Volume 4, Issue 1, January 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Analysis of Routing and Signaling Protocols in MPLS

Rukhsana Thaker
CSE Department CoET
BGSB University ,Rajouri, J&K, India

Rashed Qayoom Shawl
ITE Department CoET
BGSB University ,Rajouri, J&K, India

Abstract-The demand for MPLS is increasing day by day in most internet service provider networks. Majority of the carriers are deploying MPLS in their backbone networks to facilitate a number of services and applications such as virtual private networks, quality of service (QoS) and traffic engineering. The most prime benefit provided by MPLS to an ISP network is the separation of routing from forwarding/switching via IP address header lookup. This paper provides an analysis of two commonly used IGP link-state routing protocols used to disseminate information about topology changes and restoration after a link failure and also comparison of OSPF with IS-IS is given. It also provides a detailed working and analysis of most widely used signaling protocols used for label distribution in MPLS network.

Keywords-MPLS, OSPF, IS-IS, Link-state, Cost, Lab

I. INTRODUCTION

Multi-Protocol Label Switching (MPLS) provides a mechanism for forwarding packets for any network protocol. Its capabilities have expanded massively, for example to support service creation (VPNs), traffic engineering, network convergence, and increased resiliency. Traditional IP networks are connectionless: when a packet is received, the router determines the next hop using the destination IP address on the packet alongside information from its own forwarding table. The router's forwarding tables contain information on the network topology, obtained via an IP routing protocol, such as OSPF, IS-IS, BGP, RIP or static configuration, which keeps that information synchronized with changes in the network. MPLS similarly uses IP addresses, either IPv4 or IPv6, to identify end points and intermediate switches and routers. This makes MPLS networks IP-compatible and easily integrated with traditional IP networks. However, unlike traditional IP, MPLS flows are connection-oriented and packets are routed along pre-configured Label Switched Paths (LSPs). Multiprotocol Label Switching (MPLS) is an Internet Engineering Task Force (IETF)-specified framework that provides for the designation, routing, forwarding and switching of traffic flows through the network. In MPLS, data transmission occurs on Label-Switched Paths (LSPs). LSPs are a sequence of labels at each and every node along the path from the source to the destination. LSPs are established either prior to data transmission (control-driven) or upon detection of a certain flow of data (data-driven). The labels are underlying protocol-specific identifiers. [4] MPLS is a versatile solution to address the problems faced by present-day networks-speed, scalability, quality-of-service (QoS) management, and traffic engineering. MPLS has emerged as an elegant solution to meet the bandwidth-management and service requirements for next-generation IP-based backbone networks.

II. MPLS PROTOCOLS

MPLS is a forwarding mechanism. It uses other protocols to established LSPs.
Two types of protocols are used: routing protocols and signaling protocols. We will discuss these protocols in detail.

III. ROUTING PROTOCOLS

The routing protocol distributes network topology information through the network so that the route of an LSP can be calculated automatically. An interior gateway protocol, such as OSPF or IS-IS, is normally used, as MPLS networks typically cover a single administrative domain.

A. *OSPF Background Information*

OSPF protocol was developed due to a need in the internet community to introduce a high functionality non-proprietary Internal Gateway Protocol (IGP) for the TCP/IP protocol family. [1] The discussion of the creation of a common interoperable IGP for the Internet started in 1988 and did not get formalized until 1991. At that time the OSPF Working Group requested that OSPF be considered for advancement to Draft Internet Standard. The OSPF protocol is based on link-state technology, which is a departure from the Bellman-Ford vector based algorithms used in traditional Internet routing protocols such as RIP. OSPF has introduced new concepts such as authentication of routing updates, Variable Length Subnet Masks (VLSM), route summarization, and so forth.

Link-States: OSPF is a link-state protocol. We could think of a link as being an interface on the router. The state of the link is a description of that interface and of its relationship to its neighboring routers. A description of the interface would include, for example, the IP address of the interface, the mask, the type of network it is connected to, the routers connected to that network and so on. The collection of all these link-states would form a link-state database.

