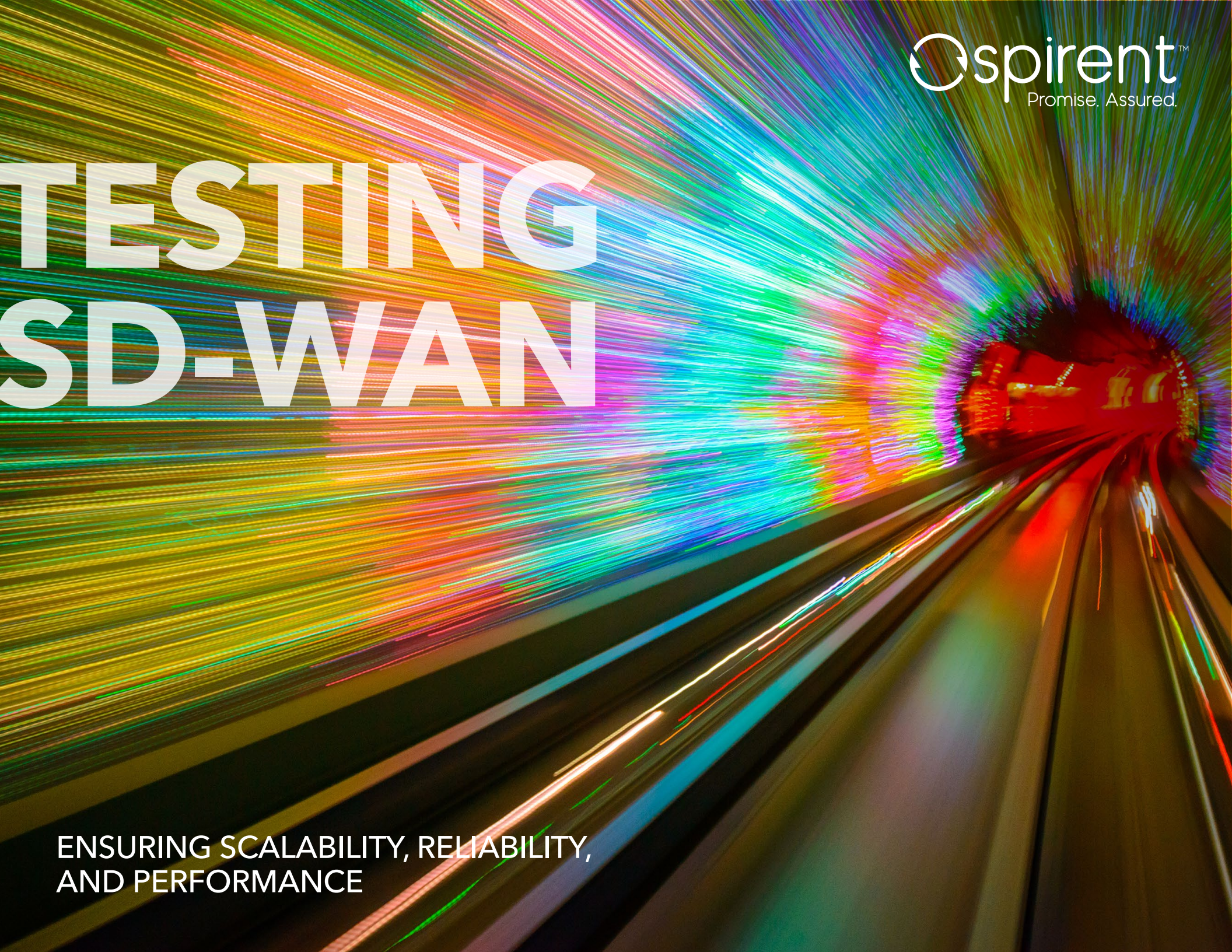

Spirent™
Promise. Assured.
TESTING
SD-WAN
ENSURING SCALABILITY, RELIABILITY,
AND PERFORMANCE

Contents

SD-WAN Overview

Software-Defined Wide Area Networking (SD-WAN) is an emerging alternative to provisioned Multi-Protocol Label Switching (MPLS) circuits, providing more distributed flexibility by using a more centralized control model at the customer premises or within the cloud. SD-WANs are built on the core Software-Defined Networking (SDN) principle of strict separation of data and control planes. SD-WANs can manage multiple types of connections, including MPLS, LTE, and broadband cable or DSL, while delivering a variety of services such as VPN, security and load-balancing. SD-WANs can be deployed much faster than an MPLS circuit, which must be provisioned by a service provider with a range of contractual Service Level Agreements (SLAs).

