EANTC Independent Test Report

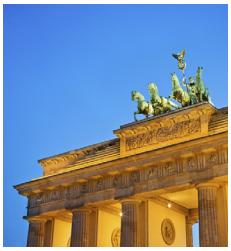
Huawei SD-WAN Solution

December 2017

EANTC

HUAWEI

About EANTC



EANTC (European Advanced Networking Test Center) is internationally recognized as one of the world's leading independent test centers for telecommunication technologies.

Based in Berlin, the company offers vendor-neutral consultancy and realistic, reproducible high-quality testing services since 1991. Customers include leading network equipment manufacturers, tier 1 service providers, large enter-prises and governments worldwide. EANTC's Proof of Concept, acceptance tests and network audits cover established and next-generation fixed and mobile network technologies.

Table of Contents

Introduction 2
Test Highlights 2
Hardware and Software 3
Test Bed 3
Test Equipment 3
Test Results 4
Scalability 4
Number of VPNs per Site 4
Throughput per Number of VPNs per Site (CPE Performance) 5
Endpoint and Link Resiliency 6
CPE Failure 6
Primary Link Failure 7
Performance Monitoring 8
Performance Monitoring Accuracy 8
Application-based Traffic Steering 10
Conclusion 12

Introduction

The market for Software Defined Wide Area Network (SD-WAN) solutions has grown rapidly over the last two years. In an area where cloud computing enables customers to deploy compute resources on-demand and in a matter of seconds, and where SDN is being actively deployed in data centers networks, enterprises request a flexible and affordable connectivity solution for the Wide Area Networks (WAN).

Test Highlights

- 2,000+ full-mesh VPNs per CPE
- Protection switching within milliseconds in the event of a CPE failure or a primary link failure
- Application-aware traffic re-routing based on live network performance
- Accurate performance monitoring and GIS-based multi-dimensional visualization

By aggregating different types of WAN links and making intelligent forwarding decisions across these links based on policies and network conditions, SD-WAN has become an important transformation technology for the telecommunications industry. The beauty (and somehow also the challenge) of SD-WAN is its nature as an overlay technology: Adaptable to any connectivity solution while unable to control the underlying transport network, SD-WAN implementations need a different approach to ensure network quality and reliability.

EANTC has been testing IP/MPLS independently for more than 15 years and SDN-WAN solutions since 2011. Naturally, we are reviewing SD-WAN solutions as well. Huawei is the first vendor to pass SD-WAN testing at EANTC. It is our pleasure to publish their SD-WAN solution review now.

EANTC has started an SD-WAN testing initiative open to any manufacturer of SD-WAN solutions worldwide. Participating vendors have the opportunity to choose their bespoke test package from EANTC's SD-WAN testing portfolio based on the primary technical focus areas. For its participation, Huawei chose the following test areas: Scalability, Endpoint and Link Resiliency, and Performance Monitoring.

In the scalability area, we successfully verified the number of VPNs per site supported by Huawei's SD-WAN solution and the throughput per VPN per site. Two test cases out of five defined in this area were completed. This was due to the amount of time and resources required to complete some of the scalability tests.

The Endpoint and Link Resiliency tests included Customer Premise Equipment (CPE) failure and the failure of one of the primary links, which enable service providers to measure the readiness of the SD-WAN to be deployed for the transport of voice, video and data.

Finally, with their SD-WAN solution, Huawei seeks to optimize application performance and reliability by dynamically steering critical traffic across the best links, as well as potentially mitigating circuit performance issues. We were excited to test performance monitoring and application-based traffic steering, which are key enablers of the SD-WAN.

After two weeks of testing at Huawei's office in Nanjing, we are happy to present the results of our joint work with Huawei's team in this report.

Hardware and Software

Hardware Type	Software Version
Huawei AR161EW	V200R009C00 Patch Version: V200R009C00CP0711
Huawei AR169W	V200R009C00
Huawei AR1220EVW	
Huawei AR3670	
Huawei AR1220EVW	V200R008C50
Huawei AR1220C	V200R008C50
Huawei SRG1320E	V200R008C20
Huawei Agile Controller	V300R002C00

Test Bed

Huawei provided a comprehensive end-to-end lab environment for the test. The test network reflected a real production network and had a hierarchical Wide Area Network (WAN) design, consisting of three branches and a headquarter site. As depicted in Figure 1 and Figure , two branch sites with a single CPE each were associated in the management system with emulated locations of Nanjing and Shenzhen respectively; the third branch designated as Shanghai was comprised of two redundant Customer Premise Equipment (CPEs).

All branch sites were connected to the hub at the headquarter site at the emulated location of Beijing through two underlying networks, an MPLS network and an emulated Internet connection. CPEs and hub devices in turn redundantly peered with the Huawei Agile Controller cluster, acting as the SD-WAN controller via both the MPLS network and the emulated Internet. The Agile Controller cluster's deployment consisted of several Virtual Machines (VMs) carrying various components and spread across three compute nodes to provide hardware redundancy. VMware ESXi was deployed in each compute node as the virtualization technology.

The WAN constructed by Huawei included Huawei's AR161EW, AR169W, and AR1220EVW at the branch sites. A Huawei AR3670 was provided at the hub site. The underlying MPLS core network was built using Huawei AR1220C and AR1220EVW Provider Edge (PE) routers. A Huawei SRG1320E was used to emulate the Internet in the lab.

For the purpose of one single test case, we used a Windows server connected to a CPE in a branch site running a Huawei proprietary Dynamic Smart Virtual Private Network (DSVPN) application to emulate other CPE nodes, which in turn were used to simulate a large number of overlay tunnels to mimic a typical large WAN deployment scenario.

