Technical Disclosure Commons

Defensive Publications Series

November 2020

MEASURING LOSS, LATENCY AND JITTER BASED ON APPLICATION TYPES TO IMPROVE APPLICATION ROUTING DECISIONS

Sireesha Yeruva

Satyajit Das

Nirmal Govindan

Sai Swarna Latha Vempaty

Priyanka Chidambar Patil

MEASURING LOSS, LATENCY AND JITTER BASED ON APPLICATION TYPES TO IMPROVE APPLICATION ROUTING DECISIONS

AUTHORS:
Sireesha Yeruva
Satyajit Das
Nirmal Govindan
Sai Swarna Latha Vempaty
Priyanka Chidambar Patil

ABSTRACT

Current Software Defined Wide Area Network (SDWAN) solutions typically utilize a Service Level Agreement (SLA) definition in conjunction with policy to match and classify traffic types in order to direct traffic over SDWAN tunnels. An SLA definition can include values of loss, latency, and jitter, which are measured via a Bi-directional Forwarding Detection (BFD) channel that exists between two Transport Locators (TLOCs). These values collectively represent the liveliness of a network including the status of the BFD link. In current implementations, BFD control messages are sent with a high priority Differentiated Services Code Point (DSCP) marking, such as '48'. SLA metrics based on such a high priority packet, however, do not reflect the priority that it will be received by the actual data that flows through an edge device. Techniques presented herein address such issues by providing for a more accurate representation or measurements of loss, latency, and jitter for various desired traffic profiles for a network along with capabilities to use such measurements to direct different traffic types to correct tunnels.

DETAILED DESCRIPTION

Current SD-WAN solutions have the capability to direct traffic to next-hops based on SLA definitions. These SLA definitions, in conjunction with policy to match and classify traffic types, can be used to direct traffic over specific SDWAN tunnels.

An SLA definition typically includes of values of loss, latency, and jitter, which are measured via the BFD channel that exists between two TLOCs (e.g., WAN Interfaces). These values collectively represent the liveliness of network including the status of the BFD link. In current implementations, BFD control messages are sent with a high priority DSCP marking, such as '48'.

SLA metrics based on this high priority packet, however, do not reflect the priority that will be received by actual data that flows through an edge device. This is because the data (depending on the application class) can potentially be sent with different DSCP values; thereby receiving a different routing treatment from the underlying network.

Accordingly, a more accurate representation of the loss, latency, and jitter for various traffic profiles may be desired for networks along with the capabilities to use such measurements to direct traffic types to the right tunnels.

Application aware routing (app-aware-routing) typically uses policies that constrain paths that can be used to perform forwarding for an application. Constraints are usually expressed in terms of SLA-classes that contain loss, latency, and jitter requirements that must be met. This requires that these metrics be measured on all the paths to the destination of the traffic. Broadly methods to measure metrics can be classified into:

- Active Probing;
- Passive Monitoring; and
- A Hybrid of Active Probing and Passive Monitoring.

Active probing methods include generation of synthetic traffic that is injected along with real traffic. The expectation is that per-hop behavior will not differentiate between the synthetic traffic and actual traffic (i.e., probes and real traffic would be forwarded the same way). Examples of active probing mechanisms include BFD probing, Internet Control Message Protocol (ICMP) messaging, periodic HyperText Transfer Protocol (HTTP) requests, and Internet Protocol (IP) SLA measurements.

Passive monitoring methods rely on deep packet inspection (DPI) and monitoring of actual traffic. For example, Real-time Transport Protocol (RTP)/Transport Control Protocol (TCP) traffic can be monitored using passive techniques to measure loss, latency, and jitter.

Hybrid techniques have been used in the past that leverage a combination of passive/active techniques, such as through the generation of synthetic traffic in the absence of actual data traffic that can be measured. For overlay networks, an alternative to monitoring actual data traffic is to insert a "monitoring" Protocol Data Unit (PDU) into encapsulation headers of a packet transmitted over an overlay. The packet could carry all the information needed to determine the metrics over the overlay network. This alleviates the protocol/format of the data being monitored and allows for better scaling.

