Not all SD-WANs are created equal

PERFORMANCE MATTERS

While most SD-WAN offerings improve network agility and reduce WAN costs, Aruba enables enterprises to build a modern WAN that drives maximum value from cloud and digital transformation initiatives with a self-driving network that learns and adapts to the needs of the business.

THE ARUBA EDGECONNECT ENTERPRISE SD-WAN PLATFORM INCREASES PRODUCTIVITY AND LOWERS COSTS

As applications increasingly migrate from the corporate data center into the cloud, IT and business leaders are quickly realizing that traditional WANs were never architected for such a dynamic, internet-based environment. It is clear that backhauling traffic destined to the cloud from the branch to headquarters to the internet and then back again to the branch, negatively impacts application performance and user experience.

By building a modern WAN with Aruba, enterprises have the potential to increase end-user satisfaction and business productivity through improved application performance, higher reliability, enhanced quality of service (QoS), increased security and improved visibility and control of applications running in their networks, regardless of the WAN connectivity service.

Ensuring continuous operations and high levels of application performance is a challenging and often time-consuming task for IT. Adding broadband and 4G/5G/LTE connections and cloud-based SaaS and IaaS applications to the mix only makes the job even more difficult. Aruba improves the quality of experience for IT by enabling an SD-WAN that provides consistent, reliable application performance through features such as path conditioning, tunnel bonding, traffic shaping, WAN optimization and intelligent cloud breakout.

Moreover, different applications have diverse QoS and end-user experience requirements. For example, voice and video traffic require zero packet loss and extremely low delay while file transfers need large amounts of bandwidth but can tolerate higher levels of delay. Aruba enables network managers to define business intent overlays — virtual WAN

Business-Driven	Highest Quality of Experience
Continuous Adaptation	Unified Platform

overlays — that reflect application QoS requirements relevant to the business. Aruba EdgeConnect Enterprise maps applications to the appropriate business intent overlay, enabling the SD-WAN to optimize traffic handling decisions automatically. Aruba EdgeConnect Enterprise continuously monitors WAN link performance, factoring real-time data about delay, jitter, and packet loss to adapt and make intelligent real-time traffic steering decisions. Aruba EdgeConnect Enterprise continuously learns and adapts to optimize and dynamically change paths if necessary, to ensure no application disruption and peak performance at all times. Aruba EdgeConnect Enterprise application performance features include:

- Path conditioning
- Dynamic path control
- Tunnel bonding
- Adaptive internet breakout
- Daily application updates
- Intelligent internet breakout
- Microsoft O365 REST API integration

These Aruba advanced performance features make Aruba EdgeConnect Enterprise stand out from other SD-WAN solutions in the market.

ADDING BROADBAND TO THE WAN

Over the past two decades, MPLS has been the transport of choice for connecting branch offices, field locations and other business sites located remotely from headquarters or data centers. MPLS services provide secure, reliable WAN connectivity, however, MPLS is expensive, complex and time-consuming to provision with long lead times from service providers.

Application migration from the corporate data center to the cloud continues to accelerate, and this is driving enterprises to re-evaluate networking requirements, including actively using broadband services to connect users in branch offices to cloud-based applications. Using the internet for branch office WAN connectivity is a logical next step, but internet connections are often unreliable, delivering unpredictable application performance and notoriously lack security.

An advanced SD-WAN can overcome these limitations. By establishing secure encrypted connections, SD-WANs remove the security concern of connecting users to business applications across the internet. It lets network managers confidently integrate commodity internet links into their WANs in addition to, or even instead of, leased line services, increasing bandwidth and potentially lowering costs. Adding broadband also allows for rapid WAN connectivity provisioning for new or temporary business locations and enables IT to add capacity at remote offices at the lowest cost to accommodate growth.

BASIC SD-WAN TABLE STAKES

Today, there are several fundamentals that nearly every SD-WAN provides. Consider these to be basic SD-WAN table stakes. First is the ability to **use any and all sources of connectivity** including broadband internet, MPLS, and 4G/5G/LTE wireless. Any SD-WAN should be able to abstract these connections and add them to the pool of available SD-WAN paths.

Second is the ability to intelligently and **dynamically direct application traffic** over the available connections. Path selection decisions should be based on the performance requirements of the application in choosing the optimal path across the WAN. This is especially true for cloud-based applications and if the organization has more than one data center.

Third is **centralized orchestration** where configuration and administration of the SD-WAN is tuned and optimized from a single location. IT programs initial configurations and subsequent configuration changes centrally and automatically "pushes" them to every site across the SD-WAN.

Finally, **zero-touch provisioning** (ZTP) allows network managers to easily add new sites by installing new SD-WAN appliances. Users simply plug in a physical appliance or bring up a virtual appliance and connect it to the WAN service(s).

The new appliance "phones home" to the centralized orchestrator to receive configuration information and join the SD-WAN without requiring specialized IT expertise at the branch office. Centralized orchestration and ZTP significantly reduces IT operational costs and more importantly, reduces configuration errors.

