December 2020

ADAPTIVE MODELS FOR NEXT GENERATION WIDE AREA NETWORKS

Balaji Sundararajan

Brandon Lynch

Gayathri Chandrasekaran

Reuel Gatus

Zaheer Aziz

ADAPTIVE MODELS FOR NEXT GENERATION WIDE AREA NETWORKS

AUTHORS:
Balaji Sundararajan
Brandon Lynch
Gayathri Chandrasekaran
Reuel Gatus
Zaheer Aziz

ABSTRACT

A software-defined wide area network (SD-WAN) controller in a cloud service delivery architecture may encounter a number of challenges including, for example, timeouts, download or push failures, etc. To address challenges of these types techniques are presented herein that support a holistic solution. Aspects of the solution comprise, among other things, understanding a device's ability to process configuration in a real-time network and staggering a configuration push based on, for example, a device's ability to process and consume configurations. Aspects of the solution employ, for example, the use of bandwidth knowledge to force a centralized network management system control connection to come up on a specific wide area network (WAN) interface that has higher bandwidth availability, the collection of network characteristics to profile a device's behavior for receiving different types of policies from a SD-WAN controller, the scheduling of SD-WAN customer premise equipment (CPE) devices for configuration delivery in an ordered fashion such that the devices that are chosen are the ones with the least WAN congestion, the profiling of device connectivity patterns to provide guaranteed service-level agreement (SLA) commitments for policy enforcement, the possible use of "dummy templates" for diagnostic purposes, etc.

DETAILED DESCRIPTION

Currently a SD-WAN controller in a cloud service delivery architecture may suffer from, possibly among other things, a large scale time out of WAN edge clusters, software download failures, and security policy push failures. Such occurrences may result in a customer escalating such incidents to a networking vendor leading to, for example, a possible loss of business for the vendor.

To address challenges of these types, which are business critical for SD-WAN business, techniques are presented herein that support a holistic solution. Various of the features that are encompassed under that solution are discussed in the following narrative in connection with Figures 1 and 2, below.

