Segment-Routing-Development

Case-study

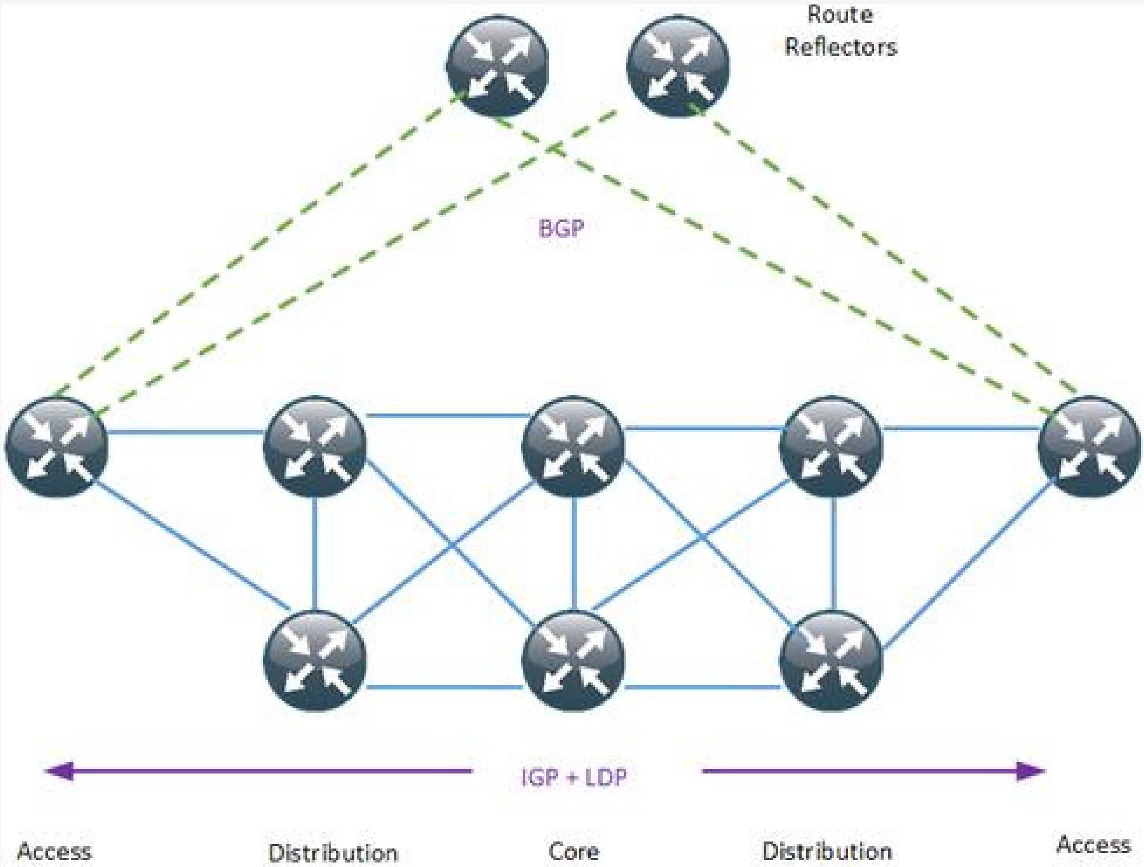
1. Introduction

This document describes the project undertaken by PalC Networks for developing **Segment Routing Features.**

1.1. Segment Routing Introduction

Segment Routing is a new source routing technology that will add benefit to IP and MPLS networks. It will allow to have FRR protection for any topology, simpler to operate and more scalable. For future SDN services it provides a quicker interaction with the applications. Segment routing is a technology that is gaining popularity as a way to simplify MPLS networks. It has the benefits of interfacing with software- defined networks and allows for source-based routing. It does this without keeping state in the core of the network.