Basic SD-WAN table stakes	Aruba advanced SD-WAN performance innovations
Dynamic path selection	Path Conditioning
Sub-optimal performance of all aggregated underlying links	Tunnel Bonding
Static active/standby configuration	Dynamic Path Control
Basic Deep packet inspection (DPI) and port level approaches	First-packet iQ application classification
Irregular application updates	Cloud Intelligence
Rudimentary operational efficiency with increased latency	Microsoft O365 REST API integration
Inability to use the best available internet link in real-time	Intelligent internet breakout

PERFORMANCE MATTERS: DELIVERING EVEN MORE WAN VALUE

Several key innovations of the Aruba EdgeConnect Enterprise SD-WAN platform enable IT to deliver predictable end-user experiences across the business, optimize performance of cloud-based applications and save money at the same time. While basic SD-WAN offerings provide more WAN connectivity options and the potential to lower WAN costs, they do not mitigate the application performance impacts of latency nor do they increase bandwidth efficiency

Aruba EdgeConnect Enterprise technologies deliver the highest levels of application performance, QoS and enable application SLAs over any combination of transport services including consumer broadband and LTE.

- Path conditioning to overcome the adverse effects of packet loss and out-of-order packets
- Tunnel bonding to support packet-based load sharing and higher application availability
- Traffic shaping to ensure low-priority traffic does not override higher priority traffic
- Optional WAN optimization features, fully integrated as a single solution

Path Conditioning: One challenge that an SD-WAN can address is how to best use higher bandwidth internet connections that are as little as one-tenth of the cost of private line services. In general, internet (and also wireless) connections are not as reliable as private — but costly — services like MPLS. Internet and wireless links often suffer from packet loss and jitter and are more likely to experience outages. Aruba forward error correction (FEC) reconstructs lost packets which avoids TCP re-transmissions, substantially increasing the effective performance of broadband links. The ratio of FEC packets to data packets dynamically adapts depending upon the business-criticality and real-time requirements of the application. Packet order correction (POC) algorithms re-order packets that arrive out of order at their destination. This is a fairly common occurrence when load balancing across different service providers' networks. With FEC and POC, Aruba EdgeConnect Enterprise can make internet connections perform as well as or better than private lines.

Tunnel Bonding: Tunnel bonding provides several benefits including optimizing the SD-WAN for availability, throughput and efficiency. Bonded tunnels may be configured from two or more physical WAN links to form a single logical

Figure 1: Aruba forward error correction (FEC) reconstructs any packets lost in transit across the WAN without having to retransmit them. Aruba EdgeConnect Enterprise dynamically and adaptively adjusts the ratio of FEC packets transmitted in response to changing link conditions to minimize overhead.
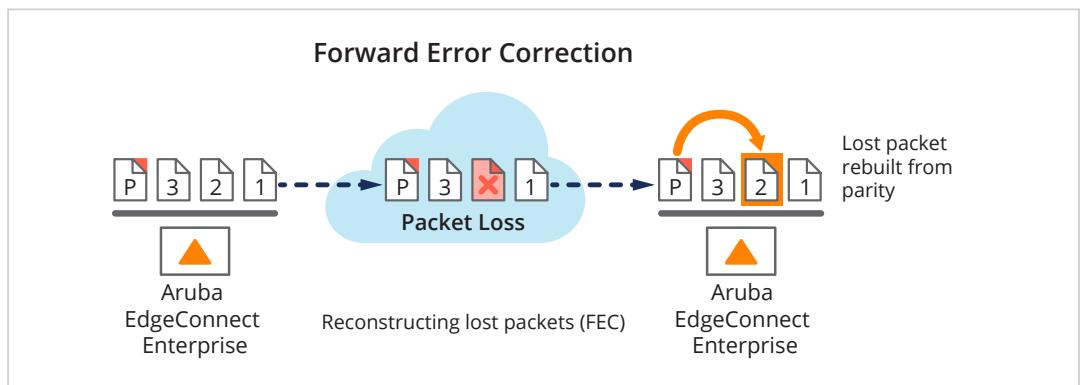

Forward Error Correction

Packet Loss

Reconstructing lost packets (FEC)

Aruba EdgeConnect Enterprise

Lost packet rebuilt from parity

Figure 2: Aruba EdgeConnect Enterprise packet order correction (POC) re-sequences packets delivered out-of-order across the WAN.

Packet Order Correction

Packet Loss

Reordering any out-of-sequence packets (POC)

