aruba
a Hewlett Packard Enterprise company

TECHNOLOGY BRIEF

ARUBA SD-WAN DYNAMIC PATH STEERING WITH SERVICE LEVEL AGREEMENTS

Policy-Based Application Visibility and Control

INTRODUCTION

Aruba SD-WAN's Dynamic Path Steering (DPS) feature provides visibility and a simple way to control network traffic over multiple WAN uplinks across distributed enterprises. Traditionally, branches were connected using MPLS with SLA guarantees; however, with the increasing adoption of Internet broadband circuits at the branch, it's vital for organizations to deploy DPS policies on the gateway to ensure a superior user experience while accommodating changing WAN conditions.

To achieve these benefits, DPS relies on loss, latency, jitter and utilization WAN performance measurements that are updated every few seconds per WAN link. DPS policies then determine the WAN uplinks that are best suited to satisfy the SLA for specific users, applications, and roles and destinations to intelligently steer traffic onto those links. This ensures that applications are sent over paths most appropriate to their needs.

DPS also allows the network administrator to define Service-Level Agreements (SLAs) for an application based on the same WAN path characteristics mentioned previously; the gateway will select a path based on which available link meets the SLA criteria. The selected forwarding path can be a single WAN uplink, or traffic can be load-balanced across a group of WAN uplinks. Load balancing algorithms are based on round robin, session counts, or utilization.

KEY BENEFITS

- Complete visibility and control over all enterprise WAN traffic
- Full enforcement of WAN Service Level Agreements (SLA)
- Path selection based on role-based policies for users, devices, and applications
- Intelligent routing based on real-time health monitoring of WANs link
- Load balancing across links based on round robin, utilization or session counts
- Supports private MPLS circuits, high speed Internet and LTE
- Ability to map application flows and those specific to roles to most-suited paths across the WAN

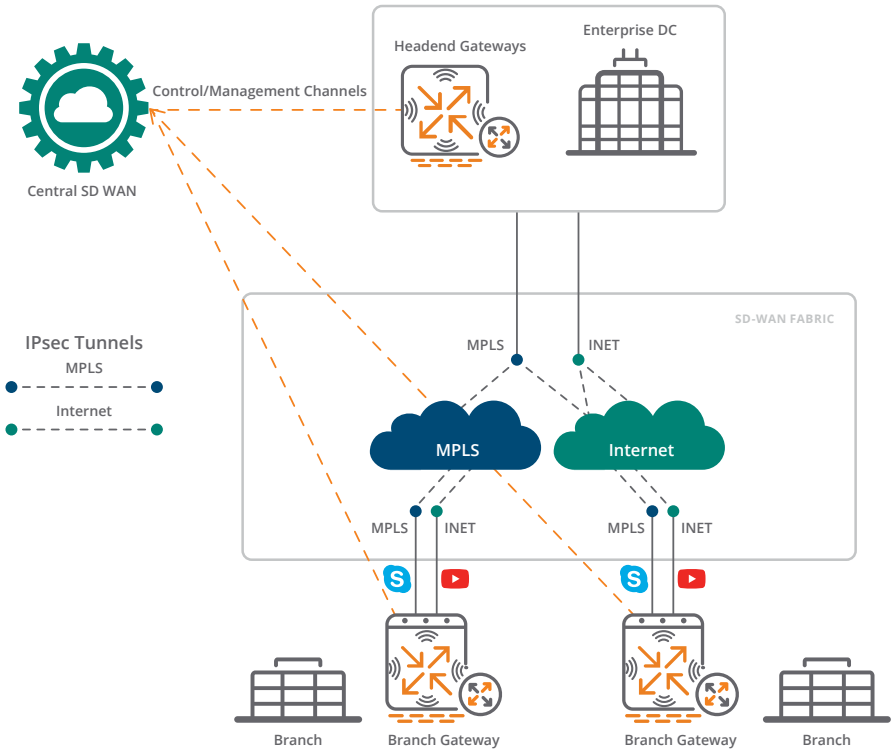

Figure 1: A Default Scenario for VoIP and Streaming Traffic over Different Link Types

SAMPLE DPS SCENARIO

In the following scenario (Figure 1), the two branches are using multiple uplinks; VoIP (Skype) traffic is defaulting to the MPLS uplink and YouTube is defaulting to the Internet uplink.

