An Architecture of Central Controlled Border Gateway Protocol (BGP)

draft-li-idr-cc-bgp-arch-00

Zhenbin Li, Mach Chen, Shunwan Zhuang
Huawei Technologies

IETF 88, Vancouver, BC, Canada

Introduction

- As the Software Defined Networks (SDN) solution develops, BGP is extended to support central control.
- This document introduces an architecture of using BGP for central control.
- Some use cases under this new framework are also discussed. For specific use cases, making necessary extensions in BGP are required.

Architecture -- Reference Model

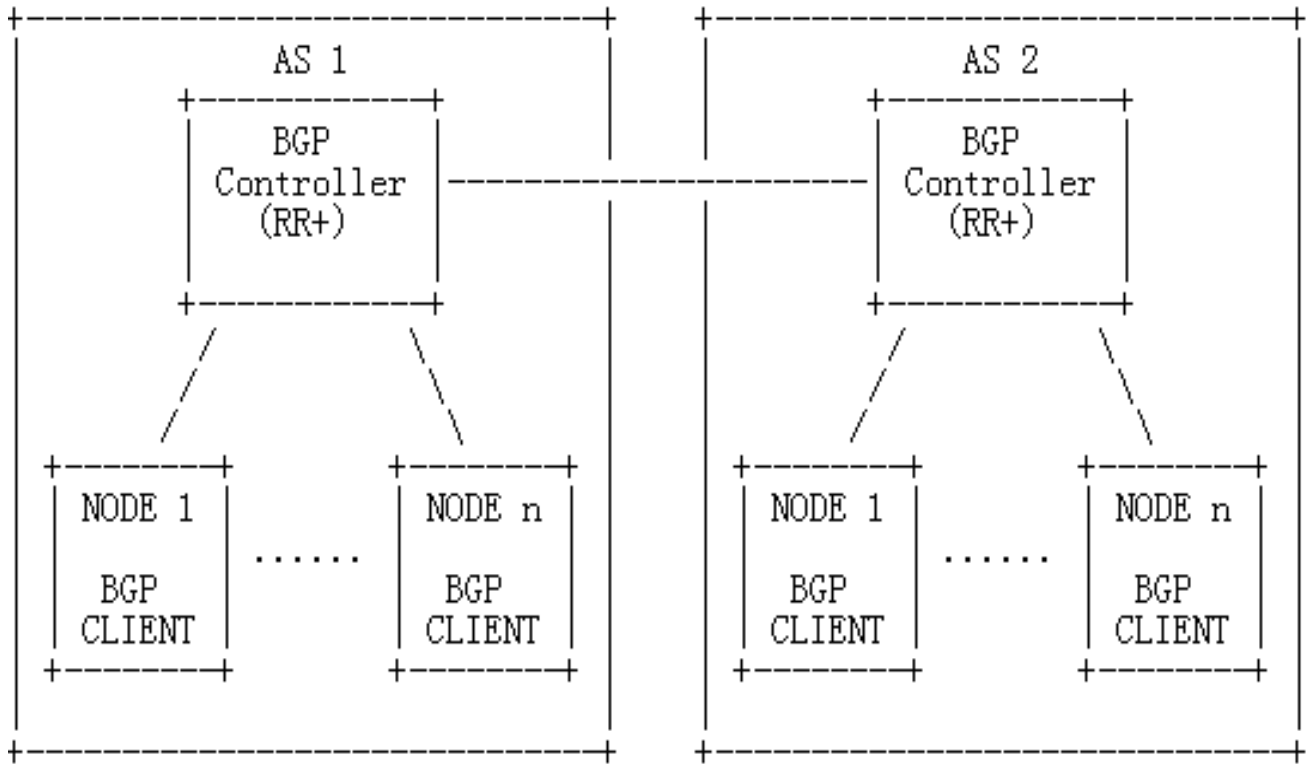

Figure 1: An Architecture of Central Controlled BGP

- BGP Controller controls all the BGP Clients within its administrative domain by communicating with them.
- BGP sessions are also set up between multiple BGP controllers.

