DoyleResearch

Simplifying the Branch Network

By: Lee Doyle, Principal Analyst at Doyle Research

Sponsored by Aruba, a Hewlett Packard Enterprise company

Executive Summary

A majority of IT organizations are experiencing significant changes that impact the requirements for their distributed branch networks. Mobility, cloud-based applications, and Internet of Things (IoT) are altering traffic flows and increasing bandwidth requirements. Employees and guests expect Internet connectivity, which means that employee-facing and IoT devices need reliable, low latency access to their data and applications, and must be securely on-boarded as they interact with centralized services. IT organizations do not have the level of control they once did with traditional architectures, and now face increasing pressure to support these new initiatives even as budget and resources remain lean.

IT is looking to Software-defined WAN (SD-WAN) to satisfy price-performance benefits of using the Internet, deeper application visibility into WAN traffic, simpler transport across multiple uplinks, and greater flexibility to connect with cloud service. This means that new WAN architecture can improve Total Cost of Ownership (TCO) with simpler operations, reduced hardware costs, and more efficient bandwidth utilization. As IT organizations take these learnings and apply software-defined architecture across all branch network elements, they can deliver greater CAPEX and OPEX savings. Those elements include:
-    Wireless and Wired access for employee and guest users
-    Policy and security services for onboarding endpoints
-    Quality of Service for application traffic end-to-end
-    Closer integration with third-party applications and services

This expanded approach to networking delivers a Software-defined Branch (or SD-Branch) solution to converge all network elements onto a single, easy-to-manage platform. This unified approach provides cloud management and policy enforcement to simplify WAN, WLAN, and LAN, introduces role-based context awareness to the WAN, and integrates multiple services to eliminate onsite appliances. SD-Branch simplifies branch design, reduces Capital Expenses (CAPEX), and optimizes WAN utilization for greater savings than SD-WAN alone.
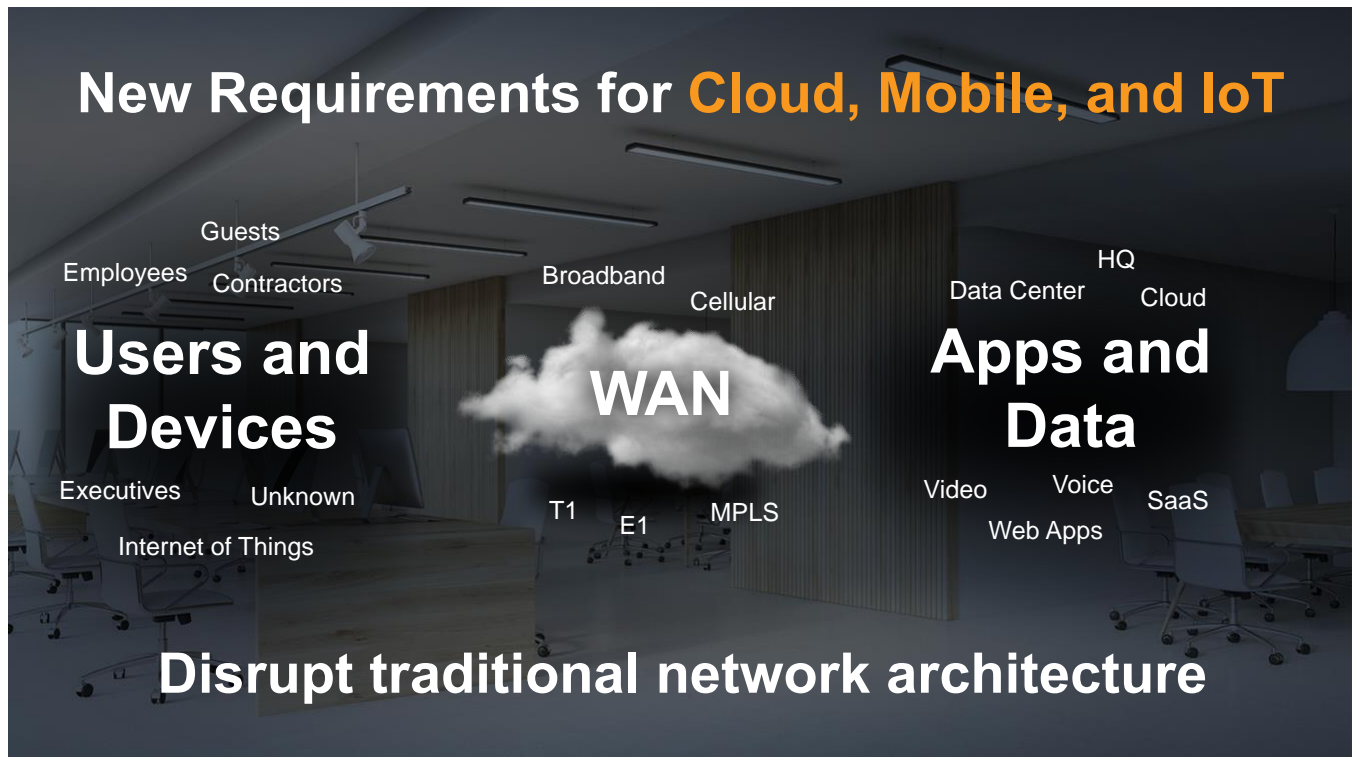
Challenges of Building and Operating Branch Networks

