

# Protocol Assisted Protocol (PASP)

draft-li-rtgwg-protocol-assisted-protocol-06

**Zhenbin (Robin) Li**, Shuanglong Chen, Zhen Tan, Yunan Gu,

# Overview

- Recapitulation
  - Why we want such a protocol
  - What do we want in such a protocol

# Why an east-west assisted protocol is needed?

- Challenges of North-South methods
  - Large amount of data to be exported: There may be too many devices, protocols and data.
  - High performance requirements on the Controller or NMS to complete all these tasks
- User habits
  - Local configuration and maintenance, more convenient
  - Take time to be adapted to NMS/Controller
  - Need knowledge about various vendors
- Existing east-west methods in use:
  - RSVP-TE PathErr/ResvErr
  - BGP Notification
  - Other protocol-specific error-shooting mechanisms

# Why a general assisted protocol is needed?

- If a routing protocol is failed by itself, it very likely cannot advertise the its own maintenance information.
- Restrictions on maintenance mechanisms of the existing protocols
  - If more maintenance mechanisms were introduced, it might have much effect on the current operation, either in performance or complexity.
  - BGP extension of the Path attribute will have influence on the normal routing in parsing and route-selection performance.
  - RSVP extends the cause code for path setup failures. Only two ULONGs are available.
- Protocol extensibility:
  - Error-shooting mechanisms are protocol-specific, duplicate extensions
  - If a common protocol is used, it is more extensible and convenient to define and advertise related information.

# PASP (Protocol assisted Protocol)

- A new semi-distributive semi-centralized approach
  - A generic “pipeline” for exchanging troubleshooting data of various protocols
- Designed for exchanging protocol related information between devices
  - Separates routing and non-routing data
- Merits
  - A uniform error-shooting way for all routing protocols, facilitates automatic troubleshooting
  - No additional information on routes, won't affect existing routing system
  - More network-wide data accessible for individual device
  - Not relying on a centralized server
  - Less bandwidth & CPU pressure, comparing to a centralized data collection & analysis mechanism

# Use Cases for Troubleshooting

- Use Cases 1 - BGP route oscillation
  - Send a request message to the oscillating route for oscillation source check
  - Receiver send an ACK claims whether they are the oscillation sources, and send a further request until they get a ACK from the oscillation source
- Use Cases 2 - RSVP-TE set up failure
  - The failure device could actively send a notification with cause code to the ingress device
- Use Cases 3 - Peer disconnection (for IGP/BGP/LDP/BFD)
  - Device that suffers the disconnection could send a request message
  - Device that triggers disconnection send an ACK with reason of disconnection, including manual shutdown, TCP down and etc.

# More Use Cases (1)

- Use Cases 4 – Detecting Route Interruption
  - PASP could collect route change history, so that rapid route interruptions can be detected. Certain data could be fetched up on request from a trusted source.
- Use Cases 5 – BGP Route No-advertise
  - Device that suffers from a no-advertise situation could send a request message with the specific IP.
  - Receiver will send an ACK with reason of no-advertise, including egress filters, no-advertise attribute and etc.
- Use Cases 6 – Route Abnormal
  - Device could send a request message with the specific IP to another device for abnormal situations
  - Receiver will send an ACK with situation code including nexthop unreachable, outbound interface down, suppression and etc.

# More Use Cases (2)

- Use Cases 7 – Management protocol failures
  - O&M personnel could send a request on a neighbor device to the target device, asking for the reason of a login failure on a management protocol, such as SNMP or SSH.
- Use Cases 8 – Collecting other O&M Events
  - PASP could record O&M events, such as: IP-address conflict, memory leak and Etc.
  - Certain data could be fetched up on request from a trusted source, so that O&M personnel can get those information without checking every single devices.



# Discussion

- There are two possible options to implement PASP:
  - Option 1. PASP is developed independently as a protocol
  - Option 2. PASP reuses the existing protocol (GRASP)

	<b>GRASP</b>	<b>PASP</b>
Vision	The vision is a network that configures, heals, optimizes and protects itself.	Focuses on the exchange of east-west fault information about control-plane protocols. Assists fault locating and self-healing on the control plane.
Message Definition & Interaction Process	Try to reuse the defined messages and procedures of the GRASP protocol.	Defines a new PASP protocol
Scalability	High resource consumption persistent Connection	Flexible connection, relatively low resource consumption
Reliability	TCP / UDP(Need extension)	UDP (The application layer need supports)
Security	ACP	MD5

# Next Step

- Welcome more comments and discussion

Thank You!