From the viewpoint of metrics, loss, latency, and jitter are typically side effects of over provisioned and congested networks. One of the challenges with active measurement techniques is that the frequency of probe generation should be chosen carefully—enough to detect congestion in the network and measure jitter/loss, while not generating so much traffic that it causes congestion.

Typically, voice and video applications are sensitive to jitter and delay. It becomes essential to have higher frequency of probing in the network for determining jitter and latency to route these classes of traffic correctly. In addition, these two classes of traffic typically warrant a quicker switch/convergence to a better link in instances when the metrics cross the thresholds set in the SLA-class.

Measurements alone do not force reconfiguration of the overlay next-hops. For this, a convergence time is needed. Typically for a network design, the lowest required convergence timer necessitated by traffic type should be used for the overall convergence period of the device.

Typically, current SDWAN implementations utilize active probing with BFD. While it is possible to progress to a more hybrid approach, the first step is to address the immediate problem – metric accuracy. Therefore, a first phase of this proposal is to perform the following:

- Perform measurements using BFD @ 10pps (pulse per second) for metrics (e.g., loss, latency, and jitter);
- Enqueue BFD probe packets to the configured output queue of an interface;
- Mark BFD probes with configured DSCP values; and
- Measure liveliness/reachability of the network on the default DSCP configured value, which would continue to be defaulted to its current value of '48'.

A second phase of this proposal involves striving to measure the metrics from data (i.e., utilizing passive monitoring based techniques) by:

- Carrying metadata in overlay headers to help aid in measurements; and

- Responding back with a generated probe if there is no data to send back to the receiver. The generated probe would carry the metadata back for the sender to utilize in app-aware-routing calculations.

Figure 1, below, illustrates example operational details associated with techniques of this proposal.

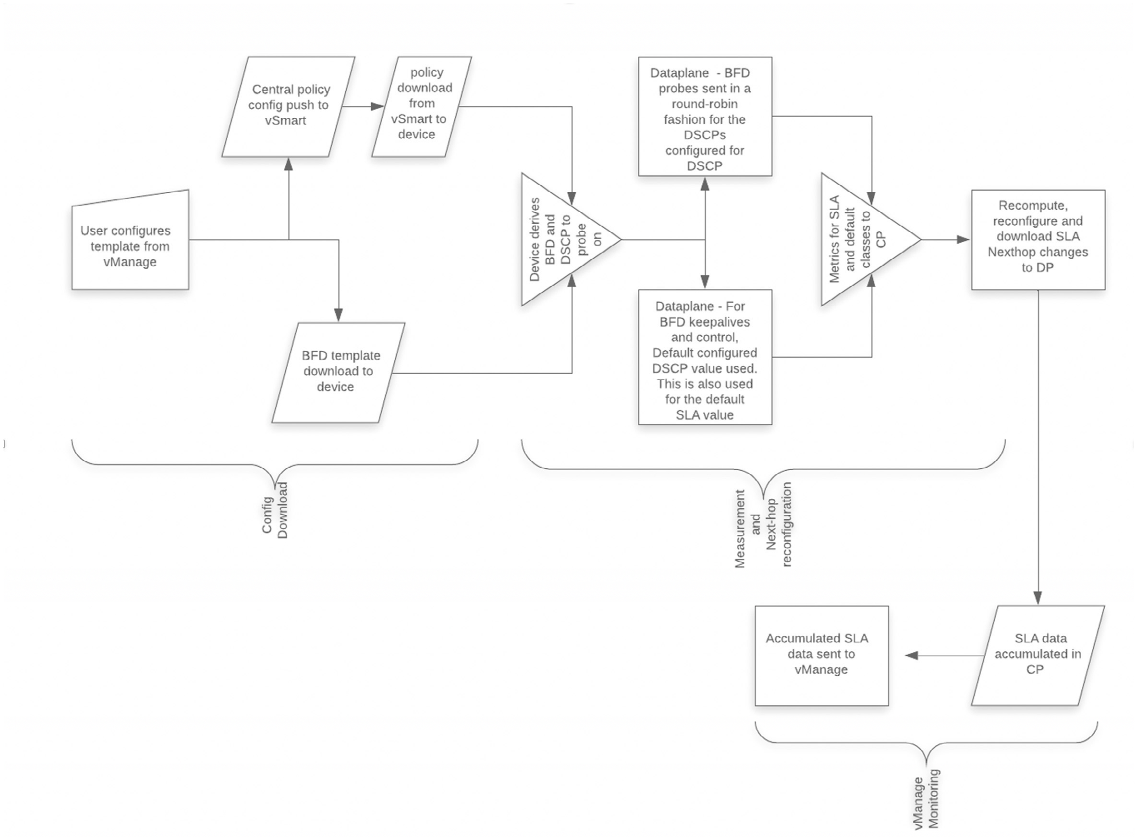
Central policy config push to vSmart
policy download from vSmart to device
User configures template from vManage
BFD template download to device
Device derives BFD and DSCP to probe on
Dataplane - BFD probes sent in a round-robin fashion for the DSCPs configured for DSCP
Dataplane - For BFD keepalives and control, Default configured DSCP value used. This is also used for the default SLA value
Metrics for SLA and default classes to CP
Recompute, reconfigure and download SLA Nexthop changes to DP
Config Download
Measurement and Next-hop reconfiguration
SLA data accumulated in CP
Accumulated SLA data sent to vManage
vManage Monitoring