Aruba EdgeConnect Enterprise
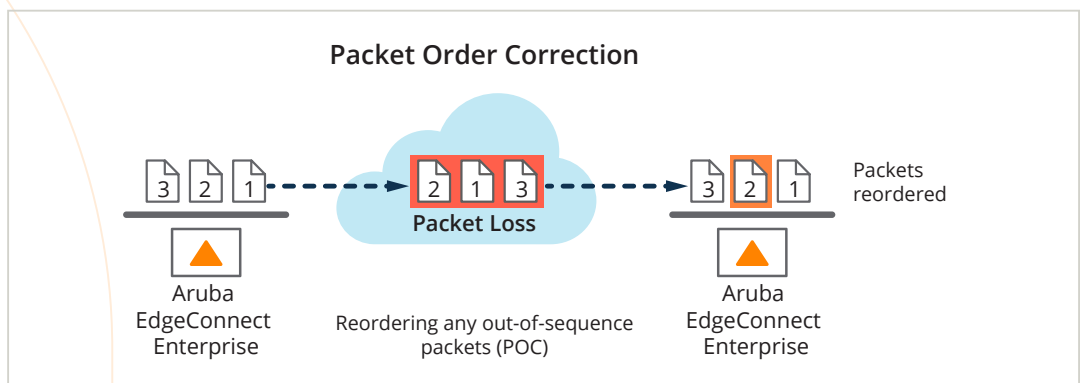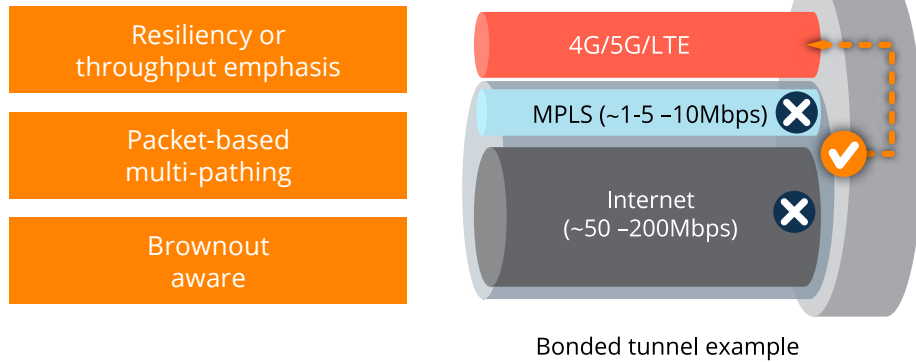
Packets reordered

Figure 3: A bonded tunnel configured with an MPLS service plus an internet service delivers higher performance and higher availability than either single WAN service alone.

| Resiliency or throughput emphasis |
| Packet-based multi-pathing |
| Brownout aware |

4G/5G/LTE

MPLS (~1-5 –10Mbps) ✗

✓

Internet (~50 –200Mbps) ✗

Bonded tunnel example

overlay connection. As an example, bonded tunnels can be configured with two MPLS connections to create a primary bonded tunnel. One MPLS connection might be serviced by AT&T and the other by Verizon.

In another scenario, a single tunnel (logical connection) can be configured with an MPLS link and an internet link, even if the speeds of these services are not the same. Depending upon application requirements that are mapped into a virtual WAN overlay policy (business intent overlay), Aruba EdgeConnect Enterprise can load share traffic across both physical links or can map data traffic to one and FEC packets to the other. If one link were to fail, the remaining link would continue to carry all the traffic including FEC packets to keep the connection active and the application alive, avoiding any interruption or data loss.

Traffic Shaping: Aruba EdgeConnect Enterprise performs both egress and ingress traffic shaping. IT can program minimum and maximum bandwidth limits on the egress traffic shaping engine per traffic class to ensure no single application consumes all of the WAN bandwidth. Ingress shaping can be programmed to ensure that low-priority traffic does not override higher priority traffic. An example is to prevent video streaming or social media applications from compromising the performance of higher-priority business applications.

WAN Optimization: Aruba takes SD-WAN performance even further for latency-sensitive applications or applications where large amounts of data must be transferred across the WAN. With the optional Aruba Boost software performance pack, Aruba EdgeConnect Enterprise integrates Aruba's field-proven WAN optimization features in a single SD-WAN solution.

Overlay	Application	Virtual Topology	WAN Path	SLA	Path Conditioning	QoS	Security Policy	Boost
Real-Time	Cisco webex	Mesh	MPLS / Broadband / 4G LTE	1% Loss 150ms Jitter 300ms Latency	High Availability	Real Time	Trust	○
Credit Card Processing	VISA mastercard DISCOVER Square	Hub & Spoke	MPLS / Broadband	2% Loss 200ms Jitter 500ms Latency	High Throughput	Real Time	Trust	●
Enterprise Web Apps	Office 365 salesforce SAP workday	Local Internet Breakout	Broadband / MPLS / 4G LTE	None	High Efficiency	Best Effort	Stateful Firewall	○
Guest WiFi	WiFi	Local Internet Breakout	Broadband **Drop**	None	High Efficiency	Best Effort	Send to SWG	○

