2018 Guide to WAN Architecture and Design

Applying SDN and NFV at the WAN Edge

Part 2: Key Considerations when Choosing new WAN and Branch Office Solutions

By ***Dr. Jim Metzler, Ashton, Metzler & Associates***
Distinguished Research Fellow and Co-Founder
Webtorials Analyst Division

Steven Taylor, Webtorials
Publisher and Editor-in-Chief
Co-Founder, Webtorials Analyst Division

Platinum Sponsors:

apcela

CATO NETWORKS

cradlepoint

DELL

TALARI Networks

TELOIP®

Table of Contents

Executive Summary

One of the goals of the 2018 Guide to WAN Architecture and Design (The Guide) is to discuss the state of WAN architecture and design with an emphasis on the current SD-WAN solutions. Another goal of The Guide is to provide insight into the emergence of solutions that leverage the key concepts of SDN and NFV to support all components of the WAN edge. Within The Guide these topics will be put into the context of the current state of the enterprise environment and the solutions being brought to market by industry-leading vendors.

A discussion of wide area networking is extremely timely for two reasons. One reason is that for most of the last fifteen years there has been little investment in the development of new WAN technologies and services. Hence, until recently there hadn't been a fundamentally new WAN technology or service introduced into the marketplace since the turn of the century. That situation began to change a couple of years ago with the introduction of a new class of WAN solution that is typically referred to as a Software Defined WAN (SD-WAN). Most of these SD-WAN solutions focus on providing connectivity between the users in a company's branch offices and the resources they need to access in both internal and external data centers.

A discussion of the WAN edge is also very timely. One reason for that is the burgeoning use of the Internet of Things (IoT). For example, Gartner has forecasted that 8.4 billion connected things will be in use worldwide by the end of 2017, up 31% from 2016, and that there will be 20.4 billion connected things by 2020. Another reason why a discussion of the WAN edge is timely is that several branch office solutions that leverage SDN and NFV are being brought to market. These solutions are often referred to as software defined branch office solutions (SD-Branch). While these solutions exhibit many similarities, there are many differences amongst the solutions.

The Guide will be published both in its entirety and in a serial fashion. The first publication focused on providing insight into the current state of the WAN, the status of SD-WAN adoption and the status of the branch office.

The 2017 Guide to WAN Architecture and Design discussed a number of topics, such as how to pull together a project team and how to build a business case, that are important considerations relative to the overall process of WAN redesign. This publication will expand that discussion to include other considerations that network organizations need to keep in mind as they evaluate alternative SD-WAN and SD-Branch solutions. The goal of this discussion is to ensure that network organizations choose solutions that meet their current and future requirements and are to the maximum degree possible, future-proof.

The third publication of The Guide will discuss the ecosystem of vendors who supply SD-WAN and/or SD-Branch Office solutions and it will present a profile of each of the sponsors of The Guide. Each profile will focus on how their solution(s) fit into the overall ecosystem and the value add that the solution(s) provide. Each profile will also contain some proof points that highlight the value add that the solution(s) provide.

The final publication of The Guide will consist of the three chapters of The Guide plus an executive summary.

Introduction

It is universally accepted that reducing cost is a key consideration when evaluating alternative WAN and branch office solutions. However, cost isn't the only consideration and choosing the solution with the lowest cost isn't always the best decision. Because of that, this publication will identify and discuss several considerations other than cost, that should be included in the evaluation of alternative WAN and/or branch office solutions.

The majority of considerations discussed in this publication fall into two categories. One category is the business challenges that network organizations may be facing now, or will likely face in the near term; e.g., supporting the Internet of Things (IoT). Network organizations will not be successful if they implement solutions that respond only to today's challenges. To be successful they must implement solutions that also respond to the challenges that their organization will face in the near term. This puts pressure on network organizations to correctly identify those challenges.

The other primary category of considerations is the emerging set of IT technologies and techniques. It is highly unlikely that the optimum solution to emerging business challenges will be constructed entirely of legacy technologies and techniques. This puts pressure on network organizations to correctly determine which of the emerging technologies and techniques will both meet their needs and be successful in the market.

How network organizations incorporate the considerations discussed in this publication into their evaluation of alternative WAN and branch office solutions will vary based on the nature of each of the considerations. Two of the considerations that exemplify that concept are:

- Complexity
- Software defined

Nobody would argue against reducing complexity. However, complexity is hard to measure and as a result it is difficult to quantify how much complexity a given solution will reduce. It is even harder to quantify the business impact of reducing complexity. That said, some network organizations, particularly small and mid-sized organizations, place a lot of value on reducing complexity and hence tend to favor solutions that achieve that objective.

Being *software defined* is an example of the opportunities and challenges that are associated with adopting a solution based on emerging technologies and techniques. Whether or not a solution qualifies as being software defined is an important consideration because a broad set of vendors are making huge investments relative to developing and applying software defined techniques to myriad technological domains. Typically, the greatest gains in functionality and cost effectiveness occur in areas where there is a high level of investment and so it makes sense for network organizations to look closely at solutions that are software defined. However, the initial application of software defined techniques to data center networks was far less successful than was predicted. As a result, while network organizations need to pay attention to software defined solutions they must also realize that just because a solution is software defined doesn't mean that the solution will be successful in the market.

Key Considerations

Software Defined

The first modern instance of there being a broad discussion of IT functionality being *software defined* was the discussion of Software Defined Networks (SDNs) that started in earnest about five years ago. At that time, the acronym SDN referred exclusively to data center networks.

As previously mentioned, the initial SDN architecture and related protocols have not been widely adopted by enterprise organizations. However, many of the key concepts of SDN, such as a focus on software vs. hardware, the abstraction of the logical from the physical and a focus on an end-to-end approach to management and security have become an integral part of how new classes of software defined solutions are brought to market. Those new classes include: SD-WAN, SD-Branch, Software Defined Storage, Software Defined Data Centers and a Software Defined Perimeter (SDP).

Bottom Line: Because they potentially will benefit from the massive investments being made in the enabling techniques, network organizations should examine solutions that qualify as being software defined. In many instances, a given solution contains multiple components that are each software defined; e.g., a combination of SD-WAN and SDP functionality as part of a single solution.

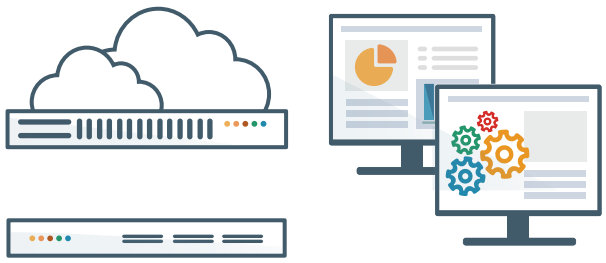
TALARI Networks™

SD-WAN SOLUTION OVERVIEW

Talari Networks, SD-WAN technology innovator, is engineering the internet and branch for maximum business impact by delivering a Failsafe Software Defined WAN (SD-WAN) solution that offers increased capacity, improved reliability, higher quality of experience while lowering costs. Talari's solution also enables a secure and consolidated branch infrastructure which delivers application and service deployment flexibility, without sacrificing availability or performance.

With the explosive growth in real time applications, distributed workforces and cloud computing, a company's productivity and customer responsiveness have never been more dependent on the WAN infrastructure. Because of this, organizations are turning their focus to their wide areas networks (WANs) and cloud access networks, knowing that having enough bandwidth to support the increased demand and predictable reliability to ensure continuous application availability are keys to their success.

The cloud is rapidly changing demands on enterprise IT legacy resources. The traditional WAN deployment of the last decade - MPLS circuits and enabling devices, often augmented by separate WAN-Op and firewall equipment - no longer offer enterprise IT the necessary requirements for cost savings, flexibility, bandwidth, manageability and streamlined cloud connectivity. Talari's failsafe WAN offers organizations the unique combination of availability, performance and reliability, yielding a highly resilient remote site with platinum application Quality of Experience.



Talari Solution Components

A Talari Networks Software Defined WAN, built on a comprehensive physical and virtual appliances portfolio, engineers the internet and branch for application reliability and unparalleled resiliency. Customers have great flexibility in determining how a Talari SD-WAN solution is deployed at the physical edge, the virtual edge, or in the cloud through the use of Talari's Controller, a full suite of appliances and centralized orchestration and analytics platform.

Failsafe Software Defined WAN

A Talari SD-WAN solution delivers a resilient network that ensures application availability while lowering cost. The following are some of the leading capabilities and benefits of this solution:

Secure Cloud Access with Visibility

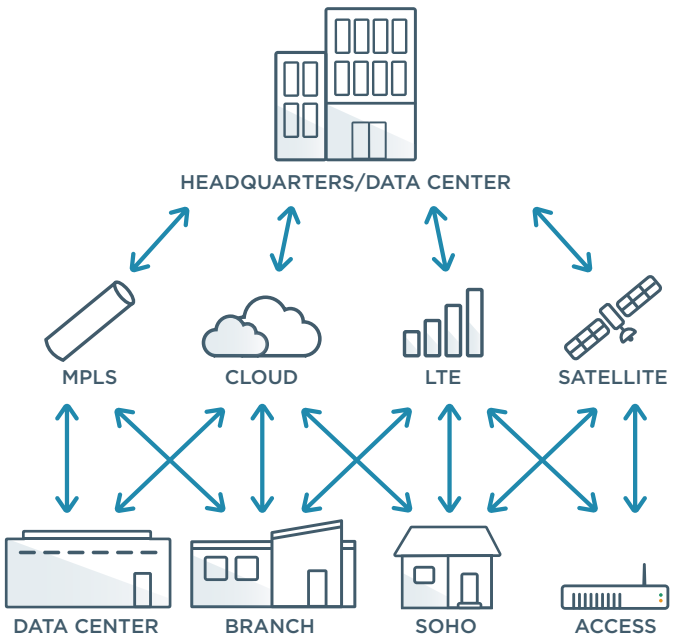
Talari extends the reach of the corporate WAN into the cloud by delivering an encrypted infrastructure with the performance, reporting and control capabilities a company requires to ensure a successful deployment.

