LABEL DISTRIBUTION PROTCOL & LOOP FREE ALTERNATIVE

Piyush Garg

University of Alberta

Supervisor: Juned Noonari

Submitted to: Dr. Mike Macgregor

ABSTRACT

Multiprotocol Label Switching has been used by service providers as well as the enterprises for its scalability and also for providing end to end IP services with simple and easy configuration. With the increase in the multiprotocol label switching networks it is important to understand the components which make this protocol so easy to configure.

Label Distribution Protocol is one such component which has made the working and configuring of the multiprotocol label switching networks very easy. In this report, we are going to see the working of label distribution protocol along with their use in various multiprotocol label switching topologies.

It is very important to have a protection in case of failure in the network and this backup becomes more important when the that network is being used by the service providers. So, in this report we are going to look into loop free alternative which provides a protection to the multiprotocol label switching networks in case there is any failure.

Contents

INTRODUCTION

In this report, we have analyzed and demonstrated the working of label distribution protocol and its working in various topologies of the multiprotocol label switching networks. Also, advantages and disadvantages related to the working of label distribution protocol has been covered along with the new research in the field of label distribution protocol.

A protection mechanism which is used in the multiprotocol label switching networks known as free loop alternative has been introduced in this report along with its working. Also the advantage of using loop free alternative has been shown with new advancements in loop free alternative.

The section A covers the working of label distribution protocol and loop free alternative. The section B covers the lab in which it has been demonstrated that how label distribution protocol and loop free alternative are used. The section C covers the final part and that is the conclusion of the report which answers the question that why label distribution protocol and loop free alternative is required.

SECTION A

LABEL DISTRIBUTION PROTOCOL

LOOP FREE ALTERNATIVE

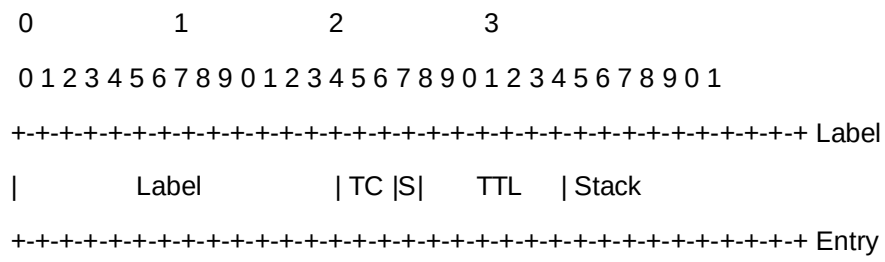
MULTIPROTOCOL LABEL SWITCHING

Multiprotocol Label Switching has not only enabled Enterprises but also the Service Providers to be able to provide and build such an amazing network which are capable of delivering a wide variety of advanced services by using a single infrastructure.

Multiprotocol label switching has provided networks which are protocol independent, highly scalable and provide advanced as well as value added services over a single infrastructure. In multiprotocol label switching every data packet is given a label and the packets will be forwarded by using that label. The benefit of label is that an end to end circuit can be created over any medium and with any protocol. Therefore, Multiprotocol Label Switch can be integrated on any existing technology such as ATM, Frame Relay or Ethernet without any difficulty and it can also be integrated with different technologies without any need to change their environment. Multiprotocol Label Switching can also be viewed as layer 2.5 protocol as it lies between layer 2 and layer 3 protocol.

Multiprotocol Label headers are twenty bits in length and are inserted between the layer three packets and its layer two header.

The illustration below has been taken from the IETF's RFC3032 and depicts the format of an MPLS label.



Label: Label Value, 20 bits

TC: Traffic Class field, 3 bits

S: Bottom of Stack, 1 bit

TTL: Time to Live, 8 bits

S: Bottom of Stack, 1 bit

TTL: Time to Live, 8 bits

In Multiprotocol Label Switching, more than one label can be on top of the packet so that the packets can be routed through that network. In order for this labels are put into the stack. The label which is at the top of the stack is called the top label and the label which is at the last of the stack is called the bottom label. There are some Multiprotocol Label Switching applications which requires more than one label so that the labeled packets can be forwarded. MPLS VPN and AToM are such Multiprotocol Label Switching application that requires two labels in the label stack.

In the front of Layer 3 packet the label stack is present. It lies before the header of the transported protocol, but after the Layer 2 header. The Multiprotocol Label Switching label stack is also known as the shim header because of the way it has been placed.

LABEL SWITCH ROUTER

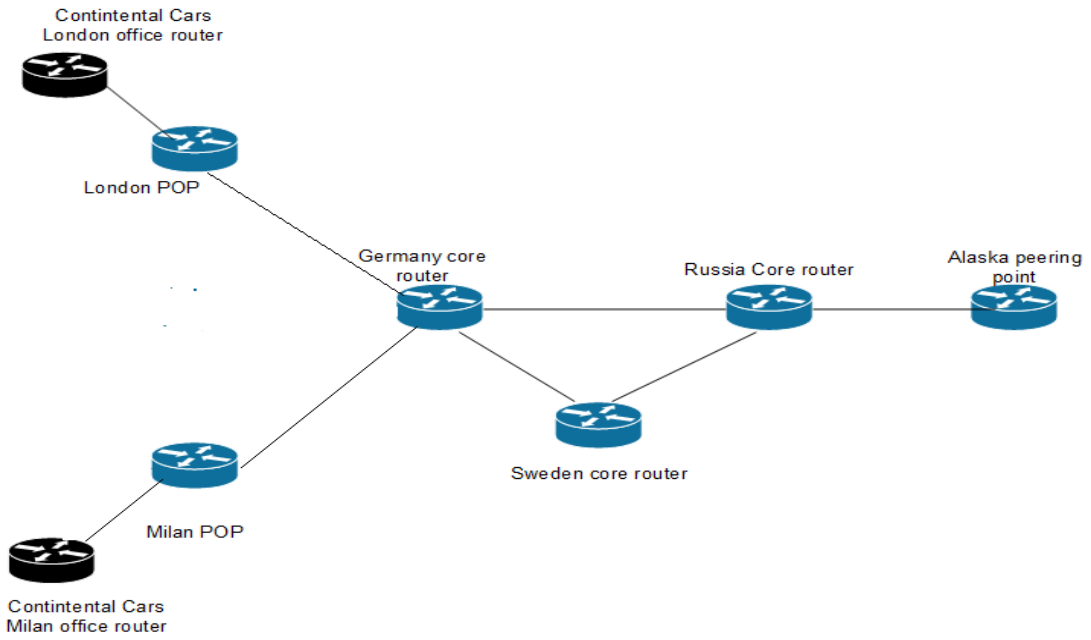
A label switch router is a router that is used for performing and supporting MPLS functions. Label Switch Routers are used for switches labels in order to route packets through the MPLS network. There are three kinds of Label Switch Routers:

a) Ingress LSR**-** This router is at the edge of the MPLS network and the ingress router will receive the packets which has not been labelled. The ingress LSR will attach the label on the packet and the packet will be forwarded through the MPLS network.

b) Intermediate LSR**-**The routers which are situated within the MPLS networks are known as intermediate routers. These routers are responsible for performing operations within the MPLS networks.

c) Egress LSR**-**The egress LSR is also at the edge of the MPLS network. The egress LSR is the last point in the MPLS network as it will receive the labelled packet and it will remove the labels from the packets.