Architecture -- Deployment Mode

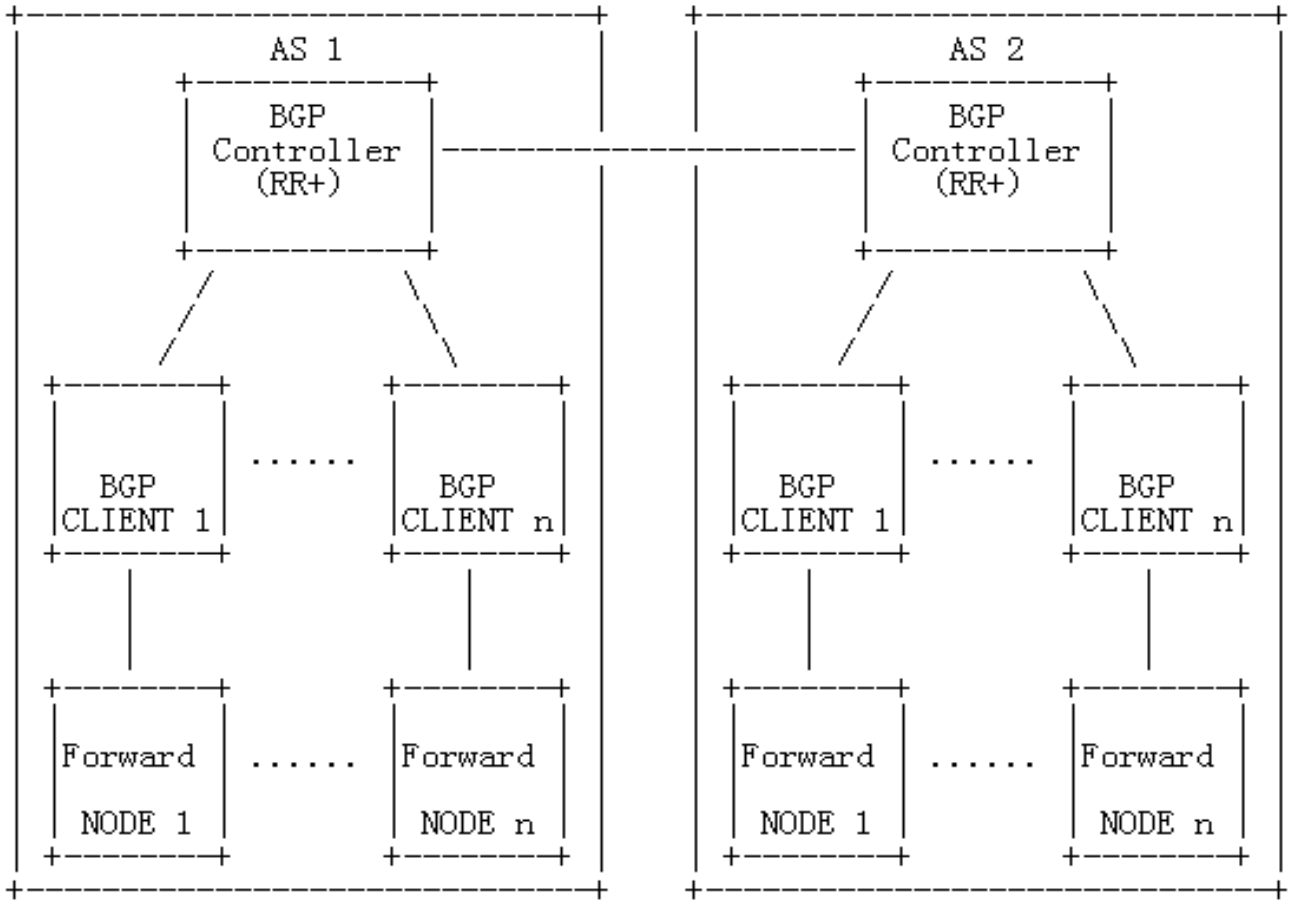

Figure 2: Decoupling BGP Client and Forwarding

- BGP Controller and BGP Client can run on a general-purpose server or a network device.
- It is more meaningful to decouple control plane and forwarding functionality on BGP Client because this manner enables network devices focusing on forwarding functionality.

Architecture -- Protocol Extensions

- Building Connectivity:
  - Connectivity between BGP Controller and BGP Clients in an AS can be built by extending IGP protocol.
  - In order to simplify network operations, such connectivity SHOULD be automatically established.
- Roles Auto-Discovery:
  - BGP Controller and BGP Client roles can be auto-discovered by extending IGP protocol to flooding the role information within an AS.
  - When IGP has finished the flooding process of role information, BGP Controller and BGP Client can establish a BGP session on demand.
- Capability Negotiation:
  - In order for BGP Controller and BGP Client to support BGP-based Central Controlled framework in a friendly way, this document suggests to defines a new BGP Central Control Capability.
- High Availability:
  - To void one-point-failure of BGP Controller, it is possible to run redundant BGP Controllers for high availability.
- Security

Use Cases

In BGP-based Central Controlled framework, new use cases are emerging：

- Network Topology Acquirement
  - BGP has been extended to distribute link-state and traffic engineering information.
- Simplifying Network Operation and Maintenance
  - By using I2RS APIs, it would allow network operator to setup BGP policy configuration and apply route policy easily from an central point.
  - In the new Central Controlled framework, VPN Service can be deployed rapidly according to business requirements. More detailed description could be found in [draft-li-l3vpn-instant-vpn-arch-00].

Use Cases(Cont.)