Increased Application Quality of Experience

Talari ensures that applications work without interruption, even in the case of link failure or network impairments such as high jitter, delay, or packet loss.

Change WAN Economics with a Hybrid WAN

Companies can now modify their MPLS WAN infrastructure to incorporate low-cost, high-bandwidth broadband links that Talari technology converts into a business-class network.



SD-WAN Resiliency Benefits

- Continuous per-packet, unidirectional performance analytics that factor in packet loss, latency, jitter, and bandwidth between all paths and aggregated links
- Adaptive, deterministic per-packet optimal WAN-path decisions, and in particular sub-second response to degrading network issues such as link/device failures and/or congestion-based disruption or outages
- Enabling "liquid" application flows that are not impeded even when heavy loss/jitter occurs, let alone link failure
- Enabling single priority flows across multiple links; using all m/x/n paths between location pairs
- Ability to leverage all available bandwidth across multiple links, even for a single high-bandwidth flow
- Customizable by bandwidth availability: highly efficient bandwidth utilization
- Replication of flows and packets across disparate links, especially real-time apps like VOIP that require platinum QoS support
- Enables unmatched support for real-time and highly interactive apps
- Extremely scalable (thousands of WAN links with continuous, real-time path measurement) to accommodate QoE standards set by cloud service access providers and edge-network co-location facilities (carrier agnostic)
- Superior inbound congestion avoidance; that is, "bandwidth reservation and control" that enables business-quality app predictability

TALARI'S LEADING IT BENEFITS

- Gain resiliency, reliability and superior QoE
- Maintain high availability and uptime of business-critical apps
- Leverage bandwidth aggregation with commodity Internet services to reduce WAN legacy costs

DAYTON SUPERIOR

"Talari gives us the quality of service and guaranteed bandwidth we need to meet our service-level agreements for VDI and business applications." **- Dayton Superior**

Taft/

"I bought Talari to make the network more reliable, and it did exactly what it promised."
- Taft, Stettinius & Hollister, LLP

Driscoll's ONLY THE FINEST BERRIES

"After we implemented Talari...we went from paying $600 per Mbps to $100 per Mbps for bandwidth for our distribution centers. We scaled up the WAN bandwidth without scaling up the pricing." **- Driscoll Strawberry Associates**

Bremer Bank

"We can leverage Talari's capabilities to negotiate the highest bandwidth at the lowest cost without compromising reliability/availability in preparation for more rich content, video and streaming applications in the future." **- Bremer Bank**

Maricopa Region 911

"If a WAN link goes down, the call-takers are unaware. The peace of mind and visibility we get with Talari is invaluable." **- Maricopa 911**

United FEDERAL CREDIT UNION

"Talari provides the bandwidth we need to sustain our growth in an efficient and reliable platform."
- United Federal Credit Union

TO LEARN MORE OR REQUEST A DEMO, VISIT TALARI.COM

TALARI Networks

Talari Networks, Inc.
1 Almaden Blvd, Suite 200
San Jose Ca, 95113

Phone: +1 408.689.0400
info@talari.com
www.talari.com

SOLUTION-OVERVIEW-201707-007

Location of Key Functionality

In a traditional WAN or branch office, all relevant functionality is provided onsite. That's still a viable option. However, there are several other viable options. Examples include:

- On site at a customer's remote location;
- On site at a customer's regional or central location;
- In a Communications Service Provider's (CSP's) central office;
- In a co-location facility;
- In a public site dedicated to providing functionality such as optimization;
- In an IaaS provider's facility;
- In a SaaS provider's facility.

Bottom line: The traditional approach to hosting WAN and branch office functionality onsite still has value. However, there are numerous alternatives that enterprise organizations should consider. In many instances network organizations will find that the best solution is to locate functionality in multiple types of sites.

Application Delivery

There is no doubt that a company's WAN is critical to its business success. However, in the vast majority of instances a company's business unit managers don't appreciate the value of the WAN or any other component of IT other than the applications they use to run their business unit. As such, the value of a WAN to a company's business unit managers is primarily determined by the role that the WAN plays in application delivery.

To ensure successful application delivery, and hence enable the network organization to show value to a company's business unit managers, a company's WAN must:

- Ensure acceptable levels of application performance and availability;
- Provide monitoring and management functionality that enables the organization to perform rapid root cause analysis and remediation;
- Provide appropriate security.

Bottom Line: When evaluating alternative WAN and branch office solutions, network organizations must evaluate the solutions in large part based on the ability of those solutions to ensure successful application delivery.

Edge Computing

Over the last decade, the adoption of cloud computing has been a strong factor driving the centralization of resources into a relatively small number of public and private data centers. Recently a new form of computing has started to emerge and it is driving the decentralization of at least some resources. This new form of computing, edge computing, is intended in large part to address the challenge of massive data build-up by performing data processing at the edge of the network, near the source of the data. The goals of edge computing include both minimizing cost and latency as well as controlling network bandwidth.

There are several compelling use cases for edge computing. In one of the key use cases, network functions that an enterprise might otherwise run on site are run at an edge locations that are close to the users. This includes network functions such as WAN optimization, load balancing and security.

Another key use case is exemplified by the CORD (Central Office Re-architected as a Datacenter) initiative and the transformation taking place in Radio Access Networks. Both of these activities are intended to enable service providers to fully realize the promise of NFV. The Radio Access Networks transformation was initiated in late 2014 when ETSI announced the creation of an Industry Specification Group (ISG) for Mobile-Edge Computing. Per that announcement "Mobile-Edge Computing provides IT and cloud-computing capabilities within the Radio Access Network (RAN) in close proximity to mobile subscribers. Located at the base station or at the Radio Network Controller, it also provides access to real-time radio and network information such as subscriber location or cell load that can be exploited by applications and services to offer context-related services. For application developers and content providers, the RAN edge offers a service environment characterized by proximity, ultra-low latency, high-bandwidth, as well as real-time access to radio network information and location awareness. Mobile-Edge Computing allows content, services and applications to be accelerated, maintaining a customer's experience across different radio and network conditions."

Bottom line: As discussed in the preceding chapter of The Guide, network organizations have a strong interest in running L4 – L7 functionality in the cloud. Running this functionality at edge locations provides the same benefits as running it in the cloud. In addition, this approach eliminates some of the issues, such as latency, that are associated with the cloud.
As discussed below, distributed NFV enables organizations to implement a wide range of functionality wherever they see fit. For example, a given organization may choose to implement Virtualized Network Functions (VNFs) at the edge; in a highly centralized fashion; or in a hybrid fashion with some VNFs being deployed at the edge and others in central sites.

Elements of a Successful Digital Transformation and the Role of SD-WAN

apcela

A network evolution is happening and at the heart are applications. Apps, once secured and accessed via enterprise data centers, are moving to the cloud at an accelerating pace and users have moved beyond enterprise firewalls, requiring remote access and mobility.

Enterprise IT is now distributed and apps are delivered across hybrid IT environments resulting in performance challenges and complexity. This fragmented landscape requires a new application delivery model – hybrid WAN – supporting an evolution in how applications are delivered, secured and managed to ensure optimal performance and end-user experience. However, to ensure speed, performance and security in this model, companies are turning to SD-WAN solutions to enhance and extend the key functions of their enterprise for a higher performing, next-generation, distributed IT infrastructure.

Hybrid IT at the Foundation

Hybrid IT, an enterprise approach that manages some IT resources in-house and uses cloud-based services for others is a reality. Previously, IT utilized public cloud computing for non-critical IT services such as development and test applications or for turnkey SaaS applications like web analytics. All of which could replace internal applications and enable access for a mobile workforce. Today, enterprises aggressively pursuing digital transformation are running behind cloud first mandates and deploying new applications as SaaS wherever practical. Additionally, public IaaS platforms are no longer the domain of development and test environments as enterprises re-factor and even re-architect legacy, mission-critical applications to run in public cloud environments.

To stay ahead of this accelerating transformation, network infrastructure must evolve as rapidly as the cloud environment. Unfortunately, many legacy enterprise network architectures cannot keep pace. Traditional enterprise network architectures are built around a hub-and-spoke, carrier MPLS network anchored on the legacy premises-based data center. These typically interconnect the business operations of the enterprise, including regional offices and branches - bringing all traffic back through the datacenter. Any users and traffic destined for the cloud, typically go through a centralized, security DMZ (demilitarized zone of firewalls and web gateways) in the datacenter. This worked in the past when applications were in the datacenter, but it's becoming obsolete. So, what is the solution?

Consider Hybrid WAN

Because the internet is critical to enterprise cloud connectivity, its performance is not consistent making it impossible to rely on for business and mission-critical applications. This is where hybrid WAN comes into play. Hybrid WAN leverages both internet and MPLS - meeting the requirements of broad and increasingly distributed application deployments. Hybrid WAN also keeps the MPLS network interconnected to the distributed enterprise operations and legacy applications in the enterprise datacenter and local internet connections. This allows direct transit to cloud-based applications and services without the latency and costs associated with bringing all traffic back through a centralized, security DMZ.

While a hybrid WAN architecture solves hybrid IT performance challenges, it poses security challenges. DMZs are centralized for easier management. This leaves enterprise IT managers with a potentially costly and complex alternative of deploying firewalls in front of every internet connection. This is why enterprises have turned to a software-defined WAN (SD-WAN), which in a hybrid WAN environment overcomes many of these challenges - with additional benefits. Most SD-WAN technologies include at least some basic firewall functionality such as packet filtering, while others include fully featured, next-generation firewalls.

