The 2017
Guide to WAN Architecture & Design

WAN Evolution

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

Sponsored in part by:

Table of Contents

Executive Summary

The wide area network (WAN) is a critically important topic for number of reasons. Those reasons include:

- The latency, jitter and packet loss that is associated with the WAN often cause the performance of applications to degrade;
- The WAN can be a major source of security vulnerabilities;
- Unlike most of the components of IT, the price/performance of WAN services doesn't obey Moore's Law;
- The outage of a WAN link often causes one or more sites to be offline;
- The lead time to either install a new WAN link or to increase the capacity of an existing WAN link can be quite lengthy.

A discussion of wide area networking is extremely timely for two reasons. One reason is that, for the first time in well over a decade, the wired WAN is the focus of considerable innovation which is leading to the deployment of a wide range of new WAN-related products and services. The second reason is that on a going forward basis, the WAN needs to support a new set of requirements such as providing connectivity to a growing number of mobile workers and public cloud providers as well as to the Internet of Things (IoT).

The primary goals of the 2017 Guide to WAN Architecture and Design (The Guide) are to make enterprise network organizations aware of the emerging alternatives to the traditional approaches to WAN architecture, management and security and to help them understand the key differences in those alternatives. The Guide will be published both in its entirety and in a serial fashion. This document, Part 2, is the second of the serial publications. This document contains the description of a hypothetical company called NeedsToChange and it also contains how Cradlepoint suggests that NeedsToChange should evolve its WAN.

Hypothetical Company: NeedsToChange

Each of the 7 sponsors was given the description of a hypothetical company: NeedsToChange. The goal was to present each sponsor with the description of a company that has a traditional WAN and ask them to provide their insight into how the company should evolve its WAN.

Even within the context of a traditional WAN, there is a wide breadth of options relative to a company's WAN topology, services, applications and goals. As a result of this breadth, it wasn't feasible to cover all possible options in a reasonably sized description of NeedsToChange's WAN. In order to limit the size of the description of NeedsToChange's WAN and yet still bring out a wide array of important WAN options, Cradlepoint was allowed to embellish the description of NeedsToChange's WAN. They could, for example, add additional data centers or key applications; vary the amount of traffic that was backhauled; prioritize the factors impacting NeedToChange's WAN or identify business drivers such as the need to support mergers and acquisitions.

Below is the description of NeedsToChange's WAN that Cradlepoint received.

1. **Data Centers**
   NeedsToChange has a class A data center in Salt Lake City, Utah. The site has two diversely routed T3 links into an MPLS network and a 100 Mbps link to the Internet.

2. **Traffic Prioritization**
   In the current environment, traffic is prioritized in a static manner; e.g., voice traffic always gets top priority and it receives a set amount of bandwidth.

3. **Business Critical Data Applications**
   Two of NeedsToChange's business critical applications are SAP and Product Data Management (PDM). PDM is NeedsToChange's most bandwidth intensive application, however it is widely understood that NeedsToChange runs its business on SAP and so the performance of SAP is critical. In addition to the applications that NeedsToChange uses to run its business, the company uses an Infrastructure as a Service (IaaS) provider for disaster recovery (DR).

4. **Public Cloud Computing Services**
   Other than its use of an IaaS site for DR, NeedsToChange currently makes relatively modest use of public cloud computing services. However, the company has started to implement Office 365 and the decision has been made that on a going forward basis, unless there is a compelling reason not to do it, any new application that the company needs will be acquired from a Software as a Service (SaaS) provider.

5. **Voice and Video**
   NeedsToChange supports a modest but rapidly growing amount of real time IP traffic, including voice, traditional video and telepresence.

6. **Internet Access**
   NeedsToChange currently backhauls over half of its Internet traffic to its data center in Salt Lake City. The company is looking to enable direct Internet access from their branch offices but they are concerned about security. NeedsToChange is also concerned that it is supporting non-business related Internet traffic that is negatively impacting business traffic.

7. **Mobile Workers**
   Roughly half of NeedsToChange's employees regularly work somewhere other than a company facility.

8. **Guest Workers**
   NeedsToChange's network organization is considering offering guest WiFi access from at least some of its facilities.