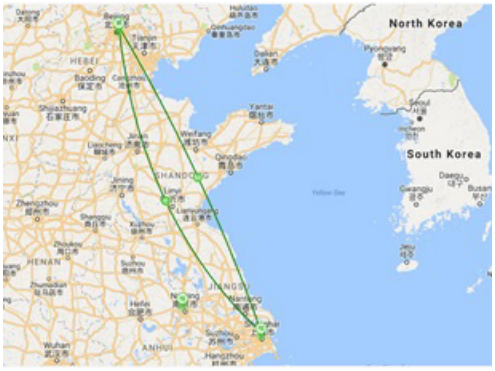


Figure 1: Test Setup - SD-WAN Controller's View

Test Equipment

Executing the test required a traffic generator, an analyzer and an impairment tool. We used Spirent Test Center equipped with EDM-20038 24-ports GigabitEthernet cards for traffic generation and analysis. For impairment generation, we used Wide Area Network Emulator (WANem) from TATA consultancy services.

We complemented the test equipment (traffic generator/emulator) with an x86 Windows server. Based on the test bed design, a single CPE would have to establish a large number of spoke to spoke DSVPN tunnels. Based on this requirement, we used a DSVPN application, running on an x86 Windows server to emulate a large number of DSVPNs towards the CPE.

Test Results

In the following section we describe the test results for the test areas selected by Huawei.

Scalability

As SD-WAN gains popularity as an alternative to the traditional wide-area VPN technologies, it is only logical that enterprises and service providers are concerned with the scalability of the solution that they are buying.

Through the following series of tests, EANTC verified the various scalability and performance claims of Huawei's SD-WAN solution, specifically:

- Number of VPNs per Site
- Throughput per number of VPNs per site (CPE Performance)

Number of VPNs per Site

In a large-scale multi-tenant SD-WAN deployment with a large number of branch sites per customer tenant, a single CPE device is often required to support a high number of overlay tunnels to enable connection to multiple hub and spoke sites.

Since the test setup would have required a large number of physical CPEs and hub devices to verify the ability of a CPE to support a large number of DSVPNs, we deployed a windows server at a branch site and connected it to the CPE to complement our test bed. The intention was to run a Huawei proprietary DSVPN application on the server to simulate a large number of spokes connected to the CPE, acting as the hub device. This allowed us to simulate a scenario where a CPE creates a high number of dynamic spoke-spoke DSVPNs.

In our test scenario we installed two SD-WAN edge devices — Huawei AR3670, acting as the hub node and Huawei AR1220EVW, served as the CPE — as depicted in Figure 4. The devices were connected to the SD-WAN controller via both an MPLS network and the emulated Internet. Both SD-WAN edge nodes were in turn interconnected via two WANs: the path over the MPLS network comprised of a single link between the two sites. The path over the Internet was made up of three links between the two sites.