Add SD-WAN for Success

A fully functional hybrid WAN includes a range of architectural enhancements built for true cloud interoperability that includes a high-performance core network, carrier-neutral commercial data centers and extensive interconnection with both SaaS and IaaS cloud platforms. The combination of hybrid WAN and SD-WAN enables users and traffic destined for more critical cloud applications to reduce reliance on the unpredictable performance of the public internet and makes the interconnection with cloud applications directly to the user. Carrier-neutral commercial datacenters also serve as distributed security points and when combined with SD-WAN, enterprises can deploy a number of smaller distributed security DMZs. SD-WAN provides a comprehensive, distributed security approach providing access to policies across the network. Additionally, to further reduce network costs, SD-WAN:

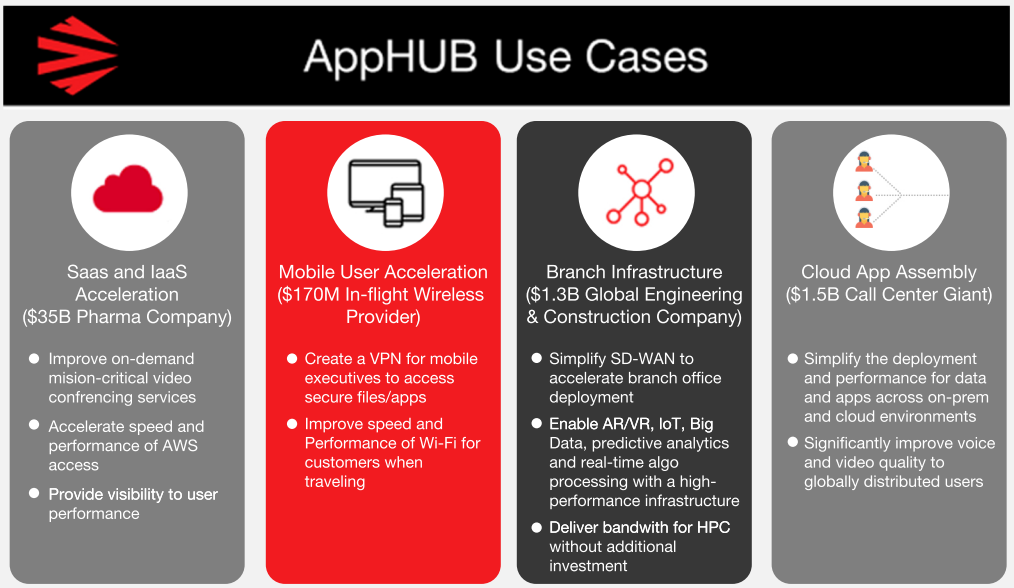
- Addresses latency and capacity issues;
- Provides an improved application performance – user location and application needs are not an issue;
- Creates an automated and simplified network connecting multiple locations with one overlay; and
- Offers telemetry that determines data traffic priorities.

Apcela, the high-performance application delivery company recognizes these three elements for a successful digital transformation. Apcela serves more than 100 of the Forbes Global 2000 including banks, exchanges, financial services and biopharma companies across 185 markets in 41 countries worldwide. Apcela enables enterprises to move to a cloud environment – keeping some of an organization's WAN and enhances and extends what companies already have with its AppHUB solution.

AppHUBs Enhance and Extend Key Functionalities with SD-WAN

AppHUBs are virtual datacenters deployed at network and cloud service provider-dense, carrier-neutral colocation facilities and datacenters. Built from colocation, network connectivity, hardware-optimized, virtualized network functions (VNFs) and hyper-converged compute and storage, each AppHUB is equipped with a complete network telemetry solution: AppMon. This ensures the underlay network and customer overlay networks meet SLAs. Additionally, AppHUBs' machine learning capabilities and run-over operating logs reduce the time-to-diagnosis for Apcela's NOC and in many cases, to the point where enterprises are unable to perceive an issue.

Enterprises can leverage computing capabilities with AppHUBs to eliminate bottlenecks in their networks, shorten the distance between edge locations and application hosting hubs, distribute security and improve overall performance of their WAN and application delivery platform. Apcela deploys SD router instances at each one of its AppHUBs to ingress- and egress-encrypted traffic to and from the AppHUB and network backbone. These instances are internet-connected, allowing enterprises to utilize Ethernet, DIA, broadband, or local access to securely connect to the WAN in the local AppHUB market. Additional AppHUB benefits include:



Distributed Security Extending across the Enterprise

AppHUB's suite of functions ensure security across its distributed system including:

- ***Distributed Endpoint and Cloud Security:*** Firewall, URL and file filtering, IDS/IPS, user Distributed Endpoint and Cloud Security: Firewall, URL and file filtering, IDS/IPS, user and application-based policies, malware detection and more.

- ***Improved Performance:*** By distributing firewalls closer to the edge, latency can reduced by more than 50%. VPNs can terminate closer to users and harness the low-latency backbone to move data across the WAN.

- ***Latency Optimized Internet Routing:*** AppHUBs include a network-based firewall with performance IP Internet. Performance IP leverages peering agreements with 6-12 ISPs and intelligently routes traffic to the ISP providing the best latency.

Network Connectivity for Best Performance

Carrier neutrality in an AppHUB facility ensures that WAN connectivity balances the best performance and best price. Carrier diversity ensures competition which drives carrier and path diversity as well as optimizes Apcela's opex for its underlay network infrastructure.

Cloud Gateways for Secure and Dedicated Connectivity

AppHUBs are Apcela's cloud gateways, offering secure and dedicated connectivity to the industry's leading cloud service providers like AWS, Google Cloud, Microsoft Azure and others. By leveraging the low-latency, core network connecting AppHUBs, along with Apcela's powerful telemetry tool AppMon, customer traffic can be routed to SaaS, IaaS and XaaS providers through the closest AppHUB location, lowering round-trip times and increasing application performance.

With innovation comes pitfalls. However, they can be avoided with these key elements: hybrid WAN, SD-WAN and with Apcela's AppHUB to ensure business and mission-critical applications function with the necessary speed and performance. No matter the location, company size, market or the amount of legacy infrastructure you have – AppHUB works to solve any issues you have moving to the cloud, while enabling growth for tomorrow.

Complexity

There are many factors driving the increasing complexity of IT, including the rapid adoption of cloud computing, virtualization, big data, IoT, mobility and new application architectures. Adding to the complexity inherent in the adoption of new technologies is that fact that when IT organizations adopt new technologies they seldom eliminate the existing technologies, at least not in the short term. As a result, IT organizations must combat the complexity that is associated with the legacy environment, the emerging environment, and the intersection of the two environments.

Part of the reason why complexity is a key concern relative to the WAN is because a highly complex environment makes it difficult for a network organization to achieve the application delivery goals previously discussed. High levels of complexity also tend to increase cost, reduce availability, create new attack vectors and increase the time it takes to add new sites or to implement new functionality. In addition, a highly complex environment is difficult to automate.

Bottom Line: The implementation of any new solution always adds complexity, at least initially. On a going forward basis, IT organizations should only adopt solutions that once in production will reduce notably more complexity than is added during the adoption process.

Mobility

Over the last two years most of the conversation about the WAN has focused on providing connectivity to an organization's branch offices. While providing that connectivity is clearly important, there are other WAN edge points that also need effective and efficient connectivity. The various devices used by an organization's mobile workers constitute an important class of WAN edge points. The size and hence importance of the mobile work force was documented in an analyst report that stated that the global mobile workforce is set to increase from 1.32 billion in 2014, accounting for 37.4% of the global workforce, to 1.75 billion in 2020, accounting for 42.0% of the global workforce.

Bottom Line: It may well be that in the short term that the best option that a network organization has is to implement a WAN solution that just supports branch offices. However, before implementing a WAN solution with a narrow scope, network organizations should develop a WAN strategy that includes how they will effectively and efficiently support mobile workers.

IoT

As noted above, branch offices are not the only class of WAN edge point. In a large and growing number of instances, the enterprise WAN must also support the IoT. The importance of the IoT was highlighted in a report published in early 2017. According to that report, 8.4 billion connected things will be in use worldwide by the end of 2017, up 31 percent from 2016, and that there will be 20.4 billion connected things by 2020. As discussed in a recent blog, the IoT impacts every industry with business-critical use cases being developed in many verticals including retail, healthcare, agriculture and transportation.

Bottom Line: It may well be that in the short term that the best option that a network organization has is to implement a WAN solution that just supports branch offices. However, before implementing a WAN solution with a narrow scope, network organizations should develop a

WAN strategy that includes how they will effectively and efficiently support the IoT. As described below, a major component of supporting the IoT is providing effective security.

The Role of Cellular

Cellular services have long been used as a back-up to wireline WAN services. In the current environment, cellular services are increasingly being used as either the primary WAN link or are used in conjunction with a wireline service in an active-active configuration. In the latter case, traffic is typically load-balanced over the cellular and wirelines services based on policy. Some of the other key use cases for cellular services in an enterprise WAN include:

- Temporary networks
  The time that it takes to get a wireline service such as MPLS installed is typically a month or longer. In the vast majority of cases that means that wireline services are not a feasible solution for the types of temporary networks that are needed to support locations such as construction trailers or pop-up stores.
- In-vehicle networks
  While it may or may not be desirable to use an MPLS or DSL-based Internet service to provide connectivity to a fixed site such as a branch office, it isn't possible to use these services to provide connectivity to vehicles such as cars, trucks and school buses.
- Internet of Things (IoT)
  The acronym *IoT* refers to the internetworking of a wide range of physical devices, buildings and other things that are embedded with electronics and/or sensors. For example, *a thing* may be a sensor inside of a traffic light. In many such instances, cellular services are the only feasible WAN option for supporting the IoT.