If the MPLS link does not meet the SLA for the Skype traffic, it will be redirected to the Internet link.

In the screen capture below (Figure 2), we see an example of where the MPLS link is not fully satisfying the agreed upon SLA. Because the SLA is not being met, the voice traffic fails over to the Internet link.

Figure 2: Compliance Summary for Branch Uplinks

USING PROBES AND MEASURING PATH QUALITY

In order to measure WAN quality, Aruba branch gateways will probe the installed Aruba headend gateways (measures latency, packet loss and jitter for applications reached through the SD-WAN overlay) or they use the Aruba Path Quality Monitoring Service (PQMS) for applications reached through the underlay. The PQMS is a distributed global probe responder that can be used to measure link quality on Aruba gateways managed by Aruba Central.

The points of presence (PoPs) for this global service are the following:

- Americas: North and South America
- EMEA: European Union
- APAC: Australia, China and Asia Pacific

In order to prevent Denial of Service (DoS) attacks, this probe responder is configured to rate-limit queries from anything other than branch gateways managed by Aruba Central. Once the health of an uplink is defined (using PQMS), Aruba's SD-WAN solution will probe headend gateways as well as the PQMS to monitor all uplinks (unless marked as backup). This allows the gateway to determine which links are meeting defined SLAs and which aren't. It then uses that information to make path steering decisions.

CONFIGURATION STEPS FOR APPLICATION-BASED POLICIES

This section discusses how to configure application-based routing policies on Aruba gateways. Figure 3 outlines a high-level overview of this process.