9. **Branch Offices**
   NeedsToChange categorizes its branch offices into three categories: small, medium and large.
   - A small office/site has between 5 and 25 employees. These sites are connected by an MPLS network with each site having either a single T1 link or multiple T1 links that are bonded. All of its Internet traffic is backhauled.
   - A medium office/site has between 25 and 100 employees. These sites are connected by an MPLS network with each site having capacity between a single T1 link and a link running at 10 Mbps. All of its Internet traffic is backhauled.
   - A large office/site has more than 100 employees. These sites are connected to an MPLS network either by using bonded T1 links or by a T3 link. They also have direct Internet connectivity which in most cases runs at 10 Mbps over DSL.

10. **Branch Office Availability**
    NeedsToChange wants to improve the availability of the WAN access at its branch offices and has established a goal of 99.99% availability.

11. **IoT**
    The company has begun a smart business initiative which the company believes is just the first in a number of initiatives that will quickly drive the need for them to support thousands, if not tens of thousands, of devices.

12. **Visibility**
    In the majority of instances in which the performance of one of NeedsToChange's business critical applications begins to degrade, the degradation is noticed first by the end users. In addition, the time it takes to identify and resolve performance problems has been increasing.

13. **Regulations**
    NeedsToChange is subject to PCI compliance. That is just one factor driving NeedsToChange to seek out ways to increase its security.

14. Factors Driving Change

While not in priority order, the following factors are driving NeedsToChange to seek alternative WAN designs:

- Improve application performance, notably for SAP;
- Reduce cost;
- Increase uptime;
- Reduce the time it takes to identify and remediate performance problems;
- Increase security;
- Reduce complexity;
- Provide access to public cloud computing services in general and Office 365 in particular;
- Provide better support for real time applications;
- Reduce the time it takes to implement new network services;
- Increased agility both in terms of supporting new facilities and in supporting growth within existing facilities

Balancing off the factors driving NeedsToChange to seek alternative WAN designs is the fact that NeedsToChange will not be allowed to increase the size of its network organization.

SD-WAN for People, Places and Things at NeedsToChange Corp.

Introduction

This document outlines Cradlepoint's approach to a new SD-WAN for NeedsToChange Corporation (referred to as NTC). The guiding principle was to meet the NTC's operational, performance, and security requirements while significantly reducing one-time capital costs and recurring operational expense.

Cradlepoint Overview

Cradlepoint is the global leader in software-defined and cloud-delivered network solutions for connecting people, places, and things over wired and wireless broadband. More than 15,000 enterprise and government organizations around the world—including 75 percent of the world's top retailers and 50 percent of the Fortune 100—rely on Cradlepoint to keep critical sites, workforces, vehicles, and devices always connected and protected.

Cradlepoint NetCloud™

Cradlepoint NetCloud™ is a software-defined and cloud-delivered platform that powers and extends a portfolio of LTE-enabled routers with unified management, overlay networking, and virtualized network services. The NetCloud platform consists of the following elements:

NetCloud Manager (formerly Enterprise Cloud Manager) is a single-pane-of-glass cloud management platform that goes beyond ease-of-use to provide the "ease-of-scale" needed to connect hundreds of thousands of people, places, and things distributed around the globe. NetCloud Manager capabilities include:

- Simplified configuration with mass templating
- Zero-touch deployment capability
- Schedulable software and configuration updates
- LTE SIM and carrier management
- End-to-end policy management
- Orchestration and automation
- WAN analytics and health monitoring

NetCloud Engine is a cloud-based Network-as-a-Service that provides a private virtual overlay fabric across the public Internet. Its SDN architecture consists of a distributed data plane that runs on standard virtual machines within public cloud datacenters throughout the world. Each of these data plane entities, called ServicePoints, can host one or more virtual overlay networks, which are called Virtual Cloud Networks (VCNs). The ControlPoint is a collection of micro-services that together comprise the SDN control plane and provide orchestration, oversight, and management of the service. The ControlPoint also gives a VCN its self-organizing, self-optimizing, and self-healing properties.

ServicePoints also enable the integration of virtual network services utilizing Cradlepoint's Network Service Virtualization (NSV) technology. NSV is a distributed, micro-services form of NFV that runs each service function as a discreet process within a VCN's packet path. NSV can also provide a "last-in-chain" egress to external VNFs or cloud services, like firewalls or secure web gateways. A ServicePoint also can act as a Secure Cloud Gateway (SCG) to provide a secure egress point from a VCN to the Internet for connecting to public cloud, SaaS, and the web.