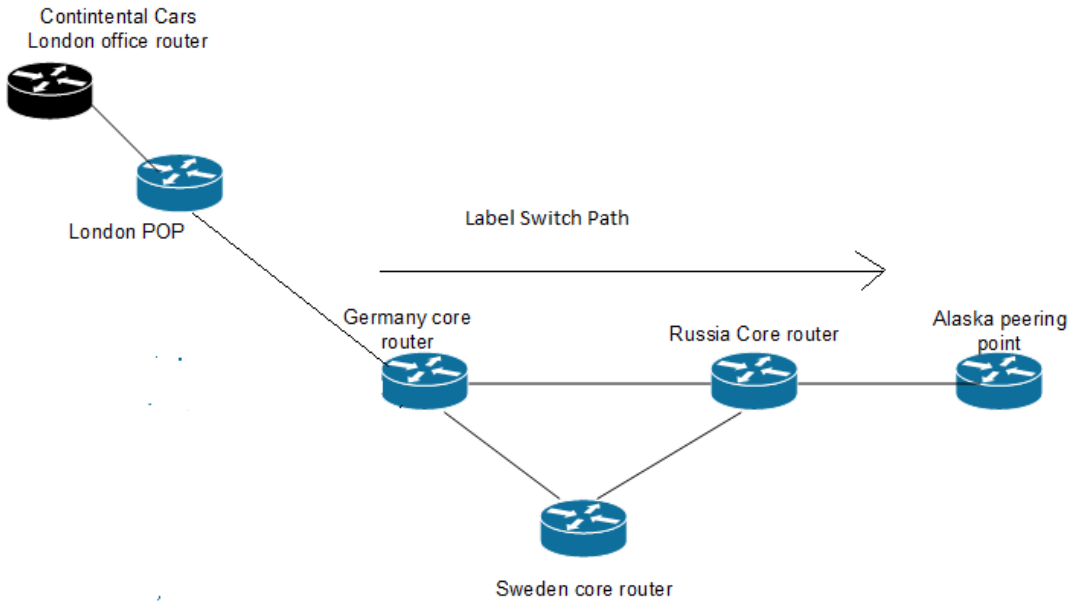
The Label switch routers are responsible for three operations which are swap, pop as well as push. Imposing LSR are the LSR which impose label to the packet which has not been labelled. Ingress LSR is one of the imposing LSR. Disposing LSR are the LSR which will remove the labels from the packet before the packet is moved out of the MPLS network. Egress LSR is one of the disposing LSR.



In the above figure, London POP will be the ingress label switch router as the label will be attached at this router. The Germany core router will be the intermediate label switch router as operations like pop, swap and push will be performed at this router. The Milan POP will be the egress label switch router as the label will be removed at this router.

LABEL SWITCHED PATH

A label switched path consists of series of Label Switch Routers which are combined to form a path so that a labelled packet can be transported through a MPLS network. In the Label Switched Path, the first Label switch router where MPLS label is attached will be the ingress label switch router. The last label switch router where the MPLS label will be removed will be the egress router for that label switched path. In the labelled switch path, the label switch routers which will lie between the ingress label switch router and egress label switch routers will be intermediate label switch routers.



In this figure, the direction of the label switched path has been shown. The label switch path is unidirectional and if the direction of traffic is reversed it would become a new label switched path.

FORWARDING EQUIVALENCE CLASSES

Forwarding Equivalence Classes groups, the packets and these groups of packets are then forwarded along the same path and are treated according to the forwarding treatment. In Forwarding Equivalence Classes, all the packets which are using the same forwarding equivalence classes must also have the same label but it is not necessary that all the packets which are having the same label are belonging to the same forwarding equivalence classes as there might be difference in their forwarding treatment or their EXP value can also be different or they can belong to a completely different forwarding equivalence classes. It is the decision of ingress label switch router that which packet will belong to which forwarding equivalence class because ingress label switch router is responsible for putting labels on the packets.

LABEL FORWARDING INSTANCE BASE

The label forwarding instance base is a table which is used for forwarding labelled packets in multiprotocol label switching networks. The label forwarding instance base table contains the information for both the incoming as well as outgoing labels for all the label switch paths. The label which contains information regarding the local binding on the label switch router becomes the incoming label whereas the label which is selected by the label switch router from all the remote bindings becomes the outgoing label. These remote bindings are present in label information base. The remote labels are selected on the basis of the best path which is present in the routing table. The outgoing label which has been chosen from all the remote bindings is then installed in the label forwarding instance base. However, whenever an incoming packet which is labelled has to be forwarded label forwarding instance base will be used.

DISTRIBUTION OF LABEL

The ingress label switch router will attach the label with the packet and that label will represent one label switch path. This label switch path will contain the information regarding the path of the packet through the MPLS network. The changes are made at the top label where at each hop the top label is swapped with another label and the packet is transmitted which is done by the intermediate label switch router. The egress label switch router will remove the label in the end and will then forward the packet.

For example, in case of IPv4-over-MPLS which is made up of label switch routers that run Interior Gateway Protocols like Open Shortest Path First, Enhanced Interior Gateway Routing Protocol and Intermediate System to Intermediate System. Here the ingress label switch router will look for the IPv4 destination, label will be attached and the packet will be forwarded. The intermediate label switch router will receive that packet and it will also swap the incoming label with the other outgoing label before the packet is forwarded. The egress label switch router will remove the label from that packet and that IPv4 packet will be forwarded without having any labels.

This scenario can only work if the adjacent label switch routers have knowledge regarding the label which is being used for each Interior Gateway Protocol prefix because it is important for the intermediate label switch router to know which incoming label must be switched with which outgoing label.

Therefore, a way is needed by which the routers can be told that which label will be used when the packet has to be forwarded. This can only happen if the routers are able to communicate with each other otherwise they will not be able to figure out which incoming label needs to be exchange with the outgoing label. So, a mechanism known as label distribution protocol has been used.

The label could be distributed by the following methods: -

a) The functionality of the exciting protocols could be extended

b) By creating a separate protocol for distributing labels

FUNCTIONAITY OF EXCITING PROTOCOL

By using the first method, no new protocol will be needed for running the label switch router but the functionality of the exciting protocols will be extended for carrying the labels. This will not be an easy task as there are different numbers of routing protocols and it can also cause interoperability issues between routers which support this new technique and those routers which doesn't. The main advantage of using this functionality is that routing and label distribution will always be in synchronization and incase the prefix is missing there will not be any label and vice versa.

In distance vector routing protocol, the router will take a prefix from the routing table and bind the label with that prefix. However, the working of link state routing protocol is different as every router will generate link state updates and these updates are exchanges with each other within one area. For the above functionality to work, for every prefix a label will need to be distributed by all the routers even by those routers which are not originating that prefix. This is not the way link state routing protocol works and therefore a new protocol is needed by link state routing protocol for distributing labels.

The first method was never used with any Interior Gateway Protocols and Border Gateway protocol is the only protocol capable of distributing labels and it can also carry prefix.

SEPARATE PROTOCOL FOR DISTRIBUTING LABLELS

The advantage of using separate protocol for distributing labels is not being dependent on the routing protocols. A separate protocol will distribute the labels and the routing protocol will distribute the prefixes irrespective of IP routing

protocols and whether that protocol has the ability to distribute labels or not. The only disadvantage of using this separate protocol is that label switch routers will have to run a new protocol. A new label distribution protocols were chosen to distribute labels. Some of these protocols are: -

a) Tag Distribution Protocol

b) Resource Reservation Protocol

c) Label Distribution Protocol

TAG DISTRIBUTION PROTOCOL

The first protocol to be used for label distribution purposes was tag distribution protocol. This protocol was developed by cisco and was cisco proprietary. Labels were attached with IP packets and it used to be called tag switching. The implementation of the tag switching was introduced by the cisco in 1998. At that time labels were known as tags and these tags were assigned to the network. These tags were then attached with the packet and forwarded to its destination. However, in 1999 tag switching was standardized into label distribution protocol. Both label distribution protocol and tag switching protocol have similarity in operation but label distribution protocol has more advantage as compared to tag distribution protocol it has more functionality. Therefore, label distribution protocol replaced tag distribution protocol and tag distribution protocol is becoming obsolete in today's scenario.

RESOURCE RESERVATION PROTOCOL

For the Multiprotocol label switching traffic engineering two signaling protocols were introduced. One was resource reservation protocol and the other one was constraint based label distribution protocol. However, at the Internet engineering task force it was decided that the resource reservation protocol will be developed as the signaling protocol for multiprotocol label switching traffic engineering and no further work will be done on the progress of constraint based label distribution protocol which has been documented in RFC 3468.

Resource Reservation Protocol is a signaling protocol which is used by Multiprotocol label switching Traffic Engineering. This protocol helps the intermediate label switch router to verify if the incoming and outgoing labels are for

that label switch path on the traffic engineering tunnel. By using this protocol, intermediate label switch routers know regarding the labels being used from the head end router. In order to carry multiprotocol label switching labels information and other traffic engineering specifics like record route object and explicit route certain modifications were made on the resource reservation protocol. The role of resource reservation protocol is to signal the traffic engineering tunnel which starts from head end label switch router and which ends at the tail end label switch router according to the result taken form the traffic engineering database which is on the head end label switch router.