Figure 4: Business intent overlays abstract applications from WAN transport services to deliver application priority, performance and availability based on business requirements.
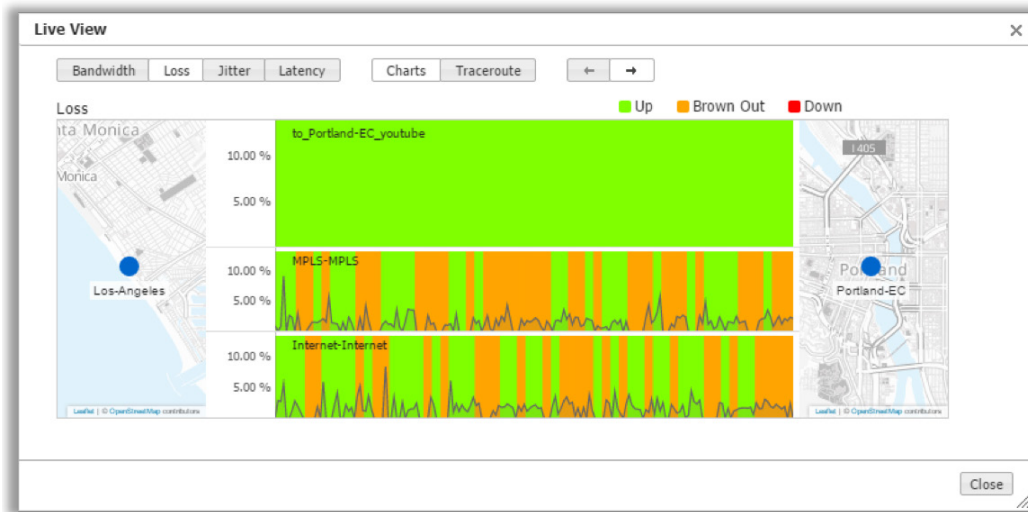
Figure 5: Aruba Live View image displays the benefits of tunnel bonding and FEC in real-time. In the example shown, both MPLS and internet connections experience packet loss (orange areas) however, the virtual WAN overlay delivers an uninterrupted video stream.

TCP/IP applications such as transaction processing or data backup use a sliding data window and require handshaking or acknowledgements between end points before more data can be sent. No matter how much WAN bandwidth is available, latency caused by distance is a physical reality — the distance between San Francisco and London doesn't change whether there is one megabit or 10 gigabits per second of WAN bandwidth. TCP acceleration shortcuts the handshaking, resulting in faster application response times, ultimately improving user and business productivity.

Data deduplication and data compression techniques minimize repetitive transmission of data across the WAN. This allows IT to complete backups within their allotted time window or recover from data loss rapidly. Combined, TCP acceleration and data management technologies further improve application performance and WAN efficiency, enabling IT to maximize the return on their WAN investments.
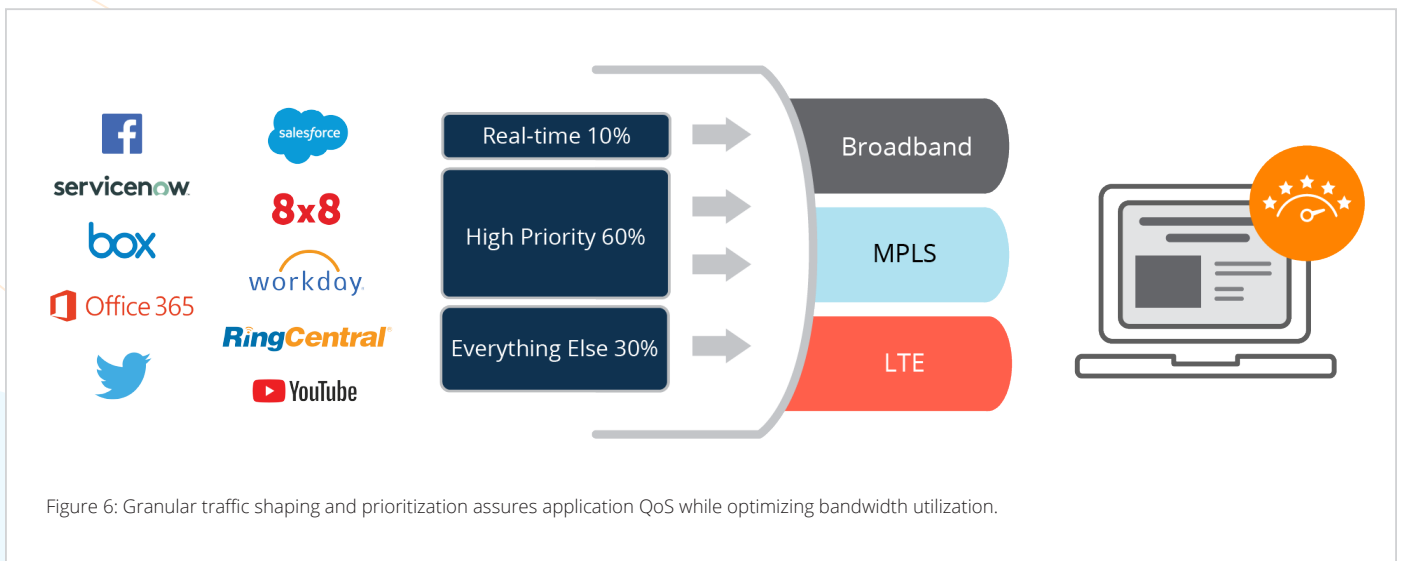

Figure 6: Granular traffic shaping and prioritization assures application QoS while optimizing bandwidth utilization.

INTELLIGENT CLOUD BREAKOUT

Most UCaaS providers (e.g. RingCentral and 8x8) and many SaaS application providers like Dropbox, Box, Salesforce, Slack, Skype for Business and G Suite have deployed high-speed backbone connections with massive bandwidth between their data centers and leading IaaS platforms such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). With Aruba, customers can deploy Aruba EdgeConnect Enterprise virtual (EC-V) appliances in their IaaS instances. Connections between branch locations and the cloud benefit from Aruba performance features including tunnel bonding, path conditioning and optional Aruba Boost WAN Optimization. This "ruggedizes" the first mile between the branch and the cloud, providing improved network quality as well as application performance and availability.

