DP Service Provider Series

BGP Security

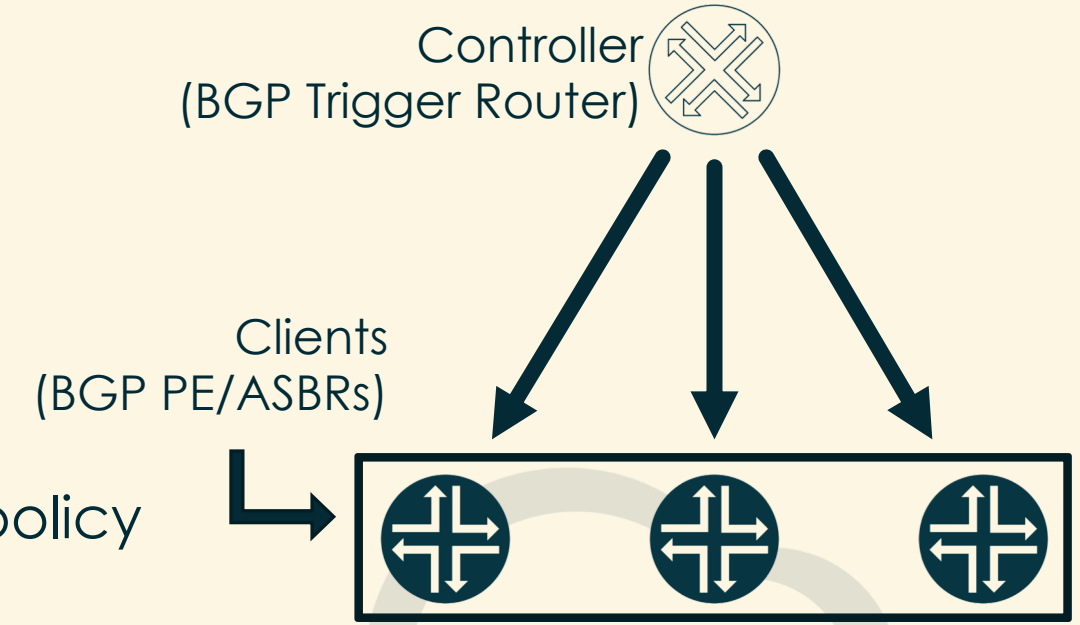
BGP Flow Specification

Agenda

- Introduction to BGP Flow Specification
- BGP Flowspec Concepts

BGP Flow Specification

- Mechanism for centralization of traffic policy management
  - Access Control List or Firewall rules
  - Policy Based Routing rules
  - Traffic rate limiting rules
  - QoS remarking rules
- BGP infrastructure is leveraged to distribute policy
  - SDN like concept of Controller and Client
  - Policy implemented on ingress traffic
- Policy implementation is done in hardware
  - Implementation is identical to an ACL or a Firewall Rule



What is a Flow Specification?

- Defined in RFC 5575
  - Dissemination of Flow Specification Rules

"A flow specification is an n-tuple consisting of several matching criteria that can be applied to IP traffic."

- RFC 5575

Leveraging BGP

- New NLRIs
  - SAFI 133 (Global Unicast) and 134 (L3VPN Unicast)
  - The NLRI is of variable length
    - The various fields are coded as TLVs
  - This flexibility is necessary
    - The n in n-Tuple is variable
- The "fields" are called components
  - Each of them have a Type and Length

But What Really is a Flow Specification?

- n-Tuple
  - An ordered set of n elements
- n-Tuple for Flow Specification
  - An arbitrary set of matching criteria for a single packet
  - E.g. {A Source IP, A Destination IP, A Protocol}
  - E.g. {A Destination IP, A Protocol, A Range of Destination-Ports}
- A packet's header is compared to the n-Tuple
  - A HIT if each field in the header matches positively
  - A MISS if one or more fields do not match

Leveraging BGP

- New NLRIs
  - SAFI 133 (Global Unicast) and 134 (L3VPN Unicast)
  - Coded as TLVs
- The NLRI flexible
  - This flexibility is necessary
  - Each rule may consist of different fields (E.g. Protocol, port, QoS Marking)
- The "fields" are called components
  - The various fields are coded as TLVs

BGP Advantages

- Efficient point-to-multipoint distribution of control plane information
- Inter-domain capabilities and routing policy support
- Tight integration with unicast routing, for verification purposes

Match – NLRI Component Types

- Type 1 - Destination Prefix
- Type 2 – Source Prefix
- Type 3 – IP Protocol
- Type 4 – Port
- Type 5 – Destination Port
- Type 6 – Source Port
- Type 7 – ICMP Type
- Type 8 – ICMP Code
- Type 9 – TCP Flags
- Type 10 – Packet Length
- Type 11 – DSCP
- Type 12 – Fragment

- The NLRI needs at least one component
- No component is mandatory

Action – BGP Communities

- Once a match occurs, an action must be determined
- Actions are carried in attached communities

- Type `0x8006` – Traffic Rate
  - Bit Rate in Bytes per second
  - 0 Bps for drop
- Type `0x8007` – Traffic-action
  - Sample traffic
  - Continue action
- Type `0x8008` – Redirect
  - Route Target of a VRF
- Type `0x8009` – Traffic-marking
  - DSCP Value
- Type `0x0800` – Redirect to IP
  - Mirror to an IP address

In Our Next Video…

- BGP Flowspec Demo

DP Service Provider Series

BGP Security

BGP Flowspec Demo

Scenarios

- Topology overview
- IPv4 and IPv6 Flowspec
  - BGP Session Creation
  - IOS-XR as Controller
  - Junos as Controller
- VPNv4 and VPNv6 Flowspec
  - BGP Session Creation
  - IOS-XR as Controller
  - Junos as Controller

Thanks!