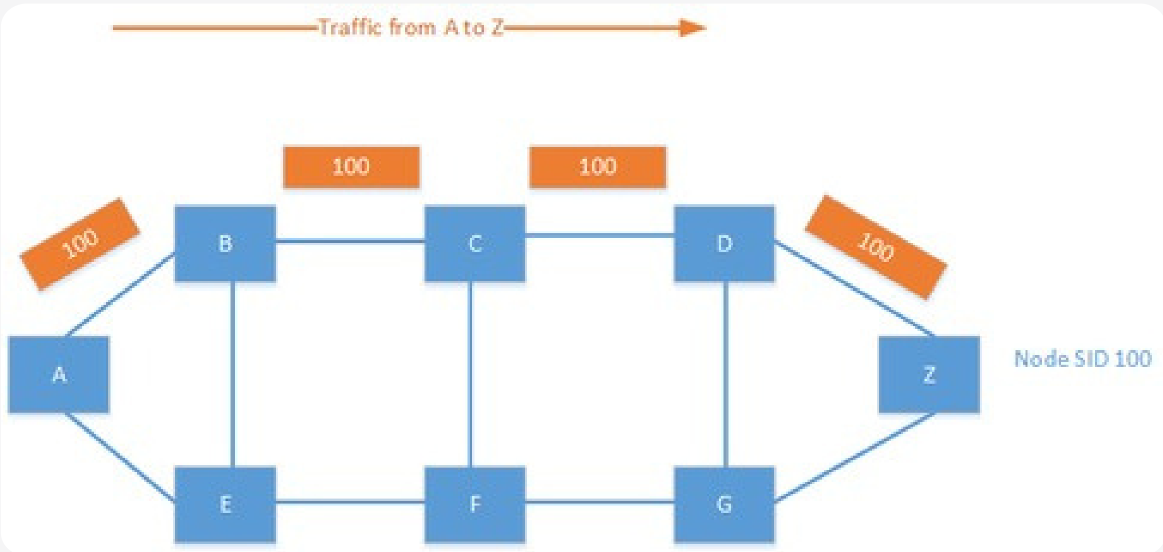
Multi-Protocol Label Switching (MPLS) is the main forwarding paradigm in all the major service providers (SP) networks. MPLS, as the name implies, uses labels to forward the packets, thus providing the major advantage of a Border Gateway Protocol (BGP)-free core. To assign these labels, the most commonly used protocol is the Label Distribution Protocol (LDP). A typical provider network can then look like the diagram below.

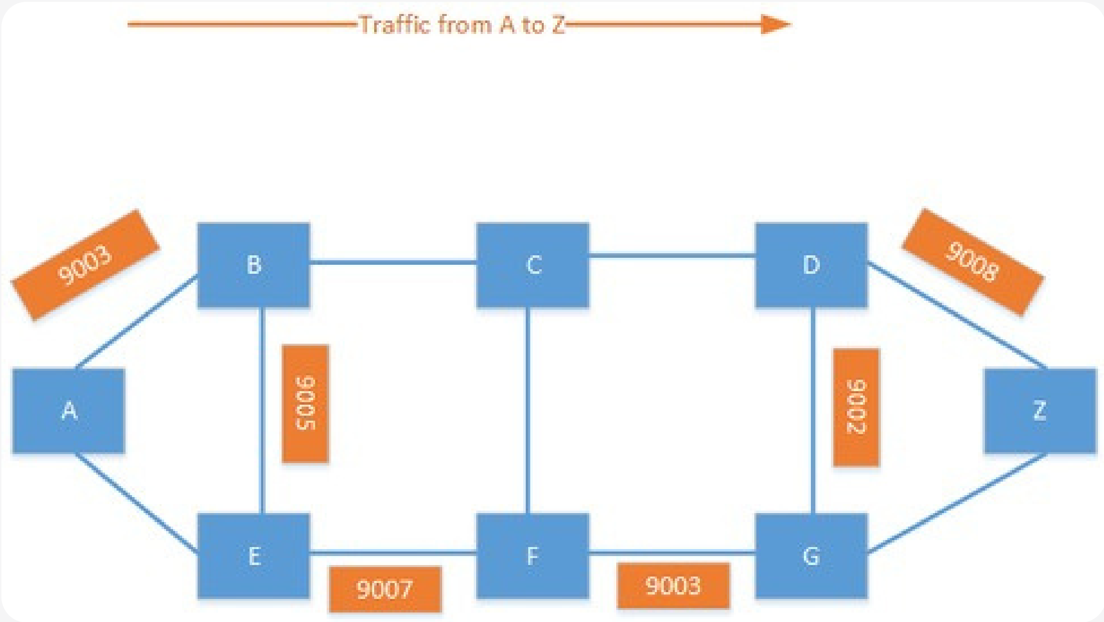


In order to provide stability and scalability, large networks should have as few protocols as possible running in the core, and they should keep state away from the core if possible. That brings up some of the drawbacks of LDP:

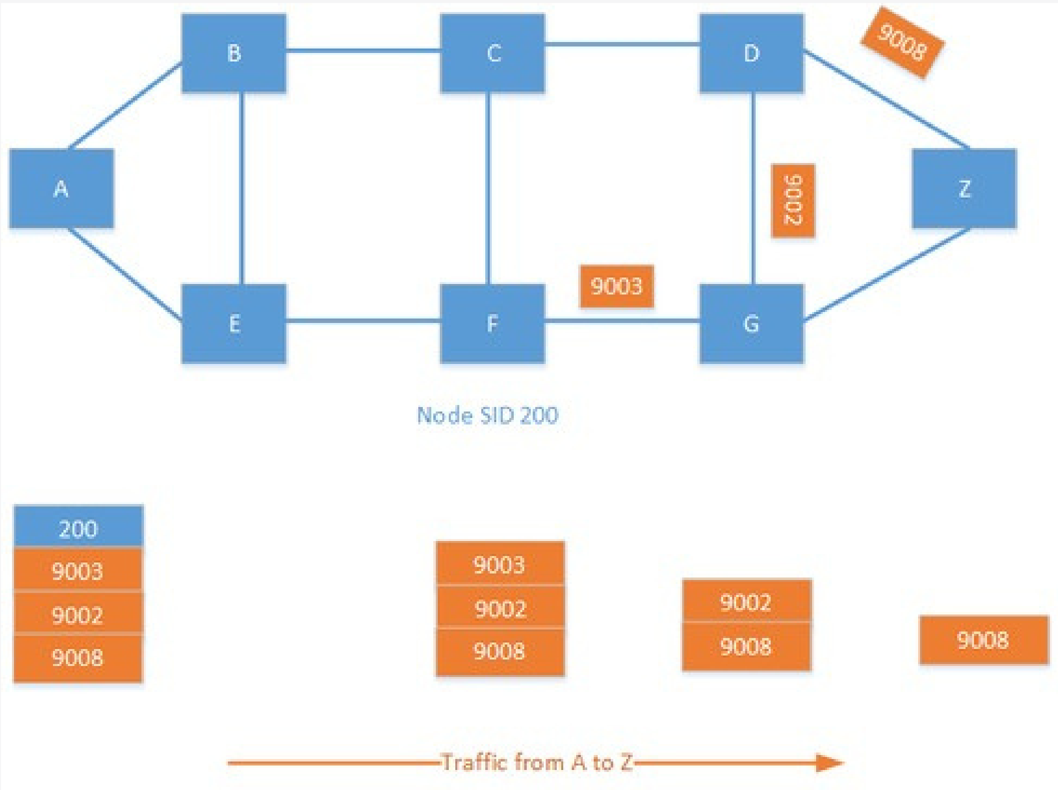
- It uses an additional protocol running on all devices just to generate labels.
- It introduces the potential for blackholing of traffic, because Interior Gateway Protocol (IGP) and LDP are not synchronized.
- It does not employ global label space, meaning that adjacent routers may use a different label to reach the same router.
- It's difficult to visualize the Label Switched Path (LSP) because of the issue above It may take time to recover after link failure unless session protection is utilized.

Segment routing is a new forwarding paradigm that provides source routing, which means that the source can define the path that the packet will take. SR still uses MPLS to forward the packets, but the labels are carried by an IGP. In SR, every node has a unique identifier called the node SID. This identifier is globally unique and would normally be based on a loopback on the device. Adjacency SIDs can also exist for locally significant labels for a segment between two devices.