LABEL DISTRIBUTION PROTOCOL

Label distribution protocol is used by the Label Switch Router (LSR) to collect and distribute information regarding the label prefix binding from and to the other label switch routers present in the network. By using label distribution protocol, label switch routers are able to discover peers and able to exchange information regarding the label binding by forming sessions with these peers and the information regarding the label bindings which that label switch router has made can be forwarded to the another label switch router.

A label switch path is established when the pair of routers agree on the label distribution parameters. With the help of label distribution protocols, labels are distributed by the label switch routers along the routed path so that multiprotocol label switching forwarding can be supported and this method is known as hop-by-hop forwarding. In multiprotocol label switch forwarding, once the packet reaches the router, it will check the incoming label, that label will be looked up in the table and that packet will then be forwarded onto the next hop. Label distribution protocol can easily be applied on hop-by-hop forwarding. Therefore, MPLS VPNs can use label distribution protocols easily as they use hop-by-hop forwarding mechanism.

Label distribution protocol provides a functionality by distributing hop by hop or dynamic labels to those routers which are in use by the Interior Gateway Protocol routing protocols. By using this functionality, a Label Switch Path is created for forwarding traffic across the MPLS network which can be used for implementing MPLS VPN and IP ATM services.

TYPES OF LABEL DISTRIBUTION PROTOCOL

Label Distribution Protocol is of three types which is: -

a) Link Label Distribution Protocol

b) Target Label Distribution Protocol

c) Constraint Based Label Distribution Protocol

LINK LABEL DISTRIBUTION PROTCOL

Link label distribution protocol is also called as interface label distribution protocol or iLDP. The link label distribution protocol is used for distribution of labels for the label switch path which are used as transport tunnels. The main difference between link label distribution and target label distribution protocol is that in link label distribution protocol the neighbors have be to directly connected for setting up a label distribution protocol session with each other. In the link label distribution protocol, the hellos are send using multicast address to the peers.

TARGET LABEL DISTRIBUTION PROTCOL

Target label distribution protocol is also known as T-LDP and is used for distributing labels for layer 2 virtual private network and ATOM networks in multiprotocol label switching. Specific customer traffic is carried inside the multiprotocol transport tunnels and in these traffic tunnels, specific transport tunnels ae used for doing different customer services. These service tunnels are setup by using target label distribution protocol. The another difference between the target label distribution protocol and link protocol is that the for setting up a label distribution protocol session the peers may or may not be attached directly with each other. However, the peers have to be on the same subnet in case they are not connected directly with each other. Also, target label distribution protocol uses unicast address for sending hellos to its peers during the discovery phase. The advantage of using target label distribution protocol with the directly connected router is that the convergence time improves when the links are flapping between two directly connected label switch router as an alternate path gets setup by the use of target label distribution protocol. In case the link between the link goes down between the directly connected label switch router, due to the target label distribution protocol the label distribution protocol session will remain functioning and there the labels will not be discarded which will help in installing the labels

from the label information base into the label forwarding instance base when the link between the two label switch router is restored.

CONSTRAINT BASED LABEL DISTRIBUTION PROTOCOL

Constraint based label distribution protocol is a multiprotocol label switching protocol which is an extension of label distribution protocol and is used for signaling in traffic engineering for the multiprotocol networks. This protocol extends the capabilities of label distribution protocol by taking into account various constraints such as quality of service, explicit routes and other constraints which are not present in the label distribution protocol. By using constraint based label distribution protocol the requirements required for the functioning of the traffic engineering has been meet. The structure of this protocol is same as the structure of the basic label distribution protocol except for a few extra type, length and values. Explicitly routed label switch path can be established with the help of constraint based label distribution protocol and along with label switch path request many other parameters can also be requested through this protocol. Resource Reservation Protocol and Constraint Based Label Distribution Protocol are the two protocol which provide same functionality in the multiprotocol label switching networks and at the Internet Engineering Task Force it was decided that the Resource Reservation Protocol will be developed as the signaling protocol for multiprotocol label switching traffic engineering and no further work will be done on the progress of constraint based label distribution protocol which has been documented in RFC 3468. Due to which the working on constraint based label distribution protocol has now been deprecated and the primary focus is on the resource reservation protocol.

LABEL DISTRIBUTION PROTOCOL OPERATION

LABEL SPACE

The labels which are used in label bindings are derived from the sets of a possible labels which is known as label space. A label space is of two types: -

a) Per-interface label space
b) Per-platform label space

PER-INTERFACE LABEL SPACE

In per-interface label, the labels are unique with every interface and the forwarding decision for the per-interface label space is based upon the incoming interface and the incoming label. Therefore, if one label switch router sends the label to another label switch router using per-interface label space, it will be a part of different forwarding equivalence class than if the labelled packet had arrived on a different interface even though both of them are carrying the same labels. An example of per-interface label space is label-controlled ATM which will use virtual channel identifiers or virtual path identifiers for labels. Another example is frame relay interfaces which will use data link connection identifiers for labels. The per-interface label space should be used when both the label switch routers are connected directly over the interface and when that label will be used for traffic sent over that interface.

PER-PLATFORM LABEL SPACE

In per-platform label space, the labels are not unique for every interface but the labels are assigned over the label switch routers. By using per-platform label space the packet is forwarded on the basis of label and the label are not dependent on the incoming interface. The examples of per-platform label space are all ATM-frame based and non-ATM interfaces.

LABEL DISTRIBUTION PROTOCOL IDENTIFIER

The label distribution protocol identifier consists of 6 bytes and it is used for naming or identifying label space. If multiple label spaces are being advertised and managed by a label switch router, then for each label space a different label distribution protocol identifier will be used. More than one label distribution protocol identifier can be used if the label switch router needs to use more than one label space and when the label switch router has two links with the peer as well as both the links are using ATM with per interfaces space label. There is one more situation where more than one label distribution protocol can be used when the label switch router contains two links in which one of the link must be using ATM and the other link must be using Ethernet with per-platform label space. It is divided into two components which are: -

a) Label Distribution Protocol router ID

b) Local Label Space ID

LABEL DISTRIBUTION PROTOCOL ROUTER ID

The label distribution protocol router ID consist of the first four bytes. It is used for identifying that label switch router which is using that label space and the value has to be unique globally. The router will determine the label distribution protocol router ID in the following ways: -

a) The IP address of all the interfaces which are operation will be examined by the router.

b) In case any of the interfaces contains the loopback interface addresses, the address which contains the largest loopback address will be selected by the router.

c) In case the interfaces contain no loopback addresses the router will select the highest IP address from all the operational interfaces as the router ID.

LOCAL LABEL SPACE ID

The local label space ID consists of the last two bytes and it is used for identifying the label space which is to be used within the label switch router. If the label switch router is using per-platform label space, then the local label space ID will always be zero.

PROCEDURE OF LABEL DISTRIBUTION PROTOCOL

In order to create and maintain the label distribution protocols there are three procedures. These are: -

a) Discovery of peers

b) Establishment and Maintaince of Sessions

c) Management of Labels

d) Notification messages

DISCOVERY OF PEERS

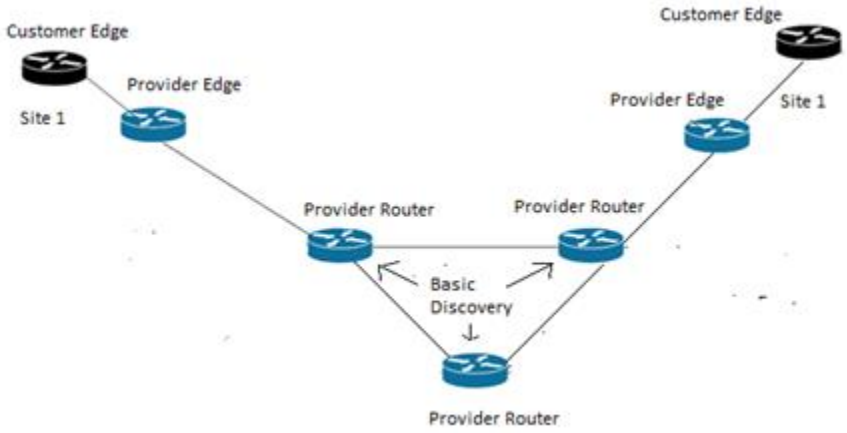
The discovery of peers is the first process in which label switch routers are able advertise to the other routers about their presence in the network and are also able to find peers. The label switch router will be sending hello messages to the other routers present in the network at a regular interval via user datagram protocol and the message is transmitted at the group multicast address in order to establish peer. There are two ways by which the label switch routers are able to discover the peers: -

a) Basic Discovery- used for discovering label switch routers which are connected directly.

b) Extended Discovery- used for discovering label switch routers which are not connected directly.