In the example shown in Figure 7, two broadband connections provisioned at the branch transport application traffic; although the branch could also be served by 4G/5G/LTE, or MPLS connections. The WAN connections can be configured to form bonded tunnels supporting the aggregate bandwidth of all provisioned WAN links for the highest performance. Aruba EdgeConnect Enterprise continuously monitors the throughput, packet loss, latency, jitter and mean-opinion-score (MOS) across all transport services and automatically adapts if performance falls below pre-defined thresholds. If a brownout or complete outage occurs, the remaining link(s) continue to carry traffic such that users don't notice any disruption to voice calls, video conferences or any other application. The performance, quality and reliability of UCaaS and other SaaS application traffic between the branch office and the IaaS platform benefit from the advanced Aruba EdgeConnect Enterprise SD-WAN features such as tunnel bonding, path conditioning, load balancing, dynamic path control and sub-second failover.

Aruba not only improves the performance and reliability of traffic across the "first mile" from the branch office to the IaaS platform, but it also provides an opportunity to leverage local high-speed backbone connections over the "last mile" to the UCaaS or SaaS provider.

DYNAMIC PATH CONTROL

Aruba EdgeConnect Enterprise performs real-time traffic steering over WAN links such as MPLS, internet and LTE or any combination of the WAN links based on company-defined policies based upon business intent. In the event
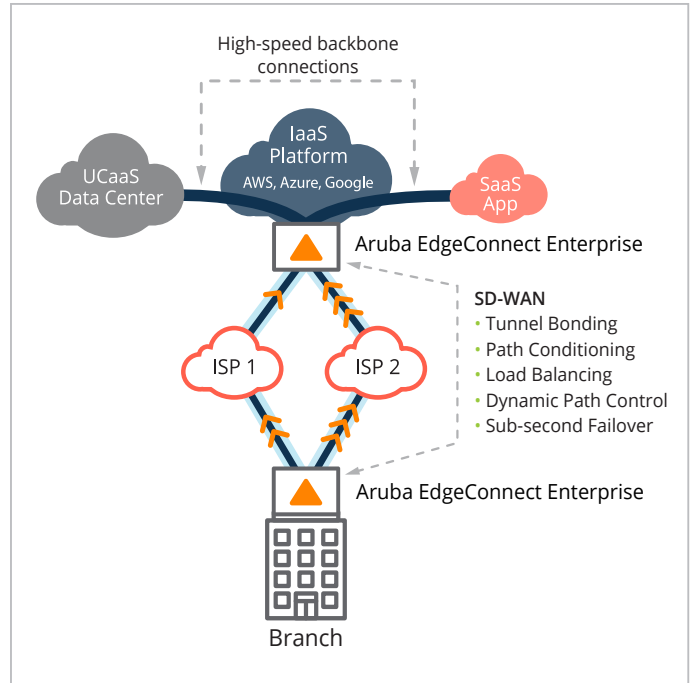

Figure 7: Aruba EdgeConnect Enterprise SD-WAN appliances deployed branch locations and in public clouds improve the performance and reliability of traffic across the "first mile" between the branch and the IaaS platform. High-speed backbone connections in the cloud improve network quality and performance over the "last mile" between the IaaS platform and SaaS infrastructure.

of an outage or brownout, Aruba EdgeConnect Enterprise automatically continues to carry traffic on the remaining WAN links or switches over to a secondary link so that application performance does not degrade or experience any disruption. Dynamic path control (DPC) enables organizations to fully utilize all deployed bandwidth at each location. DPC eliminates the active/standby configuration of WAN services, improving the reliability and performance for enterprise applications.

As shown in Figure 8, enterprises can create business-driven policies that result in more intelligent decisions about how the WAN links are used to deliver applications to users. For example, IT can create policies that would steer an organization's most critical traffic, such as VoIP, video conferencing and ERP traffic to always use the MPLS network, while load balancing the rest of the traffic across all available links. The provisioning of traffic across multiple WAN links can be configured as granularly as business needs dictate. Simple deployments can be as straightforward as a configuring single policy, while more advanced deployments might be configured to direct traffic from different classes of applications based on specific metrics that work best for each application type. For example, IT could configure a policy to steer VoIP traffic over the link with the least amount of packet loss and lowest latency at any given time, and a