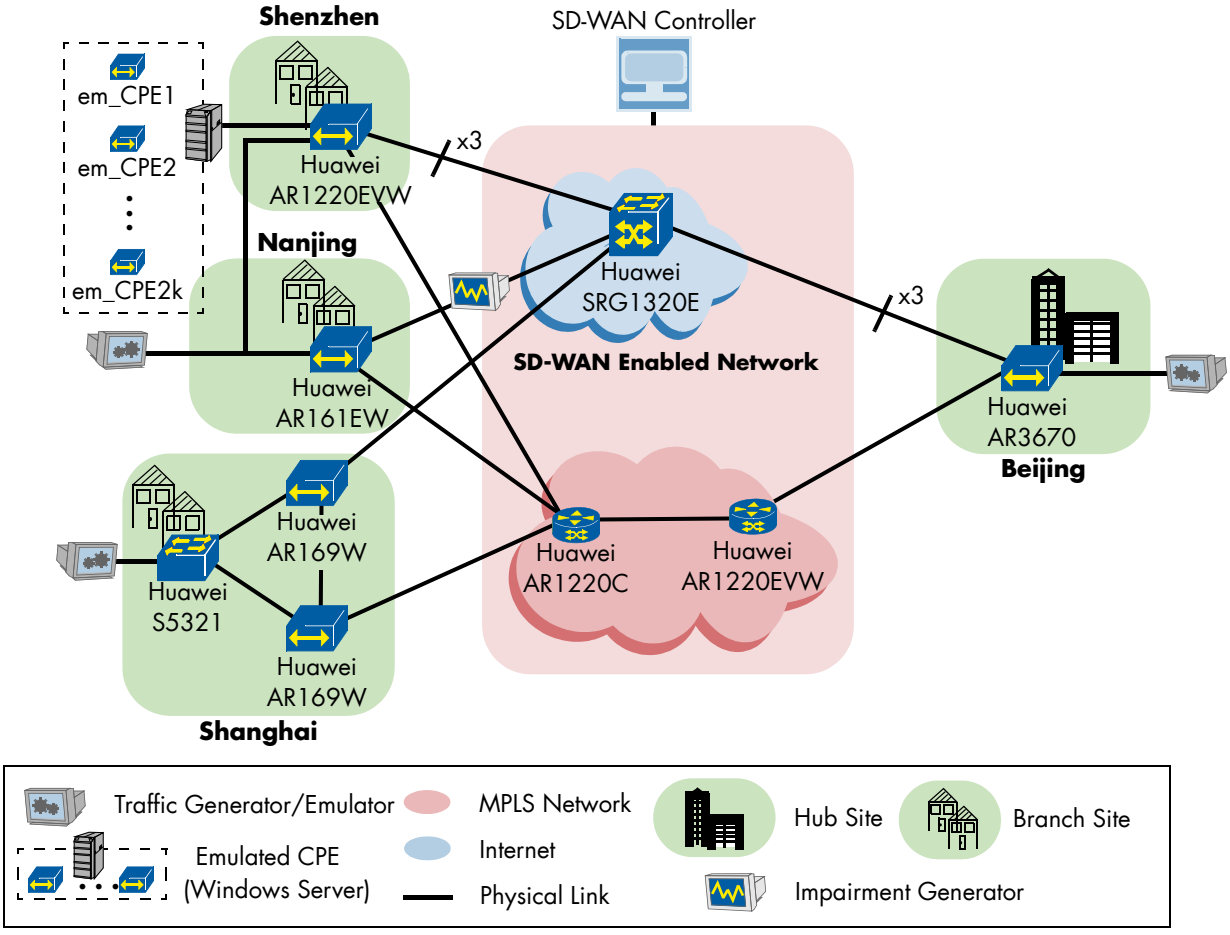


Figure 2: Physical Test Setup

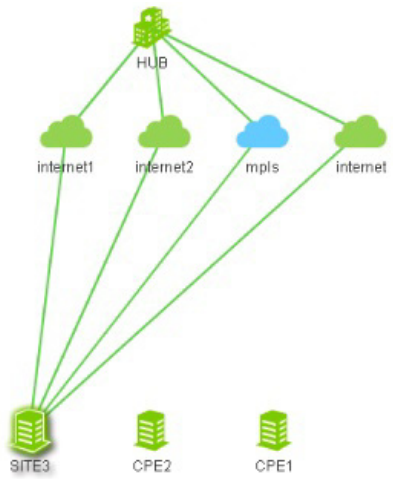


Figure 3: Number of DSVPNs per Site - Huawei SD-WAN Controller View

Initially, we configured the SD-WAN controller to orchestrate four DSVPNs between CPE and hub nodes: three DSVPNs over the emulated Internet and one through the MPLS network. We expected all four DSVPNs to be correctly deployed onto CPE and hub devices.

We started sending bidirectional UDP traffic through each of the DSVPN tunnels using Spirent Test Center to make sure that they were correctly setup. There was no packet loss observed during this reference test. While traffic was running through the four provisioned DSVPN tunnels, Huawei engineers used the DSVPN application installed on the server to request the creation of 3,000 DSVPNs on the CPE. The CPE's Command Line Interface (CLI) displayed that a total of 2,004 DSVPNs were created. During the test, we monitored the CPE's CPU utilization, which was approximately 11.4% as well as memory consumption, which was 60%. No impact was observed on the UDP traffic traversing through the four DSVPN tunnels. Our test revealed that Huawei AR1220EVW when used as an SD-WAN edge device can setup and maintain four hub-spoke DSVPNs and up to 2,000 spoke-spoke DSVPNs.

Throughput per Number of VPNs per Site (CPE Performance)

As the number of DSVPNs supported by a single CPE scales to the maximum, one can imagine that as more devices are added to the Branch/hub sites, more traffic will be generated resulting in more bandwidth. The CPE with its provisioned DSVPN is expected to deal with an increase in throughput per VPN requirements.

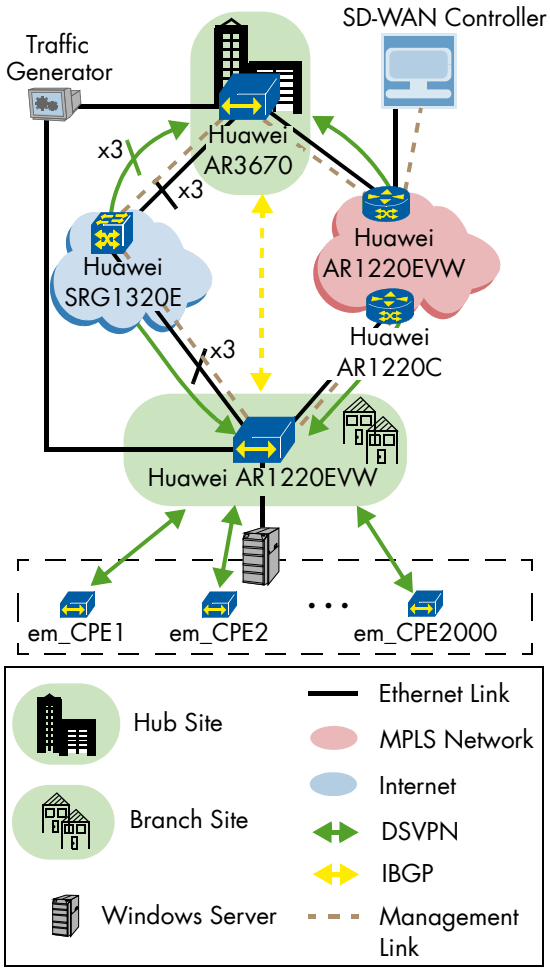


Figure 4: Number of VPNs per Site

To assess the CPE performance of Huawei AR1220EVW, acting as CPE loaded with four hub-spoke and 2,000 emulated spoke-spoke DSVPNs, our test used the same test bed as in the "Number of VPNs per Sites" test (see Figure 4). This time we intentionally offered traffic at varying loads and determined the highest rate at which the SD-WAN CPE could forward all packets with zero loss.

We used the same methodology described by the IETF in RFC 2544 for a selected range of packet sizes — 64, 100, 373, 570, 1300, 1518 bytes. Additionally we tested with Internet mix (IMIX)[1] traffic, allowing a realistic overview relevant for an SD-WAN real deployment scenario. IMIX is a packet mix that attempts to replicate real Internet traffic.

We performed the test using Spirent Test Center connected to both hub and CPE nodes and generated UDP traffic through the four hub-spoke DSVPN tunnels.

1. IMIX consisted of 5% 64-byte packets, 42% 100 byte packets, 9.5% 373-byte packets, 8% 570 byte packets, 26% 1518-byte packets and 9.5% 1300-byte packets

The aggregated bidirectional throughput test result is depicted in Figure 5.

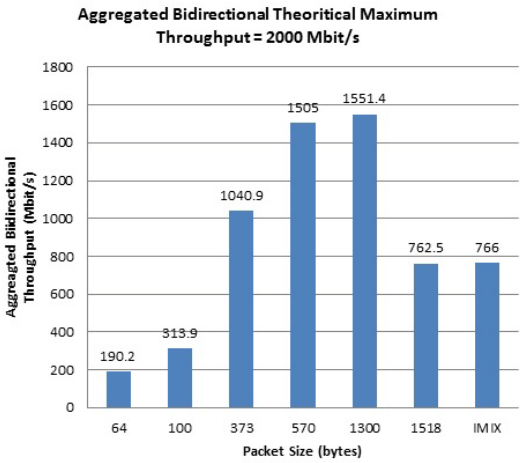


Figure 5: CPE Performance for 4 DSVPNs and Loaded with 2004 Emulated DSVPNs

Endpoint and Link Resiliency

Network reliability has been always a major concern in any enterprise and service provider network transporting voice, video and business-critical data. Whether a link fails due to cable pull or a CPE fails due to power outage, a reliable network should react to sudden failures without any manual intervention.