Another important use case for cellular services is in tertiary markets where MPLS is either not available or is prohibitively expensive. A variation of this use case involves an organization that has a large number of sites in tertiary markets. For the sake of example, assume that an organization has a few hundred sites in tertiary markets. Even if MPLS is available and somewhat affordable, the organization would be stuck with the administrative burden of having to manage contracts with a few hundred small CSPs. An alternative solution for such an organization is to deploy a router at each site that supports multiple cellular services. Based on a number of factors, including the terms of the contracts that the organization negotiated with its cellular providers, the organization may choose to implement the cellular services in an active-active configuration or in an active-passive configuration.

Bottom line: As the use of cellular evolves from being a backup service to where it is a primary service, network organizations need to include in their analysis of WAN and branch office solutions a focus on high-performing, effective cellular services. The requisite analysis involves developing an in-depth understanding of the technologies that underlie the solutions being considered. For example, the way that most SD-WAN solutions implement packet mode steering requires the solution to assemble and disassemble each packet at both ends of the WAN. While this approach is acceptable in a wired environment, in a wireless environment the associated signaling overhead can consume an unacceptable amount of the cellular capacity.

5G

Supporting the IoT is one of the drivers of a new generation of cellular services referred to as 5G. Network organizations should not look at 5G as just being a minor step in the evolution of cellular technology. For example, one analyst report discussed their belief that 5G will be as revolutionary at electricity.

Some of the characteristics of a standards based 5G service that enable it to potentially be as revolutionary as electricity include:

- Data rates of tens of megabits per second for tens of thousands of users;
- Data rates of 100 megabits per second for metropolitan areas;
- 1 Gb per second simultaneously to many workers on the same office floor;
- Several hundreds of thousands of simultaneous connections for wireless sensors;
- Coverage improved compared to 4G;
- Signaling efficiency enhanced;
- Latency reduced significantly compared to LTE.

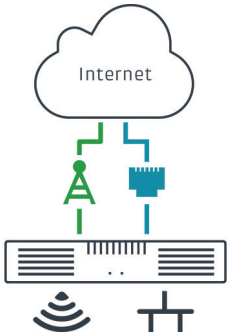
Over time 5G will encompass many wireless technologies, including 5G New Radio, Gigabit LTE for super-fast speeds; LTE IoT for low power, long battery life, and long-range coverage; Digital TV, C-V2X, or vehicle to anything; and ultra-low latency. 5G will build on the architecture of voice (2G); voice, video, and data (3G); and massive mobile data (4G)—and add massive bandwidth and density, as well as ultra-low latency. 5G also will integrate aspects of WiFi and long-range/low-power networks.

The initial trials and deployments of 5G services are based on a non-standard architecture that is designed to be easily upgraded to a standards-based architecture when appropriate. This is likely to occur in 2018. Recognizing the importance of 5G, at least one service provider has already announced their intention to offer nationwide 5G service.

Bottom line: Within the next two years, 5G has the potential to fundamentally change networking. Network organizations evaluating new WAN and branch office solutions need to ensure that those solutions will aggressively and effectively support 5G.

Elastic Edge: Pervasive Connectivity for People, Places & Things

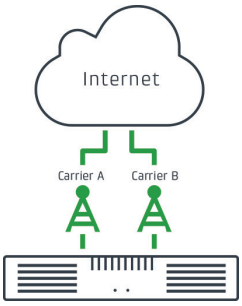
Software-Defined Branch



Cradlepoint's all-in-one branch network solutions are ideally suited for "Lean IT" organizations that demand business-critical 4G LTE connectivity. Powered by Cradlepoint NetCloud software and services, these solutions combine SD-WAN functionality with integrated WiFi, Ethernet switching with PoE support, advanced edge security, and multiple 4G LTE modems in a single platform. The entire branch network can be deployed, controlled and managed from a single of pane of glass in the cloud.

Feature Highlight: NetCloud SD-WAN functionality is optimized for LTE-dependent networks and utilizes a unique Active-Dynamic traffic steering algorithm that provides complete, policy-based control over hybrid WANs that include multiple 4G LTE connections. It can select the optimal path across any wired or wireless link based on a combination of signal strength, latency, jitter, service, carrier preference, and data plan consumption.

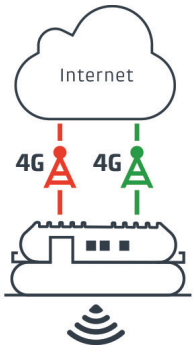
Cutting the Wire: LTE-Optimized SD-WAN



For highly distributed networks such as rural convenience stores and insurance offices, there are few options for reliable broadband. Even if wired options exist, building a nationwide network often requires stitching together more than 100 Internet Service Providers. In contrast, cellular networks provide pervasive, high-speed broadband data to cities and towns of all sizes, enabling a nationwide WAN with just a few providers. Cradlepoint leads the market in 4G LTE technology, from narrow-band IoT solutions to providing a pathway to gigabit LTE and 5G. Cradlepoint branch solutions have integrated software-defined modems supporting advanced capabilities offered by cellular providers.

Feature Highlight: Cradlepoint branch routers accommodate two LTE modems and up to four carrier SIMs. NetCloud Manager lets customers centrally configure Smart WAN Selection and perform zero-touch deployments.

SD-WAN on Wheels

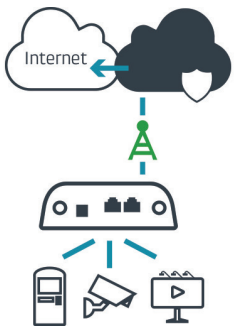


Many organizations—first responders, disaster response teams, mass transit, school districts, and more—rely on in-vehicle networks to serve their customers or the public. These mobile networks require a wireless WAN that delivers high availability, advanced security, and optimal application performance on the move.

Cradlepoint delivers the SD-WAN capabilities of its NetCloud platform in a ruggedized mobile router that combines multiple 4G LTE modems, WiFi, advanced edge security, GPS tracking, and telemetry integration—keeping vehicles, and the people and things in them, connected and protected.

Feature Highlight: Cradlepoint is the only SD-WAN mobile router that supports FirstNet, the private 4G LTE network for first responders. Policy-based Active-Dynamic traffic steering delivers persistent application sessions during cellular disruptions, and can intelligently steer applications between FirstNet and commercial LTE.

Connected & Protected IoT Devices



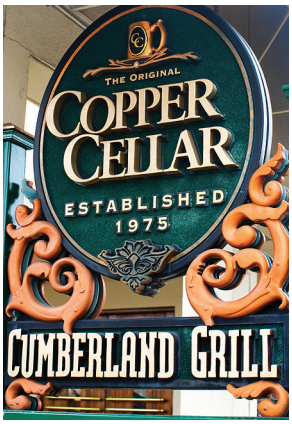
The news of Reaper and Mirai botnet attacks affecting millions of IoT devices illustrates the ever-increasing WAN vulnerabilities of IoT deployments. Cradlepoint, a global leader in 4G LTE routers for M2M/IoT networks, is the only vendor to integrate Software-defined Perimeter (SD-P) technology to provide perimeter security, a private IP overlay for Internet and enterprise WAN isolation, and micro-segmentation. Enterprises use NetCloud to orchestrate and deploy—in minutes—secure overlays for M2M/IoT devices anywhere, with no configuration or Internet-routable IP addressing required.

Feature Highlight: Cradlepoint's NetCloud Perimeter (NCP) feature is available on M2M and branch routers, enabling SD-P overlays that connect and protect M2/IoT devices in the branch or in the field. The NCP Client extends SD-P functionality to remote workforces that require secure access to Intranet and public cloud applications from laptops, tablets, or smartphones.

Stories of Software-Defined Networking in the Branch & Beyond

Stores Optimize Connectivity With SD-WAN

For its rapidly expanding restaurant chain, The Copper Cellar needed more flexibility, less hardware, better WAN uptime, and the ability to manage everything through the cloud.



The Copper Cellar streamlined its branches with Cradlepoint's SD-WAN solution, including a dual-modem router with wired broadband set up as the primary link and 4G LTE for failover.

Cradlepoint's NetCloud platform provides zero-touch deployment, single-pane-of-glass management, and SD-WAN services for optimized path selection. The IT team easily sets up business-based policies that seamlessly move traffic such as voice and video to the best-performing link.

Remote Sites Use LTE as Primary WAN

Professional Contract Services Inc. (PCSI) needed connectivity for its offices located in areas without access to wired WAN. With Cradlepoint's NetCloud Manager (NCM) and routers, PCSI's small IT team provides connectivity quickly and cost-effectively – with limited man-hours and simplified configuration, deployment, and remote management.

The IT team configures its routers at headquarters through NCM's single-pane-of-glass platform, then later can push out firmware upgrades, security patches, and other updates instantly.

"I was overwhelmingly impressed with how simple, quick, and easy it was to deploy Cradlepoint solutions," said Nathan Matarazzo, systems analyst at PCSI.

Cities Use SD-WAN in Police Vehicles

In major U.S. cities, police departments often face unreliable connectivity and insufficient bandwidth for their high-tech cruisers. With Cradlepoint's cloud-managed in-vehicle routers and extensibility docks with SD-WAN capabilities, officers are always connected to critical information and applications in the field.

This dual-modem SD-WAN solution enables cellular-to-cellular failover when a connection drops and dynamic traffic steering when it deteriorates. IT teams also can push out updates through the cloud rather than bringing each vehicle to headquarters.