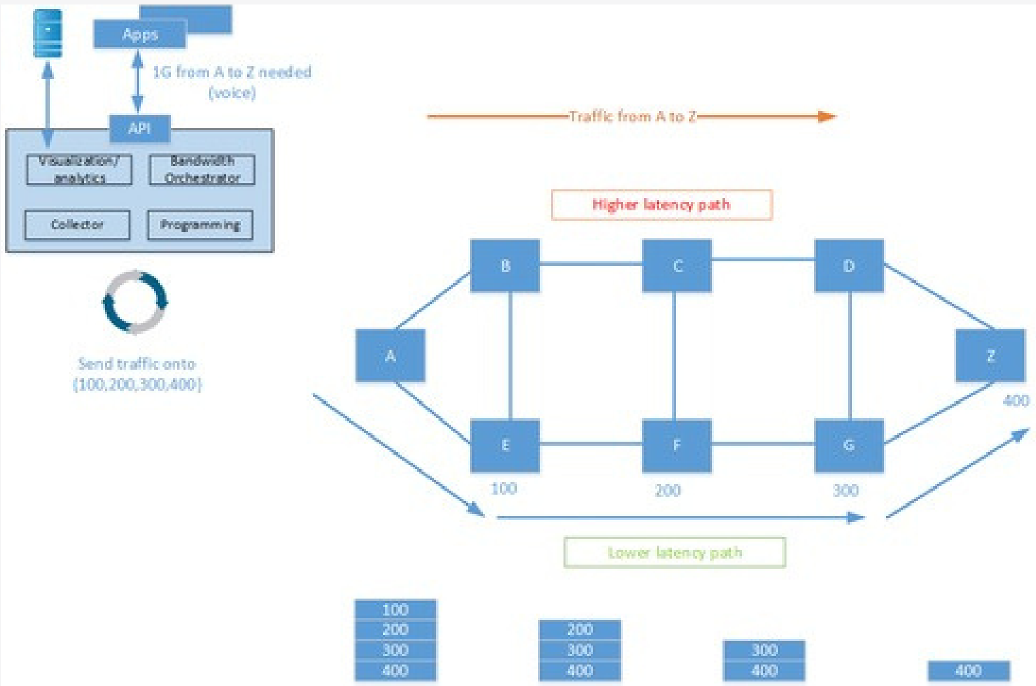




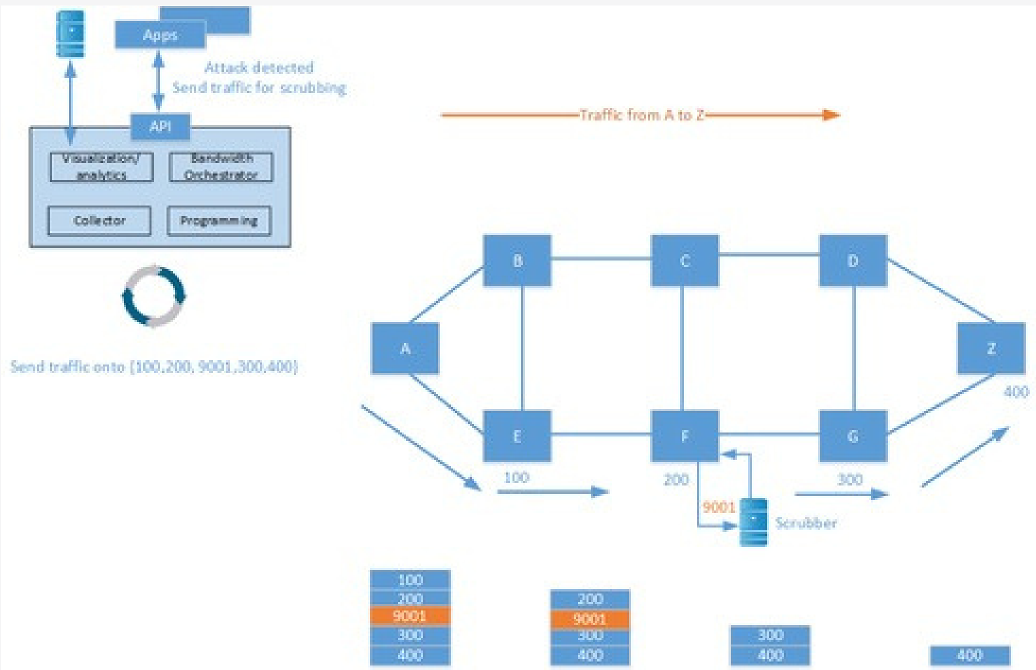
It is also possible to combine the node SID and adjacency SID to create a custom traffic policy. Labels are specified in a label stack, which may include several labels. By combining labels, you can create policies such as, "Send the traffic to F; I don't care how you get there. From F, go to G, then to D and then finally to Z." This creates endless possibilities for traffic engineering in the provider network.



One of the main applications for SR is to enable some kind of application controller that can steer traffic over different paths, depending on different requirements and the current state of the network. Some might relate to this as software-defined networking (SDN). It is then possible to program the network to send voice over a lower latency path and send bulk data over a higher latency path. Doing this today requires MPLS-TE, as well as keeping state in many devices. With SR, there is no need to keep state in intermediary devices.



SR can also help protect against distributed denial of service (DDoS) attacks. When an attack is detected, traffic can be redirected to a scrubbing device which cleans the traffic and injects it into the network again.



1.2. Requirement

The requirement is to develop most of the features mentioned in TR.101 Spec from the aggregation switch side on top of one of the commercial Whitebox NOS vendor. Refer to the xxx section for more information about the list of features developed as part of this project.

2. NOS Platform Architecture

The below diagram represents the high-level overview of the NOS architecture.

3. Network Architecture

This section talks about the deployment models and network architectures.

4. Supported Features

Below is thelist of features, which we had supported for the Leaf-spine deployment.

5. GLOSSARY

BFD: Bidirectional Forwarding Detection
CE: Customer Edge
H&S: Hub & Spoke
IDU: Indoor Unit
ODU: Outdoor Unit
PE: Provider Edge
PoC1: Point of Concentration 1st level (aggregation level next to the core network)
PoC2: Point of Concentration 2nd level (intermediate aggregation level)
PoC3: Point of Concentration 3rd level (first aggregation point after last mile/access)
SDN: Software Defined Networks
DCSG: Disaggregated Cell Site Gateways