Huawei SD-WAN solution provides a range of solutions to address such network failures.

CPE Failure

To ensure the highest level of availability for gold and silver level service, SD-WAN requires a configuration that has redundant CPEs at a branch location to peer with the remote hub site using multiple circuits. Since both circuits can be grouped into single link groups, they can be used to simultaneously carry different application types in an active-active fashion. While one circuit is active for a specific application, it is used as backup for other applications running on a different circuit. Upon failure of one CPE, the SD-WAN solution causes the switchover of applications from the failed CPE to the other CPE.

This test was carried out with the network configuration shown in Figure 6. Our test setup consisted of a branch site with two redundant SD-WAN CPEs (two Huawei AR169W's) each of which was connected to the hub device (Huawei AR3670) over an emulated Internet and an MPLS network. CPEs and hub were connected to the SD-WAN controller by SSL sessions. Both CPEs were configured to operate in master-backup redundancy mode using the Virtual Routing Redundancy Protocol (VRRP).

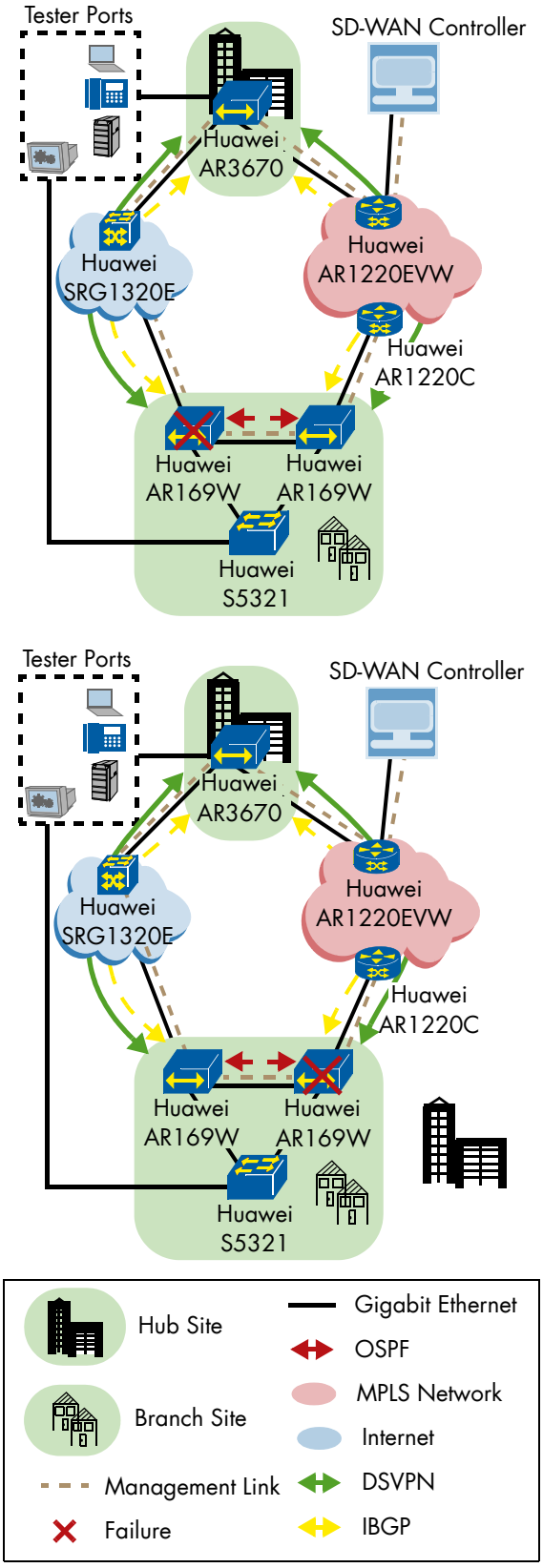


Figure 6: CPE Failure

For testing purposes, we used Huawei's SD-WAN controller to define two DSVPNs, each starting at different CPEs, terminating on the same hub and traversing different links.

Both tunnels were configured to be in an active state.At that point, we validated that the CPE connected to the MPLS network was the VRRP master and the one connected to the Internet was the VRRP slave.

The SD-WAN solution was asked to identify the different traffic types and steer them towards the correct link using pre-defined policies:

- Steer general UDP traffic towards the Internet link as the primary link and use the MPLS link on failure of the Internet link
- Steer FTP traffic towards the MPLS link as its primary link and make use of the Internet link as backup

Once the Huawei Agile controller displayed established DSVPN tunnels as shown in Figure 7, we supplied bidirectional FTP and UDP traffic between SD-WAN edge devices using Spirent Test Center and the FTP application server respectively.

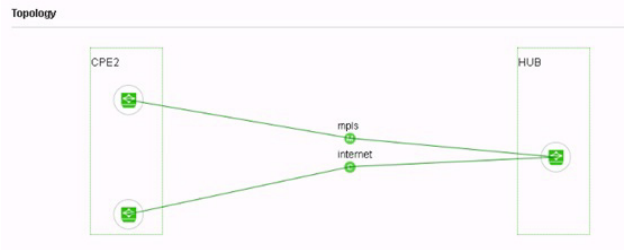


Figure 7: DSVPNs between on Two CPEs and a Hub

Huawei configured Bidirectional Forwarding Detection (BFD) on the VRRP interface on the link between both CPEs. Additionally the OSPF session, running between both CPEs, was monitored by BFD. Same for the overlay IBGP session, configured between CPEs and the hub. All BFD sessions were used to monitor the liveness of the connections.