© 2014, IJARCSSE All Rights Reserved

Shortest Path First Algorithm

OSPF uses a shorted path first algorithm in order to build and calculate the shortest path to all known destinations. The shortest path is calculated with the use of the Dijkstra algorithm. The algorithm by itself is quite complicated. This is a very high level, simplified way of looking at the various steps of the algorithm:

- Upon initialization or due to any change in routing information, a router generates a link-state advertisement. This advertisement represents the collection of all link-states on that router.
- All routers exchange link-states by means of flooding. Each router that receives a link-state update should store a copy in its link-state database and then propagate the update to other routers.
- After the database of each router is completed, the router calculates a Shortest Path Tree to all destinations. The router uses the Dijkstra algorithm in order to calculate the shortest path tree. The destinations, the associated cost and the next hop to reach those destinations form the IP routing table.
- In case no changes in the OSPF network occur, such as cost of a link or a network being added or deleted, OSPF should be very quiet. Any changes that occur are communicated through link-state packets, and the Dijkstra algorithm is recalculated in order to find the shortest path.

OSPF Cost

The cost (also called metric) of an interface in OSPF is an indication of the overhead required to send packets across a certain interface. The cost of an interface is inversely proportional to the bandwidth of that interface. A higher bandwidth indicates a lower cost.

OSPF Router Types

- Internal Router
- Backbone Router
- Area Border Router (ABR)
- Autonomous System Boundary Router (ASBR)
- Designated Router (DR)
- Backup Designated Router (BDR)

Internal Routers:

An internal router connects only to one OSPF area. All of its interfaces connect to the area in which it is located and does not connect to any other area.

If a router connects to more than one area, it will be one of the following types of routers.

Backbone Routers:

Backbone routers have one or more interfaces in Area 0 (the backbone area).

Area Border Router (ABR):

A router that connects more than one area is called an area border router or ABR. Usually an ABR is used to connect non-backbone areas to the backbone. If OSPF virtual links are used an ABR will also be used to connect the area using the virtual link to another non-backbone area.

Autonomous System Boundary Router (ASBR):

If the router connects the OSPF Autonomous System to another Autonomous System, it is called an Autonomous System Boundary Router (ASBR).

OSPF elects two or more routers to manage the Link State Advertisements:

Designated Router (DR):

Every OSPF area will have a designated router and a backup designated router. The Designated Router (DR) is the router to which all other routers within an area send their Link State Advertisements. The Designated Router will keep track of all link state updates and make sure the LSAs are flooded to the rest of the network using Reliable Multicast transport.

Backup Designated Router (BDR)

The election process which determines the Designated Router will also elect a Backup Designated Router (BDR). The BDR takes over from the DR when the DR fails.

OSPF Areas

OSPF areas are used to impose a hierarchical structure to the flow of data over the network. A network using OSPF will always have at least one area and if there is more than one area, one of the two areas must be the backbone area. OSPF has only 2 levels to its hierarchy, the backbone, and all other areas attached to it. Areas are used to group routers into manageable groups that exchange routing information locally, but summarize that routing information when advertising the routes externally. A standard OSPF network looks something like a big bubble (the backbone area) with a lot of smaller bubbles (stub areas) attached directly to it. Area Border Routers (ABR) are used to connect the areas. Each area will elect a designated router (DR) and a backup designated router (BDR) to assist in flooding Link State Advertisements (LSAs) throughout the area.[10]

Backbone (Area 0)

The backbone is the first area you should always build in any network using OSPF and the backbone is always Area 0 (zero). All areas are connected directly to the OSPF backbone area. When designing an OSPF backbone area, you should make sure there is little or no possibility of the backbone area being split into two or more parts by a router or link failure. If the OSPF backbone is split due to hardware failures or access lists, sizeable areas of the network will become unreachable.

