Enterprise Case Study

Using Atrinet Network Controller with Segment Routing PCE in a big enterprise in Israel

Overview

The customer is a big enterprise in Israel that build a private IP/MPLS network based on Cisco devices and NetFusion network controller. The network services are mainly L2 VPN (EVPN VPWS). The customer needs to discover the network topology, including updates on any network topology and resources changes, as well having path computation and bandwidth admission control helping to automate network provisioning. Atrinet NetACE™ Segment Routing management coupled with PCE provides the customer the required traffic engineering and automate the network services provisioning.

NetACE™ Solution

NetACE™ is used as a Packet Network Controller with PCE layer between the network devices domains and NetFusion – the hierarchical network controller. NetACE™ provides the enterprise the ability of topology discovery that is done by BGP-LS, incl. domain stitching and link parameters (delay, SRLG, affinity, etc.). NetACE™ optimize network resources by detecting any topology change, such as additional device/link, updating NetFusion controller and re-compute all affected Segment Routing policies according to the new topology.

NetACE™ provides **segment routing PCE** that enables the customer to use bandwidth CAC (Connection Admission Control) and path computation helping to automate the service provisioning in the network.

NetACE™ also provides an open API to NetFusion network controller including service and LSPs discovery.

Customer Challenges

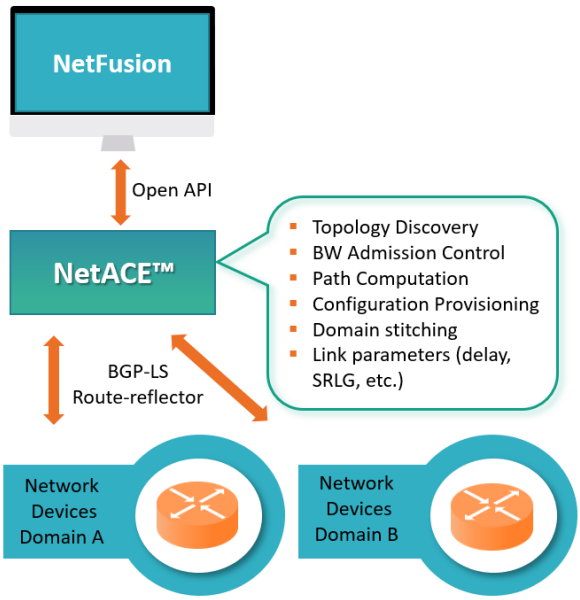
- *Service provisioning*
- *Automatic topology discovery for equipment, services and real-time network resource changes*
- *Visual display of current network devices and services topology*
- *Bandwidth Admission Control*
- *Path Computation*
- *Open APIs towards the network controller*

NetACE™ Segment Routing PCE:

» ***Provision*** services, by point-and-click, assuring the shortest path and guaranteed SLA. It also automatically assigns a secondary path

» ***SRLG*** – to prevent any scenario of a network failure caused by a set of links that are sharing a common risky resource

» ***Selected list*** (whitelist /blacklist) that helps the service provider to overcome known constraints of the network, by binding services to pass via specific selected links or bypass them



Customer Benefits

» Very agile solution to match special features required by the customer

» Providing on-line traffic engineering capabilities across multi-domains

» Solving the scalability challenges of MPLS networks

Atrinet
Intelligent Network Automation