Scenario, Simulation and Suggestion of PCE in Native IP Network
draft-ietf-teas-native-ip-scenarios-03

Abstract

This document describes the scenarios, simulation and suggestions for PCE in native IP network, which integrates the merit of distributed protocols (IGP/BGP), and the power of centrally control technologies (PCE/SDN) to provide one feasible traffic engineering solution in various complex scenarios for the service provider.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on October 11, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of
1. Introduction

Service provider network is composed of thousands of routers that run distributed protocol to exchange the reachability information between them. The path for the destination network is mainly calculated and controlled by the IGP/BGP protocols. These distributed protocols are robust enough to support the current evolution of Internet but have some difficulties when application requires the end-to-end QoS performance, or in the situation that the service provider wants to maximize the link utilization within their network.

MPLS-TE technology is one solution for finely planned network but it will put heavy burden on the routers when we use it to meet the dynamic QoS assurance requirements within real time traffic network.

SR (Segment Routing) is another solution that integrates some merits of distributed protocol and the advantages of centrally control mode, but it requires the underlying network, especially the provider edge router to do label push and pop action in-depth, and need complex
mechanic for coexisting with the Non-SR network. Additionally, it can only maneuver the end-to-end path for MPLS and IPv6 traffic via different mechanisms.

This draft describes scenarios that the centrally control dynamic routing (CCDR) framework can easily solve, without adding more extra burden on the router. It also gives the path optimization simulation results to illustrate the applicability of CCDR framework. Finally, it gives some suggestions for the implementation and deployment of CCDR.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. CCDR Scenarios.

The following sections describe some scenarios that the CCDR framework is suitable for deployment.


With the emerge of cloud computing technologies, enterprises are putting more and more services on the public oriented cloud environment, but keep core business within their private cloud. The communication between the private and public cloud will span the WAN network. The bandwidth requirements between them are variable and the background traffic between these two sites changes from time to time. Enterprise applications just want to exploit the network capabilities to assure the end-to-end QoS performance on demand.

CCDR, which integrates the merits of distributed protocol and the power of centrally control, is suitable for this scenario. The possible solution framework is illustrated below:
By default, the traffic path between the private and public cloud site will be determined by the distributed control network. When applications require the end-to-end QoS assurance, it can send these requirements to PCE, let PCE compute one e2e path which is based on the underlying network topology and the real traffic information, to accommodate the application’s QoS requirements. The proposed solution can refer the draft [I-D.ietf-teas-pce-native-ip]. Section 4 describes the detail simulation process and the result.

3.2. Link Utilization Maximization

Network topology within MAN is generally in star mode as illustrated in Fig.2, with different devices connect different customer types. The traffic from these customers is often in tidal pattern that the links between the CR/BRAS and CR/SR will experience congestion in different periods, because the subscribers under BRAS often use the network at night and the dedicated line users under SR often use the network during the daytime. The uplink between BRAS/SR and CR must satisfy the maximum traffic volume between them respectively and this causes these links often in underutilization situation.
If we consider to connect the BRAS/SR with local link loop (which is more cheaper), and control the MAN with the CCDR framework, we can exploit the tidal phenomena between BRAS/CR and SR/CR links, maximize the links (which is more expensive) utilization of them.

---

3.3. Traffic Engineering for Multi-Domain

Operator’s networks are often comprised by different domains, interconnected with each other, form very complex topology that illustrated in Fig.4. Due to the traffic pattern to/from MAN and IDC, the utilization of links between them are often asymmetric. It is almost impossible to balance the utilization of these links via the distributed protocol, but this unbalance phenomenon can be overcome via the CCDR framework.
Solution for this scenario requires the gather of NetFlow information, analysis the source/destination AS of them and determine which pair is the main cause of the congested link. After this, the operator can use the multi eBGP sessions described in [I-D.ietf-teas-pce-native-ip] to schedule the traffic among different domains.


In more general situation, there are often temporal congestions within the service provider’s network. Such congestion phenomena often appear repeatedly and if the service provider has some methods to mitigate it, it will certainly increase the degree of satisfaction for their customers. CCDR is also suitable for such scenario in such manner that the distributed protocol process most of the traffic forwarding and the controller schedule some traffic out of the congestion links to lower the utilization of them. Section 4 describes the simulation process and results about such scenario.