Figure 1: Example Operational Details

As illustrated in Figure 1, techniques of this proposal may include a configuration download portion, a measurement and next-hop reconfiguration portion, and a monitoring portion. In the configuration download portion, a user may configure a template by interfacing with a network management system (such as vManage). A BFD template may be downloaded to a device, and a central policy configuration may be pushed to a system controller (such as vSmart). The policy may then be downloaded from the system controller to the device. The method may then proceed to the measurement and next-hop reconfiguration portion.

In the measurement and next-hop reconfiguration portion, the device derives the BFD and DSCP to probe on. In the dataplane, BFD probes are sent in a round-robin fashion for the relevant DSCPs. Also in the dataplane, for BFD keep-alives and control, a default configured DSCP value is used. This can also be used for the default SLA value. Metrics for the SLA and default classes can be sent to a control plane. The metrics can be used for reomputing, reconfiguring, and downloading SLA nexthop changes to the dataplane. The method may then proceed to the monitoring portion.

In the monitoring portion, the SLA data is accumulated in the control plane and the accumulated SLA data is sent to the network management system.

In summary, the SLA metrics based on a high priority packet might not reflect the priority that will be received by the actual data that flows through the edge device. This is because, the data (depending on the application class) can potentially go out with different DSCP values thereby getting a different treatment from the underlying network. Therefore, a more accurate representation of the loss, latency, and jitter for the traffic profiles may be desired for the networks along with the capabilities to use such measurements to direct traffic types to the right tunnels.

In some instances, techniques of this proposal may provide advantages compared to systems for which SLA definition characteristics are determined via a BFD channel that uses only the high priority DSCP marking. For example, techniques herein provide for the ability to determine SLA characteristics based on configured DSCP and the potential queuing mechanism used by the actual traffic.

In still some instances, techniques of this proposal may provide advantages compared to systems that determine SLA definition characteristics via metadata riding on top of actual traffic. For example, systems that determine SLA definition characteristics via metadata riding on top of actual traffic may have limitations in the sense that SLA characteristics are dependent on regular data traffic on all the tunnels and the initial data traffic will not have the characteristics available. The metadata approach consumes bandwidth which is highly dependent on the data rate. By contrast, techniques of this disclosure provide a better control on the overall bandwidth consumption.

Accordingly, techniques provided herein that may include determining loss, latency, and jitter measurements associated with a traffic profile, wherein the loss, latency, and jitter measurements are determined for each of a plurality of paths to a destination; determining a path for sending data corresponding to the traffic profile, the path determined from the plurality of paths based on comparing the loss, latency, and jitter measurements to a service level defined for the traffic profile; and sending the data corresponding to the traffic profile via the determined path.