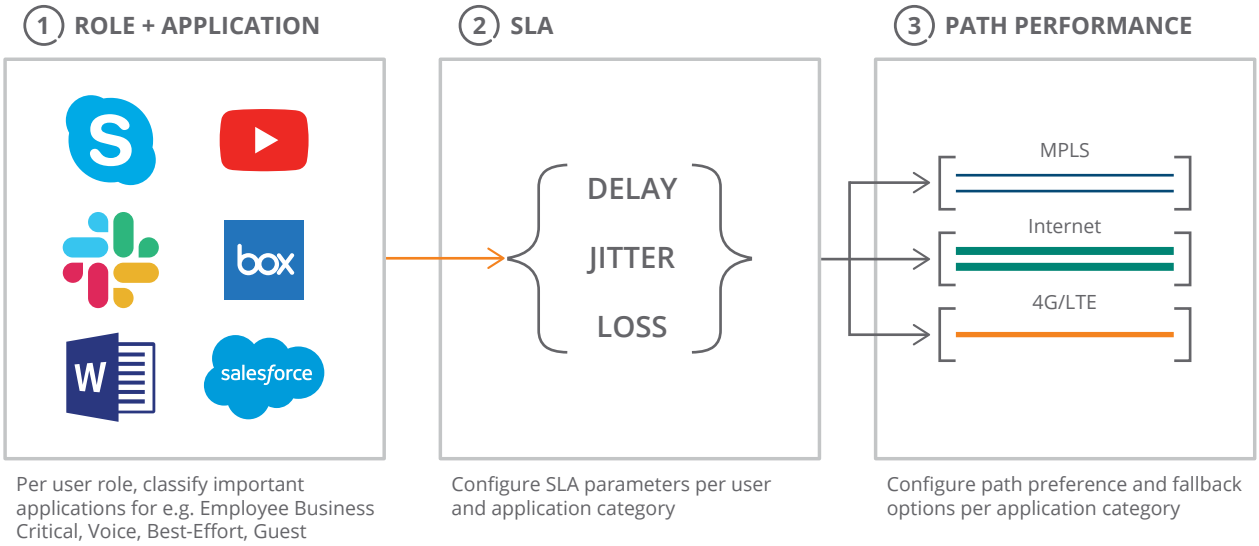

Figure 3: Dynamic Path Steering Overview

The SD-WAN solution is based on unified role-based application centric policies that centrally defined for all users and entities, and network domains. Not only can the administrator specify policies for approximately 3200 different applications, they can also leverage user and device roles to classify traffic (e.g. employee, contractor, and guest) or (e.g. camera, printer, or HVAC unit). Classifications include, but are not limited to applications thar are employee business critical, voice or video related, point of sale (PoS) specific, or related to guest Internet access. As such, the first step is to classify important applications that will be available per specific user or device roles.

The SLA parameters for each of these classifications can be setup per user and application category. The parameters include maximum values for delay, jitter, loss and utilization. For example, you can say that voice should never exceed a 150ms SLA, or have more than a 1% packet loss.

These settings determine the path preference (in this case, MPLS, Internet or LTE) and fallback options per application category, which you configure. For example, customers augmenting MPLS circuits with broadband links may configure user voice application flows to dynamically fail over to an Internet path without dropping the call. This delivers a minimal impact to voice quality upon re-steering from MPLS to the Internet links and vice-versa.

Setting up a DPS Policy

The process for setting up a policy is very easy and includes specifying "interesting" traffic, and choosing SLA parameters to measure the performance of the WAN. You then configure the path selection parameters for primary, secondary, and paths of last resort (Figure 4).

Here are the 3 required steps:

1. Specify classification rules for the specified mission-critical policy. In this case, the applications for these employees include Workday, Microsoft Exchange, and any traffic over Port 22 (i.e., FTP, SSH, or SMTP).
2. Specify required SLA thresholds. In this case, we are choosing from the following values, which are Highly Available, Best for Internet, or Voice traffic.
3. The last step is to define path preference by identifying which is the primary (MPLS in this case), the secondary path (Internet or LTE), or path of last resort (none in this case). In this example, the MPLS paths are favored for performance reasons, and the traffic is load balanced between two MPLS uplinks. If the threshold is not being met, then traffic will fail over to the secondary path, which would result in load balancing across all of the Internet uplinks.

Figure 4: A Sample DPS Policy for a Mission Critical Application

Policy and SLA Examples

As shown in the example above, DPS allows you to match the right characteristics specific to individual applications. There are traffic specification rules, SLA settings, and the corresponding path selection. Table 1 shows some other examples of policies assigned to different applications, and sample path selections as a result of whether those policies are being met.

The sample policy for Zoom is specific to collaboration and instant messaging traffic. This is being implemented at the branch because they only have Internet and Metro Ethernet options for cost reasons. In this case, traffic will be load balanced across those uplinks.

For the handling of SaaS traffic (types of traffic include Office 365, Salesforce and Dropbox), the matching of traffic is based on Deep Packet Inspection (DPI) which is performed on the SD-WAN gateway. The primary path for the SaaS traffic will be over the Internet; in the event of a failure, the plan is to switch over to a local data center via the MPLS uplink that connects to a local metro Ethernet network, and proceed to the SaaS cloud from there.

Corresponding SLA numbers for the recreational Internet use case are also shown. Types of traffic may include streaming or social networking apps such as YouTube or Netflix. Most businesses will not set an SLA for this, but it would be very common this traffic to follow the Internet path and if the Internet link is down to use the cellular 4G/LTE link (path of last resort).

Measuring service level agreements

The SLA measurements that influence DPS may be user configurable or passive. When passive, they are updated at a frequency of two seconds. As previously discussed, latency is measured by probes sent over the WAN uplinks. There is also a probe sent to the PQMS (pqm.arubanetworks.com) to ensure consistency of the measurement. When an SLA parameter violates the SLA policy, the application/role is moved to the specified second uplink.