Leading IT trends, including the migration of key applications to the cloud, use of a wide range of mobile devices (BYOD), and the increased deployment of numerous IoT end-points, pose new challenges for operators of distributed branch networks. Increased cloud and Software-as-a-Service (SaaS) utilization has resulted in profound changes in traffic flows (towards the Internet and away from the corporate data center) that increase demands on branch performance. The increased number and variety of devices (personal and IoT) mandates real-time application performance and security monitoring to ensure user experience.

Forecasts from leading analyst firms highlight the challenges:

- Growing IoT: There will be over 25 billion IoT devices by 2020
- Increased Branch security threats: 30% of advanced attacks enter via the branch (Gartner)
- Changing traffic flows: According to IDC, 40-60% of enterprise data traffic is migrating from WANs to the Internet

Leading IT organizations realize that the inevitable challenges for managing current branch networks include ease of deployment and operations, application identification and prioritization to ensure Quality of Service (QoS), and real-time security/network health metrics. Capital and operational costs are also key concerns as it is expensive to deploy and manage a complex assortment of hardware and software remote branch locations. See Figure 1.
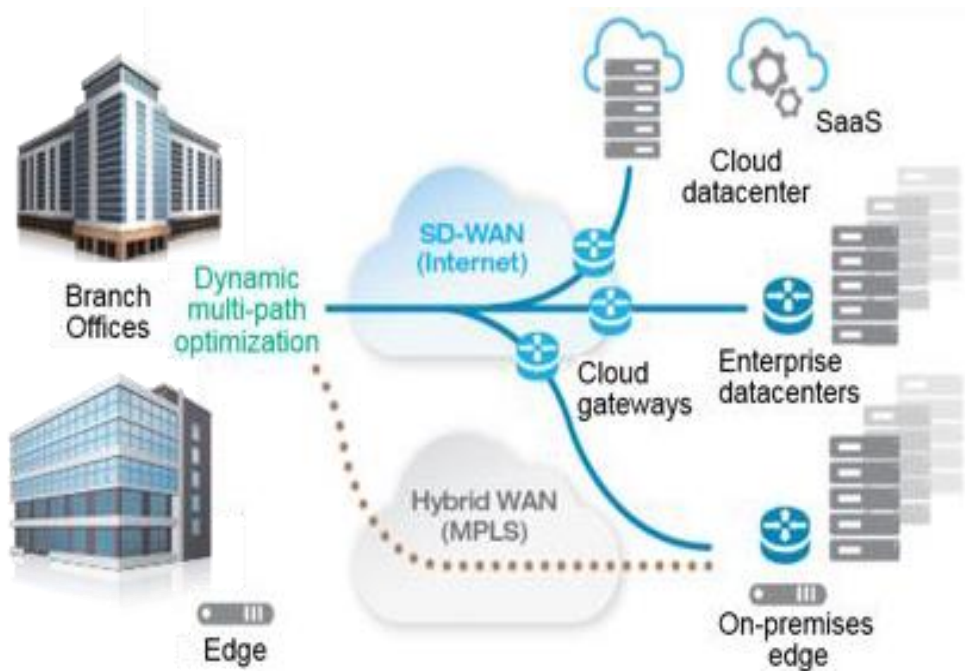
New Requirements for **Cloud, Mobile, and IoT**