Additionally, four-nines uptime enables officers to file report from anywhere instead of at the office, which improves incident response times.

Stores Protect IoT With Secure Perimeter

Many large retail and restaurant chains are installing video surveillance cameras to monitor employee and guest activity. However, without cloud access to their DVR systems, these enterprises lack PCI-compliant options for real-time monitoring.

IT teams address their IoT connectivity and security needs with cloud-managed Cradlepoint routers and NetCloud Perimeter (NCP), which enables a Virtual Cloud Network to be created in minutes. With NCP running on every router and on each manager's mobile device, a Software-defined Perimeter is established. With its own cloud-based network attached to a devoted VLAN, end-to-end encryption keeps data protected.

LEARN MORE ABOUT NEXT-GENERATION ELASTIC WAN CONNECTIVITY: **CRADLEPOINT.COM/ELASTIC-WAN**

cradlepoint

Cloud Computing

When the WAN architecture that was introduced at the turn of the century was first developed, enterprises made very little use of the Internet and so effectively and efficiently supporting Internet traffic wasn't central to that architecture. As a result, even though it both added to the cost of the WAN and it made applications run slower, the vast majority of organizations opted for backhauling Internet traffic.

A recent article in Forbes quantified how the use of cloud computing has grown over the last several years and how it is expected to grow over the next few years. According to that article, "Cloud computing spending has grown at 4.5 times the rate of IT spending since 2009 and is expected to grow at better than 6 times the rate of IT spending from 2015 through 2020." The article added that "Worldwide spending on public cloud computing will increase from $67B in 2015 to $162B in 2020 attaining a 19% CAGR."

Bottom Line: Given the size and growth of cloud computing and the resultant size and growth of Internet traffic, backhauling Internet traffic is no longer acceptable from either a financial or an application performance perspective. This has given rise for the need to deploy Direct Internet Access (DIA) at the branch, which fundamentally alters the prevailing security paradigm. This is one of the several factors driving the need to implement NFV somewhere at the edge of the WAN.

Security

Large scale security breaches have become common place. One measure of the impact of security breaches comes from an IBM report which stated that by 2019 cybercrime will become a 2.1 trillion-dollar problem. Another measure is that because of the impact that a cyberattack can have on a company's profitability, brand and stock price, in many instances cyber security is both a CEO and a board level issue.

Many of the newer WAN solutions support DIA from branch offices. This approach provides a lot of value but it also creates a new attack surface. Branch offices, however, are not the only WAN end point that presents a security risk. A recent article stated that "29 percent of organizations have already experienced either a data loss or breach as a direct result of mobile working." The article went on to say that "As many as 44 percent expect that mobile workers will expose their organization to the risk of a data breach." The title of another recent article highlights the fact that the adoption of the IoT comes with significant security challenges. The title of that article is *Five nightmarish attacks that show the risks of IoT security.* One of the attacks that the article discussed was the Mirai botnet, which was used to flood DNS provider Dyn with a DDoS attack. The Mirai botnet took down Etsy, GitHub, Netflix, Shopify, SoundCloud, Spotify, Twitter, and a number of other major websites.

Bottom line: Since branch offices are not the only class of WAN edge points, network organizations also need to ensure that their WAN architecture provides effective security to all the relevant WAN edge points, including mobile workers and the IoT.

Software Defined Perimeter

The legacy security model of the WinTel era is based on the concept of a well-defined perimeter. The security tools of this era, including VPNs and firewalls, are labor-intensive to implement and manage and in addition, these tools don't leverage user context to make access decisions.

In addition to the limitations of the security tools of the WinTel era, driven in part by the adoption of the IoT, the concept of a well-defined perimeter no longer makes sense. These factors lead to the development of a Software Defined Perimeter (SDP) which is a contemporary security framework that is designed to provide on-demand, dynamically provisioned network segmentation. The SDP framework dynamically creates one-to-one network connections between the user and the resources that they access. The framework also ensures that all the endpoints attempting to access a given infrastructure are authenticated and authorized prior to being able to access any resources on the network. According to the Software Defined Perimeter working group, the SDP security model has been shown to stop all forms of network attacks including DDoS, Man-in-the-Middle, Server Query (OWASP10) as well as Advanced Persistent Threat (APT).

Bottom Line: The legacy security model of the WinTel era is rapidly becoming obsolete. As part of their adoption of new solutions to connect WAN edge points, IT organizations need to fundamentally rethink their approach to security in part to ensure that it is not based on obsolete concepts such as the existence of a well-defined perimeter. For most IT organizations this will involve adopting at least some of the key concepts of an SDP.

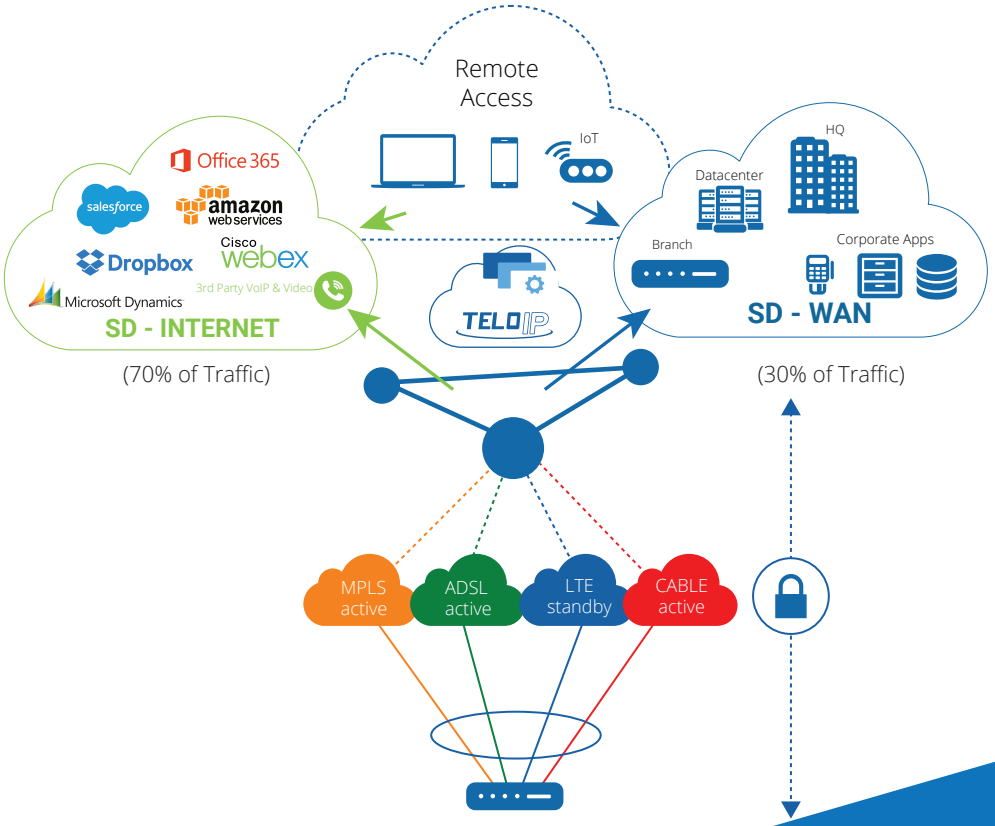
RISK FREE SD-WAN

Experience

For over 15 years, TELoIP has been managing converged voice, video and data solutions that deliver the promise of the internet for business customers.

Hardened Infrastructure

TELoIP Cloud network is carrier-class SD-WAN-as-a-Service infrastructure providing both high-availability and high-performance plus a long haul WAN transport network for the lowest overall cost.



SIMPLIFYING CLOUD ACCESS
WITH SOFTWARE DEFINED NETWORKS

VINO SD-WAN

CLOUD CONNECTIVITY

We eliminate barriers to SD-WAN adoption by leveraging a turnkey, multi-tenant cloud (the TELoIP Cloud) with nine points of entry in North America. We located each point of entry in carrier-neutral facilities, allowing us to take advantage of a plethora of blended transit services co-located in these sites.

COST-EFFECTIVE

VINO SD-WAN allows enterprises to take advantage of broadband pricing and carrier diversity to create a non-stop network ensuring virtual private network reliability and performance at 'best effort' price points.

CLOUD MANAGED

The TELoIP Cloud creates a Virtual Intelligent Network Overlay (VINO) that unifies all branch traffic into a single cloud-managed SD-WAN overlay connection.

WHY IS TELOIP DIFFERENT

TELoIP has long held that the battleground is on the network edge, where our patented ANA/IPDE/MPDS technologies provide a measureable performance advantage over any other SD-WAN competitor — especially with poor underlays or under congested busy hour conditions..

TELoIP's VINO architecture provides a patented Virtual Network Function (VNF) Control Plane that builds a full mesh topology between points of entry. The multi-patented Data Plane provides comprehensive underlay management and Virtual Network Functions (VNF) for IPQoS, Firewall, Link Aggregation, Failover and Routing. The VINO Portal offers complete Management Plane with service orchestration, move, add, change delete support and performance visualization.