© 2014, IJARCSSE All Rights Reserved

Totally Stub Area

A totally stubby area is only connected to the backbone area. A totally stubby / totally stub area does not advertise the routes it knows. It does not send any Link State Advertisements. The only route a totally stub area receives is the default route from an external area, which must be the backbone area. This default route allows the totally stub area to communicate with the rest of the network.

Stub Area

Stub areas are connected only to the backbone area. Stub areas do not receive routes from outside the autonomous system, but do receive the routes from within the autonomous system, even if the route comes from another area.

Not-So-Stubby (NSSA)

Frequently, it is advisable to use a separate network to connect the internal enterprise network to the Internet. OSPF makes provisions for placing an Autonomous System Boundary Router (ASBR) within a non-backbone area. In this case, the stub area must learn routes from outside the OSPF autonomous system. Thus, a new type of LSA was required--the Type 7 LSA. Type 7 LSA's are created by the Autonomous System Boundary Router and forwarded via the stub area's border router (ABR) to the backbone. This allows the other areas to learn routes that are external to the OSPF routing domain.

Enabling OSPF on the Router:

Enabling OSPF on the router involves the following two steps in config mode:

1. Enabling an OSPF process using the router ospf <*process-id*> command.
2. Assigning areas to the interfaces using the network <*network or IP address*> <*mask*> <*area-id*> command.

The OSPF process-id is a numeric value local to the router. It does not have to match process-ids on other routers. The network command is a way of assigning an interface to a certain area. The mask is used as a shortcut and it helps putting a list of interfaces in the same area with one line configuration line. The mask contains wild card bits where 0 is a match and 1 is a "do not care" bit, e.g. 0.0.255.255 indicates a match in the first two bytes of the network number.

The area-id is the area number we want the interface to be in. The area-id can be an integer between 0 and 4294967295 or can take a form similar to an IP address A.B.C.D.

B. *IS-IS Background*

The IS-IS protocol was developed by Digital Equipment Corporation as part of DECnet Phase V. It was standardized by the ISO in 1992 as ISO 10589 for communication between network devices which are termed Intermediate Systems (as opposed to end systems or hosts) by the ISO. The purpose of IS-IS was to make possible the routing of datagrams using the ISO-developed OSI protocol stack called CLNS. IS-IS was developed at roughly the same time that the Internet Engineering Task Force IETF was developing a similar protocol called OSPF. IS-IS was later extended to support routing of *datagrams* in the Internet Protocol (IP),[5] the Network Layer protocol of the global Internet. This version of the IS-IS *routing* protocol was then called *Integrated IS-IS* (RFC 1195). In recent years, the IS-IS routing protocol has become increasingly popular, with widespread usage among Service Providers. It is a link state protocol, which enables very fast convergence with large scalability. It is also a very flexible protocol and has been extended to incorporate leading edge features such as MPLS Traffic Engineering. Features of IS-IS include:

- Hierarchical routing
- Classless behaviour
- Rapid flooding of new information
- Fast Convergence
- Very scalable
- Flexible timer tuning
- Cisco IOS implementation of multi-area routing
- Cisco IOS implementation of route-leaking
- Cisco IOS implementation of overload-bit

C. *Comparison Of IS-IS with OSPF*

Both IS-IS and OSPF are link state protocols, and both use the same Dijkstra algorithm for computing the best path through the network. As a result, they are conceptually similar. Both supports variable length subnet masks, can use multicast to discover neighboring routers using *hello packets*, and can support authentication of routing updates.

While OSPF is natively built to route IP and is itself a Layer 3 protocol that runs on top of IP, IS-IS is natively an OSI network layer protocol (it is at the same layer as CLNS). The widespread adoption of IP worldwide may have contributed to OSPF's popularity. IS-IS does not use IP to carry routing information messages. IS-IS is neutral regarding the type of network addresses for which it can route. OSPF, on the other hand, was designed for IPv4. This allowed IS-IS to be easily used to support IPv6. To operate with IPv6 networks, the OSPF protocol was rewritten in OSPF v3 (as specified in RFC 2740).