SD-WANs enable and enhance branch and remote-office connectivity in a cost-effective manner. The evolution from traditional to SD-WANs is driven by many market and technological factors:

- Mission-critical applications are moving from the enterprise premises to the cloud (e.g., Office 365 & Salesforce)
- MPLS circuits, deployed in traditional WANs, remain expensive, while Internet broadband connections are becoming cheaper and more reliable
- Reflecting the trends of a geographically dispersed workforce, the number of branches, home offices and wireless devices connecting into an enterprise network are growing substantially
- SD-WANs are characterized by significant enhancements to the WAN architecture and new functional components, which are described below.
- SD-WANs use a **central controller** to enforce routing and security policies and route application flows over the appropriate links.
- SD-WANs provide **differentiated QoS** to the various application flows. For example, they have the ability to throttle Facebook or YouTube traffic while providing guaranteed QoS to voice calls or Office 365 traffic.
- The SD-WAN Controller provides the capability to **dynamically route** around congested or failed paths.
- SD-WAN implementations almost always leverage **NFV technologies**, both on the customer premises and in the provider edge/cloud. SD-WANs also support **Virtual Network Functions (VNF)**, in part through reliance on commodity x86-based hardware.

SD-WAN generates significant architectural and technology churn. Vendors, Cloud Service Providers and Enterprises, who are contemplating using SD-WAN, need to thoroughly validate their implementation before deployment.

SD-WAN and Security

The promise of SD-WAN solutions over traditional MPLS based WANs center around several fundamental aspects:

- Improved performance
- Better bandwidth allocation
- Improved application policy enforcement
- Improved network visibility
- Lower costs

However, with all these potential improvements, security concerns continue to be a focal point as more organization adopt SD-WANs.

SD-WANs shift IT organizations from the known world of centralized device level WAN deployments and move them to decentralized and distributed environments. Does this change the landscape and attack surface area? Are SD-WANs a more structured approach to WAN and security servicing? The answer is yes to both. Spirent security and application testing solution help our customer mange risks associated with security infrastructure.

SD-WANs employ end-to-end encryption as a matter of course for all sites on an SD-WAN infrastructure. This provides in-flight encryption for all data that will traverses an SD-WAN environment. While this universal level of encryption will keep traffic away from eavesdropping and other nefarious access, the impact to performance may not be obvious.

Testing emulated application flows that are defined of a specific Enterprise's traffic conditions can prove whether newly deployed SD-WAN services are improving or impeding network performance and access.

An aspect of SD-WANs is the definability of network segmentation (also called micro-segmentation). IT organizations can define down to specific applications, highly specific network, and security policies. This can limit the expanded attack surface an SD-WAN creates to mode siloed applications or segments.

For example, polices may be created where at a satellite office, policies are applied to vertical applications such as Salesforce or media services. With security policies segmented, attacks or vulnerabilities that impact one application may be prevented from having an impact on other applications or aspects of the Enterprise network. Understanding how these policies work can help IT originations optimize SD-WANs for the best balance of security and performance. Spirent's security and applications appliance testing solutions can create very specific Enterprise traffic mixed from a database of over 10,000 applications flows to determine how accurate SD-WAN policies are enforced.

SD-WANs are not meant to be an overall panacea for network security, they have to work in conjunction with inline firewalls, Next Generation Firewalls, IDS/IPS and other security solutions. Many of these solutions will have attack and anti-malware inspection blocking characteristics. Understanding how malware and other attack traffic could be mitigated in the everything encrypted realm of an SD-WAN is vital. Spirent CyberFlood provides the ability to quickly create tests to send attacks or malware between defined test endpoints on our appliance solutions effectively and safely, to verify security rulesets and malicious content blocking capabilities.

Testing both the security and applications aspects of SD-WANs at L4-7 with real-world emulated legitimate and malicious traffic is crucial to keeping the finger on the pulse of next generation SD-WAN services.

SD-WAN and vCPE

The successful validation of SD-WAN implementations will address the following concerns:

- **Scalability–**Capability to bring-up and successfully operate hundreds or thousands of branch offices as required
- **Security–**SD-WAN has a large attack surface. Sensitive data must be securely accessed in an environment that is geographically dispersed, and open to multiple service providers and enterprise domains
- **Reliability–**Providing continuous availability for business-critical applications
- **Performance–**Key applications make use of expensive, dedicated bandwidth, but can burst to the cloud during peak utilization, preempting lower priority traffic and giving higher overall scale

A properly validated SD-WAN will allow enterprises to focus on their core competencies instead of worrying about their branch connectivity.