BASIC DISCOVERY

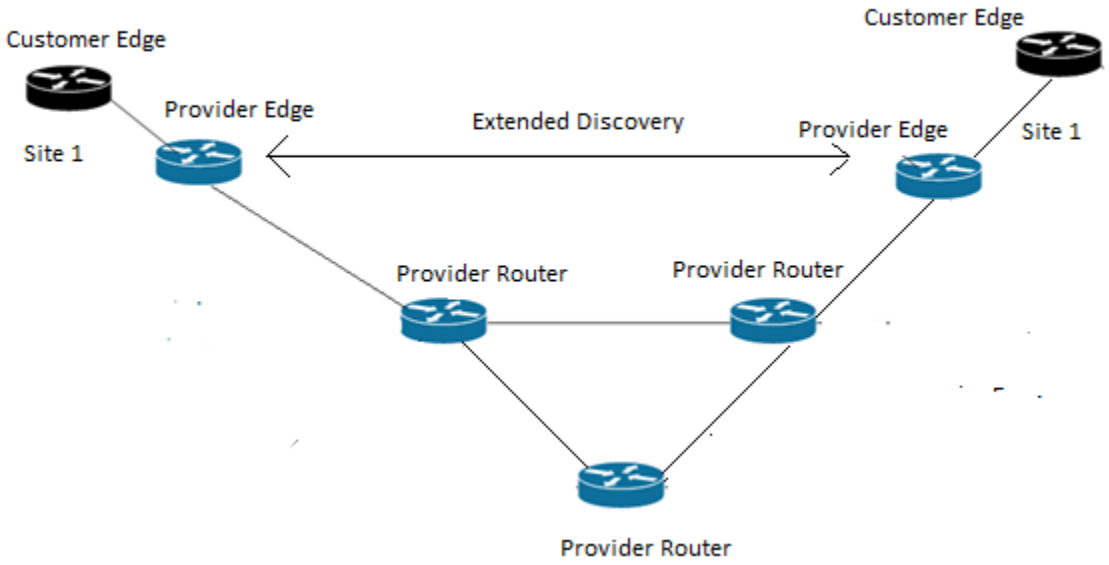
A directly connected label switch router is that which is one hop from its neighbor. In basic discovery mechanism, the label switch router will send label distribution protocol link hellos at a regular interface from the interface in the form of user datagram packets from to the label distribution port on the group multicast address.



The label distribution protocol link hellos contain label distribution protocol identifiers which are used for the label space and other additional information. The neighboring label switch router can respond to the link hello messages which will allow the both the label switch routers to form a label distribution protocol session. The label switch router which will receive the link hellos will form a hello adjacency with the peer which is reachable at the link level and will also inform its peer about the label space it will use for the interface.

EXTENDED DISCOVERY

A non-directly connected label switch router is that which is more than one hop away from its neighbor. In case of non-directly connected label switch routers extended discovery mechanism will be used. In this mechanism a target hello messages which are in the form of unicast message and as a user datagram packet are sent to the address of that particular label switch router.



The label distribution protocol targeted hellos contain label distribution identifiers which are used for the label space and other additional information. A label switch router will initiate the discovery by sending targeted hellos with the another label switch router and it will depend on the another label switch router to accept that targeted hellos or not. If the another label switch router wants to accepts the targeted hellos it will do so by periodically sending hellos to the label switch router which initiated the hellos. The label switch router which will receive the link hellos will form a hello adjacency with the peer which is reachable at the link level and will also inform its peer about the label space it will use for the interface.

The main differences between basic discovery and extended discovery are: -

a) In basic discovery the label distribution protocol link hellos are sent to a multicast address whereas in extended discovery the targeted hellos are sent to an address which is specific.

b) Extended Discovery is asymmetric in nature whereas basic discovery is symmetric in nature.

ESTABLISHMENT AND MAINTAINACE OF SESSIONS

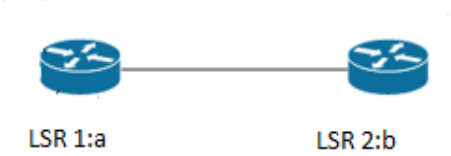
After the hellos has been exchanged between the two label switch routers the next step will be of establishing sessions between those label switch routers. In order to establish sessions between the label switch routers two steps are required: -

a) Establishment of transport connection

b) Initialization of Sessions

ESTABLISHMENT OF TRANSPORT CONNECTION

Let us assume we have two label switch routers, Label switch router 1 with label space LSR1: a and Label switch router 2 with label space LSR2: b. A session will be established between Label switch router 1 and label switch router 2 from the label switch router 2 point of view.



At label switch router 1, hello Adjacency is created after the exchange of hellos and this will bind the link and label spaces. A new transmission control protocol connection will be initiated with label switch router 2 for forming a new label distribution protocol session for the exchange of label spaces if label switch router 1 doesn't already have a label distribution protocol session with label switch router 2.

The address which will be used at the label switch router 1 end which is denoted by A1 and label switch router 2 end which is denoted by B2 by the transmission control protocol is determined by label switch router 1. In order to determine the label switch router 1 end address A1 following method is used: -

a) A1 will be the address advertised by label switch router 1 through the optional object if transport address optional object (TLV) is used by label switch router 1 for sending hellos to label switch router 2 for advertising an address.

b) A1 will be the source address which will be used for sending the hellos to the label switch router 2 if transport address optional object (TLV) is not being used by label switch router 1.

Similarly, in order to determine the label switch router 2 end address B2 following method is used: -

a) B2 will be the address advertised by label switch router 1 through the optional object if transport address optional object (TLV) is used by label switch router 2 for sending hellos to label switch router 1 for advertising an address.

b) B2 will be the source address which will be used for sending the hellos to label switch router 1 if transport address optional object (TLV) is not being used by label switch router 2.

In order to decide if label switch router 1 will play the active or passive both A1 and B2 addresses will be compared as unsigned integers and label switch router 1 will play the active role only if A1 > B2 otherwise it will play in the passive role. For determining which address is greater following procedure is used: -

a) No session will be established if both A1 and B2 doesn't belong to the same address family as it will difficult to compare them.

b) Let us assume that Z1 is the unsigned integer which has been issued from A1 after it has been treated as a sequence of bytes where the most significant byte is the byte that appears in the beginning and the least significant byte is the byte that appears in the last of the address. Similarly let us assume that Z2 is the unsigned integer which has been issued from A2 after it has been treated as a sequence of bytes where the most significant byte is the byte that appears in the beginning and the least significant byte is the byte that appears in the last of the address. Now both Z1 and Z2 are compared and if Z1 is greater than Z2 then A1 will be greater than B2 and if Z2 is greater than Z1 then B2 will be greater than A1.

The label switch router which will become active will try to connect at the label distribution protocol port of the other label switch router through the transmission control protocol. So if label switch router 1 is active it will try to connect with label distribution protocol port of label switch router 2 via transmission control protocol and if label switch router 1 becomes passive, label switch router 2 will try to connect at the label distribution protocol port via transmission control protocol and label switch router 1 will wait until the connection is established.

The same transport address needs to be advertised in the hellos by the label switch router that are advertising the same label space. This will enable both the label switch routers which are having the same label space and are attached by various hello adjacencies to form a same connection establishment for every adjacency.

INITIALIZATION OF SESSIONS

After the transport connection has been established between the both label switch router 1 and label switch router 2, they will exchange Label distribution protocol initialization messages to negotiate session parameters. Virtual path identifier and virtual circuit identifier, data link connection identifier ranges for the frame relay, label distribution methods are some of the session parameters which are negotiated between the two label switch routers. After the session parameters has been successfully negotiated between the two label switch routers, they will establish a label distribution protocol session so that the label spaces can be advertised.