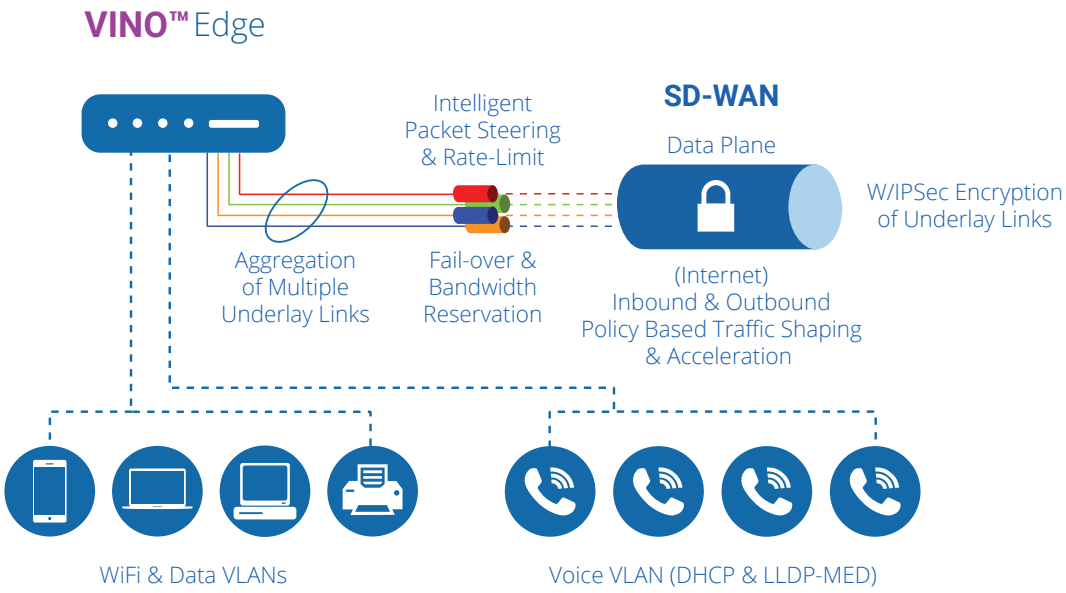
TELoIP offers substantial differentiation, with patented technology in each of the data plane, control plane and management plane that delivers higher aggregated speeds and better quality of experience than competitive solutions when tested using the same underlay links and test scenarios. We believe that TELoIP is well-positioned in the SD-WAN market because:

- Only TELoIP provides both WAN and Internet optimization
- TELoIP enables high-quality voice and video calls with no drops
- We address the need to connect remote and mobile users securely
- We can address scalable security requirements for IoT ecosystems
- VINO SD-WAN aligns network services to user, application and business requirements

TELoIP Inc. | 1-5430 Timberlea Blvd., MIssissauga, ON L4W 2T7 | TEL: +1 416 203 7838 | www.teloip.com | info@teloip.com

VINO SD-WAN DELIVERS

- VoIP Quality-of-Experience
- 'Hitless' VoIP/Video Fail-over
- Increased Performance
- Software Defined Perimeter
- Cloud Managed Network
- Centralized Orchestration
- Secure Remote Access Solutions
- Cloud Agility
- Lower WAN Costs



WHY VINO SD-WAN

INNOVATION

Deploy knowing TELoIP has the deepest intellectual property portfolio in the SD-WAN business. We turn business challenges into technology solutions, with award-winning technology that has been awarded 21 patents and counting

EASY TO BUY & DEPLOY

We ensure customer success by combining all the VINO SD-WAN components into a simple, predictable license fee that includes professional design, installation and ongoing 24/7/365 support.

NON-STOP BROADBAND

We build unbreakable cloud tethers backed with impeccable network engineering and support services. Working with our partners we ensure that you have a risk-free experience.

KEY CHALLENGES WE ADDRESS

- Network Reliability & Uptime
- VoIP & UCaaS Performance Issues
- Multi-Cloud Reliability & Performance
- End-User Productivity
- Network Capacity/Bandwidth
- Branch Office Security
- Branch Office Complexity
- Network Visibility and Control
- Remote/Mobile/IoT Device Access
- Support of Digital Transformation Efforts
- IT Budget Pressure

CONTACT

SMB or Enterprises – Call us for SD-WAN consultations from Network Design to ROI Calculation and Price Quotes at info@teloip.com

WAN Optimization

One of the promises of an SD-WAN is that it enables network organizations to add large volumes of relatively inexpensive Internet bandwidth. Because adding bandwidth often either eliminates or significantly reduces application performance problems, it's possible to conclude that implementing an SD-WAN negates the need for WAN optimization functionality.

There are, however, multiple use cases in which WAN optimization adds value. One of those use cases is disaster recovery (DR). DR requires large files be transmitted between a primary and a secondary data center that are usually far apart. Due to the well documented impact of the TCP window size on WAN throughput, the DR application may not be able to fully utilize the WAN bandwidth and hence may not be able to transmit all the data needed to support the company's DR plan.

While traditional WAN optimization solutions were focused on the connections between a company's branch offices and their internal data centers, increasingly WAN optimization functionality is being focused on the connections between a company's branch offices and myriad cloud providers. If a branch office is connected to an IaaS provider's facility, it is possible to have a WAN optimization functionality on both ends of the connection. Another option is that many service providers offer private cloud connect services that securely connect their managed VPN customers to some of the IaaS and SaaS providers using the service provider's MPLS infrastructure. This direct connect approach provides improved performance and security, but adopting this approach means that network organizations will not experience the cost savings that comes with substituting Internet connectivity for MPLS connectivity.

Bottom line: There is no doubt that in many instances adding WAN bandwidth eliminates application performance problems. However, there is also no doubt that in many other instances just adding bandwidth doesn't eliminate application performance problems and that WAN optimization functionality of some type is required.

Network Functions Virtualization (NFV)

While the European Telecommunications Standards Institute (ETSI) champions the interest that CSPs have with NFV, the Open Networking User Group (ONUG) has emerged to champion the corresponding interest that enterprises have. In a white paper entitled *Open Networking Challenges and Opportunities*, ONUG discussed the cost and complexity of managing a large number of Layer 4 - 7 network appliances from different vendors with different management tools. The appliances they mentioned included WAN optimization controllers and a variety of security appliances. When initially conceptualized, NFV was a centralized architecture. However, in order to support the large and growing range of WAN edge points, NFV has evolved to be a highly distributed architecture.

Bottom Line: The transition that the IT industry is undergoing is a lot broader than just improving the functionality found in the WAN or in the branch office. At its core, the transition is about focusing broadly on supporting a wide and enlarging set of people, places and things. Distributed NFV is a key enabler of this transition.

As previously discussed, as part of the ongoing industry transition, there now is a large set of locations where functionality can be housed. Determining where functionality should be housed requires careful analysis. For example, just because functionality such as a next generation

firewall can be virtualized doesn't mean that it makes sense financially or operationally to put a virtualized next generation firewall in every WAN endpoint.

*CPE

A major part of the transition that is happening in the IT industry is the movement away from solutions in which each service is comprised of hardware and software that is both tightly integrated and proprietary. The goal of this transition is to move to a more modular architecture in which a general hardware and software platform can support a wide range of services. The two primary forms of CPE which have evolved to enable this transition are uCPE and vCPE.

uCPE
Universal Consumer Premise Equipment (uCPE) is a term coined by AT&T. It denotes CPE that is not reliant on a centralized cloud for additional network functions and orchestration, but is entirely self-contained. Due to being self-contained, the hardware employed for uCPE needs to be more powerful than does the hardware used for Cloud vCPE solutions.

vCPE
This is what is most commonly thought of as being a software-defined CPE. In this type of CPE, the network functions that are provided are entirely supported by commodity hardware and virtualized network functions instead of by proprietary ASIC's. The phrase *Cloud vCPE* refers to a subset of vCPEs that include remote carrier-grade management, deployment and orchestration functionality.

Bottom line: Solutions based on either uCPE or vCPE can provide value in large part because they host multiple network functions. However, one of the limitations of branch office solutions that are based on either uCPE or vCPE is that it can be very challenging for these solutions to provide sufficient WiFi support or to tightly integrate with branch office functionality such as Ethernet switching with PoE.

SD-WAN Solutions

We're Ready When You Are

Dell EMC is ready to provide turn-key hardware and software solutions designed to simplify and accelerate production-ready SD-WAN deployments and services, with a choice of SD-WAN software from Versa Networks, Silver Peak, or VeloCloud.

Introducing Dell EMC SD-WAN Ready Nodes

At Dell EMC, we view SD-WAN as a critical and necessary component for Digital Transformation. For Service Providers, SD-WAN represents an opportunity for creating new services, accelerating time-to-revenue and increasing service agility. For enterprises large and small, SD-WAN represents an opportunity to lower cloud connectivity costs, while also optimizing WAN traffic patterns and usage. Dell EMC has double down on strategy of open and verified solution choices, to build SD-WAN for production, by offering validated product options for SD-WAN services, that is built upon the industry's foremost virtualization infrastructure, and hardware platforms.

We're meeting this need with a family of Ready Node offerings, designed for Service Providers and Enterprises alike intended to simplify and accelerate SD-WAN adoption. At the heart of our Ready Nodes are validated, pre-tested solutions comprising of Dell EMC compute platforms and industry leading SD-WAN software offerings from Silver Peak, Versa Networks, and VeloCloud. Included in the Ready Node offerings are Bill of Materials (BOM), partner software SKUs for the appropriate use-cases, pre-installed drivers and firmware settings.

The choice of multiple ready node hardware platforms provides maximum deployment flexibility for large, medium or small environments. Moreover, multiple SD-WAN partners furthers that flexibility by supporting many use cases.

