Network Working Group
Internet-Draft
Intended status: Informational
Expires: August 18, 2014

L. Zhang
Z. Li
Huawei Technologies
D. Liu
China Mobile
S. Hares
Hickory Hill Consulting

February 14, 2014

Use Cases of I2RS in Mobile Backhaul Network
draft-zhang-i2rs-mbb-usecases-01

Abstract

In a mobile backhaul network, traditional configuration and diagnoses mechanisms based on device-level management tools and manual processing are ill-suited to meet the requirements of today's scalable, flexible, and complex network. Thanks to the new innovation of Interface to the Routing System's (I2RS) programmatic interfaces, as defined in [I-D.ietf-i2rs-architecture], an alternative way is available to control the configuration and diagnose the operational results. This document discusses the use case for I2RS in mobile backhaul network.

Requirements Language

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].

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 http://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 August 18, 2014.

Table of Contents

1. Introduction

In mobile backhaul network, traditional configuration and diagnoses mechanisms based on device-level management tools and manual processing are ill-suited to meet the requirements of today's scalable, flexible, and complex network. The mobile backhaul network now needs to serve various radio access modes and applications across 2G/3G / LTE/5G, build various network architectures based on the

number of network devices or the integration of different Areas or Autonomous System Numbers (ASNs), and support various network protocols that can be adopted to meet different network requirements. These needs make the mobile backhaul network configuration more and more arduous.

Interface to the Routing System's (I2RS) Programmatic interfaces, as defined in [I-D.ietf-i2rs-architecture], provides an alternative way to control the configuration and diagnose the operational results. The use cases described in this document cover the critical elements of mobile backhaul networks, such as: application configuration, route policy enforcement, service tunnel implementation, protection mechanisms and network monitoring. The goal is to increase the community's understanding of the mobile backhaul requirements for I2RS in a the context of an entire network solution.

2. Definitions

I2RS: Interface to the Routing System

IGP: Interior Gateway Protocol

BGP: Border Gateway Protocol

MPLS: Multi-Protocol Label Switching

LDP: Label Distribution Protocol

RSVP-TE: Resource Reservation Protocol Traffic Engineering

PWE3: Pseudo Wire Emulation Edge-to-Edge

VPN: Virtual Private Network

L2VPN: L2 Virtual Private Network

L3VPN: L3 Virtual Private Network

SS-PW: Singe Segment PW

MS-PW: Multi-Segment PW

HVPN: Hierarchical VPN

EPC: Pseudo Wire Emulation Edge-to-Edge

LTE: Long Term Evolution

FRR: Fast Reroute

ECMP: Equal Cost Multi-path

3. Application Configuration

3.1. Application Configuration

The mobile backhaul network has evolved into an IP-based network, which faces three main challenges in network construction:

1. various radio access modes:

   To protect existing investment and end user resource, TDM/ATM-based access modes belonging to 2G and 3G will coexist with Ethernet-based access mode belonging to 3G, LTE, and 5G for an extended time into the future. The radio architecture evolution will bring out new radio interfaces, such as the X2 interface in LTE which will not work in hub-spoke communication mode and needs much more shorter latency. A mobile backhaul network must be built to have the ability to adapt to all the mobile access modes, providing PWE3 service for TDM /ATM-based access mode and Native IP/Ethernet, PWE3/ VPLS or L3VPN service for IP-based access mode.

2. various radio applications:

   A variety of radio applications (such as OM, signaling, data, video, etc.) which have different quality of services (QoS), should be delivered in specific service channels in mobile backhaul networks, meaning there will be more than one PW or L3VPN instances binding with specific interfaces and service tunnels.

3. various network architectures:

   The mobile backhaul network maybe consist of hundreds of nodes in a small county or thousands of nodes in a populous region. It will be an integration of different ASNs rather than a single AS, when EPC is deployed in the Core network with LTE. The network devices on different points of the network (e.g. access\aggregation\core) have different routing and protocol processing capabilities, resulting in an integration of different IGP routing areas rather than a single large IGP routing area. Within various network architectures, different service modes should be provided, such as SS- PW or MS-PW, E2E L3VPN or HVPN, Seamless MPLS, and the integration of them.

