
Copyright 2010 [please consult the authors]
Evaluation of Distributed Control Signaling Protocols in GMPLS

Ahmad Ali Iqbal, Waqar Mahmood, Ejaz Ahmed, Kashan Samad
National University of Science and Technology
NUST Institute of Information Technology, Rawalpindi, Pakistan
{ahmad.ali, drwaqar, ejaz, kashan.samad }@niit.edu.pk

Abstract—GMPLS is a generalized form of MPLS (MultiProtocol Label Switching). MPLS is IP packet based and uses MPLS-TE for Packet Traffic Engineering. GMPLS is the extension to MPLS capabilities. It provides separation between transmission, control and management plane and network management. Control plane allows various applications like traffic engineering, service provisioning, and differentiated services. GMPLS control plane architecture includes signaling (RSVP-TE, CR-LDP) and routing (OSPF-TE, ISIS-TE) protocols. This paper provides an overview of the signaling protocols, describes their main functionalities, and provides a general evaluation of both the protocols.

Index Terms—forward path, GMPLS, label switching, QoS provisioning, signaling protocols, soft state, traffic engineering.

I. INTRODUCTION

Generalized Multi Protocol Label Switching (GMPLS) extends the signaling and routing ability of MPLS to incorporate the areas of wavelength, space and time division multiplexing (TDM), providing support for optical crossconnects (OXCs) and DWDM. GMPLS delivers a single control plane, providing a high-speed, reliable low-cost end-to-end data-centric network.

The common control plane simplifies network operation and management by automatically end-to-end provisioning of connections, managing network resources, and providing the level of QoS as shown in fig. 1. GMPLS control plane architecture includes the following protocols:

- Signaling Protocols: RSVP-TE and CR-LDP
- Intra-domain Routing Protocols like OSPF-TE and ISIS-TE
- Inter-domain Routing Protocol: BGP
- Link Management Protocol (LMP)

GMPLS defines only the forwarding mechanism using the control plane architecture; it uses other protocols to establish the LSPs. The control plane is divided into two parts [1], the signaling plane contains signaling protocols and the routing plane contains routing protocols.

II. PREVIOUS WORK

Bosco et al. [2] proposed a novel approach for Admission Control in Traffic Engineered data networks, which applied on a variety of scenarios, including IP/MPLS networks, ATM or Generalized MPLS. The proposed solution allows more efficient usage of network resources, especially at medium/high load, and increased robustness of the network. Tao Li et al. [3] specified a subset of CR-LDP for reconfigurable hardware implementation, such as FPGA based on specific architecture, SONET operating at STS-1 crossconnect rate for specific applications, file transfer and restoration in a SONET ring. He has emphasized that even with state-of-the-art processors, software implementations of signaling protocols are rarely capable of handling over 1000 calls/sec. He has stated that given the complexity of these signaling protocols, it is not feasible to implement these protocols in a “pure” hardware based design. Instead, only a subset of the protocol should be implemented in hardware and the remaining portion in software for execution on a general-purpose processor. In order to achieve high performance a careful selection of specific messages and parameters is requested so that a high percentage of signaling messages can be handled by the hardware module.
Guillermo [4], in his article describes the main functionality of GMPLS protocols and the extensions to existing protocols in Routing and Signaling. He also provides a review on the current status and outstanding issues to be solved prior to a wide deployment.

III. GMPLS DISTRIBUTED CONTROL PROTOCOLS

The major enhancements in the signaling protocols for GMPLS [5] are:
- A generalized label that can be encoded as a time slot, wavelength, or a port/fiber number.
- Label suggestion by upstream - It is very useful for faster LSP set up and also important when alternate LSPs are to be established after a network failure.
- Waveband switching support – Waveband is a set of contiguous wavelengths that can be switched together as a single unit to a new waveband. This may reduce distortion of individual wavelengths.
- Bi-directional LSP set up – Both upstream and downstream data paths between initiator and terminator can be set up using single set of signaling messages. This reduces setup time and amount of control messages are same as a unidirectional LSP. Thus, no additional overhead is involved.
- Capability for an upstream node to suggest a label or restrict the range of labels that may be selected by a downstream node.
- Capability to specify labels in explicit routes and record labels along a path.
- Extensions for rapid failure notification and handling capability.