Given that Huawei configured the BFD hello interval at 50 milliseconds and the multiplier at three, we expected that the detection time would be theoretically between 100 and 150 milliseconds. After a failure is detected, time for convergence is needed and this may take additional time

First we verified that FTP and general UDP traffic were indeed steered towards the MPLS and the Internet link respectively and that traffic was forwarded to the destination without any packet loss.

Once this step was completed, we emulated the failure of the CPE connected to the Internet link and acting as the VRRP backup by issuing an administrative "Reboot Fast" command, causing the SD-WAN solution to steer the UDP traffic towards the MPLS link. We recorded out of service time of maximum 135 milliseconds in the direction from the hub to the CPE and of maximum 295 milliseconds in the opposite direction. We tested the recovery scenario during the restart of the CPE. After the Wait to Restore (WTR) timer expired, traffic loss and reversion time was measured when the general UDP traffic was steered again towards the Internet link. We measured recovery time of maximum 167 milliseconds in the direction from the CPE to the hub and no packet loss at all in the opposite direction.

Afterwards, we emulated the failure of the second CPE - the VRRP master - connected to the MPLS link, by powering it down using "Reboot Fast" command. Once successful, we followed the recovery test wherein the device was powered up. We measured failover time of maximum 132 milliseconds in the direction from the hub to the CPE and of maximum 139 milliseconds in the other direction. We measured recovery time of maximum 424 milliseconds in the direction from the hub to the CPE and no packet loss at all in the opposite direction. During this step, we observed that as soon as the previously failed master recovered from failure, it took over the VRRP mastership.

In this test, Huawei R3670 participated as the hub node at the headquarter site, and Huawei AR169W served as the CPE access device at the branch site. Huawei Agile Controller successfully participated as SD-WAN controller.

Primary Link Failure

One of the key advantages of SD-WAN technology is the ability to aggregate different WAN links (such as MPLS, xDSL, LTE/4G). The ability of the SD-WAN solution to mitigate the failure of the primary link is critical.

Our setup consisted of one CPE (Huawei AR161EW) and one hub device (Huawei R3670), each of which were connected to the Huawei Agile Controller using the MPLS and Internet network, over which the SSL controller channel was established. CPE and hub nodes were in turn connected together via two WANs: an MPLS network and a network emulating the public Internet.

The SD-WAN controller was configured to setup two DSVPN tunnels between the CPE and the hub device: one DSVPN across the MPLS network and another one over the emulated Internet. Likewise the traffic policies were provisioned on the SD-WAN controller to steer general UDP traffic towards the Internet and FTP towards the MPLS network. To perform this test, Huawei engineers setup two Internal Border Gateway

Protocol (IBGP) sessions — one over each DSVPN tunnel — between CPE and hub to distribute all local prefixes available on the SD-WAN sites.

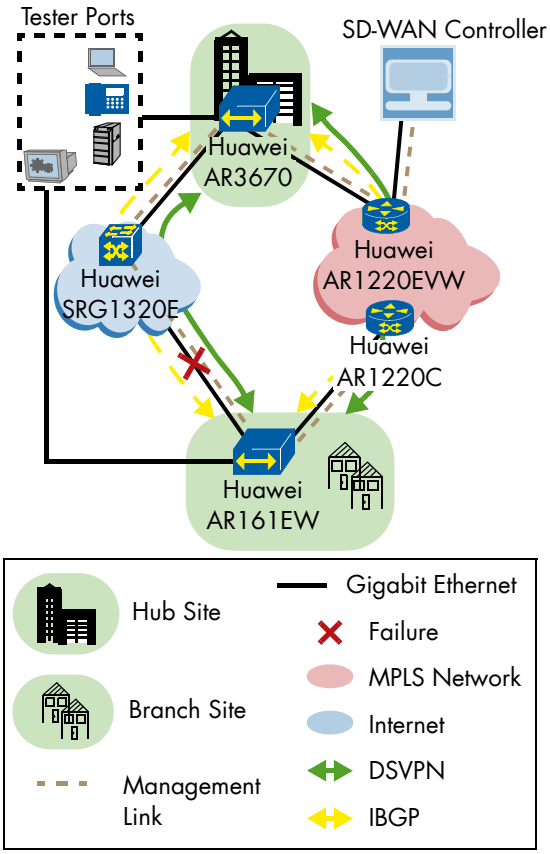


Figure 8: Primary Link Failure

Once CPE and hub were successfully registered with the SD-WAN controller, we validated that all DSVPN and traffic policy configurations were correctly deployed to CPE and hub nodes. We verified that all control plane sessions had been established and IP prefixes had been exchanged between SD-WAN edge nodes.

Figure 9: SD-WAN edge devices registration to controller

When we sent UDP and FTP traffic using Spirent Test Center connected to both Huawei AR161EW and Huawei AR3670, we validated that the UDP traffic was indeed steered towards the emulated Internet and the FTP traffic was steered towards the MPLS network. We observed no packet drops.

On failure of the Internet link, which was induced by physical link disconnection between the CPE and the Internet node, we successfully verified that UDP traffic was redirected to the backup MPLS link as expected. The simulated Internet connectivity failure generated failover times ranging from 127 to 155 milliseconds in the direction from the hub to the CPE and from 170 to 200 milliseconds in the opposite direction.

We also tested the recovery scenario by reconnecting the previously disconnected link. After the Wait to Restore (WTR) timer expired, we expected the UDP traffic in this case to be steered towards the Internet link. We measured the recovery time of 0 seconds. All test runs showed no traffic loss at all.

During this test, a Huawei engineer configured BFD on the overlay BGP sessions between CPE and hub devices to monitor the liveness of the connection.

Performance Monitoring

One of the main drivers for SD-WAN is the ability to aggregate WAN links and to make intelligent forwarding decisions across these links based on policies and network conditions. To allow real-time visibility into these WAN links, which is key for SD-WAN intelligent application-based forwarding, accurate performance monitoring is required.