Guests

Employees Contractors   Broadband   HQ

                                              Cellular   Data Center   Cloud

Users and   **WAN**   **Apps and**
Devices   **Data**

Executives   Unknown   Video   Voice   SaaS

Internet of Things   T1   E1   MPLS   Web Apps

Disrupt traditional network architecture

Simplifying Branch Network Operations

To meet the challenges of evolving branch network requirements, IT organizations are deploying new software and cloud-based tools to optimize WAN, WLAN, and LAN. By applying SDN and SD-WAN methodology, existing network context information about users, devices, and applications can be used to dynamically improve Quality of Service (QoS), policy, and configuration. This information provides SD-WAN functionality with deeper network and application insights even as hybrid WAN architectures leverage commodity Internet bandwidth to augment traditional MPLS networks. Centralized management provides for rapid (zero-touch) provisioning, pre-staging configurations, and real-time changes at remote branch locations.

Cloud-based intelligence provides for improved visibility into traffic flows with its ability to identify potential security threats. Centralized policy management allows the policy to follow the client/user and eliminates security risks associated with time-consuming, manual management tasks for various network overlays and functions. With centralized

management consoles, IT can leverage established branch and headend rules to reduce the complexity of setting up secure VPN tunnels and establishing the virtual WAN topology. New security services can easily be service chained with existing branch network software. See Figure 2.

Figure 2: SD-WAN Architecture

Further benefits accrue when organizations collapse an array of WAN, Wireless Local Area Networks (WLAN), and LAN services on to a single branch gateway platform. Under this model, complete branch network functionality is combined unto a unified and centralized management framework. This functionality includes:

- Wireless LAN (Wi-Fi)
- Ethernet switching
- SD-WAN and WAN optimization
- Routing and VPN
- Firewall and network security

The platform provides wireless and wired access for employees, guests, mobile devices,

and IoT devices. All policy management is centralized, thus requiring little or no intervention at the branch location. See Figure 3.

Figure 3: Branch Network Element Consolidation

WLAN
LAN
WAN Opt
Firewall
VoIP

Cloud-based Apps
Centralized Services

Branch-in-a-Box

Benefits of the Software Defined Branch Network

Intelligent software provides a number of significant benefits for branch network deployment and ongoing operations. SD-Branch provides context awareness to optimize QoS for critical applications in the access layer and improve SD-WAN routing functionality. The consolidation of network functions to software on a common platform reduces initial hardware costs (CAPEX) and ongoing maintenance fees. Cloud-based management speeds deployment and reduces complexity – thus providing operational (OPEX) benefits. Services can be deployed via a subscription-based model that reduces equipment costs and allows IT to easily deploy new services.

Reduce Bandwidth Costs

As a critical element of SD-Branch, SD-WAN provides organizations the ability to build hybrid WAN networks that leverage multiple WAN connections (e.g. MPLS and Internet) to efficiently deliver bandwidth to branch locations. Its context aware routing identifies applications and steers traffic to the appropriate network with the correct quality of service. This allows organizations to benefit from the "Internet economics" where circuits (ethernet, DSL, cable, etc.) typically are 1/3 the cost of comparable speed MPLS links. Internet services also have the advantage of wide availability and rapid provisioning times as compared to MPLS. SD-WAN also provides the ability for organizations to leverage multiple Internet service providers with the benefits of cost competition and diversity of circuits for high reliability.

CAPEX

SD-Branch allows organizations to selectively consolidate WAN services including routing, Wi-Fi, ethernet, firewalls, VPNs, and application visibility into a single platform. This consolidation provides the potential for a significant reduction in the hardware costs associated with the multiple box solutions. Consolidation of hardware also reduces ongoing maintenance costs (typically 15% of the initial purchase fee) for each box at each branch location.