If the label switch router 1 is active after the connection has been established, it will be the responsibility of label switch router 1 to initiate the negotiation of session parameters with label switch router 2 by sending the initialization messages and if label switch router 1 is passive, then label switch router 1 will have to wait until label switch router 2 will initiate the negotiation of the session parameters. If label switch router 1 and label switch router 2 have multiple links between them and both of them are advertising multiple label spaces, then until passive label switch router gets the initialization message on that connection, the passive label switch router will not be able to decide to advertise which label space over the new connected transmission control protocol connection.

The label distribution protocol identifier for the active label switch router which is the sender label space and the label distribution protocol identifier for passive label switch router which is the receiver label switch space are the information which is contained in the initialization message.

From the label switch router 1 point of view the session initialization will take place in the following ways when the label switch router 1 is in passive phase: -

a) If an initialization message is received by label switch router 1, then the label switch router will try to match the label distribution protocol identifier with the hello adjacency.

b) If the label distribution protocol identifier gets matched with the hello adjacency, then the local label space is specified and the session parameters are checked by the label switch router 1 to ensure that those parameters are acceptable. If the parameters are acceptable to label switch router 1, it will send an initialization message in which it will send the parameters which it will intend to use and a keep alive message by which it will send a signal to label switch router 2 that it has accepted the parameters that the label switch router 2 wishes to use. In case the parameters are not acceptable to label switch router 1, it will close the transmission control protocol session by sending a session rejected and parameters error notification message to the label switch router 2.

c) Label switch router 1 will close the transmission control protocol connection by sending a session rejected and no hello error notification messages to the label switch router 2 if no matching hello adjacency is found by label switch router 1.

d) The session will become operational if and only if label switch router 1 receives a keep alive message from label switch router 2 in response to the initialization message that the label switch router 1 had send to the label switch router 2 and if label switch router 1 gets an error notification message the session has been rejected by the label switch router 2 and label switch router 1 will have no choice but to close the transmission control protocol connection.

From the label switch router 1 point of view the session initialization will take place in the following ways when the label switch router 1 is in active phase: -

a) If label switch router 1 gets an error notification message, the session has been rejected by the label switch router 2 and label switch router 1 will have no choice but to close the transmission control protocol connection.

b) If an initialization message is received by label switch router 1, session parameters are verified by the label switch router 1 and if these parameters

are acceptable the label switch router will send a keep alive message to the label switch router 2 and in case the parameters are not acceptable to label switch router 1, it will close the transmission control protocol session by sending a session rejected and parameters error notification message to the label switch router 2.

c) When label switch router 2 has accepted the parameters which were proposed by the label switch router 1, the label switch router 2 will send a keep alive message to the label switch router 1.

d) After an initialization message and a keep alive message has been accepted by the label switch router 1 which was send from the label switch router 2, the session between the two label switch routers becomes active.

No messages except those messages which has been shown above in the list can be exchanged between the two label switch routers until the label distribution protocol session has been formed and in case a message is transmitted which is not in the list, the transmission control protocol connection is closed by sending a shutdown message between those two label switch routers.

If the label switch routers are configured incorrectly it can possibly result in disagreement between the two label switch routers on the session parameters which can result in endless transmission of messages between those two label switch routers as they will not acknowledge each other's initialization message and will send error notification messages. In such a situation an exponential backoff is setup for every session retry attempt by the label switch router so that the session setup can be controlled and it is recommended that label switch router must take action so that the operator can be notified. The retry attempt after a negative acknowledgement is received for the initialization message must not be less than 15 seconds and if there is continuous negative acknowledgement the delay will go more than 2 minute. The action that needs to be delayed is the label switch router which is in the active phase from opening the transmission control protocol connection with the other label switch router. Until one of the label switch router is reconfigured by the operator these notification messages will not stop and after the reconfiguration has been done there is no need to control the session setup until the above event occurs again.

As the session establishment is asymmetric in nature, the active label switch router will not be able to notice the reconfiguration of the passive label switch router. So, in order to be able to tell the other label switch router regarding its reconfiguration

the passive label switch router will use an optional mechanism which will send a signal to the passive label switch router's peers.

MAINTAINCE OF SESSIONS

In order to maintain the session two ways are used: -

a) Hello adjacencies are maintained

b) Label distribution protocol sessions are maintained

HELLO ADJACENCIES MAINTAINCE

When a label switch router forms a label distribution protocol session with another label switch router multiple hello adjacencies are created between the two label switch routers. This type of adjacency is created when both the label switch routers are sharing the same label space which are connected to each other via multiple links and label distribution protocol identifier is same which the label switch router sends on those multiple links. To keep a check on the condition of label distribution protocol session and hello adjacency a mechanism is included in the label distribution protocol. If a label switch router wishes to use the label space which is identified by the hello, the label distribution protocol will use regular receipt which is present in the label distribution protocol discovery hellos. In case there is no receipt of the matching hellos from the peers and the timers expires then the label distribution protocol will conclude that either the peer has failed or the peer doesn't want to label switch by using that label space and the hello adjacencies will be deleted by the label switch router. The label distribution protocol session will be terminated by the label distribution protocol when all the hello adjacencies has been deleted. The label switch router will send a notification message and the transmission control protocol connection will be closed.

LABEL DISTRIBUTION PROTOCOL SESSIONS MAINTAINCE

In order to check the integrity of the label distribution protocol session the label distribution protocol has included a mechanism. To check the integrity of the sessions, label distribution protocol monitors the session transport connection by using the regular receipt of label distribution protocol's protocol data unit. Whenever a protocol data unit is received from the session peer, the keep alive timer which is maintained by label switch router for every peer session is reset and

incase the timer is dead and no receipt of the protocol data unit is received the label switch router will conclude that either the peer has failed or transmission control protocol connection has gone bad. Label switch router will then close the connection by terminating the transmission control protocol connection.

The label switch router must ensure that the protocol data unit are being received by its peer for every keep alive time period. This is done in order to be sure that session keep alive timer is restarted by the peer. For doing this the label switch router can send any protocol message and a keep alive message will be end in case the label switch router has no way of communicating with its peer.

A label distribution protocol session can be terminated by the label switch router with its peer at any time and for doing that a shutdown message will be sent by the label switch router to its peer.

MANAGEMENT OF LABELS

LABEL ADVERTISEMENT MODE

In order to distribute label bindings two modes are used: -

a) Downstream on Demand label distribution mode

b) Unsolicited Downstream label distribution mode

DOWNSTREAM ON DEMAND LABEL DISTRIBUTION MODE

In this mode, a label binding for the forwarding equivalence class is requested by every label switch router from its next hop label switch router which is downstream on its label switch path. The next hop router which is indicated in the IP routing table is known as the downstream label switch router. The downstream label switch router will forward one binding per forwarding equivalence class to every label switch router for that forwarding equivalence class. In the downstream on demand label distribution mode only one label binding is shown in the label information base and all LC-ATM uses this mode for label distribution.

UNSOLICITED DOWNSTREAM LABEL DISTRIBUTION MODE

In this mode, label bindings are distributed for the forwarding equivalence class by the label switch router even when they have not been explicitly requested by the

adjacent label switch routers. Each adjacent label switch router will send a remote binding to the label switch router and therefore there are more than one bindings shown in the label information base and all the interfaces uses unsolicited downstream label distribution mode for distributing label except for the LC-ATM.

In the same network both of these label distribution mode can be used simultaneously but the label switch router must know what its peers are using for the label distribution for any given label distribution protocol session so that the situation can be avoided where one the label switch router is using downstream on demand label distribution mode but its peer is using unsolicited downstream label distribution mode.

LABEL SWITCH PATH CONTROL MODE

There are two ways by which the behavior of label switch path can be determined and both types of control are supported by the label switch router. The two ways are: -

a) Independent Label Distribution Control Mode

b) Ordered Label Distribution Control Mode

INDEPENDENT LABEL DISTRIBUTION MODE

In this mode, the label mappings are advertised by the label switch router to its neighbors at any time when the label switch router seems is right and the label bindings for the forwarding equivalence class is created separately by the label switch router as compared to the other label switch routers. As soon as the forwarding equivalence class is recognized, a local binding is created for that particular forwarding equivalence class by each label switch router and the routing table contains the prefix for that forwarding equivalence class. For example, the label switch router without waiting for the label mapping form its neighbor can start answering request for label mapping immediately while operating in independent downstream on demand label distribution mode and a label switch router can advertise to its neighbor a label mapping for the forwarding equivalence class while operating in independent unsolicited downstream label distribution mode.

