center, security devices were also centralized there, instead of being located in the branches.

This led to architectural decisions that met past business requirements, but that are starting to be revisited, as limitations in bandwidth capacity or security concerns have arisen. Traditionally in the branch, IT groups installed multiple physical devices for different functionality as business needs changed. Those may have included elements like routers, firewalls, WAN optimization, and later, SD-WAN equipment. This arose due to the way devices and functionality were incrementally added, which was encouraged by the principle of "one-function/one-box." Furthermore, the links to the corporate data center were expensive, typically using MPLS, so businesses were eager to optimize their use.

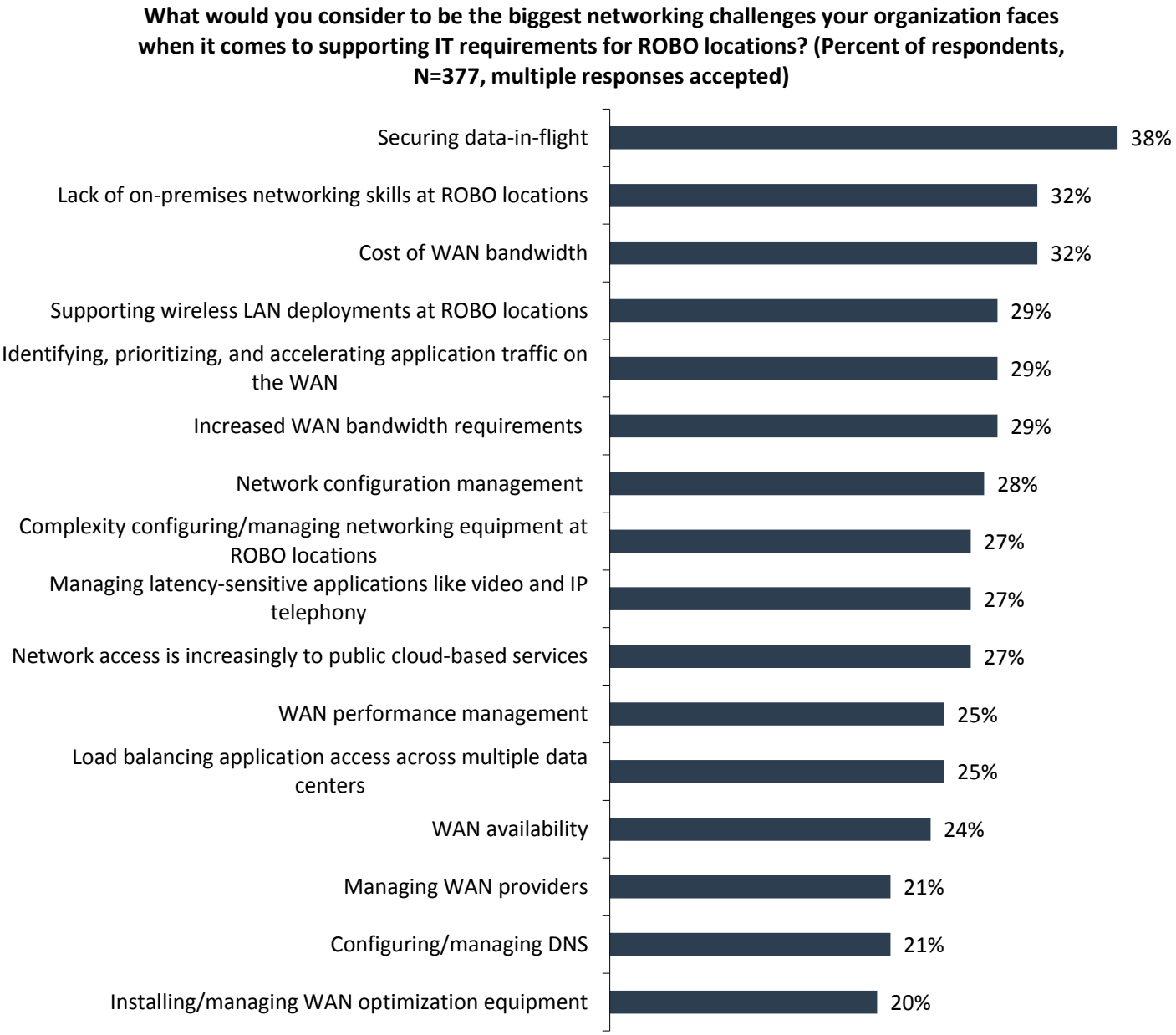
As architectural models and business requirements change, IT organizations need to respond to those challenges. However, given that current branch networking equipment has a slow upgrade cycle of five to seven years, it is possible that businesses will experience several years of delays between the scoping of business requirements and the capabilities to support the new models at branch offices.