4. CCDR Simulation.

The following sections describe the topology, traffic matrix, end-to-end path optimization and congestion elimination in CCDR applied scenarios.

4.1. Topology Simulation

The network topology mainly contains nodes and links information. Nodes used in simulation have two types: core node and edge node. The core nodes are fully linked to each other. The edge nodes are connected only with some of the core nodes. Fig.5 is a topology example of 4 core nodes and 5 edge nodes. In CCDR simulation, 100 core nodes and 400 edge nodes are generated.
4.2. Traffic Matrix Simulation.

The traffic matrix is generated based on the link capacity of topology. It can result in many kinds of situations, such as congestion, mild congestion and non-congestion.

In CCDR simulation, the dimension of the traffic matrix is 500*500. About 20% links are overloaded when the Open Shortest Path First (OSPF) protocol is used in the network.

4.3. CCDR End-to-End Path Optimization

The CCDR end-to-end path optimization is to find the best path which is the lowest in metric value and each link of the path is far below link’s threshold. Based on the current state of the network, PCE within CCDR framework combines the shortest path algorithm with penalty theory of classical optimization and graph theory.

Given background traffic matrix which is unscheduled, when a set of new flows comes into the network, the end-to-end path optimization
finds the optimal paths for them. The selected paths bring the least congestion degree to the network.

The link utilization increment degree (UID) when the new flows are added into the network is shown in Fig. 6. The first graph in Fig. 6 is the UID with OSPF and the second graph is the UID with CCDR end-to-end path optimization. The average UID of the first graph is more than 30%. After path optimization, the average UID is less than 5%. The results show that the CCDR end-to-end path optimization has an eye-catching decreasing in UID relative to the path chosen based on OSPF.

Fig. 6 Simulation Result with Congestion Elimination
4.4. Network Temporal Congestion Elimination

Different degree of network congestions are simulated. The congestion degree (CD) is defined as the link utilization beyond its threshold.

The CCDR congestion elimination performance is shown in Fig. 7. The first graph is the congestion degree before the process of congestion elimination. The average CD of all congested links is more than 10%. The second graph shown in Fig. 7 is the congestion degree after congestion elimination process. It shows only 12 links among totally 20000 links exceed the threshold, and all the congestion degree is less than 3%. Thus, after scheduling of the traffic in congestion paths, the degree of network congestion is greatly eliminated and the network utilization is in balance.
5. CCDR Deployment Consideration.

With the above CCDR scenarios and simulation results, we can know it is necessary and feasible to find one general solution to cope with various complex situations for the complex optimal path computation in centrally manner based on the underlay network topology and the real time traffic.
[I-D.ietf-teas-pce-native-ip] gives the solution for above scenarios, such thoughts can be extended to cover requirements in other situations in future.

6. Security Considerations

This document considers mainly the integration of distributed protocol and the central control capability of PCE/SDN. It certainly can ease the management of network in various traffic-engineering scenarios described in this document, but the central control manner also bring the new point that may be easily attacked. Solutions for CCDR scenarios should keep these in mind and consider more for the protection of PCE/SDN controller and their communication with the underlay devices, as that described in document [RFC5440] and [RFC8253]

7. IANA Considerations

This document does not require any IANA actions.

8. Contributors

Lu Huang contributes to the content of this draft.

9. Acknowledgement

The author would like to thank Deborah Brungard, Adrian Farrel, Huaimo Chen, Vishnu Beeram and Lou Berger for their supports and comments on this draft.

10. Normative References

[I-D.ietf-teas-pce-native-ip]


Authors’ Addresses

Aijun Wang
China Telecom
Beiqijia Town, Changping District
Beijing, Beijing  102209
China

Email: wangaj.bri@chinatelecom.cn

Xiaohong Huang
Beijing University of Posts and Telecommunications
No.10 Xitucheng Road, Haidian District
Beijing
China

Email: huangxh@bupt.edu.cn

Caixia Kou
Beijing University of Posts and Telecommunications
No.10 Xitucheng Road, Haidian District
Beijing
China

Email: koucx@lsec.cc.ac.cn

Zhenqiang Li
China Mobile
32 Xuanwumen West Ave, Xicheng District
Beijing  100053
China

Email: li_zhenqiang@hotmail.com