Figure 8: This example shows a branch office with dual WAN links deployed with an MPLS service defined as the primary and an internet service configured as a secondary. Critical enterprise applications are being routed via MPLS link and cloud-based applications are being load balanced between Internet and MPLS links.
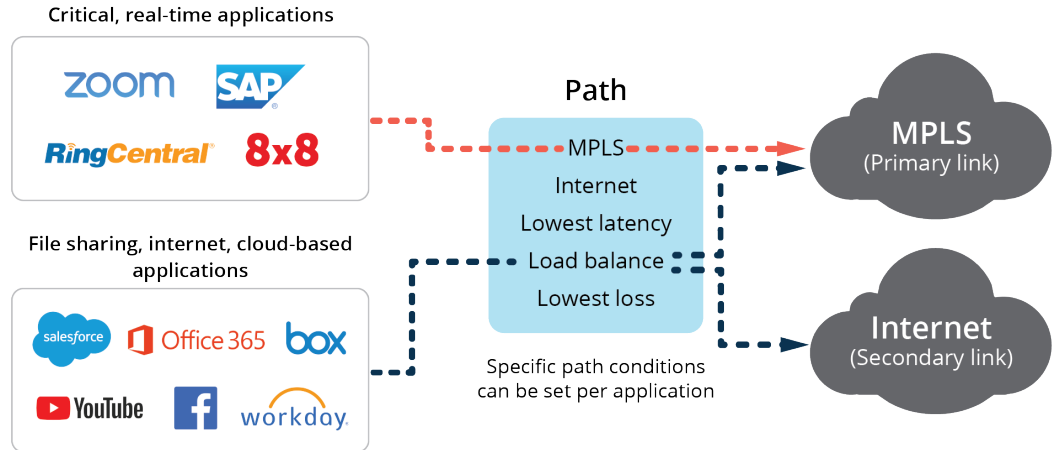
second policy that directs storage replication traffic across the link (or bonded tunnel) delivering the highest throughput capacity.

ADAPTIVE INTERNET BREAKOUT

With the increasing use of cloud-based SaaS applications and IaaS, secure direct-to-internet traffic steering from the branch delivers the highest application performance to end users and minimizes wasted bandwidth resulting from backhauling traffic to the data center. However, first-packet application classification is essential to automatically steer trusted SaaS and web traffic directly to the internet for the highest performance, while directing unknown or suspicious traffic to a regional hub or data center firewall or a cloud-hosted security service for further security inspection.

Cloud-hosted security services such as those available from Zscaler, Netskope or Check Point coupled with the application-aware, business-driven Aruba EdgeConnect

Enterprise platform streamlines WAN edge infrastructure at the branch. Enterprises no longer need to deploy expensive, complex-to-manage next-generation firewalls at every branch location. Aruba First-packet iQ application identification enables intelligent, granular traffic steering on the first packet (Figure 9). This enables granular security policy enforcement based on business requirements, securing the organization while delivering the highest performance for all applications. For example, business-driven security policies might include:

1. Send enterprise data center-hosted application traffic directly to headquarters
2. Send only Office 365 and UCaaS traffic directly to providers' cloud services
3. Send all other internet-bound traffic, including Salesforce, Facebook, YouTube, Box and web browsing traffic to a Zscaler cloud point of presence (PoP) for security inspection prior to handing off to providers' cloud or web services

First-Packet iQ enables application visibility and control
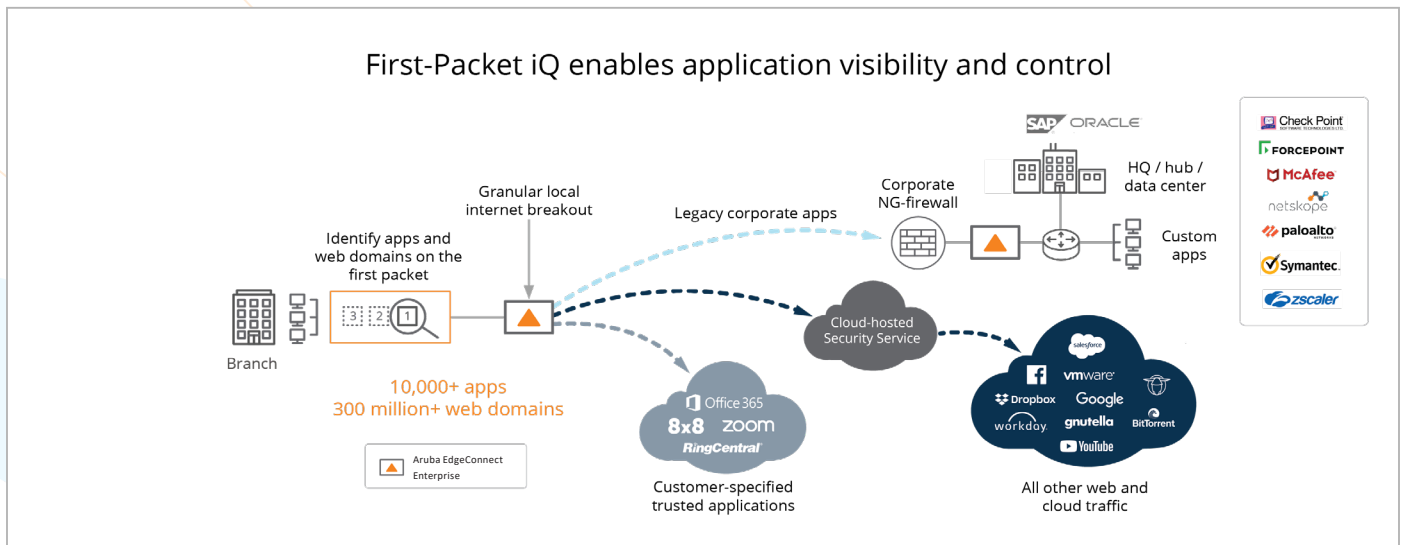
DAILY APPLICATION UPDATES