Signaling to establish a traffic-engineered LSP is done using a label distribution protocol that runs on every MPLS node. The most popular protocols are RSVP-TE and CR-LDP. RSVP-TE is an extended version of RSVP to piggyback and distribute labels on its messages and to provide traffic-engineering, whereas, CR-LDP was specifically designed for this purpose.

Once a path has been selected, signaling protocols are used to set up each network element in the path. At each node, resource management is performed to ensure that setting up the service will allow the new service and all existing ones to meet their quality of service (QoS) obligations. Each node along the path does a final check and reserves the resources for the service. If any node cannot fulfill the service requirements, an error is generated and all the reserved resources at other nodes in the path are released. At this point, path calculation is repeated with updated information.

Once service signaling is complete, the service can be made available to the end user. The work of the control plane does not stop once the service has been created. It continually updates its ‘traffic engineering database’ to deal with failures and changing network load.

a. CR-LDP

One of the most important services that may be offered using MPLS in general and LDP in particular is support for constraint-based routing of traffic across the routed network. CR-LDP contains extensions for LDP to extend its capabilities such as setup paths beyond what is available for the routing protocol. For instance, an LSP can be setup based on explicit route constraints, QoS constraints, and other constraints. The impetus for this design was to use an existing protocol LDP and give it traffic-engineering capabilities. The traffic engineering requirements are met by extending LDP for support of constraint-based routed label switched paths (CR-LSPs) [6]. A major effort by Nortel Networks was made to launch the CR-LDP protocol.

Like any other LSP, CR-LSP is a path through an MPLS network. The difference is that while other paths are setup solely based on information in routing tables or from a management system, the constraint-based route is calculated at one point at the edge of network based on criteria [7] including but not limited to routing information.

b. Enhancements in CR-LDP

CR-LDP is a label distribution protocol specifically designed to support traffic engineering. It is largely based on the LDP specification with a set of extensions for carrying explicit routes and resource reservations. The new features [8] introduced in CR-LDP include:
- Explicit routing
- Resource reservation and classes
- Routing pinning
- Path Preemption
- Handling failures
- LSP ID

The call set-up procedure for CR-LPD is a very simple two-step process: a request and a map. The reason for the simple set-up is that CR-LDP is a hard-state protocol – meaning that the call, link, or path, once established, will not be broken down until it is requested that it be done. The major advantage of a hard-state protocol is that it should be more scaleable because there is less communication needed in order to keep the link active [9]. The basic flow for LSP setup using CR-LDP is as shown in fig. 2 [11]:

c. RSVP-TE

The Resource Reservation Protocol (RSVP-TE) protocol is an addition to the RSVP protocol for establishing label switched paths (LSPs) in MPLS networks. The extended RSVP protocol (RSVP-TE) supports the instantiation of explicitly routed LSPs with or without resource reservations. RSVP-TE [10] also supports smooth rerouting of LSPs, preemption, and loop detection.

RSVP-TE is used to establish MPLS LSPs when there are traffic engineering requirements. It is mainly used to provide QoS and load balancing across the network core and includes the ability to control all-optical networks.