3.2. Requirements for I2RS

The challenges in mobile backhaul network construction show the flexibility and complexity requirements of network configuration and modification, such as:

- where the T-LDP should be configured,
- where a BGP peer should be established,
- where the VPN instance should be deployed, and
- where the BGP-based LSP should be set up.

Faced with flat or reduced budgets, network operators are trying to squeeze the most from their network using device-level management tools and manual processing. In contrast to management of entire network devices, I2RS' programmatic interface would allow network operators to distribute such configurations from a central location where global mobile backhaul network solution provisioning information could be stored Use of I2RS clients to distribute time-critical changes in configuration to I2RS agents associated with each node would simplify and automate configuration and monitoring of a mobile backhaul network to allow it to readily adapt to changing network sizes (and scales) and radio applications.

I2RS Clients-Agent communication needs to pass information on:

- T-LDP configurations and status;
- BGP peer configurations, peer topologies and status;
- BGP-based LSP topologies and status;
- Reset VPN topologies, and per node configurations;

While a beginning exists in the I2RS RIB Information Model [[I-D.ietf-i2rs-rib-info-model]] which includes in the route interfaces with MPLS LSP ro VPN technology, additional features need to be added to support mobile backhaul networks.

4. Route Policy Enforcement

4.1. Route Policy Description

The route policy in mobile backhaul networks mainly refers to BGP policy when L3VPN is used to serve the radio applications. The

complexity of today's network architecture and radio interfaces make it very difficult to apply a network-wide route policy, for:

- o avoiding route advertisement across entire network

  When a mobile backhaul network contains more than 500 nodes, utilizing a multi-segments service like HVPN is recommended to reduce the routing and protocol processing overhead of network devices. BGP policy should be configured with prefix filters to advertise only the default or aggregate route to the access nodes which have limited capability, while advertising to the whole network routes to the core nodes which must have capability to store large number of routes.

- o supporting best route selection for VPN FRR or ECMP

  The mobile backhaul network is recommended to be built with a multi-homed network architecture for node failure protection, where VPN FRR or ECMP should be configured. The best route selection relies on BGP Policy using Local Preference, MED or other path attributes defined in [RFC4760]. When a BGP RR is adopted to simplify the BGP peer architecture from full-mesh mode, the policy would become more complex, in some cases may make be per-peer or per-route worse.

- o allowing On-demand route advertisement

  The advent of X2 interfaces in LTE, which need specific route information between any two access nodes, makes the network route advertisement more dynamic and unpredictable. The BGP policy should be adjusted dynamically to meet this route advertisement need across the entire network.

4.2. Requirements for I2RS

Route policy enforcement in mobile backhaul networks needs to be much more dynamic and flexible. The I2RS interface provides a programmatic way to configure (both policy and device) and monitor thousands of devices individually whose configuration is based on the devices role (such as ASRSs in one AS, ASBRs between ASs and other service-touch nodes). Current methods take hours (or even days) to configure route policy across a network.

In contrast, I2RS clients could contact I2RS agents on nodes to query role-based information from the network status. After collecting the status, the I2RS client could develop the BGP policies based on role information and push the BGP policies to the I2RS agents that would load the alternate policies into the network device. The I2RS Agents

loading the alternate policies could then send status back to the I2RS Client.

5. Service Tunnel Implementation

5.1. Service Tunnel Description

In mobile backhaul network, more than one kind of Service Tunnel can be used according to network ability or other consideration in different scenarios. The Tunnel deployment use case in mobile backhaul includes:

- MPLS LDP LSP

  MPLS LDP LSP is set up through LDP protocol. Both Label Advertisement Mode of Downstream Unsolicited (DU) and Downstream on Demand (DOD) defined in [RFC3036] can be used individually or integrated across access networks and aggregate /core networks. If needed, the longest length match defined in [RFC5283] for LDP LSP should be supported. MPLS LDP LSP has excellent scalability with flexible policy to control the label advertisement of route, especially in DU mode, to decrease needless LSPs to reduce the LSP capability requirement of network devices.