OPEX

OPEX provides a measure of ongoing operational benefits provided by SD-Branch solutions. OPEX benefits accrue across a number of categories including agility, scale, management, and security.

Agility: SD-Branch provides a reduction in the time to deploy network resources to new or existing branches. The ability to quickly make adjustments to the network to support the business and optimize the application experience improves the value of the network.

Scale: Many organizations are challenged to deploy and manage networks to hundreds or thousands of branch networks. SD-Branch enables zero-touch provisioning, centralized management, and customizable logs to enable rapid remediation of networking issues at branch locations.

Management: SD-Branch solutions are cloud-based to enable IT to centrally control a large number of branch networks. Pre-configuration in the cloud provides for ease of installation and ability to improve network functionality via software updates.

Security: SD-Branch provides unified network security with UTM, firewall, and VPN capabilities. One security console with enhanced context aware visibility can identify anomalous traffic and speed resolution of security threats. It provides virtual WAN topology that reduces the complexity of setting up secure VPN tunnels.

Aruba TCO models indicate significant savings by moving to a converged branch solution leveraging SD-WAN to augment or replace MPLS links. A typical organization with 100 distributed branch locations can save $ millions over 3 years. See Table 1

Table 1

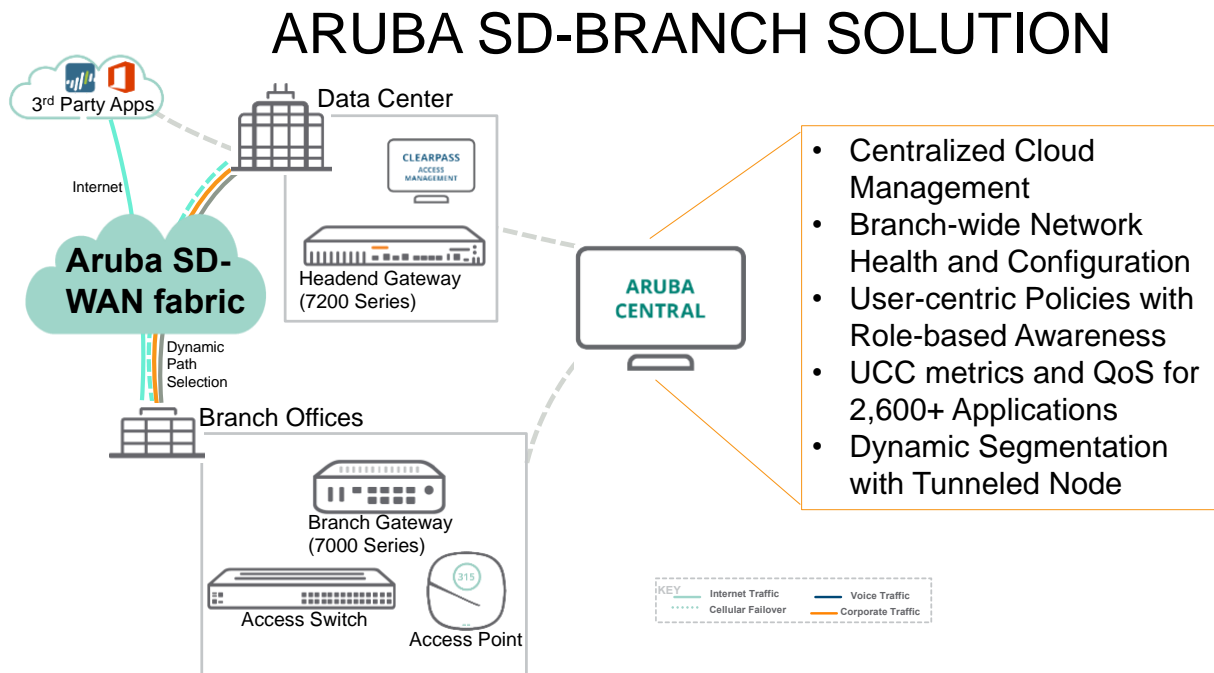| Cost Savings as Compared to Unconverted MPLS Only Solution	
MPLS + Internet	Internet Only
31%	76%

Aruba's value proposition for Branch Networks

Aruba 7000 series Branch Gateways offer integrated wireless, switching, and hybrid WAN services for distributed enterprises, all managed by cloud-based Aruba Central. They are optimized for cloud services and hybrid WAN connections, and are designed to deliver the performance, reliability and security required to support the number of IoT devices. Built-in WAN optimization and granular control over applications ensure appropriate QoS for business critical applications.