An early method designed by the IETF in 1997, called Resource ReSerVation Protocol (RSVP), was designed for this very function. The protocol was designed to request required bandwidth and traffic conditions on a defined or explained path. If the bandwidth was available under the stated conditions, then the link would be established.
d. Enhancements in RSVP-TE

The RSVP was initially designed as a protocol for setting up resource reservation in IP networks. The RSVP-TE protocol extends the original protocol to perform label distribution and support explicit routing. The new features added to the original RSVP include [8]:

- Label distribution
- Explicit routing
- Bandwidth reservation for LSPs
- Rerouting of LSPs after failures
- Tracking of the actual route of an LSP
- Preemption options

The RSVP with features added to accommodate MPLS traffic engineering, is called RSVP-TE. The traffic-engineering functions allow for the management of MPLS labels or colors. The call set-up, or signaling, process is called "soft state" because the call will be torn down if it is not refreshed in accordance with the refresh timers [9]. The basic flow for setting up an LSP using RSVP for LSP Tunnels is shown in fig. 3 [11]

Some early arguments against RSVP included the problem of scalability: the more paths that were established, the more refresh messages would be created, and the network would soon become overloaded with refresh messages. Methods of addressing this problem include; not allowing the traffic links and paths to become too granular, and aggregating paths.

IV. COMPARISON OF THE DISTRIBUTED CONTROL PROTOCOLS

The table 1 summarizes the main technical similarities and differences between CR-LDP and RSVP for LSP Tunnels.

1) Vendor Support: In the industry today, Cisco and Juniper favor the RSVP-TE model and Nortel favors the CR-LDP model. Therefore, both signaling protocols are supported by major vendors.

2) Availability of Transport Protocol: The most obvious difference between CR-LDP and RSVP is the choice of transport protocol used to distribute the label requests. RSVP uses connectionless raw IP or UDP encapsulation for message exchange. Whereas CR-LDP uses UDP to discover MPLS peers and uses connection-oriented TCP sessions to distribute label requests.

3) Multicast Support: RSVP-TE and CR-LDP are designed to operate with current and future unicast and multicast routing protocols. In the multicast case, for example, a host sends IGMP messages to join a multicast group and then sends RSVP messages to reserve resources along the delivery path(s) of that group.

4) Security: Once the path has been established and the data is being forwarded (or switched) in the device’s hardware, the frame is no longer promoted up to the upper layers and visible to the software. There is minimal chance that unauthorized individuals will be able to sniff the data or redirect the flow from its intended destination. Data is only allowed to enter and exit the LSP at locations authorized and configured by the MPLS control software (control plane). Both CR-LDP & RSVP-TE have the support of MD5 signature password and authentication [12].

CR-LDP uses TCP/IP services, which is vulnerable to denial of service attacks. Therefore, any in-between errors are reported immediately whereas RSVP-TE uses UDP services. Authentication and policy control are specified for RSVP. This allows the originator of the messages to be verified (for example using MD5) and makes it possible to police unauthorized or malicious reservation of resources. Similar features could be defined for CR-LDP but the connection-oriented nature of the TCP session makes this less of a requirement.
Table 1: Comparison of CR-LDP and RSVP-TE signaling protocols

<table>
<thead>
<tr>
<th>Comparison</th>
<th>CR-LDP Support</th>
<th>RSVP Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendors</td>
<td>Nortel</td>
<td>Cisco, Juniper, Foundry</td>
</tr>
<tr>
<td>Transport</td>
<td>TCP</td>
<td>Raw IP</td>
</tr>
<tr>
<td>Multicast Support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Security</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Multipoint-to-Point</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>State</td>
<td>Hard</td>
<td>Soft</td>
</tr>
<tr>
<td>Data Storage</td>
<td>Less</td>
<td>High</td>
</tr>
<tr>
<td>Processing Load</td>
<td>Less</td>
<td>High</td>
</tr>
<tr>
<td>High Availability</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Failure Detection</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Re-routing</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Explicit Routing</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Route Pinning</td>
<td>Yes, by recording path</td>
<td>Yes</td>
</tr>
<tr>
<td>Traffic and Policy Control</td>
<td>Forward Path</td>
<td>Reverse Path</td>
</tr>
<tr>
<td>QoS Type</td>
<td>ATM</td>
<td>IntServ</td>
</tr>
<tr>
<td>Interoperability</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Negotiation of Label Space</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Tracing Route Support</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

5) **Multipoint Support:** Multipoint-to-point LSPs allow label switched paths to merge at intermediate LSRs, reducing the number of labels required in the system and sharing downstream resources. This approach works particularly well in packet-switched networks, but requires non-standard hardware in cell-switched networks such as ATM to prevent interleaving of cells. CR-LDP and RSVP support multipoint-to-point LSPs.