IS-IS routers build a topological representation of the network. This map indicates the subnets which each IS-IS router can reach, and the lowest-cost (shortest) path to a subnet is used to forward traffic.

IS-IS differs from OSPF in the way that "areas" are defined and routed between. IS-IS routers are designated as being: Level 1 (intra-area), Level 2 (inter area), or Level 1-2 (both). Level 2 routers are inter-area routers that can only form relationships with other Level 2 routers. Routing information is exchanged between Level 1 routers and other Level 1

© 2014, IJARCSSE All Rights Reserved

routers, and Level 2 routers only exchange information with other Level 2 routers. Level 1-2 routers exchange information with both levels and are used to connect the inter area routers with the intra area routers.

In OSPF, areas are delineated on the interface such that an area border router (ABR) is actually in two or more areas at once, effectively creating the borders between areas inside the ABR, whereas in IS-IS area borders are in between routers, designated as Level 2 or Level 1-2. The result is that an IS-IS router is only ever a part of a single area.

IS-IS also does not require Area 0 (Area Zero) to be the backbone area through which all inter-area traffic must pass. The logical view is that OSPF creates something of a spider web or star topology of many areas all attached directly to Area Zero and IS-IS by contrast creates a logical topology of a backbone of Level 2 routers with branches of Level 1-2 and Level 1 routers forming the individual areas.

IS-IS also differs from OSPF in the methods by which it reliably floods topology and topology change information through the network. However, the basic concepts are similar.

OSPF has a larger set of extensions and optional features specified in the protocol standards. However IS-IS is easier to expand: its use of type-length-value data allows engineers to implement support for new techniques without redesigning the protocol. In addition to that, IS-IS is less "chatty" and can scale to support larger networks. Given the same set of resources, IS-IS can support more routers in an area than OSPF. This has contributed to IS-IS as an ISP-scale protocol.

IV. SIGNALING PROTOCOLS

The signaling protocols are used for the switches in a LSP. It informs the switches about the labels and link for each LSP. Four types of signaling protocols are used depending upon the application. These are LDP, CR-LDP, RSVP, and RSVP-TE. LDP is used when Traffic engineering is not required. CR-LDP is an extension of LDP. RSVP-TE is used for MPLS transport where Traffic Engineering is required. BGP is used for certain MPLS VPN services. We will discuss these signaling in detail.

A. *Label Distribution Protocol (LDP)*

LDP is a fairly simple signaling protocol that behaves much like one of the IGPs (OSPF and IS-IS). LDP runs on top of an IGP configuration, which means you have to get OSPF or IS-IS running first. Moreover, you must configure LDP on the exact set of interfaces as your IGP.

After you configure both your IGP and LDP on an interface, LDP begins transmitting and receiving LDP messages on that interface. [14] LDP starts off by sending LDP discovery messages to all the LDP-enabled interfaces. When an adjacent router receives the discovery message, it establishes a TCP session with the source router. In the MPLS (Multi Protocol Label Switching) 2 label switching routers (LSR) must agree on the meaning of the labels used to forward traffic between and through them. LDP (Label Distribution Protocol) is a new protocol that defines a set of procedures and messages by which one LSR (Label Switched Router) informs another of the label bindings it has made.

Two LSRs (Label Switched Routers) which use LDP to exchange label mapping information are known as LDP peers and they have an LDP session between them. In a single session, each peer is able to learn about the others label mappings, in other words, the protocol is bi-directional. Four LDP messages are used for a session to establish:

a) Discovery message: using this message LSR shows its presence in the network by sending Hello message to all the peers in the network as a UDP packet.

b) Session message: When a new session must be established, the hello message is sent over TCP. Apart from the Discovery message; all other messages are sent over TCP

c) Advertisement messages: These are used for advertisement of LSR.

d) Notification message: These are error messages and other events of interest. There are two kinds of Notification messages. Error notification and Advisory notification.