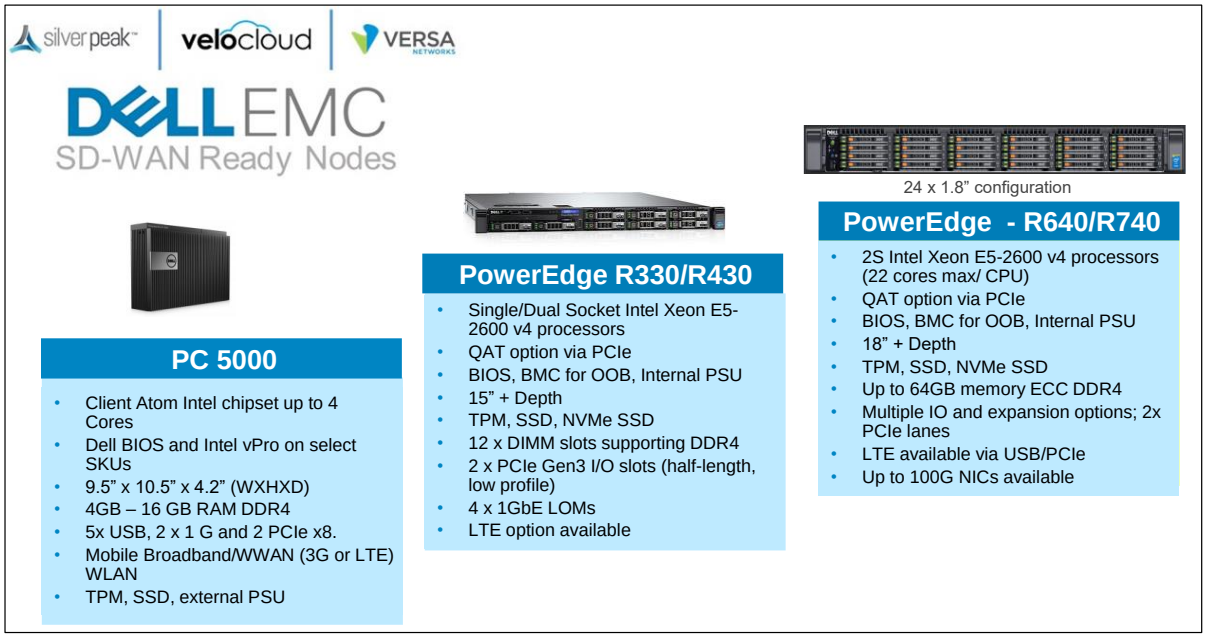


Figure 1. Dell EMC SD-WAN Ready Nodes

SD-WAN Ready Node use-cases

Service Providers can add new profitable managed services (e.g., cloud-managed SD-WAN or SD-Security service), and reduce their time-to-revenue for these new services. Communications Service Providers, for example, can improve their competitive advantage by offering a hybrid WAN allowing current customers to add managed internet bandwidth to their branches, particularly for less critical traffic flows. Managed Service Providers can generate new revenue streams by adding Managed SD-WAN services; and can further benefit in productivity improvements with features such as zero touch provisioning.

Enterprises can choose to deploy a do-it-youself on-premise SD-WAN, using the Dell EMC SD-WAN Ready Nodes. Enterprises can benefit with lower capital and operating costs, by leveraging lower-cost broadband connections and improving application performance, through intelligent route selection.

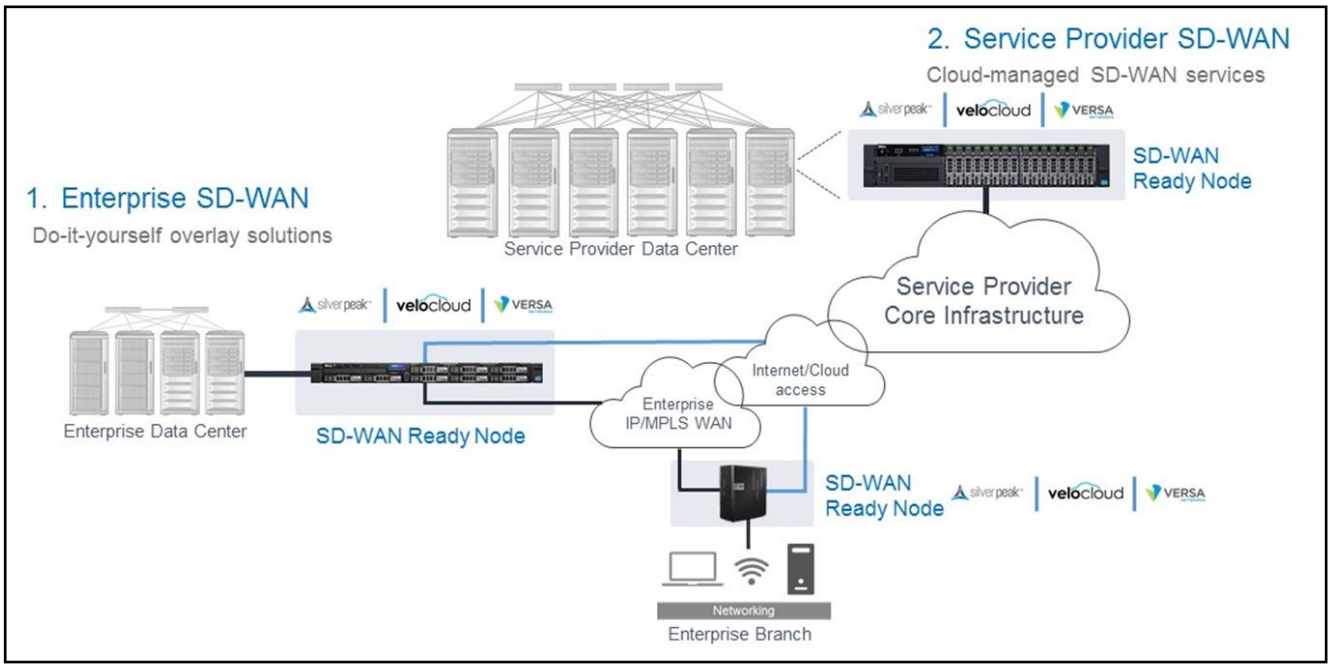


Figure 2. Dell EMC SD-WAN Ready Node use-cases

Take the next step

Contact your Dell EMC, Silver Peak, VeloCloud or Versa Networks representative to learn more about SD-WAN Read Nodes from Dell EMC.

Learn more about Dell EMC SD-WAN Solutions

Contact a Dell EMC Expert

WAN Management

An analyst report described the challenging state of WAN management. According to that report, only 13% of network organizations have all the functionality that they need to troubleshoot problems related to network and/or application performance degradation. In addition, 20% of network organizations reported that the troubleshooting functionality that they have is barely adequate. Unfortunately, in part because it introduces new functionality such as dynamic path selection, the adoption of an SD-WAN is likely to make WAN management even more demanding. Other factors that are further complicating the challenge of WAN management include the rapidly growing use both of DIA and cellular services as well as the exploding adoption of mobility and the IoT.

Bottom Line: As companies continually increase their reliance on the WAN to support virtually all of their business processes, the inability of the network organization to effectively troubleshoot the WAN will increasingly have a negative impact on those business processes. A critical challenge facing network organizations is that due to the fundamental shifts in the industry, WAN management is becoming increasingly difficult. The deployment of new WAN solutions is an opportunity for network organizations to improve their ability to troubleshoot the WAN and hence improve their ability to support the company's critical business processes. As a result, network organizations need to make effective management a central component of the analysis they do of new WAN solutions.

Machine Learning

Machine Learning is a subset of Artificial intelligence (AI) that focuses on the practice of using algorithms to parse data, learn from it, and then make either a determination or prediction about something. In contrast to a static algorithm such as Dijkstra's, a critical aspect of machine learning is that the machine is *trained* using large amounts of data and algorithms that give the machine the ability to continually learn how to perform a given task.

Machine learning has the potential to enable a huge step forward in terms of automation. One use case for machine learning is the automated detection and analysis of anomalous behavior. Potentially in the not very distant future, well-trained, machine learning based systems will be able to identify security risks and intrusions and will also be able to troubleshoot performance problems before they impact users. Another key use case that could possibly be mainstream relatively soon focuses on the path selection functionality contained in SD-WAN solutions. One example is that a properly trained SD-WAN solution may soon be able to anticipate congestion on a given WAN link and automatically divert traffic to an alternative link.

Bottom line: Machine learning has the potential to fundamentally impact how IT functionality is operated and managed. As such, as they work with vendors to explore new WAN and branch office solutions, network organizations should spend time to understand the vendors' strategies relative to machine learning. However, network organizations also need to balance the enthusiasm that the industry currently has for machine learning with the realization that while AI has been around for decades, achieving the promised benefits of AI has proven to be extremely difficult.

Ongoing Role of MPLS

In many instances when a network organization implements an SD-WAN solution it makes the assumption that it needs to include in its implementation predictable transport services such as MPLS to carry latency-sensitive traffic. Part of the reason for that approach is because the Internet is usually regarded as being too unpredictable to deliver enterprise-grade, latency-sensitive applications on a predictable basis particularly between Internet regions. Network organizations that adopt that approach will not realize all the savings that they could if they were more aggressive at eliminating their use of expensive WAN services such as MPLS, potentially through the use of NaaS-based solutions as described below.

Bottom line: While they are exploring alternative solutions, network organizations should make sure that they analyze solutions that enable them to aggressively reduce WAN transport costs.

Alternatives to a DIY Approach

As customers adopt SD-WAN and SD-Branch, one of the deployment choices they face is whether or not to implement an SD-WAN or SD-Branch on a Do-it-Yourself (DIY) basis. Using WAN as an example, in a DIY solution the customer is responsible for the entire lifecycle of their WAN. This means that the customer is responsible for the planning, designing, implementing and managing of all components of the WAN.

As discussed in the preceding chapter of The Guide, most network organizations prefer a WAN solution other than a DIY based solution. One alternative to a DIY solution is a managed service provided by a variety of types of Managed Service Providers (MSPs), including CSPs and Systems Integrators (SIs). MSPs typically acquire and implement the same SD-WAN functionality as an enterprise network organization would and MSPs leverage that functionality to provide their customers with a turnkey solution that includes active management. In the vast majority of cases, however, the MSP also provides a portal that enables the customer to at least monitor their network and, in many cases, to make changes.