- MPLS Global Label Allocation
  - MPLS Global Label should be allocated in a central point to guarantee all distributed network nodes can understand meaning of a specific global label in same.
  - The new BGP-based Central Controlled framework is particularly suitable to allocate MPLS Global Label for services deployed on the network edge nodes.
  - [draft-li-mpls-global-label-usecases-00] proposes the use cases: 1) Identification of MVPN/VPLS, 2) Local Protection of PE Node, 3) Segment-Based EVPN, etc.
- RR-Based Traffic Steering
  - RR-based Traffic Steering (RRTS) defined in [draft-chen-idr-rr-based-traffic-steering-usecase-00], is an idea that leverages the BGP route reflection mechanism to realize traffic steering in the network.
  - Therefore the operators can conduct specific traffic to traverse specific path, domains and/or planes as demand.

Use Cases(Cont.)

- Inter-Controller Applications
  - The service set up between the nodes is proxied by the BGP Controllers.
  - More detailed description could be found in [draft-li-l2vpn-ccvpn-arch-00]

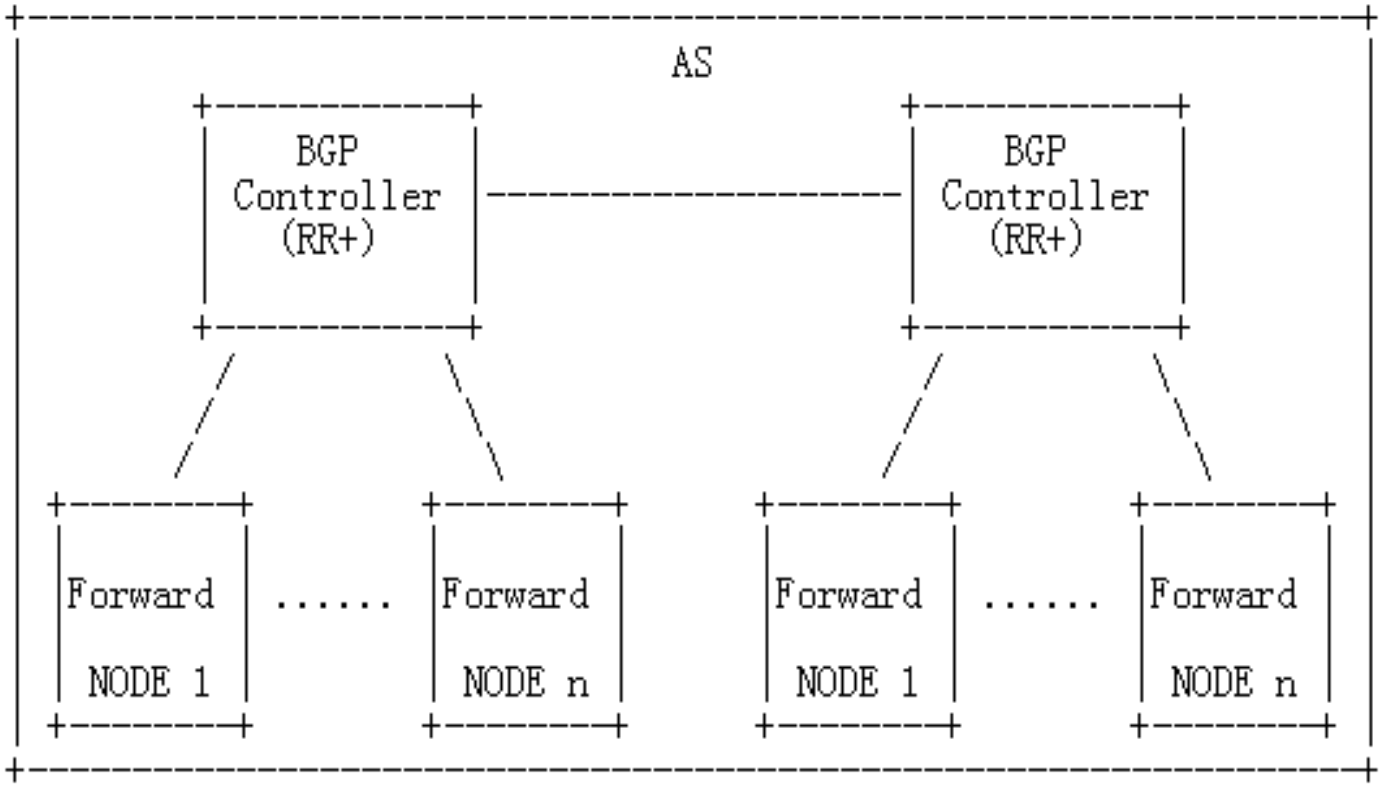

Figure 3: Removing BGP Session between Controller and NODE

Next Steps

- Solicit more comments & feedbacks
- Revise the draft