One of the disadvantage of using independent label distribution mode is that sometimes the packets are not forwarded correctly as they should have been because sometimes label switch routers starts to label switch packets before the

complete end to end setup of the label switch path and due to which the packets are dropped or are not forwarded correctly.

ORDERED LABEL DISTRIBUTION CONTROL MODE

In this mode, the transmission of the label mapping will be initiated by the label switch router only for forwarding equivalence class for which it has the forwarding equivalence class of the next hop or transmission for the label mapping can be initiated for which the label switch router is the egress router. The label switch router has to wait when there is no egress and when no mapping exists for every forwarding equivalence class until a label is received from the label switch router which is operating in downstream before the labels can be passed to the label switch router which is operating in upstream and before the forwarding equivalence class can be mapped.

LABEL RETENTION MODE

The label retention mode is used when a label binding is maintained by the label switch router for a forwarding equivalence class which the label switch router learns from its neighbor and that forwarding equivalence class is not in the next hop. There are two ways by which the labels can be retained: -

a) Conservative Label Retention Mode

b) Liberal Label Retention Mode

CONSERVATIVE LABEL RETENTION MODE

In this mode all the peer label switch routers send the advertisement of all the label mapping to all the routers. The label mapping will only be retained if those mapping are being used for forwarding packets and according to routing they are being received from a next hop which is valid if conservative label retention mode is being used. The label information base will not store all the remote bindings but only those bindings will be stored in the label information base which has information for the next hop label switch router on a particular forwarding equivalence class. According to routing if downstream on demand label distribution mode is being used, the label mapping only from the next hop label switch router will be requested by the label switch router. Since, when label conservation is required downstream on demand label distribution mode is primarily used and therefore conservative

label retention mode is generally used with downstream on demand label distribution mode.

The advantage of using conservative label retention mode is that the available memory of the router can be put to a good use and they are very few labels to store as only those labels are stored and maintained which are required for the forwarding of data which is important in cases such as ATM switch where the space is already limited. LC-ATM interface uses conservative label retention mode for retaining labels. The disadvantage of using conservative label retention mode is before labelled packets can be forwarded if there is change in the routing and the next hop changes for a destination, a new label has to be obtained from the next hop otherwise the packets will not be forwarded.

LIBERAL LABEL RETENTION MODE

In this mode, all the remote labels which are received by the label switch router are kept in the label information base and one of the remote binding is the binding which have been received for that forwarding equivalence class from the next hop router or from the downstream label switch router. The label forwarding information base will use that label from the remote bindings which contains next hop information while no other label will be put from the other remote bindings in the label forwarding information base and therefore for forwarding traffic not all the remote bindings are used. The purpose of keeping labels in the label information base which are not being used is that incase if any link goes down or if there is any change in the topology like a router is removed, it can result in changing of the next hop router for that particular forwarding equivalence class and as all the labels are already present in the label information base, the label forwarding information base can quickly choose the next hop router and update its table by choosing the new outgoing label.

The advantage of using label retention mode is that with the change in topology the reaction with label retention mode is quicker as all the labels are already present in the label information base and the disadvantage of using label retention mode is the wastage of space and memory as label mapping which may not be needed are stored and have to be maintained in the table. All the interfaces use label retention mode except for LC-ATM which uses liberal label retention mode.

NOTIFICATION MESSAGES

In order to provide significant event signals to the label distribution protocol peers the notification messages are used. There are two types of notification messages which are used for signaling. They are: -

a) Error Notification

b) Advisory Notification

ERROR NOTIFICATION

The fatal errors are signaled with the help of error notification. A label distribution protocol session is closed by the label switch router once it receives the error notification message from its peer by terminating the transmission control protocol session and all the label mappings which have been learnt throughout the session is discarded by the label switch router.

ADVISORY NOTIFICATION

Information regarding the label distribution protocol session are sent to the label switch router using the advisory notification messages. The advisory notification messages are also for sending messages regarding the status of the messages which were earlier sent by the label switch router.

DETECTION OF LOOPS

If non merging label switch routers are present, a loop detection mechanism is used for finding loops in the label switch path and to prevent looping in label request message. Path vector and hop count TLVs are used for detection of the loops which are carried by the label request and label mapping messages respectively and uses these properties of the TLV: -

The list of the label switch routers which has been transversed are contained in the path vector TLV. Unique Label switch router identifier i.e. the first four octet of the label distribution protocol identifier are used for identifying the label switch router in the path vector list. Label switch router identifier is added to the path vector list when the label switch router sends a message which contains path vector TLV. The message will transverse the loop when the label switch router receives a message containing the path vector which will have that label switch

router's identifier. The maximum allowable path vector length is also supported by label distribution protocol by which the containing message behaves as if it has transversed the loop in case the label switch router detects that the path vector has reached the maximum allowable length.

The count of the label switch router that contains how many message has been transversed by the label switch router is maintained by the hop count TLV.A count is incremented when a message containing a hop count TLV is propagated by the label switch router. The containing message will transverse the loop when the label switch router detects that the hop count has reached a configured maximum value. The hop count is said to be unknown when the count is zero and if an unknown hop count is incremented it will result in hop count value which is also unknown.

The loop detection mechanism needs to be turned on all the label switch routers within that multiprotocol label switching domain for the loop detection to work properly otherwise it can result in loops which are falsely detected and also undetected loops.

Path vectors are passed downstream i.e. from the ingress label switch router to the egress label switch router and will not be passed downstream in case of presence of non-merge capable label switch routers. The path vectors will not be passed upstream along that label switch path which will reach the egress label switch router if merge capable label switch router is present. The only time path vectors will be passed upstream when label switch router has a change of next hop and it is not able to determine from the hop count that a loop will not be formed if there is a change in next hop.

Label mapping messages are sent from egress label switch router to ingress label switch router while using ordered label distribution which will result in a natural creation of path vector. A label mapping message can be sent by the label switch router for a forwarding equivalence class before a label mapping has been received from the downstream label switch router for that forwarding equivalence class if independent label distribution is being used. The subsequent label mapping which has been received from the downstream label switch router will be forwarded to the upstream label switch router and will be treated as an update to the label switch path. In order to minimize the number of label mapping update messages it is recommended that the loop detection should be used along with ordered label distribution.

INTEGRITY AND AUTHENTICITY FOR LABEL DISTRIBUTION PROTCOL

This is a configurable option which is used for protection against the spoofing of transmission control protocol segments into label distribution protocol session and in order for this mechanism to work MD5 signature is used. The MD5 signature is used as follow: -

a) For each potential label distribution protocol peer a secret password is configured with the MD5 signature by the label switch router.

b) Before sending a transmission control protocol segment to the peer, MD5 digest is computed by the label switch router and applied to that transmission control protocol segment.

c) That transmission control protocol segment with the MD5 digest is received by the label switch router and will calculate its own MD5 digest by using its own record of password for validation of the segment. The result form its own MD5 digest is compared with the received MD5 digest and in case the two results doesn't match the segment is not accepted by the received label switch router and no response is sent to the sender.

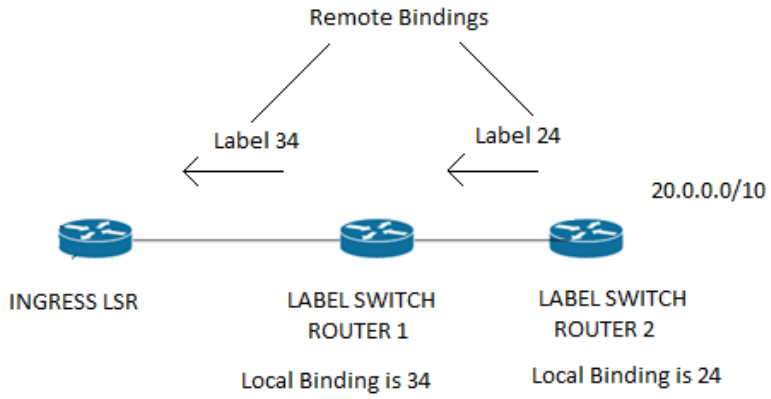
d) No label distribution protocol hellos are accepted from a label switch router which doesn't have a password configured. Therefore, this helps in ensuring that transmission control protocol connections are accepted with only those label switch routers which have password configured.