If none of the WAN uplinks meet the specified SLA, then the payload is always sent to the best link (i.e., the link with the "least unsavory" SLA). When traffic is steered to a second link, and other traffic is using that link as a primary link, QoS parameters can be set to ensure the newer traffic steered to the second link will have priority over the traffic already using that link.

TABLE 1: SAMPLE POLICIES, TRAFFIC SPECIFICATION, SERVICE LEVEL AGREEMENTS AND PATH SELECTION

Policies	Traffic Specification	SLA	Path Selection
Zoom	Collaboration and instant messaging traffic	Latency < 150 ms. Jitter < 30 ms.	Primary: Fast Internet, MPLS Metro Ethernet (load balanced)
SaaS	Office 365, Salesforce and Dropbox	Latency < 150 ms. Jitter < 150 ms. Loss < 1%	Primary: Fast Internet Secondary: MPLS Metro Ethernet (failover if SLA not met)
Recreational Internet	Streaming or social networking	Latency < 150 ms. Jitter < 150 ms. Loss < 1%	Primary: Fast Internet Secondary: MPLS Metro Ethernet

MONITORING PATH STEERING

The details for path sterring provide a summary of how your policies are being met. in the following use case (Figure 5), you are able to investigate how a single application is performing.

The monitoring dashboard informs the administrator of the DPS policies that are active and whether they are compliant with configured SLA thresholds. An administrator can then drill down into each policy to see how the individual policy has behaved over a selected time-span (3 hours, past day, past week, etc.). They can also see which links were chosen by the policy to send the application traffic, and when the WAN links were out of compliance. The details allow an administrator to quickly determine how configured policies are working, and how compliant they are with their SLA's.

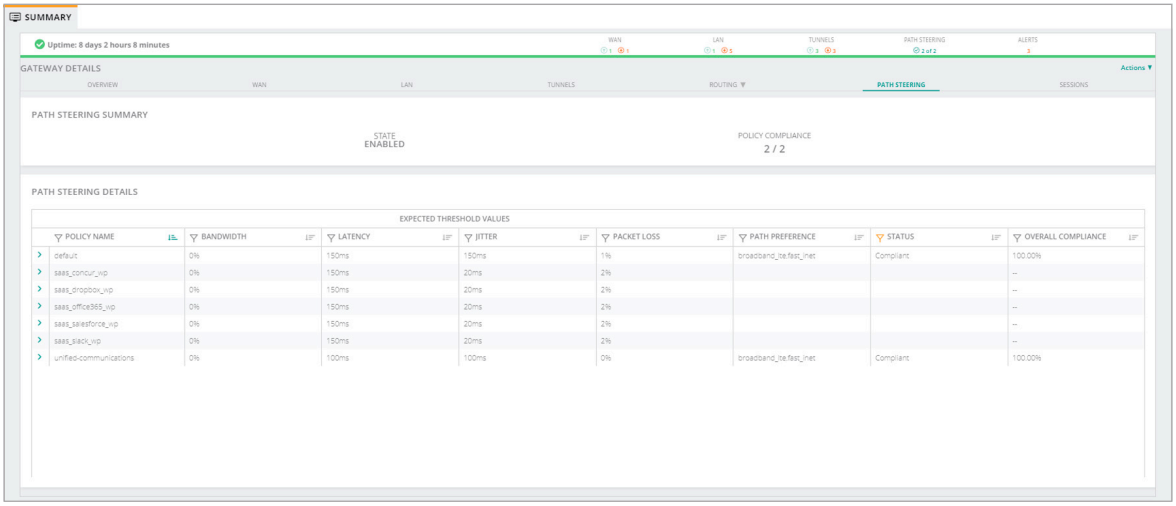

Figure 5: Path Steering Details on a Gateway

Figure 6: Expanded Policy Compliance Graph

THE MONITORING OF APPLICATION PERFORMANCE

You can check on all the traffic types for which you have set policies individually. You can also go to the application dashboard (Figure 7), which lists all of the critical applications to see information such as bandwidth used (sent and received) per application.