Error notification messages: these signal fatal errors and cause termination of the session.

Advisory notifications: these are used to pass on LSR information about the LDP Session or the status of some previous message.

MESSAGES

Messages are sent as LDP PDUs. Each PDU can contain more than one LDP message. Each LDP PDU is an LDP header followed by one or more LDP message.

LDP HEADER

2 bytes	2 bytes
Version	PDU Length
LDP Identifier 6 bytes	

Fig: LDP Header

© 2014, IJARCSSE All Rights Reserved

-Version: The protocol version number. The present number is 1.
-LDP identifier: This field uniquely identifies the label space of the sending LSR for which this PDU applies. The first 4 octets encode the IP address assigned to the LSR. The last 2 indicate a label space within the LSR

LDP MESSAGE

UMessage type	Message Length
Message ID	
Parameters	

Fig: LDP Message Format

-U: The U bit is an unknown message bit.
- Message type: The type of message. The following message types exist:

0x001 - Notification
0x100 - Hello
0x200 - Initialization
0x201 - Keep Alive
0x300 - Address
0x301 - Address Withdraw
0x400 - Label Mapping
0x401 - Label Request
0x404 - Label Abort request
0x402 - Label Withdraw
0x403 - Label Release
Default - Unknown Message Name

-Message length: The length in octets of the message ID, mandatory parameters and optional parameters:
- Message ID: 32-bit value used to identify the message.
-Parameters: The parameters contain the TLVs. There are both mandatory and optional parameters. Some messages have no mandatory parameters, and some have no optional parameters.

TLV format

UF	Type	Length
Value		

-U: The U bit is an unknown TLV bit.
-F: Forward unknown TLV bit.
-Type: Encodes how the Value field is to be interpreted.
-Length: Specifies the length of the Value field in octets.
-Value: Octet string of Length octets that encodes information to be interpreted as specified by the Type field.

The following are optional TLV parameters:

100 Fec
101 Address List
103 Hop Count
104 Path Vector
200 Generic Label
201 ATM Label
202 Frame Relay Label
300 Status
301 Extended Status
302 Returned PDU
303 Returned Message
400 Common Hello Parameters.
401 Transport Address
402 Configuration Sequence Number
500 Common Session Parameters

© 2014, IJARCSSE All Rights Reserved

501 ATM Session Parameters
502 Frame Relay Session Parameters
600 Label Request Message ID

B. *CR-LDP*

CR-LDP (constraint-based LDP) contains extensions for LDP to extend its capabilities. CR-LDP is specifically designed to facilitate constraint-based routing of LSPs. Like LDP, it uses TCP sessions between LSR peers and sends label distribution messages along the sessions.

This allows it to assume reliable distribution of control messages. This allows extending the information used to setup paths beyond what is available for the routing protocol.CR-LDP is the same as LDP but has the following additional TLV parameters.

Value	Parameter
821	LSPID
822	ResCls
503	Optical Session Parameters
800	Explicit Route
801-804	ER-Hop TLVS
810	Traffic Parameters
820	Preemption
823	Route Pinning
910	Optical Interface Type
920	Optical Trail Desc
930	Optical Label
940	Lambada Set

The basic flow for LSP setup using CR-LDP is as shown below:

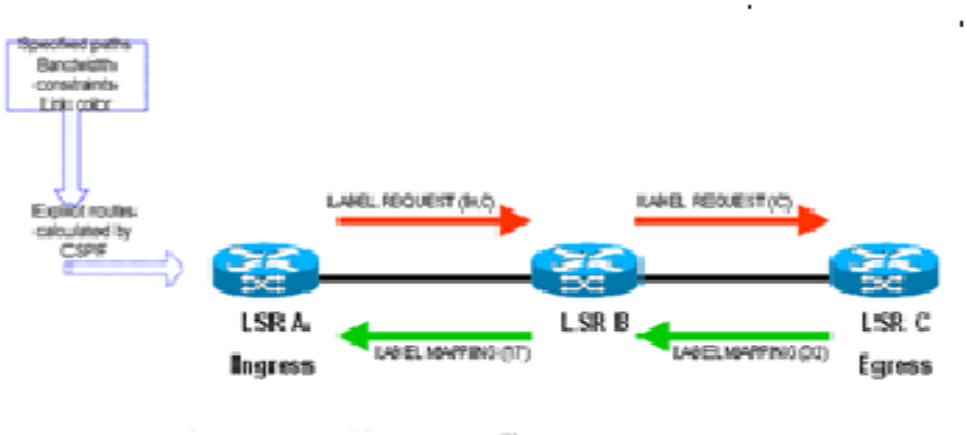

Figure 1 CR-LDP LSP flow set up

The Ingress LSR, LSR A, determines that it needs to set up a new LSP to LSR C. The traffic parameters required for the session or administrative policies for the network enable LSR A to determine that the route for the new LSP should go through LSR B, which might not be the same as the hop-by-hop route to LSR C. LSR A builds a LABEL_REQUEST message with an explicit route of (B,C) and details of the traffic parameters requested for the new route. LSR A reserves the resources it needs for the new LSP, and then forwards the LABEL_REQUEST to LSR B on the TCP session.

- LSR B receives the LABEL_REQUEST message, determines that it is not the egress for this LSP, and forwards the request along the route specified in the message. It reserves there sources requested for the new LSP, modifies the explicit route in the LABEL_REQUEST message, and passes the message to LSR C. If necessary, LSR B may reduce the reservation it makes for the new LSP if the appropriate parameters were marked as negotiable in the LABEL_REQUEST.
- LSR C determines that it is the egress for this new LSP. It performs any final negotiation on the resources, and makes the reservation for the LSP. It allocates a label to the new LSP and distributes the label to LSR B in a LABEL_MAPPING message, which contains details of the final traffic parameters reserved for the LSP.
- LSR B receives the LABEL_MAPPING and matches it to the original request using the LSP ID contained in both the LABEL_REQUEST and LABEL_MAPPING messages. It finalizes the processing at LSR A is similar, but it does not have to allocate a label and forward it to an upstream LSR because it is the ingress LSR for the new LSP.

C. *Resource Reservation Protocol (RSVP)*

RSVP is a bit more complex than LDP and offers traffic engineering features that aren't available with LDP-signaled LSPs. RSVP works by setting up unidirectional paths between an LSP ingress router and an egress router. In the configuration, we specify what the bandwidth requirements are for an LSP. After configuring these paths and enabling RSVP, the ingress router sends a path message to the egress router. The path message contains the configured information about the resources required for the LSP to be established.

© 2014, IJARCSSE All Rights Reserved

When the egress router receives the path message, it sends a reservation message back to the ingress router in response. This reservation message is passed from router to router along the same path as the original path message (in opposite order, of course). Once the ingress router receives this reservation message, an RSVP path is established that meets the required constraints.

All the LSRs along the path receive the same path and reservation messages, which contain the bandwidth reservation requirements. If they have the available bandwidth (that is, if no other higher-priority RSVP LSP has reserved bandwidth), they're included in the LSP. If a router doesn't have available bandwidth, it generates its own reservation message, and a new route that doesn't include the offending router is found. If no route can be found, the LSP isn't established.