Aruba collapses the complicated patchwork of branch appliances and access servers into a single, compact cloud services platform. The Aruba 7000 series Branch Gateways eliminate the time, cost and complexity of managing disparate single-purpose point products in the branch. Key features of the Branch Gateway include:

- **Zero-Touch Provisioning** –Reduces the time, cost and complexity of installing branch office networks.
- **Programmable Policy Enforcement Firewall** – Delivers context-aware control to a variety of branch networking requirements.
- **Cloud-based Application QoS** – WAN optimization and application visibility and control improve the performance of business-critical apps in the cloud.
- **Advanced Routing** – Implements context-based routing across dual Ethernet WAN and LTE WAN links to preserve bandwidth for prioritized, business-critical traffic.

Aruba's SD-Branch solution takes advantage of the cloud to manage and monitor WAN, Wi-Fi, and ethernet links. Monitoring, reporting and deployment is handled centrally with Aruba Central. In addition, Aruba offers integration with Palo Alto Networks firewalls and enhanced performance for Microsoft UC customers.

Figure 4

ARUBA SD-BRANCH SOLUTION

- Centralized Cloud Management
- Branch-wide Network Health and Configuration
- User-centric Policies with Role-based Awareness
- UCC metrics and QoS for 2,600+ Applications
- Dynamic Segmentation with Tunneled Node

Conclusion and Recommendations for CXOs

The emphasis of mobility and cloud-based applications is changing the requirements for distributed branches. IT organizations continue to be challenged to provide high quality, cost-effective services to distributed users. The advent of pervasive IoT deployments at the edge of the network will further stress existing branch WAN connectivity. IT organizations are challenged to update and manage the disparate elements of the remote branch – i.e. routers, firewalls, Wi-Fi, switching, etc.

These new WAN requirements (e.g. changes in traffic flows) will require a transformation of the way branch networks are built and operated.   New software-based networking technologies such as SD-WAN significantly reduce operations and capital costs while improving quality of service for critical applications. With intelligent network software, IT organizations can consolidate a host of network functions onto a single platform. The SD-Branch is a converged branch network unifies Wi-Fi and ethernet connections, identifies traffic types and routes them to the appropriate link,

and provides enhanced security. Cloud-based policy management allows centrally based IT staff to efficiently troubleshoot network issues at remote branch locations.

SD-Branch architectures provide compelling benefits via efficient bandwidth utilization, improved application QoS, and increased security. Its SD-WAN features enables the use of highly efficient (and lower cost) Internet bandwidth. SD-Branch leverages virtual software to replace dedicated hardware (e.g. network security, routers, Wi-Fi, ethernet, SD-WAN) with an all-in-one platform – thus considerably reducing branch hardware and associated maintenance costs. Its cloud-based management system provides for rapid provision and network upgrades – positively impacting IT agility and improving operations.

Aruba delivers network access and hybrid WAN solutions to remote locations that need simplified enterprise-class connectivity and secure access to corporate resources. By combining intelligent wired, wireless, and WAN into one platform, the 7000 Series delivers a single solution for LAN and WAN connectivity. IT leaders should consider the benefits of branch network consolidation, including reduced hardware and maintenance costs, improved operations agility, and superior application QoS.

Meet the Author

Lee Doyle is Principal Analyst at Doyle Research, providing client focused targeted analysis on the Evolution of Intelligent Networks. He has over 25 years' experience analyzing the IT, network, and telecom markets. Lee has written extensively on such topics as SDN, NFV, enterprise adoption of networking technologies, and IT-Telecom convergence. Before founding Doyle Research, Lee was Group VP for Network, Telecom, and Security research at IDC. Lee contributes to such industry periodicals as Network World, Light Reading, and Tech Target. Lee holds a B.A. in Economics from Williams College.