An Architecture of Central Controlled Layer 2 Virtual Private Network (L2VPN)

draft-li-l2vpn-ccvpn-arch-00

Zhenbin Li, Shunwan Zhuang
Huawei Technologies

IETF 88, Vancouver, BC, Canada

Introduction

- The architecture of central controlled BGP is defined in [draft-li-idr-cc-bgp-arch-00]. Some use cases under this new framework are also discussed.
- In the central controlled framework, control functionality of L2VPN can be done only by the Controllers. Consequently it can reduce control functionality in network nodes.
- This document defines the architecture of central controlled L2VPN and corresponding protocol extension requirement.

Architecture

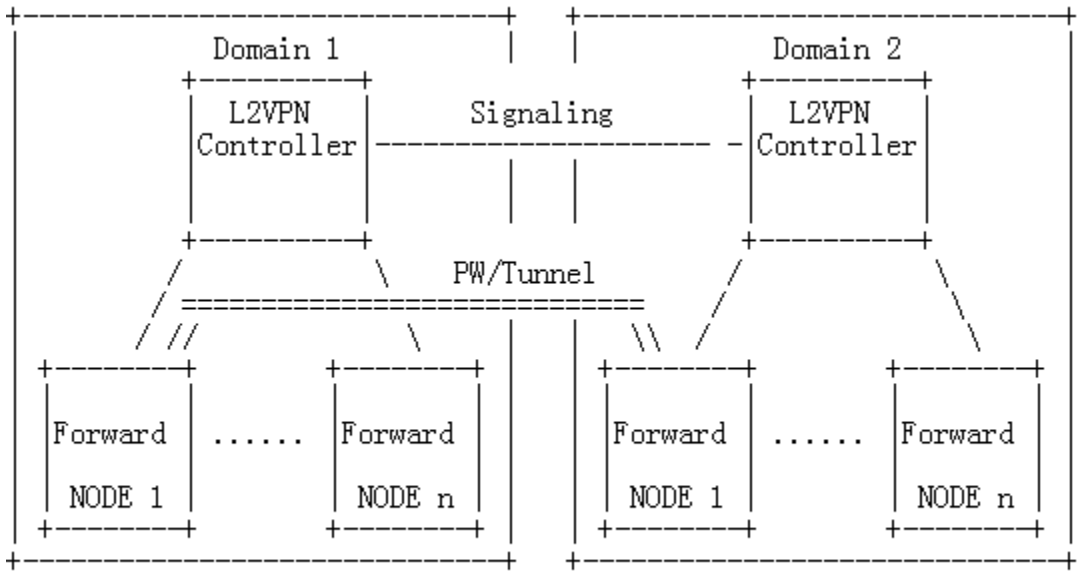

Figure 1: An Architecture of Central Controlled L2VPN

- The architecture consists of two essential network elements: L2VPN Controller and Forward Node. There is no L2VPN related control functionality in Forward Nodes. L2VPN Controller controls all the Forward Nodes.
- L2VPN Controllers need to communicate with each other via extension of existing protocols, e.g. BGP, LDP, etc.
- L2VPN service set up between the forward nodes is proxied by the BGP Controllers.

Application Scenarios

Three application scenarios for deployment of Central Controlled L2VPN service.

- Scenario 1: Partial Deployment.
  - Some network nodes are upgrading to support Central Controlled L2VPN, the other nodes are retained as legacy network nodes.
  - The new network nodes are controlled by L2VPN Controller.
- Scenario 2: Multiple Controller within a Single AS
  - There are multiple controllers in a single AS to be responsible for setup of Central Controlled L2VPN service.
- Scenario 3: Multiple Controller within Multiple Ases
  - There are multiple controllers in different ASes to be responsible for setup of Central Controlled L2VPN service.

Solutions and Protocol Extensions

- Overview: There are two options to implement the architecture of Central Controlled L2VPN.
  - Option 1: BGP for all scenarios
  - Option 2: LDP for Partial Deployment Scenario
- Procedures:
  - PW Establishment
  - PW Redundancy
  - MAC Withdraw
  - Capability Negotiation

PW Establishment

- Auto Discovery:
  - The controller SHOULD advertise the address list of Forward Nodes participating in a specific VPLS or VLL to other controllers. Then the controller can discover the PW that should be set up between the Forwarding Nodes controlled by different controllers.
- PW Label Allocation:
  - The controller will advertise the label mapping message to the other controller for the PW which should be set up between a pair of Forward Nodes.
  - The addresses of the local Forward Node and the remote Forward Node SHOULD be carried in the message to differentiate the PWs.
- PW Forwarding Entry Creation:
  - The controller will find the tunnel to the Forward Node controlled by another controller.
  - The controller will create PW forwarding entry with PW label and the tunnel information and download the forwarding entry to the specified local Forward Node controlled by itself.

PW Redundancy

- In the Central Controlled L2VPN, when advertise the status for the PW between the controllers, the addresses of the Local Forward Node and the Remote Forward Node should be carried to specify the specific PW.

- When the controller receives the message carried the PW status information, it will set the PW on the specified Forwarding Node as the state specified by the message.

MAC Withdraw

- For Central Controlled L2VPN, L2VPN Controller needs to develop an ability to remove the MAC of the specific Forward Node.
  - When a Forward Node within a L2VPN Controller wants to remove MAC Addresses that has been sent to the remote endpoint, the Controller needs to send MAC Withdraw Messages on behalf of the Forward Node.
  - In the message, the address of the remote forward node should be carried.

- When the other controller receive the message, it will remove the specified MAC addresses on the Forward Node identified by the address of the remote forward node in the message.

Capability Negotiation

- To ensure backward compatibility with existing implementations, the capability for Central Controlled L2VPN SHOULD be negotiated between the controllers.
- The capability is advertised to each other by the controllers.
- After the successful negotiation of the capability, the other control functionalities for the central controlled L2VPN can be done by the controller.

Next Steps

- EVPN functionality will be taken into account.
- The control functionality between CE and PE will be taken into account for L2VPN.
- Solicit more comments & feedbacks
- Revise the draft