Another alternative to a DIY solution is a Network-as-a-Service (NaaS) based solution. A NaaS based solution replaces the network itself by connecting business entities such as HQ facilities, branch offices, mobile workers, and cloud facilities to a cloud-based network. When compared to a DIY based solution, a NaaS based solution results in fewer entities for a network organization to own, deploy, upgrade and troubleshoot.

Bottom Line: When evaluating SD-WAN and SD-Branch solutions, network organizations need to ask themselves if they have the expertise to implement these solutions on a DIY basis and if they do, if that is the best use of their highly skilled resources. If that is not the case, then the organizations should evaluate NaaS and managed service offerings.

The Future of SD-WAN. Today.

The WAN is Incompatible with Modern Enterprise

The migration to cloud applications and a mobile workforce is changing the shape of the business. The Wide Area Network (WAN) was built to connect and secure static, physical locations - not today's fluid and dynamic businesses. Enterprises pay the price of this incompatibility with expensive connectivity and convoluted topologies that are hard to manage and secure. Adding new locations, enabling secure internet access at remote locations and for mobile users, and optimizing network resources for cost and performance, all represent a growing challenge for most organizations. Traditional SD-WAN is offering flexible capacity and agility but persists the dependency on expensive MPLS connectivity and security appliance sprawl, and lacks optimized support for cloud resources and mobile users.

True WAN Transformation with Cato Networks

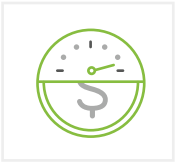
Cato Networks provides organizations with a global SD-WAN with SLA-backed backbone and built-in network security stack. The Cato Cloud reduces MPLS connectivity costs and branch office appliances footprint, provides direct secure internet access everywhere, and securely connects mobile users and cloud infrastructure into the enterprise network.

Secure And Optimized SD-WAN

Cato SD-WAN enables organizations to augment MPLS with affordable last mile services (Fiber, Broadband, 4G/LTE) and dynamically direct traffic based on applications needs and link quality. Unlike legacy SD-WAN solutions, Cato is uniquely capable to replace MPLS altogether with our global SLA-backed backbone.

Appliance Elimination

Cato eliminates branch office equipment such as UTMs, Firewalls and WAN optimization appliances. Cato protects all locations and users everywhere, without the need for unplanned hardware upgrades and resource-intensive software patches.



Affordable MPLS Alternative

Cato leverages cloud scalability, software-defined networking and smart utilization of a multi-carrier backbone to deliver a high performance and SLA-backed global WAN - at an affordable price.

Hybrid Cloud Network Integration

Cato connects physical and cloud datacenters, across all providers and global regions, into a single, flat and secure network. Customers can seamlessly extend corporate access control and security policies to cloud resources, enabling easy and optimized access for mobile users and branch locations to all applications and data anywhere.

Secure Direct Internet Access

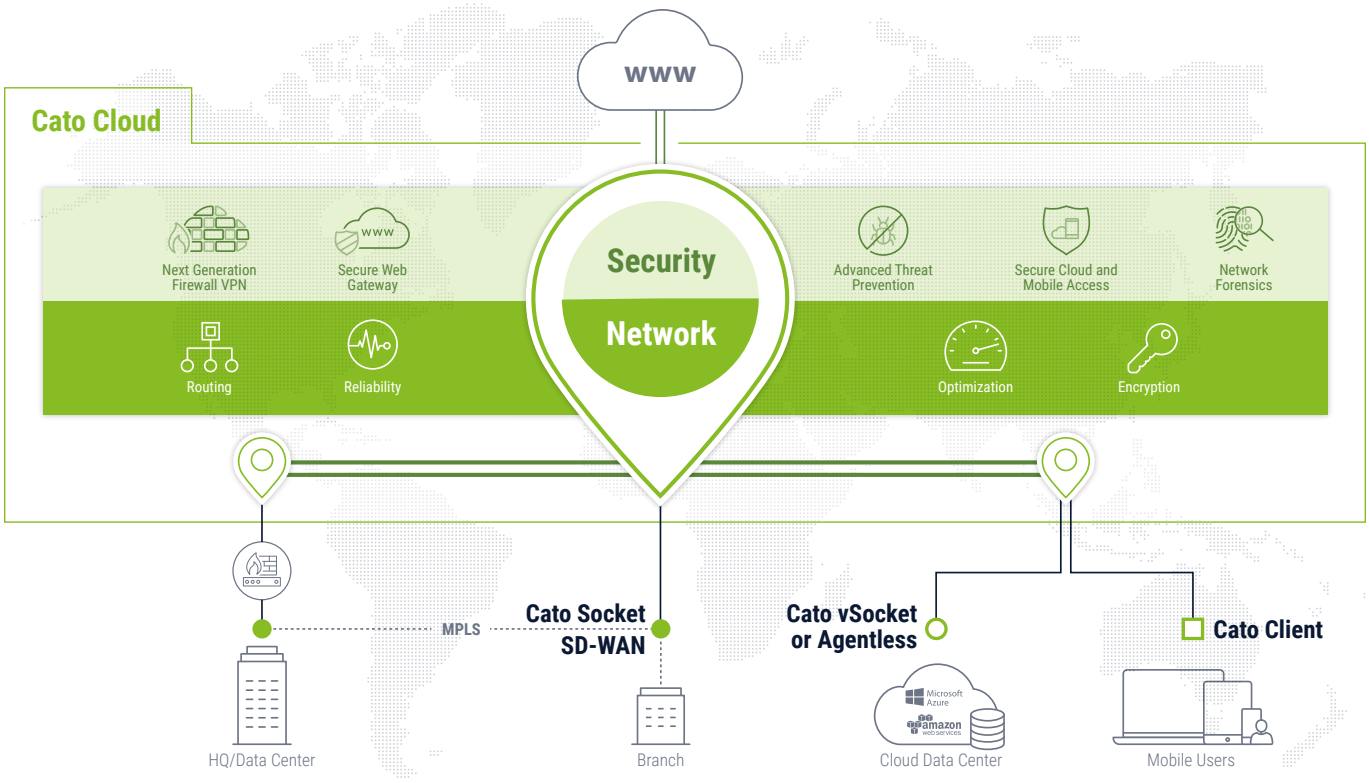
Cato connects all branch offices and remote locations to the Cato Cloud, providing enterprise-grade network security for any location without the need for dedicated appliances or traffic backhauling.

Mobile Workforce Secure Cloud Access

Cato connects every mobile user to the Cato Cloud and provides secure and optimized access to enterprise resources in physical and cloud datacenters, cloud applications and internet sites. Cato uses its global backbone to optimize routing and reduce latency to key applications like Office 365, and enforce application-aware security policies on all access.

Software-defined and Cloud-based Secure Enterprise Network

The Cato Cloud connects all locations, cloud resources and mobile users into an optimized and secure global SD-WAN. With both WAN and internet traffic, consolidated in the Cato Cloud, Cato applies a set of elastic and agile security services to protect access to enterprise applications and data, and protect users against Internet-borne threats.



Cato Cloud Network

A global, geographically distributed, SLA-backed network of PoPs, interconnected by multiple tier-1 carriers. Enterprises connect to Cato over optimized and secured tunnels using any last mile transport (MPLS, cable, xDSL, 4G/LTE).

Cato Security Services

A fully managed suite of enterprise-grade and agile network security services, directly built into the network. The services have no capacity constraints and are continuously updated to introduce new capabilities and adapt to emerging threats.

From the Creators of Network Security

Shlomo Kramer
Co-Founder and CEO

Gur Shatz
Co-Founder and CTO

Cato Networks was founded by Shlomo Kramer and Gur Shatz. Kramer is one of the founding fathers of network security and one of the leading cybersecurity innovators of our times. He is best known for introducing the first firewall to the market as a co-founder of Check Point Software, and later the first web application firewall as a founder and CEO of Imperva. Shatz has engineered the Imperva SecureSphere platform and built DDoS protection service company, Incapsula.

For more information, visit www.CatoNetworks.com

About the Webtorials® Editorial/Analyst Division

The Webtorials® Editorial/Analyst Division, a joint venture of industry veterans Steven Taylor and Jim Metzler, is devoted to performing in-depth analysis and research in focused areas such as Metro Ethernet and MPLS, as well as in areas that cross the traditional functional boundaries of IT, such as Unified Communications and Application Delivery. The Editorial/Analyst Division's focus is on providing actionable insight through custom research with a forward looking viewpoint. Through reports that examine industry dynamics from both a demand and a supply perspective, the firm educates the marketplace both on emerging trends and the role that IT products, services and processes play in responding to those trends.

Jim Metzler has a broad background in the IT industry. This includes being a software engineer, an engineering manager for high-speed data services for a major network service provider, a product manager for network hardware, a network manager at two Fortune 500 companies, and the principal of a consulting organization. In addition, he has created software tools for designing customer networks for a major network service provider and directed and performed market research at a major industry analyst firm. Jim's current interests include cloud networking and application delivery.

For more information and for additional Webtorials® Editorial/Analyst Division products, please contact Jim Metzler or Steven Taylor.

Published by Webtorials Editorial/Analyst Division
www.Webtorials.com

Division Cofounders:
Jim Metzler
jim@webtorials.com
Steven Taylor
taylor@webtorials.com

Professional Opinions Disclaimer

All information presented and opinions expressed in this publication represent the current opinions of the author(s) based on professional judgment and best available information at the time of the presentation. Consequently, the information is subject to change, and no liability for advice presented is assumed. Ultimate responsibility for choice of appropriate solutions remains with the reader.