It's easy to assume that all of these challenges would be focused on technical issues. However, ESG research shows that, when asked about the top challenges their organizations face in supporting IT requirements for remote office or branch office (ROBO) locations, 32% of respondents cited a lack of on-premises networking skills at ROBO locations, 28% cited network configuration management, 27% cited complexity of configuring/managing network equipment at ROBO locations, and 20% cited installing/managing WAN optimization equipment, which are all challenges related to available skill sets at the organization (see Figure 1).[1]

Clearly, challenges facing networking teams supporting ROBO locations are varied: They do not center solely on technical problems, but include skills issues, which indicates that remote branches, since they are detached from central facilities, have challenges due to a lack or dearth of any local IT staff, or the staffing of IT generalists who lack depth of knowledge. This means that servicing a branch office may require a "truck roll" from the central IT team, or from an outsourced partner. And, of course, bandwidth, prioritizing applications, managing complex environments, and security issues are all cited as prominent challenges in the ESG research survey results as well.

[1] Source: ESG Master Survey Results, *IT Plans and Priorities for Remote and Branch Offices*, December 2017.

Figure 1. Biggest Networking Challenges for Supporting IT Requirements in ROBO locations



Source: Enterprise Strategy Group

Changes in the IT Environment

Increasing access to public cloud-based services, which was revealed to be a challenge for 27% of respondents in the survey, shows that SaaS services are becoming popular (see Figure 1). A separate ESG research survey shows that 85% of organizations report using public cloud.[2] Apps such as Microsoft Office 365 and Salesforce.com are popular examples, but many specialized apps are propagating as well.

[2] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.

The addition of more devices to the network, as well as the increasing diversity of device types, such as mobile phones, tablets, and IoT, provides for more challenges compared with the time when most devices were wired PCs. This can lead to more challenges, such as unanticipated bandwidth requirements and the creation of more vectors for security problems to be introduced.

Additional traffic, in particular from IoT devices and initiatives, may be hard to predict, and can add requirements for increased telemetry within the network to assist with network security and operational requirements to understand traffic patterns.

Consolidation is a desire to simplify the deployment of network devices. The five- to seven-year update cycle for networking equipment has led to the addition of more network devices as needs arose before the old equipment was refreshed. Modern branches may want to reduce that. Simplification in operations and deployment may be assisted by additional levels of network automation. One example is the use of SD-WAN to help reduce costs and management complexity.

Considerations for Ongoing Branch Network Architecture Decisions

We can look at past trends and their effects on branch networking to begin to understand the considerations for architectural decisions based on the environmental changes described.

- Virtualized technology: Server virtualization exposed the need for updated processors and CPUs, which required adequate bandwidth or bus speeds, as consolidated workloads demanded more resources. However, speed is not the only issue, as security posture and differing traffic patterns contribute to the need for a server architecture that adapts to modern requirements. Therefore, similar issues can occur in branches, as increased network demands stress branch network bandwidth capacity, and app access patterns impose a need for a new security architecture.

- High availability: Enterprises need to ensure continuous business operations, which affects the design of any branch networking model. The abilities to use alternate connections if the primary connection fails, and to use backups for network appliances such as DNS, VPN, firewalls, or NAT are integral for providing holistic high availability.

- Automation: Contemporary branches may require automation if personnel are not available to handle configuration, monitoring, and other "day two" operations. Automation may be implemented via policy (a variant of intent-based networking) as opposed to automation by scripting or remote control. The introduction of intent-based networking also provides for automation, but service assurance and abstractions in IT networks, such as in the data center, may require closely examining its adoption within a new branch network.

- Functionality over form: Hardware and software advances show that single-purpose hardware appliances may be supplanted by virtualized appliances that coexist with other appliances in a shared device. However, it is important not to focus on the form factor as the indicator of progress, as capabilities are what matters. For some cases, traditional appliances may be appropriate, while in other cases, a more versatile edge computing device that combines multiple network functions may be appropriate.

- Evolutionary change: Changes do not need to be "all or nothing." It's impractical to update the entire enterprise branch network with each requirement. Sudden incompatible changes can render the old network unusable or increase operating expenses as organizations are forced to operate two incompatible networks. Finding a way to balance compatibility while introducing new functions is critical.

- ROI for early upgrades: Is it worthwhile to upgrade before the end of life or before the support of existing branch routers is terminated? It's easy to adhere to a rigid schedule, but consider the opportunity cost of not upgrading:

- Increased cybersecurity risks. Old equipment may provide less support for new security software or insufficient processing capacity to respond to modern threats.
- Inability to meet business needs such as new bandwidth demands. It may be worthwhile to upgrade earlier if that enables operating the business better to produce results such as increased revenue, higher customer satisfaction, and simply meeting business requirements for internal use. Consider the benefits of remote offices and video conferencing.