Selecting an individual application lets you see key performance indicators (KPI) and a graphical view of usage information (Figure 8). An admistrator can see the loss, latency and jitter score, calculated at an application level. If the DPS policies are indeed effective, then the administrator should expect to see it reflected in application performance KPIs.

All of this is shown in real time, along with the historical view.

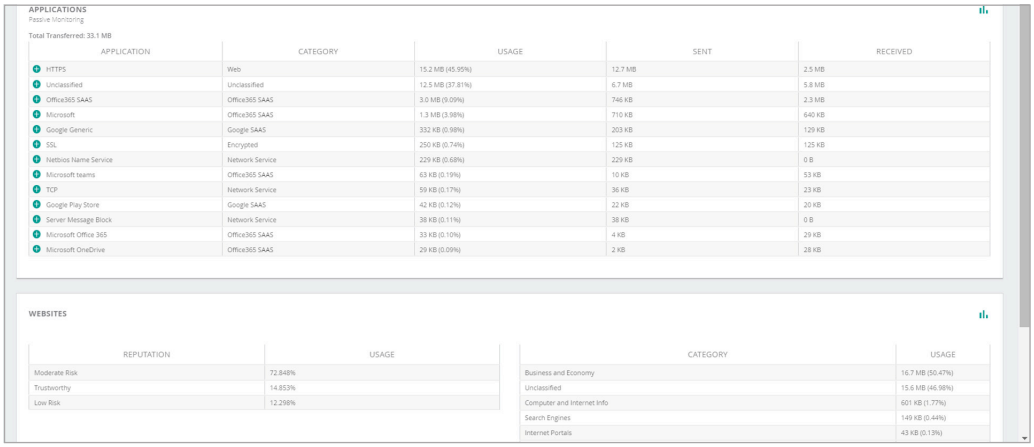

Figure 7: Gateway Application Details

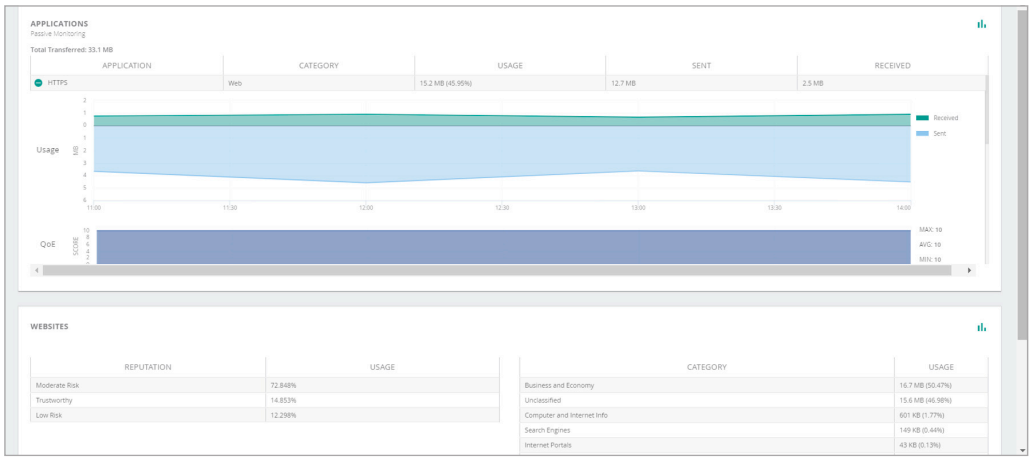

Figure 8: Key Performance Indicator Application View

CONCLUSION

DPS policies significantly improve the overall health of a WAN environment and the user experience at the branch. By continuously probing all available paths for WAN metrics, and dynamically steering traffic across available WAN uplinks in real-time, DPS policies ensure application traffic is always sent over the best available WAN links.

This allows an administrator to make optimal use of available uplink resources that match specific criteria—such as latency, jitter, packet loss and utilization—to help determine the choice of an uplink. It would be impossible for an administrator to orchestrate this without the use of Dynamic Path Steering.

TB_SDWANDynamicPathSteering_101819 a00091188enw