6) **State:** RSVP-TE is referred to as a soft state protocol. After initial LSP setup process, refresh messages must be periodically exchanged to notify the peers that the connection is still desired. This allows RSVP to pick up changes to the routing tree automatically. RSVP uses IP datagrams as its transport, meaning that control messages may be lost and that an adjacent node may fail without notification. State refreshes help to make sure that LSP state is properly synchronized between adjacent nodes. Periodic refresh messages imply the refresh overhead as a fundamental weakness in the protocol and therefore not scalable. The solution to reduce the refresh messages is bundling many refresh messages into single message to send as summary of messages in a group. This reduces the traffic volume but the processing time is still the same.

CR–LDP is referred to as a hard state protocol. This means that all the information is exchanged at the initial setup time, and no additional information is exchanged between routers until the LSP is torn down. CR-LDP does not require the LSRs to refresh each LSP after setup, since it is using TCP as the transport for control messages. CR-LDP can assume reliable delivery of messages using TCP. When the network management system or other entity determines that the LSP is no longer needed, messages must be exchanged notifying all routers that the resources should be reclaimed. This reclamation process is infrequent and consumes minimal bandwidth and CPU resources [12]. CR-LDP therefore currently presents a lower signaling load on the network itself than RSVP. However, once refresh reduction is implemented in RSVP, it will no longer be a high signaling load protocol.

7) **Data Storage Requirements**
For RSVP the requirements are much the same across the network because the state information must be kept at each LSR to be periodically refreshed. This data must include the traffic parameters, resource reservations and explicit routes. CR-LDP requires the Ingress and Egress LSRs to maintain a similar amount of state information, including the traffic parameters and explicit routes. In both the cases, it amounts to something of the order of 500 bytes per LSP. At intermediate LSRs in CR-LDP, it is possible to reduce the storage requirements to around 200 bytes by not offering support for LSP modification. Thus, the difference between RSVP and CR-LDP in an MPLS network where LSP modification is not required is made less significant.

8) **CPU Load:** The CPU load on the LSRs is determined by the number of messages they must parse and act upon, and by the complexity of the processing required for each message. The initial LSP setup flows are similar for both protocols, so the CPU load for this phase of an LSP’s life will not differ greatly. However, RSVP’s need to refresh state presents an additional load per LSP.

9) **High Availability:** Since RSVP is designed to run over a connectionless transport, it lends itself well to a system that must survive hardware failures or online software
14) Failure Detection: The failure detection techniques and speed are therefore similar for both CR-LDP and RSVP. CR-LDP uses HELLO and KEEPALIVE messages, whereas RSVP-TE uses Path and Resv messages to validate that the LSR peer and link are still active. MPLS failure detection is much faster for directly attached LSR.

11) Re-routing: Both RSVP and CR-LDP offer flexible approaches to re-routing and make-before-break provisioning of LSPs. An LSR using RSVP can install a new route by simply refreshing the Path for an LSP to a different next-hop as soon as the alternate route is available/required. The old path can be left to time out because refreshes will no longer be sent. However, this wastes resources on the old path. “Make-before-break” is a mechanism whereby the old path is used (and refreshed) while the new path is set up, and then the LSR performing the re-routing swaps to using the new path and tears down the old path.

12) Explicit Routing: Explicit routing refers to the congestion control mechanism; congestion control is done with the help of traffic engineering. Explicit routing is particularly useful to force an LSP down a path that differs from the one offered by the routing protocol. It can be used to distribute traffic in a busy network, to route around network failures or hot spots, or to provide pre-allocated back-up LSPs to protect against network failures. RSVP-TE supports this capability whereas CR-LDP does not because of unavailability of Traffic Engineering.