Performance Monitoring Accuracy

SD-WAN relies on the performance monitoring tool to provide visibility into application performance by monitoring performance parameters such as packet loss, packet delay, and packet delay variation. Accurate measurement of these performance metrics is crucial to the correct operation of an SD-WAN-enabled network.

To mimic a typical network deployment scenario, we built a test bed consisting of an SD-WAN CPE (Huawei AR161EW), an SD-WAN hub (Huawei AR3670) and an SD-WAN controller (Huawei Agile Controller). The SD-WAN CPE and hub were connected to the SD-WAN controller via the MPLS network and emulated Internet. The SD-WAN CPE was connected to the SD-WAN hub via two WANs: an emulated Internet and an MPLS network. Huawei engineers established two Internal Border Gateway Protocol (IBGP) sessions between the SD-WAN CPE and hub over each of the links to distribute SD-WAN site prefixes.

In our test, we requested the Huawei SD-WAN controller to provision two Dynamic Smart Virtual Private Networks (DSVPNs) between Branch and hub sites — one was provisioned over the emulated Internet and the other over the MPLS network. The Huawei SD-WAN controller reported both tunnels operational as depicted in Figure 10.

Once this procedure was successfully completed, we used the SD-WAN controller to configure traffic policies to steer UDP traffic towards the Internet link and FTP towards the MPLS link.

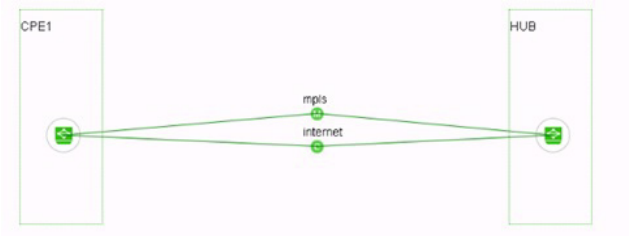


Figure 10: DSVPNs Across Internet and MPLS Network

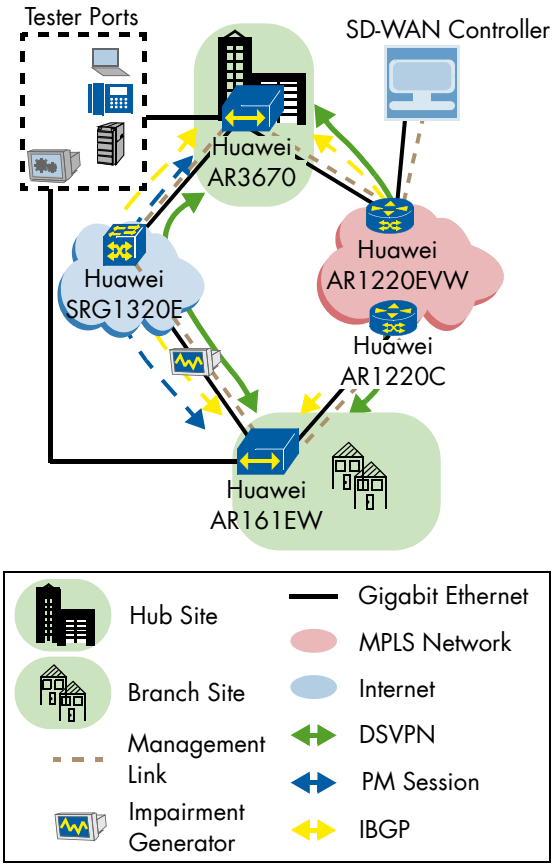


Figure 11: Performance Monitoring Accuracy Test Setup

In our test we used Wide Area Network Emulator (WANem), inserted on the link between the SD-WAN CPE and the node emulating the Internet, to introduce controlled impairment such as packet loss, packet delay and jitter to emulate network congestion. For a specific type of impairment, we verified the measurement results provided by the SD-WAN solution against the emulator configuration.

We initially ran a baseline reference test without insertion of any impairment to validate performance monitoring implementation of the Huawei SD-WAN solution. During this procedure we verified that the Huawei SD-WAN solution used a Network Quality Analysis (NQA) tool to monitor the performance and health of the network links, which reported on packet loss, packet delay and jitter. As part of the baseline, we generated UDP traffic using Spirent Test Center, connected to the SD-WAN edge nodes to validate that the test network was running correctly and experienced zero packet loss.

For loss measurement, we sent bidirectional UDP traffic through the provisioned DSVPN via the Internet link and introduced 10% loss in one direction using the WAN emulator. The Huawei SD-WAN solution showed the same loss value as shown in Figure 12.

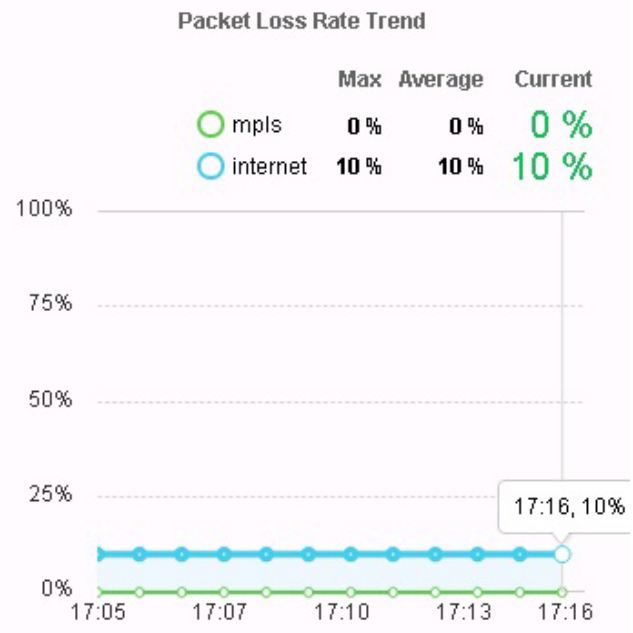


Figure 12: Packet Loss Ratio Reported by SD-WAN Controller

```
[CPE1]dis smart-policy-route link-state
link-name                       Delay       Jitter      Loss
192.168.100.1                   2           1           0
192.168.200.1                   1           1           100
[CPE1]dis smart-policy-route link-state
link-name                       Delay       Jitter      Loss
192.168.100.1                   3           5           0
192.168.200.1                   1           1           100
```

Figure 13: Packet Loss Measurement as Displayed by CPE

Once we removed the impairment profile, the loss value reverted to the normal condition.