NetCloud Services provides a library of virtual network services based on Cradlepoint and third-party technologies. These services run within the VCN overlay—using NSV—or at the Edge on **NetCloud OS**, the Linux-based open network operating system that powers Cradlepoint routers. The following is a summary of available NetCloud Services:

- Carrier-grade NAT
- PKI-as-a-Service
- Overlay DNS with Active Directory integration
- Distributed next-gen firewall
- Micro-segmentation at the user, app, or device level
- Threat management with IPS/IDS
- App control—1,500+ business and SaaS apps
- URL/content filtering
- Network Access Control (NAC)

NetCloud Client and **NetCloud Gateway** provide an on-ramp to VCN overlays for standalone and router-attached resources, including PC, mobile, and IoT devices. NetCloud Client provides LAN over WAN services for seamlessly connecting mobile users and devices anywhere to private and public cloud applications and resources. It supports Windows, Mac, Linux, Android, and iOS operating systems. NetCloud Gateway provides the same functionality within Cradlepoint routers for IP-attached users and devices.

Cradlepoint Routers

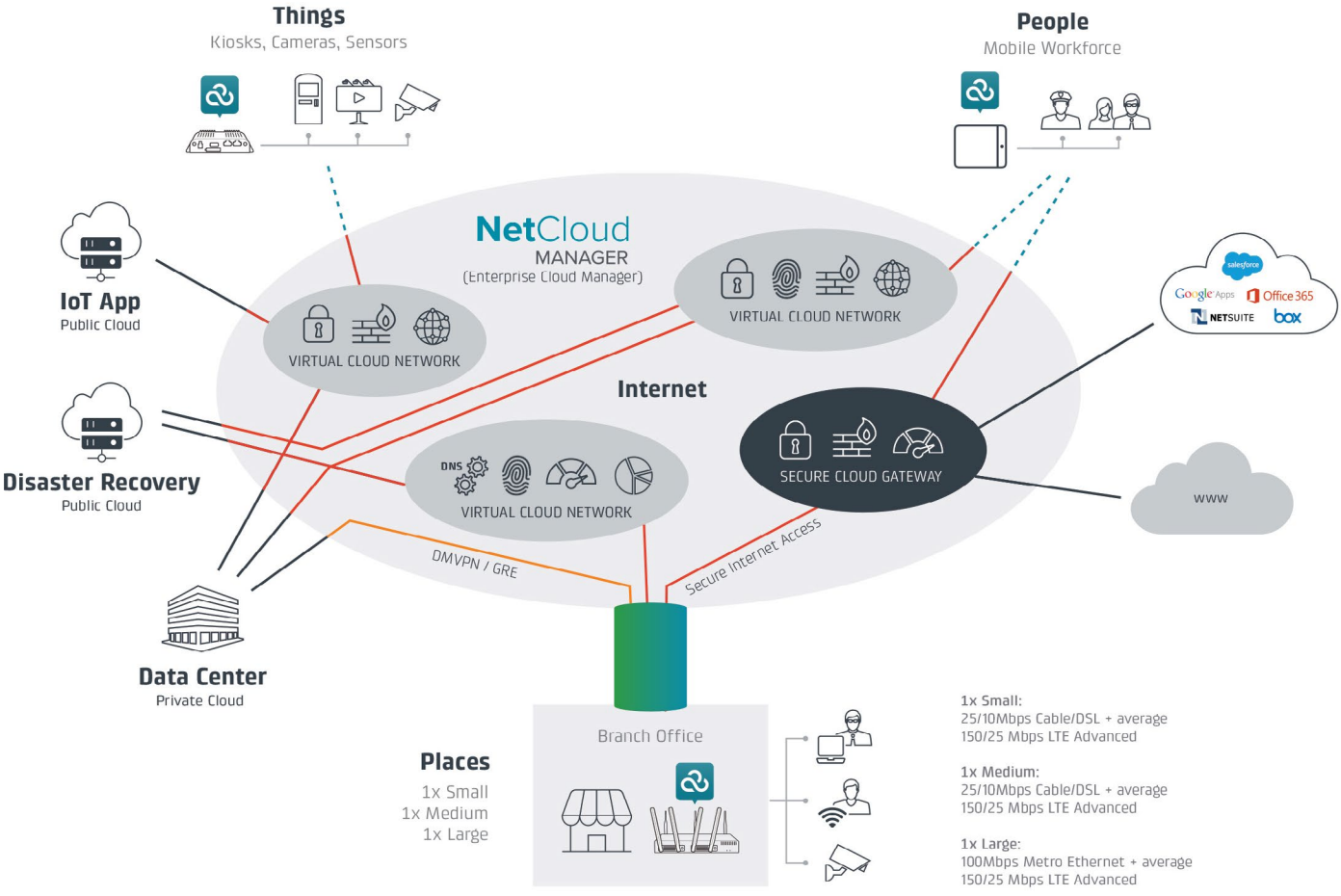
Cradlepoint offers an extensive portfolio of purpose-built, LTE-enabled routers for branch, in-vehicle, and IoT applications. For the NTC network, Cradlepoint has deployed the AER Series of converged, multi-WAN Edge routers and COR Series of IoT routers.