Figure 2, below, illustrates an example a network 200, such as an SD-WAN in which techniques of this proposal may be implemented.

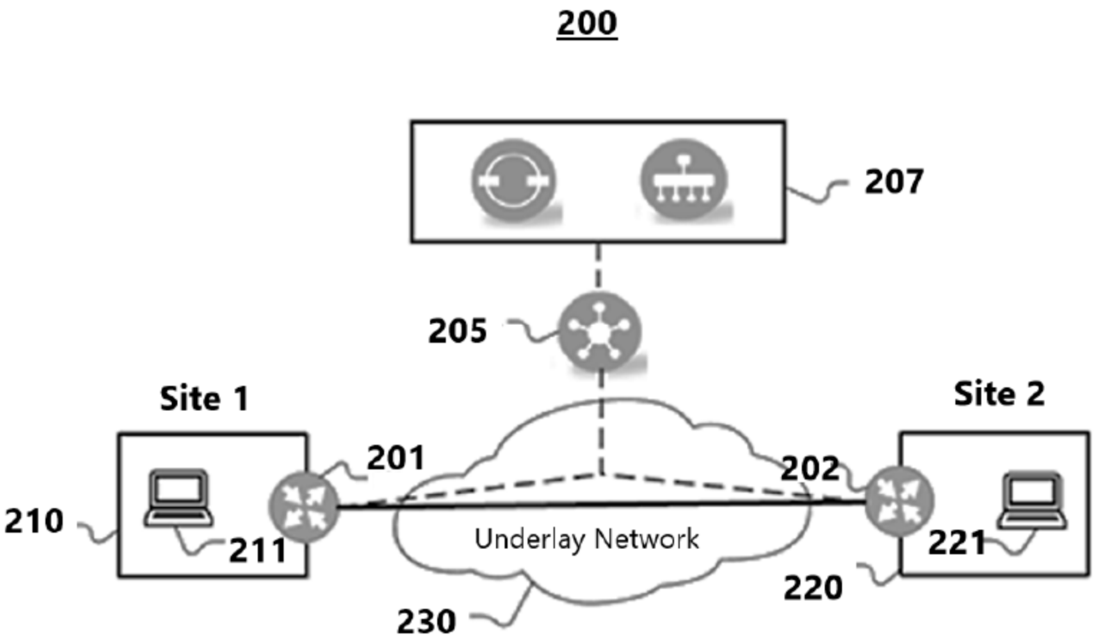

Figure 2: Example Network Implementation

An SD-WAN may include a virtual overlay network based on tunnels that carry traffic between a plurality of sites over one or more underlay networks 130. The example illustrated in Figure 2 shows two sites: a first site 210 and a second site 120. Each site may connect to the network 200 via one or more WAN-edge routers. For example, the first site 210 connects to the network 200 through an edge router 201, and the second site 120 connects to the network 200 through an edge router 202. A site connected to the network 200 may have a data plane connection to each of the other sites through Internet Protocol Security (IPSec) tunnels. The edge routers 201 and 202 may have a data plane connection over the underlay network 130. The underlay network 130 may comprise Multiprotocol

Label Switching (MPLS), Internet, and cellular networks. An SD-WAN control plane may comprise a controller 205 that may maintain a centralized routing table and the routing policies to program the forwarding behavior of the data plane. The controller 205 may maintain direct control plane connection to each edge router. The controller 205 may provision, maintain, and secure the entire overlay network. The SD-WAN network 200 may also comprise management/orchestration plane 207. Although this disclosure describes a SD-WAN network in a particular manner, this disclosure contemplates a SD-WAN network in any suitable manner.

In summary, various technical advantages of these techniques may include one or more of: allowing for more accurately determining loss, latency, and jitter measurements associated with traffic profiles; utilizing the metrics in determining where to direct various traffic types; improving the likelihood of different types of traffic being direct to the right tunnel (e.g., a tunnel that allows the SLA associated with that type of traffic to be met) and may provide better control on overall bandwidth consumption; and/or obtaining the loss, latency, and jitter measurements based on a probing technique that manages probe generation so that the probe generation does not occur so frequently as to cause traffic congestion in the network.