In order to test packet delay measurement, we added an unidirectional constant delay of 20 milliseconds to

all packets on the Internet link. One-way Packet delay on all UDP packets on the Internet link as report by the SD-WAN solution increased by 20 milliseconds.

For the average packet delay variation or Jitter measurement, we introduced 25 milliseconds delay and 15 milliseconds jitter on all packets on the Internet link. Packet delay and jitter as reported by the SD-WAN solution was increased by 25 milliseconds and 15 milliseconds respectively.

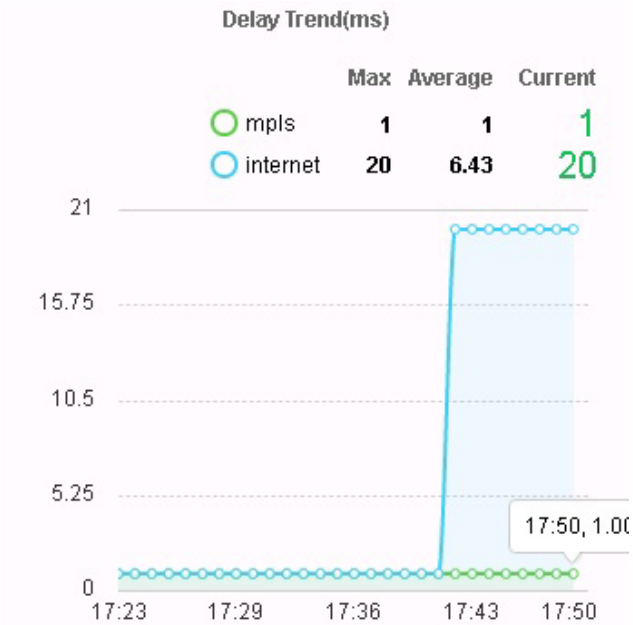


Figure 14: Packet Delay Measurement as Shown by the SD-WAN

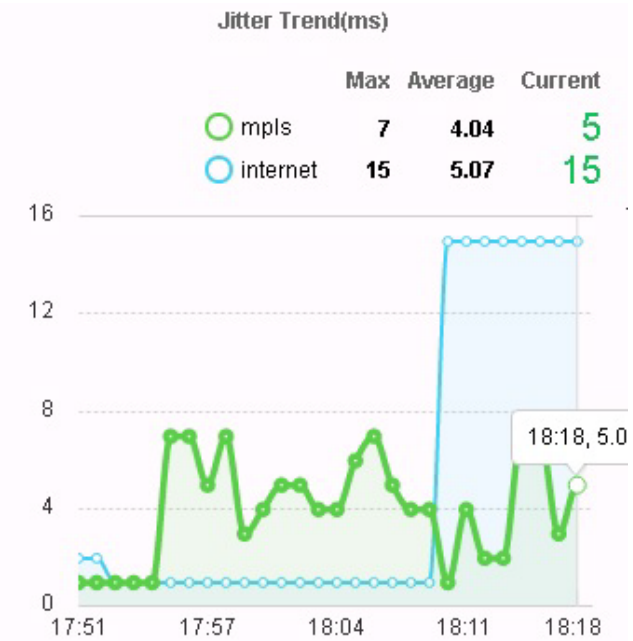


Figure 15: Packet Delay Variation Measurement as Shown by the SD-WAN

Application-based Traffic Steering

The quality, performance and reliability of the network are essential to user experience and customer satisfaction. With their SD-WAN solution, Huawei seeks to optimize application performance and reliability by dynamically steering critical traffic across the best links, as well as potentially mitigating circuit performance issues. The key element to address these requirements is the application-based traffic steering functionality of the SD-WAN solution.

The idea behind this feature is to monitor the quality of each link used by application traffic with continuous performance monitors. If a link experiences quality degradation for example due to excessive packet loss or jitter, which severely impact applications running on that link, the sending SD-WAN edge devices instantly and dynamically switch the application traffic to another link with the best quality available at that moment.

To perform this test, we used the same test bed as in the "Performance Monitoring Accuracy" test (see Figure 11). On this occasion we intentionally requested that the SD-WAN controller configure application policies as depicted in Table . Figure 16 depicts smart routing policy configuration for the UDP application on the SD-WAN controller.

To make sure that the defined policies were not bound to the link but to the application itself, we purposely steered two sets of application traffic towards the same link with different traffic policies applied on each of them.

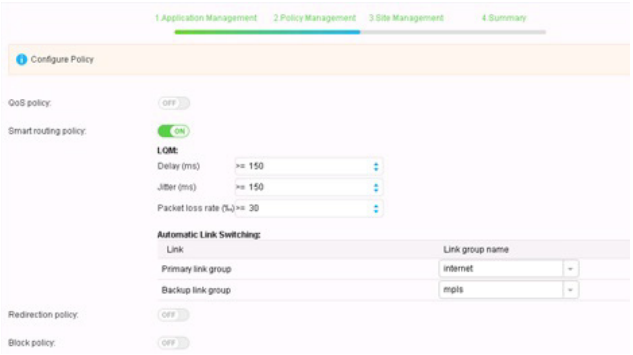


Figure 16: Smart Routing Policy for UDP Application

We started our test by validating that DSVPNs and application policies configured on the SD-WAN controller were correctly deployed on both CPE and hub nodes.