Cradlepoint SD-WAN Solution

BRANCH OFFICE WAN

For NTC's three branch offices, the Cradlepoint AER Series Advanced Edge Routers provide an "all-in-one" solution for WAN, LAN, guest WiFi, and IoT connectivity. The high-end AER3100 routers used in the NTC network cost less than $2,000 each and includes:

- Multi-WAN – MPLS, MetroE, Cable/DSL, WiFi, and LTE
- 12 Ethernet ports including four ports with PoE support
- 802.11ac WiFi – 3x3 MIMO, dual-band concurrent
- Up to two integrated 4G LTE modems, each with dual SIMs



Replace MPLS with Broadband: Cradlepoint has replaced NTC's MPLS network with a hybrid WAN consisting of pooled wired and wireless broadband connections supporting both primary and failover requirements. The price for MPLS copper connections can range from $300 to $600 per Mbps/month, while business-class wired broadband access (cable or DSL) is typically less than $5 per Mbps/month—a savings of more than 90 percent. Given the price/performance advantage, a 25Mbps downstream and 10Mbps upstream wired broadband link is used for the small and medium NTC branches at $99/month a site. For the Large NTC branch, which has more than 100 users, a 100Mbps Metro Ethernet connection is used at a cost of $10 per Mbps/month.

LTE for Primary and Failover WAN: In addition to wired broadband, Cradlepoint has deployed Advanced 4G LTE as part of the hybrid WAN connection pool for both primary and failover uses. Cradlepoint's support of LTE Category 6 enables up to 300Mbps download and 50Mbps upload throughput speeds on networks such as Verizon's Advanced LTE. However, real-word speeds likely average 150/25Mbps.

Virtual Overlay Networks: Cradlepoint's SD-WAN capabilities include several forms of virtual overlay networks. For NTC's network, corporate intranet traffic flowing from the branch to the private cloud datacenter uses a DMVPN/GRE overlay. Internet-bound traffic headed to public cloud, SaaS applications, and the web utilizes a VCN overlay. While both overlay methods support point-to-point and meshed topologies, VCN has the added value of integrated DNS, LAN emulation, and AD integration.

Intelligent WAN Selection and Steering: Cradlepoint routers provide several policy-based traffic management and steering mechanisms that enable Quality of Service (QoS) and intelligent selection across both the wired and wireless broadband links that comprise the branch hybrid WAN connection pool. Using the mechanisms summarized below, specific QoS and traffic steering polices have been set to ensure the performance of NTC's business-critical SAP and PDM applications, control VoIP latency, and shape video traffic to avoid saturating links or over-consuming LTE data plans.

Intelligent WAN Selection & Steering: Cradlepoint provides several policy-based traffic management and steering mechanisms that enable quality of service (QoS) and intelligent selection across both the wired and wireless broadband links that compose a hybrid WAN connection pool.

- Policy-based QoS: App-enabled prioritization, bandwidth allocation, and traffic shaping for traffic traversing the router in each direction.
- WAN Diversity™: Ability to combine multiple wired and wireless WAN links into a hybrid WAN connection pool in primary and failover roles.
- WAN Affinity™: Traffic steering policies that control WAN link selection based on specific algorithms, including round-robin, load balancing, most available bandwidth, and LTE data usage.
- Intelligent LTE Failover: Complete policy control over the apps and traffic allowed to utilize the LTE link if one or more primary links fail.
- Data Plan Protection: Analytics-driven policies that automatically suspend or reduce LTE usage within the hybrid WAN connection pool as monthly data plan consumption reaches a set threshold.

High Availability: AER Series routers are configured with two LTE modems, each with dual SIM cards. This allows each router to be "dual-homed" on multiple LTE carriers in either redundant carrier (dual SIM) or concurrent carrier (dual modem) mode. With this approach, NTC can achieve 99.99% availability of its branch WAN. For the utmost in high availability and fault tolerance, NTC can deploy routers in tandem using VRRP to enable full hardware, WAN, and LTE carrier redundancy.