13) Route Pinning: Both CR–LDP and TE–RSVP support route pinning. Route pinning refers to force an LSP to stay in place after setup and not be rerouted by preemption. But in CR-LDP route pinning is set at the time of setting up the paths whereas in RSVP-TE, it may be set at any time by just modifying the path message.

14) Traffic and Policy Control

CR-LDP carries the full traffic parameters on the LABEL_REQUEST. As label request forwarded to next LSR resources are allocated simultaneously. If egress router determines about all resources throughout LSP are successfully reserved then LABEL_MAPPING is sent back to Ingress router. But in the case of RSVP, Path message just determines about the available resource when it was sent by Ingress router but resource reservation is done when Resv passes through the network back to Ingress router. Both CR-LDP and TE-RSVP employee policy based admission control.

15) QoS and DiffServ: The RSVP Tspec object carried on Path messages describes the data that will flow rather than the QoS that is required from the connection. The CR-LDP specification is more explicit about how the information carried on a LABEL_REQUEST message is mapped for QoS.

16) Interoperability: The option sets are functions of the flexibility of the protocol. RSVP has more implementation options than CR-LDP and so is perhaps at more risk. However, CR-LDP is specified to allow inter-working between implementations that support different function sets.

17) Negotiation of label space: CR-LDP negotiates about the label to agree upon one such label that is available for both LSRs from the peer whereas RSVP-TE selects the label during setup via network management. Therefore, if the network is very large then selection of label becomes a considerable issue for RSVP-TE.

18) Tracing route support: The RSVP record route object can be used to request that the list of nodes actually involved in the path setup be reported back to the Ingress. This can assist the network administrator when gathering information on network status and troubleshooting.

V. CONCLUSION

Making decision for the protocols on the basis of scalability, recovery, and interoperability between the signaling protocols is a difficult task. However, the RSVP-TE protocol has a big advantage. It is due to the fact that RSVP was an established protocol, with most of its bugs removed, prior to the inception of MPLS. Still both the protocols are under study and are being tested in the market.

Some key differences in the structure of the protocols and the underlying transport will not allow then protocols to converge completely. These differences and the differences in speed and scope of deployment will be the main factors that influence vendors when they are selecting a protocol.

The choice between RSVP-TE and CR-LDP should be guided by the function of the target system. What LSP setup model will be used? How stable are the LSPs – do they represent permanent trunks or short-duration calls? How large is the network and how complex is it? Is this a stand-alone network or must the components interoperate with other hardware and other networks?

A final consideration must be the robustness of the hardware solution. What level of fault tolerance is required? How important is high availability?

REFERENCES

Ahmad Ali Iqbal received his Bachelors degree in Computer Science from University of Central Punjab (UCP-PICS) Lahore Pakistan in 2003. He is currently doing Masters of Information Technology with the specialization in networking from NUST Institute of Information Technology, Rawalpindi, Pakistan. His research interests are Mobile and Wireless Ad-hoc Networks.

Dr. Waqar Mahmood is an Assistant Professor in NUST Institute of Information Technology, Rawalpindi, Pakistan. He has done his doctorate degree from USA in electronics engineering. His research interest includes Performance Measurement, network management and optical Internet Architecture.

Ejaz Ahmed completed his Masters degree from University of New South Wales, Australia. He is a lecturer in NUST Institute of Information Technology, Rawalpindi, Pakistan. His areas of interest include Information Security and Wireless Ad-hoc Networks.

Kashan Samad received his Bachelors degree in Computer Engineering from Sir Syed University of Engineering & Technology, Karachi, in 2003. He is currently doing Masters in Information Technology with the specialization in networking from NUST Institute of Information Technology, Rawalpindi, Pakistan. His research interests are Network Security and Wireless Ad-hoc Networks.