The established LSP stays active as long as the RSVP session stays active. RSVP maintains activity through the continued transmission and response to RSVP path and reservation messages. If the messages stop for three minutes, the RSVP session terminates, and the LSP is lost. Apart from the existing message types listed in RSVP an additional message type is available:

Value	Message type
14	Hello

In addition, the following additional Protocol Object Types exist:

Value	Object type
16	Label
19	Optical
20	Explicit Route
21	Record Route
22	Hello
207	Attribute Session

The basic flow for setting up an LSP using RSVP for LSP Tunnels is shown in Fig below:

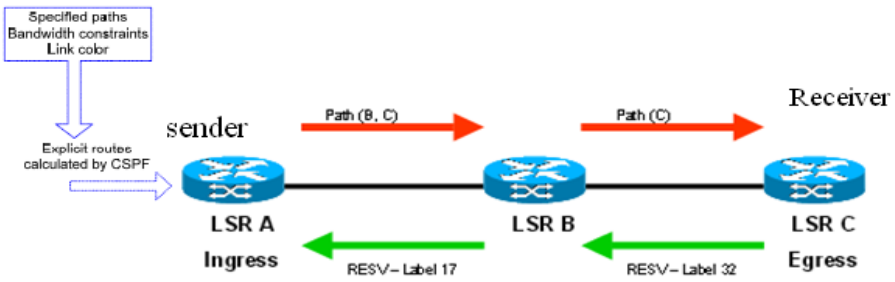

Fig 2. RSVP LSP setup Flow

The Ingress LSR, LSR A, determines that it needs to set up a new LSP to LSR C. The traffic parameters required for the session or administrative policies for the network enable LSR A to determine that the route for the new LSP should go through LSR B, which might not be the same as the hop-by-hop route to LSR C. LSR A builds a Path message with an explicit route of (B, C) and details of the traffic parameters requested for the new route. LSR A then forwards the Path to LSR B as an IP datagram.

- LSR B receives the Path request, determines that it is not the egress for this LSP, and forwards the request along the route specified in the request. It modifies the explicit route in the Path message and passes the message to LSR C.
- LSR C determines that it is the egress for this new LSP determines from the requested traffic parameters what bandwidth it needs to reserve and allocates the resources required. It selects a label for the new LSP and distributes the label to LSR B in a Resv message, which also contains actual details of the reservation required for the LSP. LSR B receives the Revs message and matches it to the original request using the LSP ID contained in both the Path and Resv messages. It determines what resources to reserve from the details in the Resv message, allocates a label for the LSP, sets up the forwarding table, and passes the new label to LSR A in a Revs message.
- The processing at LSR A is similar, but it does not have to allocate a new label and forward this to an upstream LSR because it is the ingress LSR for the new LSP.

D. *The RSVP-TE* (traffic extension)

This protocol is an addition to the RSVP protocol with special extensions to allow it to set up optical paths in an agile optical network. The RSVP protocol defines a session as a data flow with a particular destination and transport-layer protocol. However, when RSVP and MPLS are combined, a flow or session can be defined with greater flexibility and generality. The ingress node of an LSP (Label Switched Path) uses a number of methods to determine which packets are assigned a particular label. Once a label is assigned to a set of packets, the label effectively defines

© 2014, IJARCSSE All Rights Reserved

the flow through the LSP. We refer to such an LSP as an LSP tunnel because the traffic through it is opaque to intermediate nodes along the label switched path. New RSVP Session, Sender and Filter Spec objects, called LSP Tunnel IPv4 and LSP Tunnel IPv6 have been defined to support the LSP tunnel feature. The semantics of these objects, from the perspective of a node along the label switched path, is that traffic belonging to the LSP tunnel is identified solely on the basis of packets arriving from the "previous hop" (PHOP) with the particular label value(s) assigned by this node to upstream senders to the session. In fact, the IPv4 (v6) that appears in the object name only denotes that the destination address is an IPv4 (v6) address. When referring to these objects generically, the qualifier LSP Tunnel is used.[15]