CPE (Customer Premises Equipment) is a key component of SD-WAN. The CPE, located on the customer premises, receives policy from the centralized controller, and is responsible for the local enforcement of that policy and managing access to the WAN resources.

The virtualization of the CPE (vCPE) is one of the early NFV use cases being adopted by Service Providers. vCPE aligns well with the theme of centralized management and automation in SD-WAN, as it enables centralized provisioning in VNFs that constitute vCPE.

vCPE can be deployed in any of the following three flavors:

- **Cloud CPE–**CPE functionality (e.g.,NAT, Firewall) is deployed in the cloud at the Provider Edge
- **On-premises OTT vCPE–**More functionality (e.g.,NAT, Firewall) is supported at the customer premises. Customer traffic is carried over a broadband connection
- **On-premises vCPE–**Customer traffic is carried over a dedicated link owned by the service provider

SD-WAN and vCPE validation can be divided into three high-level test scenarios:

1. **Policy Validation**
2. **Path Selection**
3. **Resiliency/Fail-Over**

Spirent offers a comprehensive set of test tools and methodologies for automated validation of SD-WAN deployments in pre-deployment, turn-up and production phases.

Test Scenarios

Policy Validation

SUMMARY OF TRAFFIC STREAMS

Result: Passed

Explanation: All expected traffic streams received. When Expected Rx is True, Rx Frame Count > 0 is considered a Pass.

Stream Name	Tx Frame Count	Rx Frame Count	Dropped Frame Count	Expected on Rx Port	Pass or Fail
East_Default_Policy	2256864	0	0	False	PASS
East_ACL_1000	2256864	2046185	210679	True	PASS
East_ACL_50	2256864	2041193	215671	True	PASS
West_Default_Policy	2235375	0	0	False	PASS
West_ACL_1000	2235375	2162254	73121	True	PASS
West_ACL_50	2235375	2163128	72247	True	PASS

EXPECTED STREAMS WITH DROPPED FRAMES

Result: Failed

Explanation: At least one expected traffic stream had dropped frames.

Stream Name	Tx Frame Count	Rx Frame Count	Dropped Frame Count
East_ACL_1000	2256864	2046185	210679
East_ACL_50	2256864	2041193	215671
West_ACL_1000	2235375	2162254	73121
West_ACL_50	2235375	2163128	72247

The policies that define a given service are pushed from the SD-WAN controller to the CPE/vCPE and/or the Provider Edge devices. Ensuring policy adherence is a major challenge. The policies are stored within a database that can either be within the SD-WAN Controller, or a separate standalone database. A customer site can have thousands of policies and there may be hundreds of customer sites associated with an SD-WAN controller. In a large-scale scenario, manually validating policies is both effort-intensive and error-prone. Automated policy validation must therefore be performed both in the pre-deployment, turn-up and production phases.

SD-WAN policies can be broadly categorized as:

- **Access Control:** Port based, VLAN based, L2-L4 based, application or content specific policies
- **Traffic Shaping:** L2 & L3 QoS, DiffServ, Congestion Avoidance, 802.1p

These policies need to be evaluated for:

- Correct orchestration and operation on a single service or vCPE instance.
- Validation of the above at maximum scale and throughput.
- Optimal placement of VNFs