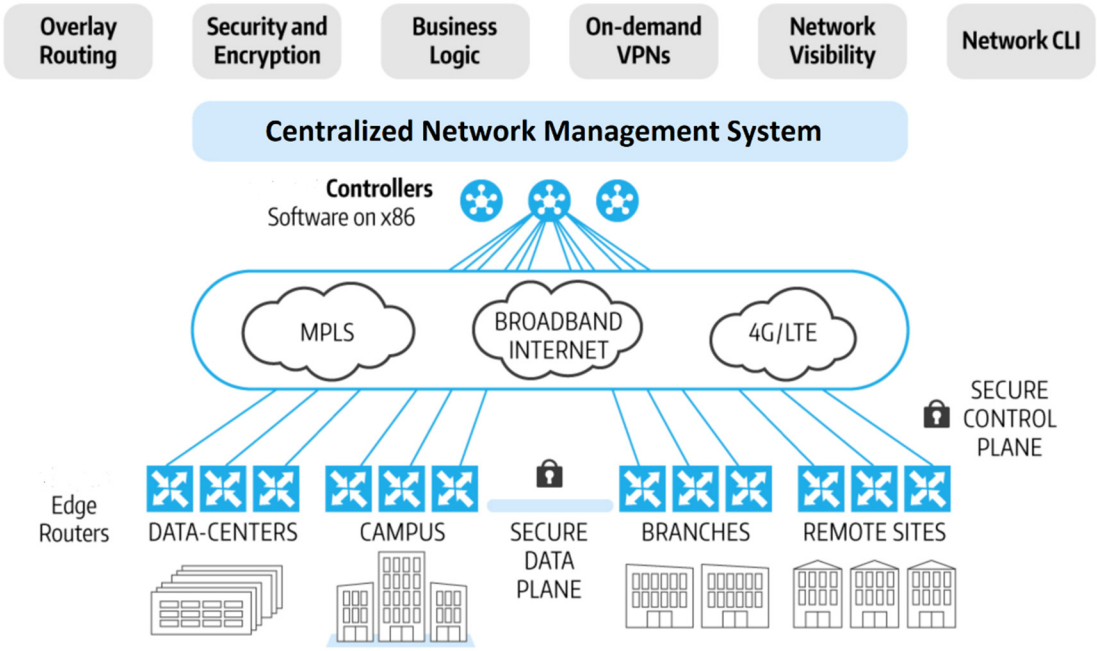

Figure 1: Illustrative Network Environment

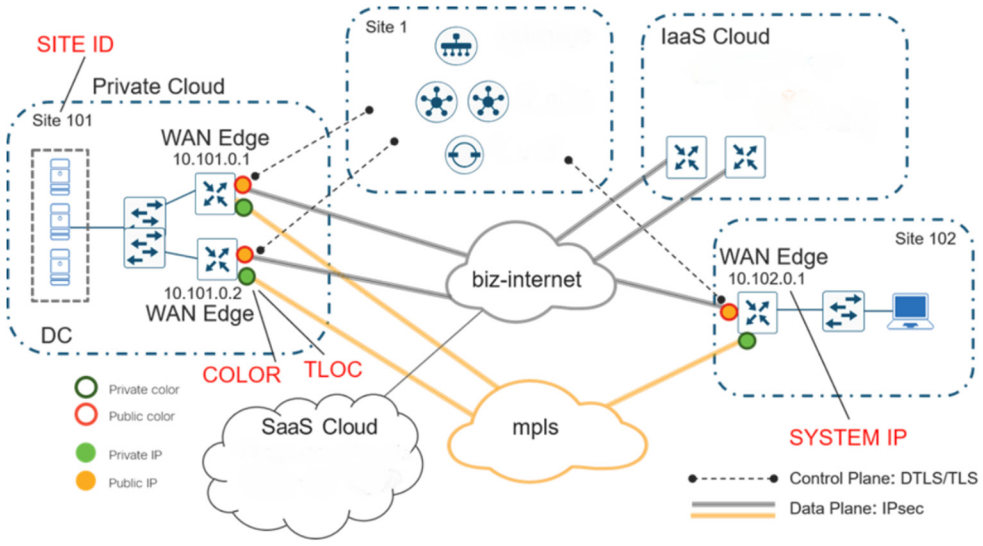

Figure 2: Illustrative Topology

One feature that is of interest in connection with the techniques presented herein comprises using, at each SD-WAN site, bandwidth knowledge to force a centralized network management system control connection to come up on a specific WAN interface that has higher bandwidth availability. Note that this is in contrast to the current approach of selecting a WAN interface that just has Internet Protocol (IP) reachability.

Additionally, network characteristics may be sent on the WAN and reported to a network analytics facility. The collected knowledge may be used to, for example, profile a device's behavior for receiving different types of policies from a SD-WAN controller. Further, SD-WAN CPE devices may be scheduled for configuration delivery in an ordered fashion such that the devices that are chosen are the ones with the least WAN congestion. Additionally, device connectivity patterns may be profiled to provide guaranteed SLA commitments for policy enforcement.

A control plane policer may be dynamically adjusted based on network activity such as, for example, software downloads, configuration policy (which may comprise a large number of lines) such as for a zone-based firewall (ZBFW), and other such configuration-heavy delivery. This would enable customers to enjoy a better network experience from a configuration delivery perspective.

The health of control connections to SD-WAN controllers may be monitored (for, possibly among other things, loss, latency, available bandwidth, etc.). Note that this should not be confused with Bidirectional Forwarding Detection (BFD) monitoring. Depending upon the health of a control connection, a daemon process may periodically connect over all of the paths and collect, for example, tunnel characteristics.

Additionally, support on a centralized network management system and on an end device may be evaluated for the pushing of "dummy templates" for diagnostic purposes, providing more insight into the performance at a particular transport locator (TLOC) including, for example, push and commit times. A daemon process may, at periodic intervals, evaluate the best performing paths on the CPE and switch the control connection to that TLOC.

Central to the techniques that are presented herein is an ability to schedule CPE devices based on a reporting for configuration changes and an ability to switch daemon

process connections based on, for example, network conditions resulting in significantly improved network performance for SD-WAN controllers.

Through the narrative that was presented above (and in connection with Figures 1 and 2, above) various WAN considerations of different devices may be evaluated to, for example, identify the business critical sites/devices that should receive policies first.

In summary, techniques have been presented that support a holistic solution to the various challenges that were discussed in the above narrative. Aspects of the presented techniques encompass, for example, the use of bandwidth knowledge to force a centralized network management system control connection to come up on a specific WAN interface that has higher bandwidth availability, the collection of network characteristics to profile a device's behavior for receiving different types of policies from a SD-WAN controller, the scheduling of SD-WAN CPE devices for configuration delivery in an ordered fashion such that the devices that are chosen are the ones with the least WAN congestion, the profiling of device connectivity patterns to provide guaranteed SLA commitments for policy enforcement, the possible use of "dummy templates" for diagnostic purposes, etc.