USE OF LABEL DISTRIBUTION PROTOCOL IN VARIOUS TOPOLOGIES

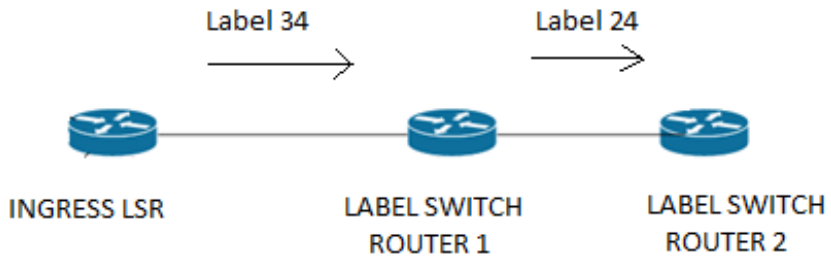
LABEL DISTRIBUTION PROTCOL IN IPv4 OVER MPLS NETWORK

Every label switch router will create a local binding for each interior gateway protocol IP prefix which is present in the routing table. Therefore, with every IPv4 prefix a label will be binned and these bindings will be distributed to all the neighbors by the label switch routers. The bindings which has been received by the neighbors will be called as remote bindings and these bindings will be stores along with the local bindings by the neighbor in its label information base table. The label switch router will choose one remote binding from all the remote bindings which are present in the table for a prefix and that remote binding will be used as the outgoing label for that prefix. The next hop of the IPv4 prefix is determined from the routing table which is called as routing instance base. The downstream label switch router will send a remote binding which is chosen by the label switch router

and this information will be used to form the label forwarding information base where the incoming label will be the label which is from the one local binding and the outgoing label will be that label from the one local bindings which will be taken from the routing table. This will enable the label switch router of changing the incoming label which was assigned by itself with the outgoing label which was assigned by the downstream label switch router.



In this figure, the binding between the label switch routers for the 20.0.0.0/10 which is advertised using label distribution protocol is shown. One label per IPv4 prefix is allocated by the label switch routers which is known as local binding and the remote bindings is that label which the label switch routers receives from its downstream label switch router.



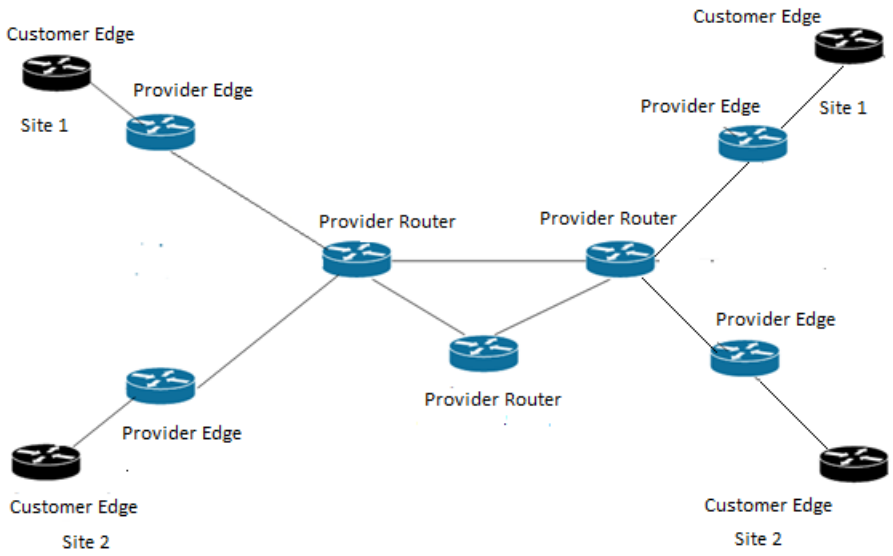
In this figure, the ipv4 packet which is going for the destination 20.0.0.0/10 will enter the multiprotocol label switching network through the ingress label switch router. On entering the network, label 34 will be put on the packet and it will be

forwarded to the next label switch router. The label switch router 1 will receive that packet and will replace label 34 with 24 and forward the packet to next label switch router and so on until the destination is reached.

LABEL DISTRIBUTION PROTOCOL IN MPLS LAYER 3 VPN NETWORKS

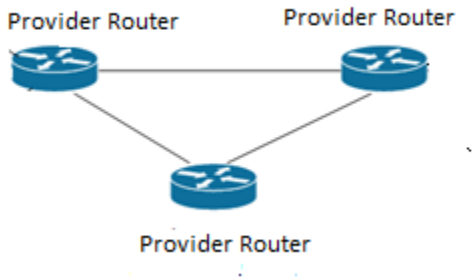
A multiprotocol label switching layer 3 virtual private network consists of provider edge or PE router, customer edge or CE router and provider or P router. The provider router maintains a direct connection with the customer edge router which is present at the layer 3. No multiprotocol layer switching is present at the customer edge router as well as provider router has no direct connection with the customer edge router. The routers which run multiprotocol label switching are the provider edge router and provider router because of which both of these routers can forward packets which are labelled and can distribute labels among themselves.

The provider routers present in the layer 3 multiprotocol label switch routing are not aware of the virtual private network so that the virtual private network can be more scalable and they don't contain any information regarding the virtual private network's route. In order to maintain a private network for each customer present in the virtual private network the IP packets have to be labelled and the routes for the virtual private network are maintained only by the provider edge routers. Since the edge routers of the multiprotocol label switching have all the knowledge related to the virtual private network due to which virtual private network is more scalable.



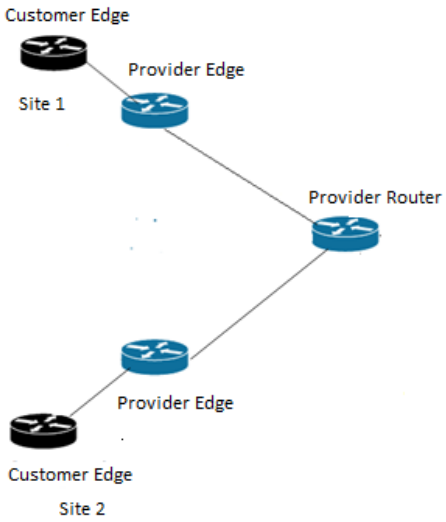
This figure shows a topology for the multiprotocol label switching layer 3 virtual private network where the traffic is sent from one site to the another site and for each customer a separate instance as well as separate routing is maintained.

In this network the first part consists of provider routers.



The provider routers play an important part in the multiprotocol label switching network as they are inside the network and all the IP traffic is labelled as well as switched by using provider router along with a multiprotocol label switching distribution protocol which is running on each of the provider router for distributing labels. Label distribution protocol, Resource reservation protocol and Constraint based routing label distribution protocol are some of the label distribution protocol that can be used on the provider router for distributing labels but label distribution protocol is mainly used as it is simple to configure as well as it is simple to use.

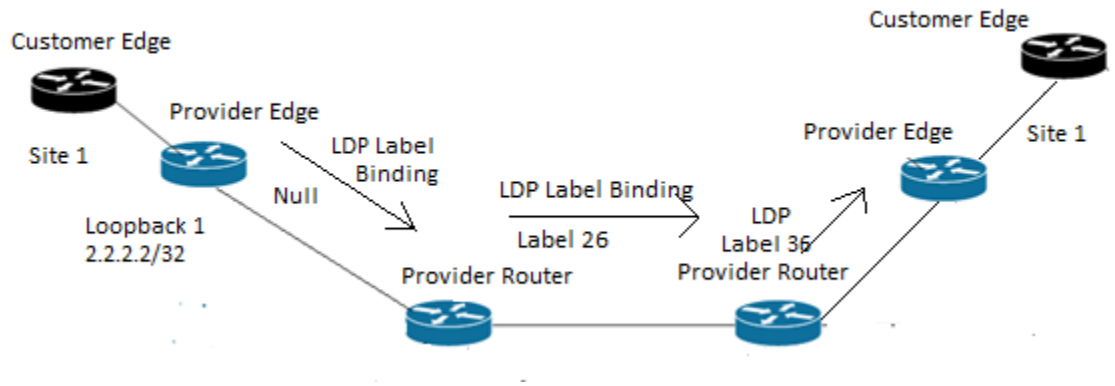
Provider edge routers are the second part of this network.