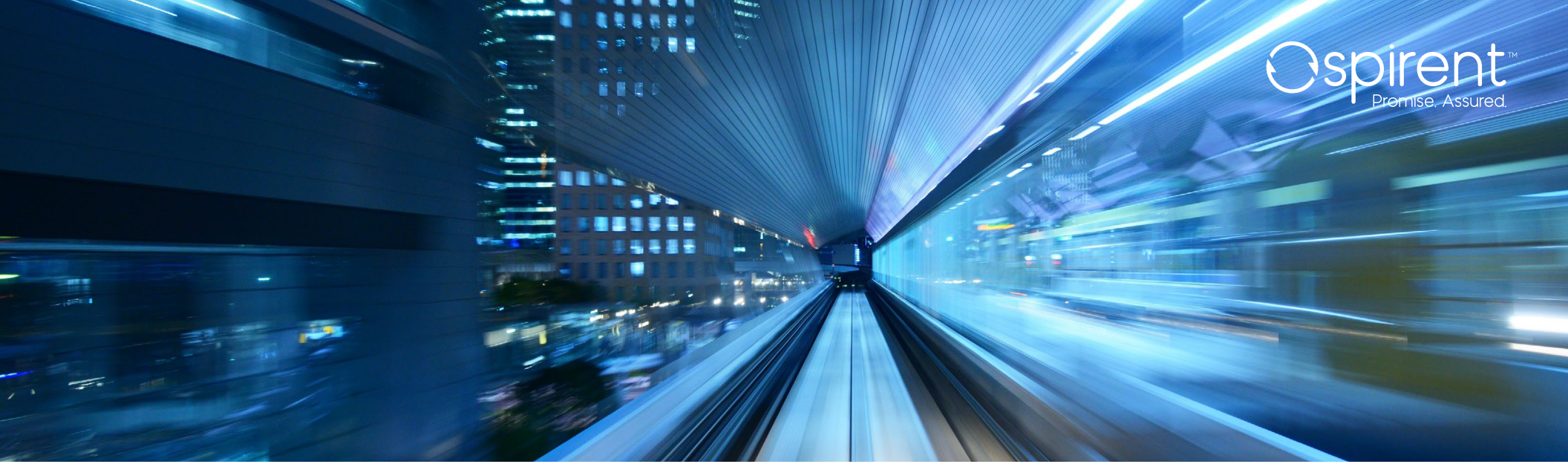
Path Selection

SD-WAN CPE devices are typically connected to the network via two or more fixed or wireless links, which, in turn, support multiple connection paths. These links range in quality from dedicated Ethernet or MPLS VPNs with guaranteed SLAs, to best effort Internet connections. Applications that use the SD-WAN service have a similarly diverse range of quality requirements, ranging from business-critical software like SAP or SalesForce, to Facebook Messenger.

Path endpoints for these services are diverse, with applications requiring connection to a range of destination types, including head-office servers, cloud-based services or Internet-based applications and services.

Algorithms within the CPE device must determine the path that best matches the policies discussed in the previous section, while taking into consideration the constantly changing state of the links, the desired end-point and the business criticality of the service. Such algorithms will grow more sophisticated over time, but are presently limited to:

- Static SLA policy-based routing
  - QOS based–throughput, latency, jitter
  - Access based
- Dynamic routing of flows based on status of the links/paths, such as congestion, link-failure and a certain level of packet loss



Resiliency/Fail-Over

An SD-WAN device's key task is assuring the resilience of business-critical services. The most critical services should receive the highest level of availability. During incidents of network failure, this may be at the expense of noncritical services. Unfortunately, network failure conditions exacerbate the problem. If a link fails, any critical service on that path must be reconnected via another path. If necessary, lower priority services will be disconnected or receive a reduced quality of service.

Two types of link failure should be considered:

- **Link Blackout–**Link fails completely (due for example to cable cut or local device failure)
- **Link Brownout–**Link capacity or quality is reduced (due for example to congestion or upstream device or link failure)

Such failures should trigger the SD-WAN's failover mechanisms, which reprioritizes services, preempting lower priority services where necessary, and reconnecting critical services via the remaining link(s).

There are high availability technologies, often found on SD-WAN devices, that can assist in this task. They include:

- Link Bonding (similar to LAG) Validation
- Load balancing across links
- Overlay Down Action: Drop, PassThrough, PassThrough Unshaped

Conclusion

Virtualization and software-defined networking technologies bring new possibilities. Spirent's NFV test solutions assist you to deploy, onboard, actively test and assure cloud and virtualized networks. Validate NFV environments including SD-WAN or VNF services to ensure performance and SLAs with proven test methodologies to realize promise of NFV.

Spirent's SD-WAN test solutions support a comprehensive set of SDN protocol emulation, automated NFV test methodologies and best-in-class virtual test agents. Spirent virtual test agent may co-reside as a Test VNF on the server that hosts vCPE or may be deployed on a standalone server.

Spirent's goal is not just to provide test tools, but to provide test solutions that help unravel the conundrum surrounding the difficult NFV problems that the industry faces.

For more details on Spirent's SD-WAN/vCPE test solution, visit:
https://www.spirent.com/Solutions/SDN-NFV-Solutions

Acronyms

CPE	Customer Premises Equipment
SD-WAN	Software-Defined Wide Area Networking
SDN	Software-Defined Networking
SLA	Service Level Agreements
MPLS	Multi-Protocol Label Switching
NFV	Network Function Virtualization
vCPE	Virtualization of Customer Premises Equipment