- MPLS-TE LSP

  MPLS-TE LSP is set up through RSVP-TE protocol, which has multiple path control attributes (such as explicit-path, path affinity property , path bandwidth assurance , path hop limitation, e.g.) and multiple protection modes (such as hot-standby, Fast Re-Route, protection group, e.g.). MPLS-TE LSP should be designed using the attributes and protection modes according to the requirements of the service delivery as integrated across access network and aggregate/cores network.

- MPLS-TP LSP

  MPLS-TP includes unidirectional LSP, bidirectional co-routed LSP, and bidirectional associated LSP, which can be calculated and set up manually or using dynamic network protocols such as GMPLS. In mobile backhaul networks, the LSP selection depends on the service need, and the creation of MPLS-TP LSP is always assumed to be decoupled with the protocol control plane running on separate network devices. Ideally, the static MPLS-TP LSP should be designed and configured on the centralized control plane.

5.2. Requirements for I2RS

The mobile backhaul network is divided into an access network and an aggregation/core network where service tunnel implementation is not constant and unique. Therefore, it may be necessary to deploy different kind of LSPs separately (such as LDP LSP or MPLS-TE LSP in both access network and aggregate/core networks) or simultaneously (such as MPLS-TP static LSP in access network while LDP LSP or MPLS-TE LSP in aggregate/core network). Network operators need to know the ability of all of the network devices and the service requirements to make the most appropriate tunnel implementation.

I2RS clients can provide centralized control of many network devices via the I2RS Client-Agent communication. The I2RS programmatic interface can automate the collection and analysis of each device's capability so that the centralized I2RS client could calculate the optimal LSP path and distribute the configuration to individual devices. While the I2RS RIB Information Model [[I-D.ietf-i2rs-rib-info-model]] provides for routes with tunnels or MPLS LSP, the features defined in this model are not sufficient to configure both types of LSPs needed for the VPN technology in mobile backhaul networks. Additional I2RS Informational models need to be created to support these features.

6. Protection Mechanism

6.1. Protection Mechanism Description

The SLA for radio services is strict, which requires interworking among multiple protection mechanisms. Two critical aspects should be taken into account for inter-working, hierarchical protection architectures and multiple OAM protocol interactions.

1. tunnel protection:

   The protection mechanisms of different the tunnel protocols, mentioned above, are different from each other. To enhance the reliability, LDP LSP should configure LDP FRR, which is calculated depending on the protect route algorithm, and be Loop-Free Algorithm (LFA), Remote-LFA, or Maximally Redundant Trees (MRT) used together with LDP MT as described in [I-D.ietf-mpls-ldp-multi-topology]. MPLS-TE LSP should apply TE Fast Reroute or TE hot-standby. When MPLS-TP LSP is used, the LSP protection group should be configured with 1:1 or 1+1 mode for MPLS-TP line protection, as well as wrapping or steering modes fault processing for MPLS-TP ring protection.

2. service protection:

Service protection is recommended to be configured for node failure handover in mobile backhaul network, where PW redundancy defined in [RFC6718] or BGP VPN FRR or ECMP realization should be deployed exactly.

6.2. Requirements for I2RS

The hierarchical protection architecture in mobile backhaul network offer high network reliability and more flexibility to meet the various needs of the tunnels and services. The I2RS interface in this use case is needed to automate the configuration and monitoring so that tunnel protection and service protection interwork in a flexible and reliable manner.

7. Network Monitoring

7.1. Network Monitoring Description

The mobile backhaul network operators are asked to give an accurate cause when a link or node failure occurs, and get the real reason for service quality reduction. They need to apply different network monitor tools for different service mode, like Network Quality Analysis (NQA), MPLS-TP OAM, and IP Flow Performance Monitor (IPFPM). Determining the exact traffic path is really significant when using IPFPM for point-to-point detection.