Many SaaS applications such as Office365, Salesforce, Workday, Box, Dropbox, and others employ hundreds or even thousands of IP addresses to support their huge number of users. These IP addresses are not static; they may be re-allocated to a different region or to a different application. New addresses are added frequently to keep up with end user demand. Some SD-WAN solutions claim to steer applications on the first packet, and they can accomplish this using ACLs. However, ACLs are static and must be manually programmed. A security policy may work properly when initially configured but fail days or weeks later after SaaS application IP addresses change. Manual re-programming of IP addresses into ACLs simply cannot stay current with the dynamic nature of SaaS applications. Aruba Cloud Intelligence maintains a centralized application database or "map of the internet" that is continuously updated on a daily basis. This includes the application definitions and address tables for more than 10,000 applications and 300 million web domains. Aruba EdgeConnect Enterprise receives automated daily updates of the application IP address database to remain current with the changing SaaS and web IP addresses eliminating the need to program any static ACLs.

MICROSOFT OFFICE 365 REST API INTEGRATION

Enterprise customers can deliver unprecedented Office 365 application performance with Aruba EdgeConnect Enterprise. With First-packet iQ application classification and automated integration with the new Microsoft Office 365 REST API, Aruba EdgeConnect Enterprise enables adaptive internet breakout directly from the branch office to the closest Office 365 entry point using the latest Office 365 endpoint data. Office 365 endpoint data is a global list of IP addresses and fully qualified domain names (FQDN) that is continuously updated and made available on a regular basis through the Office 365 REST API. With Office 365 REST API integration, Aruba continuously learns and discovers new Office 365 end points and/or IP addresses and automatically re-configures Aruba EdgeConnect Enterprise if a new, closer Office 365 end point becomes available. By doing so, users always achieve optimal Office 365 connectivity and performance by reducing the round-trip time (RTT).
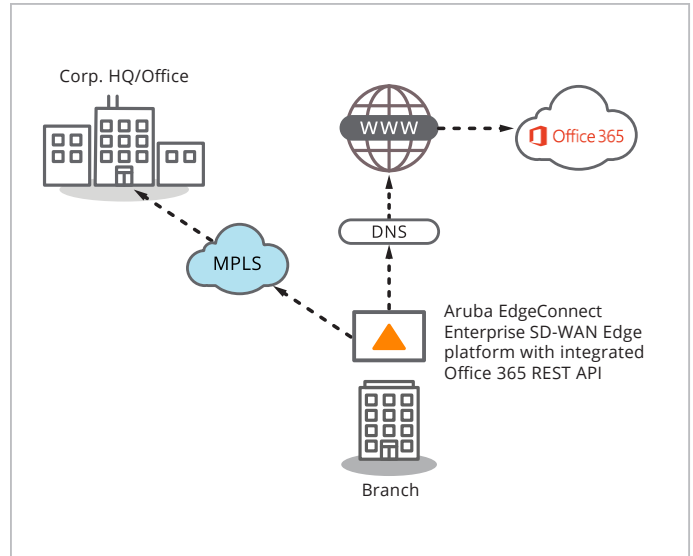

Figure 10: EdgeConnect Enterprise enables secure internet breakout directly from the branch office to the closest Office 365 entry point using the latest Office 365 endpoint data.

The Aruba EdgeConnect Enterprise SD-WAN edge platform has been independently tested and certified to support the Microsoft Office 365 Connectivity Principles and provide reliable connections directly from branch office locations to the nearest Office 365 entry point (see Figure 10). As a result of the independent testing, the Aruba EdgeConnect Enterprise platform has been inducted into the Microsoft Office 365 Networking Partner Program and has been given the official "Works with Office 365" designation.

INTELLIGENT INTERNET BREAKOUT

Often customers provision two or more WAN links from remote branch sites to increase network and application availability and performance. These links are used for breaking out traffic locally at each branch. Using the internet as an underlay transport is less expensive than private leased line connections such as MPLS since it offers much higher bandwidth at a given price point. To optimize utilization of the provisioned WAN internet links and to optimize SaaS application performance, Aruba EdgeConnect Enterprise monitors the performance of all links by continuously measuring the packet loss, jitter, latency and

mean opinion score (MOS) in real-time. Aruba EdgeConnect Enterprise uses statistical learning based on jitter, latency, loss and MOS on all provisioned internet links to dynamically determine which link is performing the best before sending traffic. This optimizes internet break out traffic to deliver the highest SaaS and cloud application performance (see Figure 11). Configuring these policies is fully automated within Aruba Orchestrator and doesn't require any manual configuration. Aruba Orchestrator also enables configuration of an automated policy for finding the best path for that traffic over the SD-WAN fabric, across MPLS or another WAN service, in the rare case that both underlying internet links are underperforming or are unavailable (see Figure 12).