In some applications it is useful to associate sets of LSP tunnels. This can be useful during reroute operations or in spreading a traffic trunk over multiple paths. In the traffic engineering application, such sets are called traffic engineered tunnels (TE tunnels). To enable the identification and association of such LSP tunnels, two identifiers are carried. A tunnel ID is part of the Session object. The Session object uniquely defines a traffic engineered tunnel. The Sender and Filter Spec objects carry an LSP ID. The Sender (or Filter Spec) object, together with the Session object, uniquely identify an LSP tunnel

Comparative Analysis:

The key differences between CR-LDP and RSVP are the reliability of the underlying transport protocol and whether the resource reservations are done in the forward or reverse direction. From these points come many of the other functional differences. The table below summarizes the main technical similarities and differences between CR-LDP and RSVP for LSP Tunnels. The sections that follow explain in greater detail the implications of these technical differences between the protocols.

Table 1: comparative analysis of CR-LDP AND RSVP

	CR-LDP	**RSVP**
Transport	TCP	IP
Security	Yes	Yes
Multipoint-to-point	Yes	Yes
Multicast Support	no	no
LSP Merging	Yes	Yes
LSP State	Hard	Soft
LSP Refresh	Not needed	Periodic, hub by hub
High Availability	No	Yes
Re-routing	yes	yes
Explicit routing	Strict and loose	Strict and loose
Route Pinning	Yes	Yes by recording path
LSP Preemption	Yes, Priority based	Yes, priority based
LSP Protection	yes	Yes
Shared Reservation	No	yes
Traffic Exchange	Yes	Yes
Traffic control	Forward path	Reverse path
Policy Control	Implicit	Explicit
Layer3 Protocol Indicated	No	yes
Resource Class Constraint	Yes	no

V. CONCLUSION

Multiprotocol Label Switching (MPLS) combines the intelligence of routing with the performance of switching and provides considerable benefits to networks with a pure IP architecture as well as those with IP and ATM or a mix of

© 2014, IJARCSSE All Rights Reserved

other Layer 2 technologies. This paper provides an overview on the working and features of routing protocols OSPF & IS-IS and also does a comparison of these two on the basis of the features and functionalities that one offers over another while being deployed in MPLS carrier network. The paper highlights most commonly used signaling techniques used in label distribution and indicates the benefits and limitations of one over another.

REFERENCES

[1] www.cisco.com *white papers* on OSPF.
[2] www.cisco.com/networkers/nw00/pres/2204.pdf
[3] S. Alouneh, S. Abed, M. Kharbutli, B. J. Mohd, "*MPLS Technology in wireless networks*", 2013, Springer.
[4] Y.Cheng, "*MPLS"*, 2003, white paper.
[5] http://en.wikipedia.org/wiki/IS-IS .
[6] Cisco press article on MPLS , www.cisco.com
[7] Cisco Systems Inc.: *Cisco Carrier Routing System* (2006). www.cisco.com
[8] MPLS networks Operations guide log reference by Juniper Networks, 2010.
[9] D. Bella, R. Sperber, "*MPLS –TP the new technology for packet transport networks*" , White paper.
[10] S.Kim, J.Chung, "*Analysis of MPLS signaling protocols and Traffic Dissemination in OSPF and MPLS*" , 2007, IEEE.
[11] M. K., Porwal, A.Yadav, S.V.Charhate, "*Traffic Analysis of MPLS and Non MPLS Network including MPLS Signaling Protocols and Traffic distribution in OSPF and MPLS*", 2008,IEEE.
[12] P.Brittain, A.Ferral,"*MPLS Traffic Engineering: A Choice of Signaling Protocols*", 2000,Data connection ltd.
[13] M M. Al-Quzwini, S K. Ibrahim ,"*Performance Evaluation Of Traffic Engineering Signal Protocols in IPv6 MPLS network* ",2012, http://www.SciRP.org/journal/cn
[14] "*Understanding the LDP singnaling Protocol*", Juniper.net
[15] K.K.Nguyen,B.Jaumard,"*A MPLS/LDP Distributed architecture for Next Generation Routers*",2013, Springer

© 2014, IJARCSSE All Rights Reserved