During this step, we observed a smart-policy-route installed on the SD-WAN CPE and hub nodes, reflecting the traffic policies defined on the SD-WAN controller. We initially ran baseline tests by generating

UDP, HTTP and FTP application traffic using either Spirent Test Center or a real application server, connected to the SD-WAN edge nodes to establish that the test bed was running correctly and experienced no loss. Indeed, UDP and HTTP traffic were steered towards the Internet and FTP towards the MPLS link and were received at the destination with no loss as expected.

	Applications		
	UDP	**HTTP**	**FTP**
Packet loss [%]	3	8	5
Packet delay [ms]	150	300	200
Packet delay variation [ms]	150	20	100
Working link	Internet	Internet	MPLS
Backup link	MPLS	MPLS	Internet

Table 1: SD-WAN Pre-defined Application Policies

We completed this test in three phases:

Phase 1. Degradation condition due to packet loss

As soon as this baseline procedure was successfully completed, we verified that despite the 2% constant packet loss introduced in the direction from branch to hub site using the impairment tool, UDP and HTTP were delivered over the Internet link as expected.

When we increased the value of the packet loss to 5% on the same link and in the same direction, we observed results that match our expectations: due to the excessive degradation condition on the Internet link, UDP traffic was rerouted to the MPLS link. HTTP traffic was steered towards the Internet and FTP towards the MPLS. We increased the packet loss on the Internet link to 10%. We expected UDP, HTTP, and FTP traffics to be all steered towards the MPLS as depicted in Figure 17.

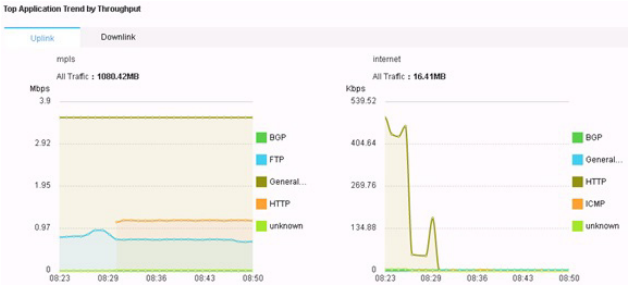


Figure 17: Intelligent Traffic Steering - Packet Loss Degradation Conditions

Once we disabled the impairment generation, we successfully validated that UDP and HTTP traffic were reverted back to the Internet link.

Phase 2. Degradation condition due to packet delay

As soon as phase 1 was successfully completed, we added a unidirectional constant delay of 100 milliseconds on all packets traversing the Internet link using the impairment generator. We expected no traffic to be rerouted by the SD-WAN solution. We then configured WANem to increase the delay on all traffic on the internet link to 160 milliseconds.

As expected, the SD-WAN solution moved the UDP traffic from the Internet link to the MPLS link. When we further increased the value of the packet delay on the Internet link to 350 milliseconds - excessive degradation condition on the HTTP traffic - the HTTP was successfully steered towards the MPLS by the SD-WAN solution as illustrated in Figure 18.

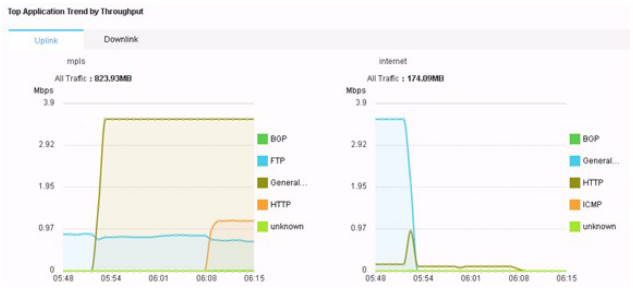


Figure 18: Intelligent Traffic Steering - Packet Delay Degradation Conditions

UDP and HTTP were steered again to the Internet link once the impairment generation was disabled.

Phase 3. Degradation condition due to jitter

To verify the degradation condition due to jitter, we first introduced a constant delay of 50 milliseconds and a jitter of 10 milliseconds on all packets on the Internet link. None of the application traffic was rerouted. When we increased the delay value to 100 milliseconds and the jitter to 50 milliseconds, the SD-WAN solution redirected HTTP traffic to the MPLS link, while the UDP remained on the Internet link as depicted in Figure 19.

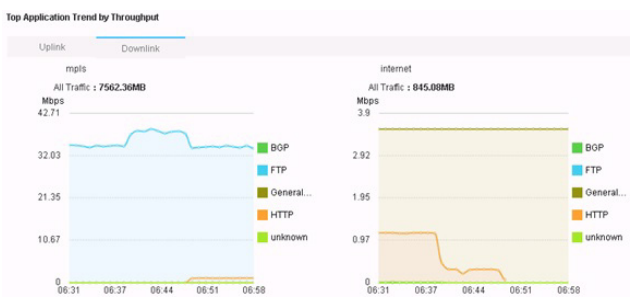


Figure 19: Intelligent Traffic Steering - Jitter Degradation Conditions

Conclusion

This section highlights the key results achieved during our test.

With the test areas selected by Huawei, we verified and measured the capability of their SD-WAN solution from a number of perspectives.

Based on the test results, we can confirm that the SD-WAN solution is meeting Huawei's claims. The solution is scalable in terms of number of DSVPNs that can be established on a single CPE node. A CPE successfully established up to 2,004 DSVPNs and remained manageable. No signs of performance degradation were observed during this test. To ensure the reliability of the solution, we ran a throughput test per CPE and per number of DSVPNs for a selected range of packet sizes, which showed acceptable results.

We also verified that Huawei's SD-WAN solution is equipped with failover mechanism to help service providers maintain operations during link and CPE failures.

The test results demonstrated that performance monitoring tools were functioning correctly and can be used by the SD-WAN edge nodes to provide visibility into application performance.

The application-based traffic steering scenario established that the Huawei's SD-WAN solution would make intelligent forwarding decisions based on policies and network conditions.

The observed results concludes that Huawei's SD-WAN solution offers a combination of CPE scalability for supporting a large number of DSVPNs, failover and application performance monitoring capabilities.

EANTC AG
Salzufer 14, 10587 Berlin, Germany
info@eantc.com, http://www.eantc.com/
[version v5] [date 20180129]