THE ARUBA ADVANTAGE

As adoption accelerates, the cost savings realized from an SD-WAN become obvious. However, customers now realize that performance matters, and not all SD-WANs are created equal. Only Aruba delivers total performance and enables application SLAs at any scale using any combination of transport services. The suite of Aruba EdgeConnect Enterprise performance features enable businesses to achieve consistent application performance even through transport interruptions and brownouts. Aruba enables enterprises to build a modern WAN that drives maximum value from cloud and digital transformation initiatives with a self-driving network that learns and adapts to the needs of the business.
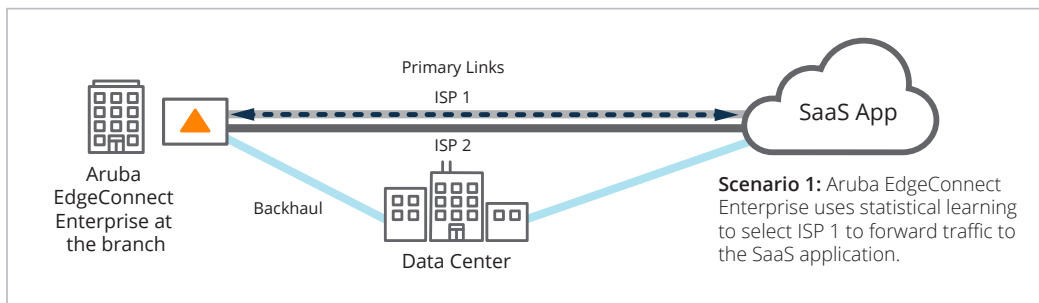

Figure 11: To optimize utilization of the provisioned WAN internet links (ISP 1 and ISP 2), Aruba EdgeConnect Enterprise monitors the performance of the two links by continuously measuring the packet loss, jitter, latency and mean opinion score (MOS) in real-time. In this example, based on statistical learning, Aruba EdgeConnect Enterprise dynamically selects ISP 1 to send traffic to the SaaS application since it is performing better than the ISP 2 service.
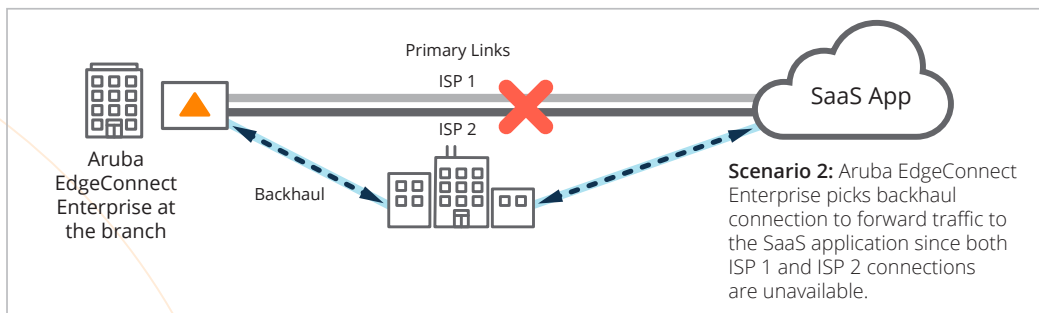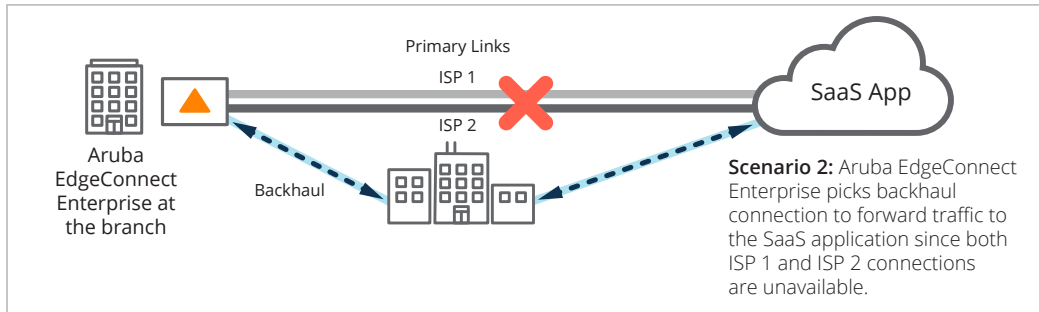

Figure 12: If both ISP 1 and ISP 2 connections become unavailable, EdgeConnect Enterprise automatically moves application traffic to the transport service configured as a backup that backhauls traffic through the data center.

Figure 12: If both ISP 1 and ISP 2 connections become unavailable, EdgeConnect Enterprise automatically moves application traffic to the transport service configured as a backup that backhauls traffic through the data center.

DEPEND ON VLCM

VLCM is a leading IT services provider. For 40 years we have helped clients design, implement and utilize technology to achieve success. We focus in 3 major areas: technology infrastructure, professional services, and cybersecurity. We are headquartered in Salt Lake City, UT with and serve over 20,000 organizations across the United States.

CONTACT US TODAY, SO WE CAN START BUILDING YOUR CUSTOMIZED CLOUD NETWORKING SOLUTION.

www.VLCM.com   Phone Number: 1-800-817-1504   852 E. Arrowhead Lane, Salt Lake City, UT 84107