- **Prioritized applications**: As new application use patterns arise, the need for some older applications may not immediately go away. Even as instant messaging or video chats (i.e., Slack and WebEx) penetrate daily use, traditional voice over IP remains important.
- **Unifying an architecture**: It's imperative for organizations to understand how the branch fits into the overall design. While the data center, clouds, and campuses are separate areas, they can interact (for example, headend systems in the data center).
- **Consistency**: Scarce IT resources cannot easily accommodate a multitude of device types. For example, Southwest Airlines simplified operations by standardizing on Boeing 737 airplanes. As IT deals with physical data centers and colocation facilities accessed by branches, how can we treat them consistently to avoid the complexity of different architectures for access?
- **Staffing and architecture**: When the time comes to refresh hardware, the question of the amount of IT resources required is important. The upgrade may be done with in-house staff or with outsourced services, but in either case, a refresh with a "DIY" approach for integrating disparate hardware probably requires more IT resources. Using virtualized appliances or even cloud-based network functions can minimize the required IT resources but may limit the level of flexibility.

Organizations can take several paths forward to update a current branch network architecture. It is not a single straight line to go from the current design to a future end-state. Depending on each branch location's needs and resources, several paths may be chosen to progress from the current state to the eventual goal. And in some cases, there may be several end-states, where IT implements multiple designs, again based on each branch's requirements.

The Best Approach to Choosing Branch Networking Architecture

The best approach to choosing an architecture and a deployment path is to perform a requirements analysis followed by a gap analysis. This is a common approach but may be neglected if inertia takes hold or tight schedules intervene. However, an investment in understanding this approach will provide for rewards in the long term.

1. Assess the current environment.
2. Take an inventory of the company's business and IT initiatives.
3. Map the initiatives to the environment in order to understand how well they are supported. The initiatives need to incorporate current and anticipated needs.
4. Prioritize the branch locations based on applications and their importance, or whether they are inadequately served.

5. Perform a gap analysis based on the assessment of the current infrastructure for each branch location, its current level of support, and the requirements for supporting anticipated need. This results in a prioritized list of the different branch locations and how urgent the needs are.

6. Create a deployment plan to resolve the areas with the highest priority or largest immediate gap.

7. Optimize for operational efficiency. This may be done while in a PoC stage, allowing for refinement of the deployment design after a period of time in actual operation. This task may include revising a runbook, improving the monitoring and management functions for efficiency or security, and defining appropriate training for the branch staff. Training is particularly important because, as we have seen earlier, skills issues are a common challenge.

The Bigger Truth

Branch networking is undergoing rapid changes. Ultimately, the branch is where business activity occurs for many businesses: At a bank, customers interact with the business at a branch location; at a retail store, restaurant, or service location, goods and services transactions happen; and at legal offices, polices stations, and factories, remote workers get their jobs done.

These locations are not static and continue to undergo change.

Initiatives are constantly emerging that may range from digital transformation to make retail branches more responsive to counter online commerce, through meeting regulatory compliance requirements, to creating a better security stance to secure the enterprise. These needs are being imposed on staff at branch offices, who may not be up to date on the latest solutions or are stretched to fulfill multiple roles due to their location in understaffed remote locations.

Bandwidth requirements increase as more devices are deployed that consume network bandwidth, such as voice, video, and IoT devices.

All of these initiatives ultimately rely on application software, and those software services are increasingly delivered from the cloud. These changes may alter the fundamental assumptions relied upon to design the current or prior generation of branch network solutions.

Therefore, it is important to understand the core needs of branches—both technical and business—and then choose the path that makes the most sense. Relying on a conventional refresh schedule may no longer make sense. An early upgrade may pay off if it accelerates the core business requirements, which can span strategy, productivity, security, and regulatory requirements.

The branch should not be considered a remote backwater by any means. It's where business activity occurs, and understanding the requirements, assessing the current architecture, and comparing them with future needs to understand the gaps is the best way to fulfill the IT and business objectives.

SDwan^4 is a new generation service that is delivered from Secure Agility's OurDC^4 cloud environment. OurDC^4 is built in secure, tier 3 Australian data centres and combines three renowned partners in Cisco, Pure Storage and Rubrik, with Secure Agility into one unique capability.

Features

Choice: Cisco Viptela or Meraki platforms, delivering proven security and network SD-WAN solutions.
Multi-Cloud Technology: Securely access business applications from your Public, Private or Hybrid Cloud by deploying Secure Agility's SDWan^4.
Seamless Integration: Seamlessly connect with resources residing within your Public Cloud (Azure, GCP) or Secure Agility's Hybrid Cloud and realise the benefits from workload portability.
Enhanced WAN edge: Enhance the experience and gain greater visibility of SaaS based applications from your WAN edge.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.