About Spirent

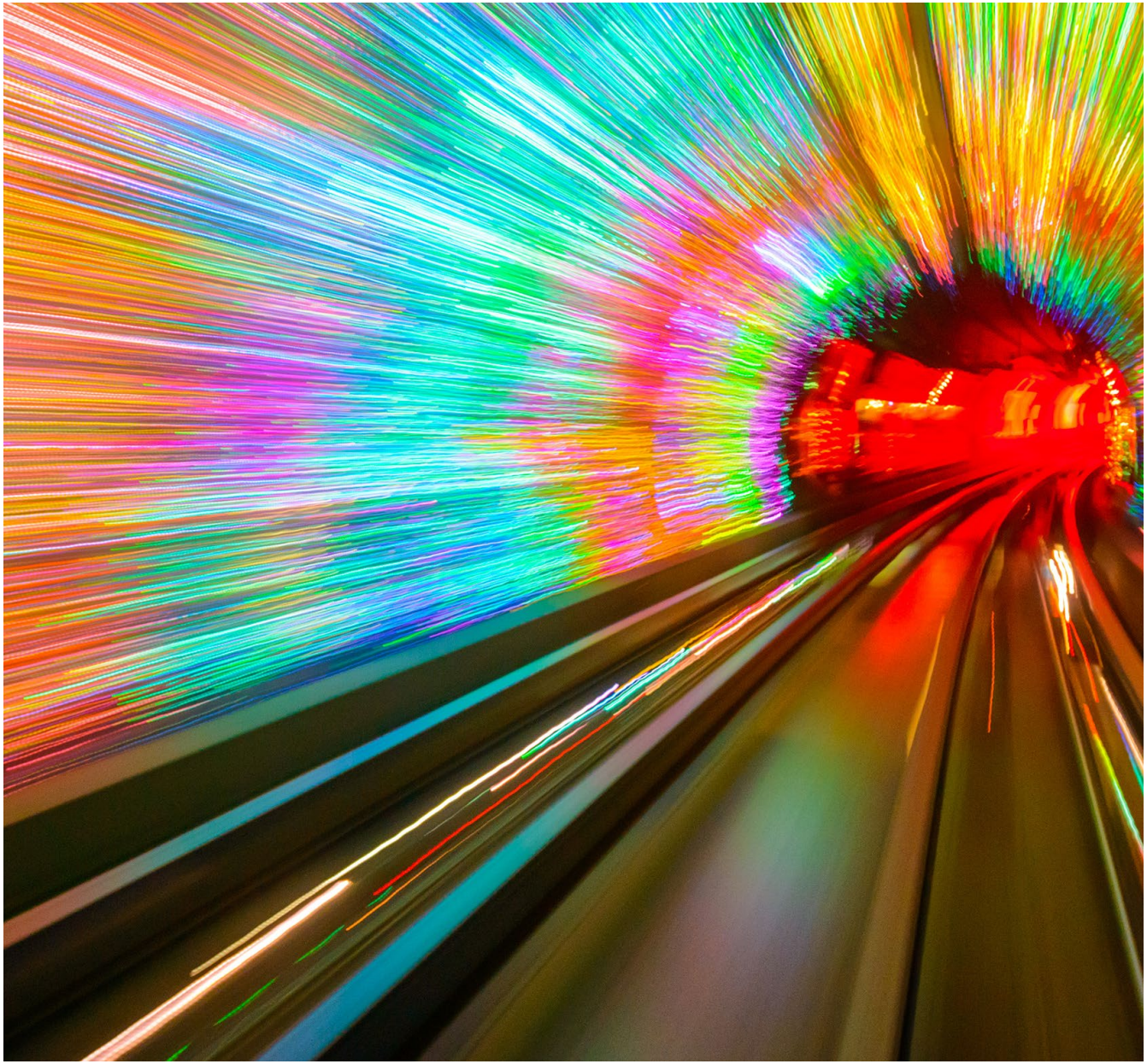
About Spirent Communications

Spirent Communications (LSE: SPT) is a global leader with deep expertise and decades of experience in testing, assurance, analytics and security, serving developers, service providers, and enterprise networks.

We help bring clarity to increasingly complex technological and business challenges.

Spirent's customers have made a promise to their customers to deliver superior performance. Spirent assures that those promises are fulfilled.

For more information, visit:
www.spirent.com



AMERICAS 1-800-SPIRENT
+1-800-774-7368
sales@spirent.com

EUROPE AND THE MIDDLE EAST
+44 (0) 1293 767979
emeainfo@spirent.com

ASIA AND THE PACIFIC
+86-10-8518-2539
salesasia@spirent.com

© 2019 Spirent Communications, Inc. All of the company names and/or brand names and/or product names and/or logos referred to in this document, in particular the name "Spirent" and its logo device, are either registered trademarks or trademarks pending registration in accordance with relevant national laws. All rights reserved. Specifications subject to change without notice.

Rev C | 09/19