Multiple monitor tools require network operators to distinguish granular traffic flow to apply the appropriate one. At the same time, getting the traffic path with traditional device-level management tools is difficult, which may enhancing the existing protocols or designing a new specific protocol to do the job. Both will increase the burden of mobile backhaul network.

7.2. Requirements for I2RS

The I2RS architecture (client-agent) should solve the two problems mentioned above naturally by enabling the use of centralized controllers, which control and manage the entire network’s devices and store the whole routing and service information directly. Meanwhile, the outages and traffic congestion or discards can be detected real-time with I2RS Client(s) connected to the I2RS agents in each node which provide real-time status via notification service. An I2RS client with this ability will allow the I2RS clients to keep optimal state dynamically all the time.

8. Security Considerations

The mobile backhaul network use cases described in this document assumes use of I2RS's programmatic interfaces described in the I2RS framework mentioned in[I-D.ietf-i2rs-architecture]. This document does not change the underlying security issues inherent in the existing [I-D.ietf-i2rs-architecture].

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

9.2. Informative Reference

[I-D.ietf-i2rs-architecture]
Atlas, A., Halpern, J., Hares, S., Ward, D., and T. Nadeau, "An Architecture for the Interface to the Routing System", draft-ietf-i2rs-architecture-01 (work in progress), February 2014.

[I-D.ietf-i2rs-problem-statement]
Atlas, A., Nadeau, T., and D. Ward, "Interface to the Routing System Problem Statement", draft-ietf-i2rs-problem-statement-00 (work in progress), August 2013.

[I-D.ietf-i2rs-rib-info-model]
Bahadur, N., Folkes, R., Kini, S., and J. Medved, "Routing Information Base Info Model", draft-ietf-i2rs-rib-info-model-01 (work in progress), October 2013.

[I-D.ietf-mpls-ldp-multi-topology]
Zhao, Q., Fang, L., Zhou, C., Li, L., and K. Raza, "LDP Extensions for Multi Topology Routing", draft-ietf-mpls-ldp-multi-topology-09 (work in progress), October 2013.

[I-D.ietf-mpls-seamless-mpls]
Leymann, N., Decraene, B., Filsfils, C., Konstantynowicz, M., and D. Steinberg, "Seamless MPLS Architecture", draft-ietf-mpls-seamless-mpls-05 (work in progress), January 2014.

[I-D.li-mpls-seamless-mpls-mbb]
Li, Z., Li, L., Morillo, M., and T. Yang, "Seamless MPLS for Mobile Backhaul", draft-li-mpls-seamless-mpls-mbb-00 (work in progress), July 2013.

[RFC3036] Andersson, L., Doolan, P., Feldman, N., Fredette, A., and B. Thomas, "LDP Specification", RFC 3036, January 2001.

[RFC4760] Bates, T., Chandra, R., Katz, D., and Y. Rekhter, "Multiprotocol Extensions for BGP-4", RFC 4760, January 2007.

[RFC5283] Decraene, B., Le Roux, JL., and I. Minei, "LDP Extension for Inter-Area Label Switched Paths (LSPs)", RFC 5283, July 2008.

[RFC6718] Muley, P., Aissaoui, M., and M. Bocci, "Pseudowire Redundancy", RFC 6718, August 2012.

Authors' Addresses

Li Zhang
Huawei Technologies
Huawei Bld., No.156 Beiqing Rd.
Beijing 100095
China

Email: monica.zhangli@huawei.com

Zhenbin Li
Huawei Technologies
Huawei Bld., No.156 Beiqing Rd.
Beijing 100095
China

Email: lizhenbin@huawei.com

Dapeng Liu
China Mobile
Unit2, 28 Xuanwumenxi Ave,Xuanwu District
Beijing 100053
China

Email: liudapeng@chinamobile.com

Susan Hares
Hickory Hill Consulting
7453 Hickory Hill
Saline, MI 48176
USA

Email: shares@ndzh.com