Guest WiFi: AER Series routers support advanced WiFi capabilities to enable secure guest access at each branch location. Guest network users can be micro-segmented from WiFi-to-WAN to isolate them from trusted branch networks. Moreover, the intelligent WAN selection and steering polices have been configured to ensure guest traffic does not interfere with business users and applications and does not utilize the LTE links. For added security and compliance, guest traffic also uses Secure Internet Access as described below.

Secure Internet Access: The new Cradlepoint SD-WAN achieves significant bandwidth savings for NTC by implementing Secure Internet Access (SIA) for branch employees and guest WiFi users. This direct access approach eliminates the backhauling of Internet traffic and avoids the cost and complexity of installing branch-based security appliances. Within each Edge router, the NetCloud Gateway provides an encrypted overlay to the nearest ServicePoint where traffic is securely routed through the NetCloud Engine SCG service to the Internet. NTC network admins can use NetCloud Manager to set the desired app, users, and device security policies, which in turn will automatically provision the appropriate virtual network services to be used for SIA traffic such as next-gen firewall (refer to NetCloud Services above for a listing of other available security functions).

Secure SaaS Access: SIA also provides branch employees with secure SaaS access from any device, including tablets and phones. NTC network admins can set user and device policies to allow or block the use of specific SaaS and web applications, such as Salesforce.com, Microsoft Office 365, or DropBox. For example, NTC may choose to allow access to all SaaS apps from any corporate-owned device but restrict access to only Salesforce.com for users of BYOD devices, like an Android tablet.

Public Cloud DR: The enclosed diagram illustrates how branch-level disaster recovery (DR) is provided using the NetCloud Engine service. At each branch, a separate disaster recovery VCN provides always-on connectivity to the public cloud DR site. In the event of a primary datacenter outage, or even loss of a single application or data store, the AER router can steer affected traffic over the DR-designated VCN.

MOBILE WORKFORCE WAN

Cradlepoint NetCloud extends the SD-WAN value proposition to NTC's mobile workforce, giving employees a secure, LAN-like connection to private and public cloud apps and files from anywhere and any device. As shown in the enclosed diagram, the NetCloud Client runs on each device and provides a persistent encrypted connection to a VCN overlay set up specifically for mobile access.

To address the security concerns around BYOD and public WiFi access, the mobile access VCN has been configured with NetCloud Services that provide NAC, micro-segmentation, next-gen firewall, and app control so that devices are isolated from one another and access is only granted to specific servers and applications at the datacenter and public cloud DR site. Mobile employees also are configured for SIA to provide secure and compliant access to SaaS applications and the web.

IoT WAN

Cradlepoint NetCloud and routers are optimized for IoT deployments in the field or within a branch. The ruggedized COR Series IoT router can support NTC's future field IoT deployments, such as kiosks, vehicles, digital signage, and surveillance cameras. It supports WiFi (for LAN or WAN), Ethernet and 4G LTE interfaces, DMVPN/GRE and VCN overlays, and the full suite of NetCloud Services. Within the branch, the AER3100 router with integral PoE can connect, protect, and power IoT devices such as cameras and sensors.

SINGLE-PANE-OF-GLASS MANAGEMENT

NetCloud Manager enables zero-touch branch and field deployments of AER Series and COR Series routers and utilizes a proprietary Stream management protocol that's 700 times more WAN-efficient than SNMP. Stream allows fine-grain management and control of routers, WAN interfaces, LTE carriers, and policies without the overhead of traditional management approaches, which can consume up to 30 percent of bandwidth.

Summary

With more than 15,000 customer deployments in some of the world's most demanding enterprise and IoT networks, and recognized leadership in 4G LTE solutions, Cradlepoint brings a unique pedigree to the SD-WAN market.

Cradlepoint NetCloud and router platforms provide a versatile SD-WAN solution that utilizes a single virtual overlay fabric to connect people, places and things, with advanced security and single-pane-of-glass management. For NTC, this all translates to a new software-defined and cloud-delivered WAN that makes its network more agile, secure, efficient, and extensible than ever before.

TO LEARN MORE, VISIT **CRADLEPOINT.COM**.

cradlepoint

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

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.

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

For editorial and sponsorship information, contact Jim Metzler or Steven Taylor. The Webtorials Editorial/Analyst Division is an analyst and consulting joint venture of Steven Taylor and Jim Metzler.