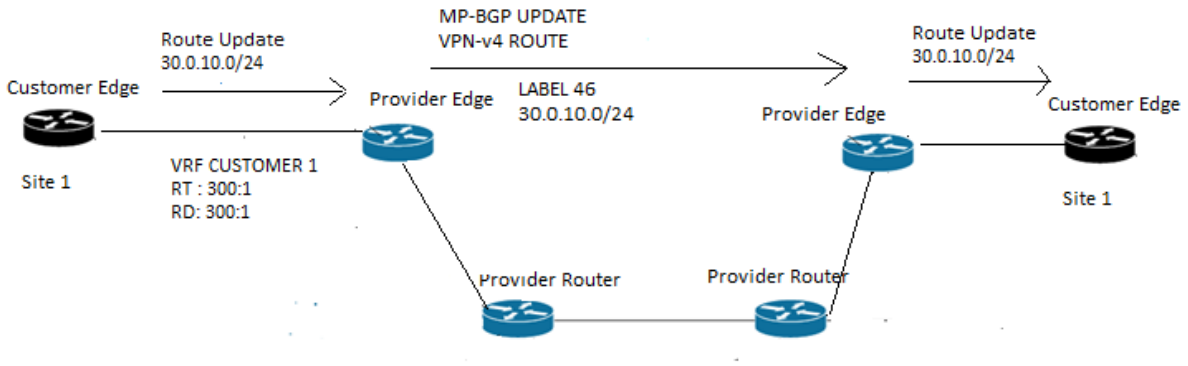
The provider edge routers are the routers which are in between both the customer edge routers and the provider routers. They are responsible for using label distribution protocol with the provider routers so that a label switch path can be created with the other edge provide routers. The packets between the ingress provider edge router and egress provider edge routers are switched in such a way that no lookup for the destination IP address is needed by the provider router and the label is referred as IGP label or also known as transport label. This is because in the routing table of both provide edge router as well as the provider router the label is bound with an IPv4 prefix.

In order to exchange VPNv4 information, provider edge routers form a MP-BGP connection with other provider edge routers and the information which is exchanged is the address of the virtual private network that is distributed as label which is known as VPN label. For every customer edge router, the provide edge router need to have a separate routing instance for every customer which is done by using a separate virtual routing and forwarding instances. By using virtual routing and forwarding, on a single device multiple routing as well as multiple forwarding tables can co-exist with each other. It is used along with Route Distinguisher and Route Targets.

The purpose of the route distinguisher is to maintain a globally unique IPv4 prefix for the exchange of routes and route targets are used for informing the provider edge devices that in the virtual private network routing table which prefixes can be imported or exported by using BGP extended attribute.

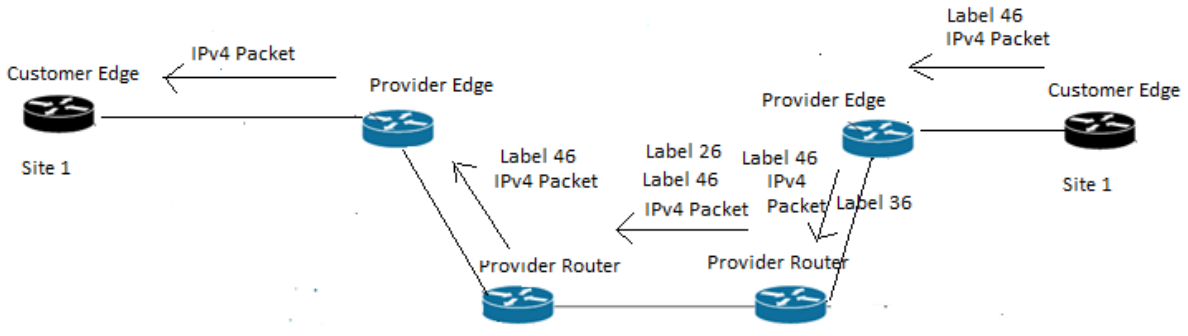


In this figure, it is shown that how an IP packet moves across the multiprotocol label switching network. Label distribution protocol needs to be created form the loopback of the provider edge router to the other provider edge router using hop by hop mechanism which will create a label switch path. In this scenario, for loopback 1 a label switch path will be created and the labels which will be used are null, 26 and 36.



After the formation of label distribution protocol between the two provider edge routers, the next step is a route update will be sent by the customer from the customer edge router and it will be advertised by using the routing protocol which was configured between the protocol edge router and customer edge router. The route update will be received by the provider edge router which will be signaled to the other provider edge router using MP-BGP as a VPNv4 route. A label, route target and route distinguisher which will be attached with a prefix will also be sent by the provider edge router. Here, the route 30.0.10.0/24 will be sent with route target 300:1, route distinguisher 300:1 and label is 46.

In the next and final step, the customer edge router which is present at the other end of the network will send packet for the signaled router which will be forwarded to the provider edge router as IPv4 packets. The VPN label which is signaled by the MP-BGP and IGP which is signaled by the label distribution protocol will be encapsulated with the IPv4 packets. The VPN label is used for sending the traffic to the opposite provider edge router by telling the correct VRF and IGP label is used for hop by hop forwarding of the packet across the multiprotocol label switching network.

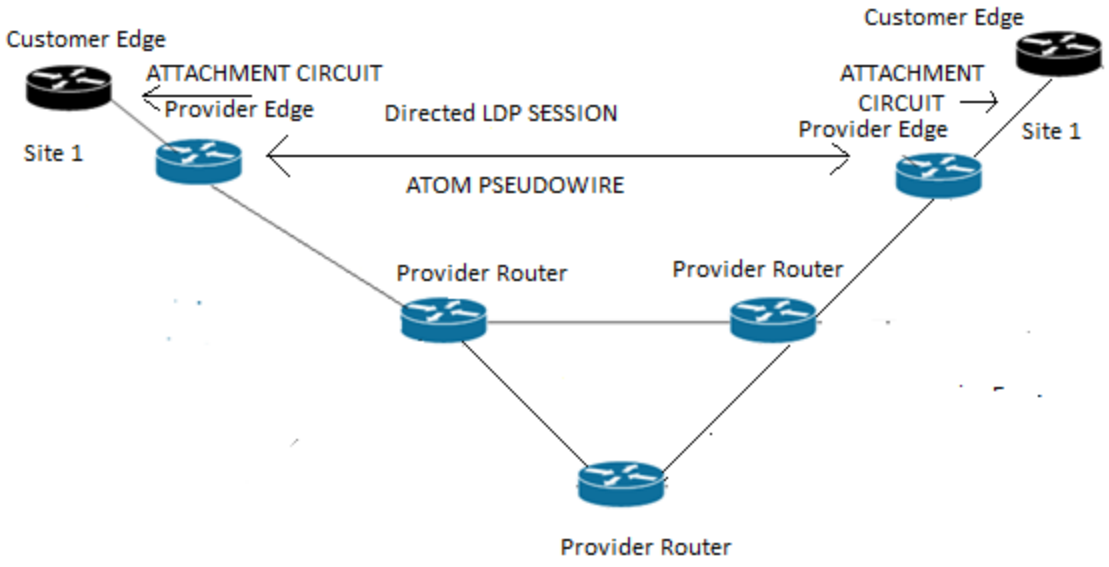


In this figure, for the destination 30.0.10.0/24 the IPv4 packet will be forwarded from the customer edge router to the ingress provider edge router. The provider edge router will perform the lookup for the destination address in the forwarding table. The provider edge router will find the interface through which the routes came so that it can find the correct VRF to send the traffic. The IPv4 packet will then be encapsulated with IGP label i.e. 36 and VPN label i.e. 46 and the IPv4 packet will be forwarded to the provider router. Based on the next hop address the IGP label will be changed and at the last provider router because of the null label the final label will be removed before it enters the provider edge router. The provide edge router will check the VPN label in the forwarding table and according to the information in the table the packet will be forwarded to the customer edge router without containing any labels.

LABEL DISTRIBUTION PROTOCL IN MPLS LAYER 2 VPN NETWOKS

USE OF LABEL DISTRIBUTION PROTOCOL IN ATOM OPERTATIONS

Any Transport Over MPLS is used for transporting layer 2 traffic through the pseudowire emulation application in the multiprotocol label switching network. Two same layer 2 protocols can be connected end to end with the help of AToM and it can also be used to connect two different layer 2 protocols with the help of layer 2 internetworking. The service providers have been able to save money as they can run virtual private network and AToM on a single network infrastructure. AToM is used on the provider edge routers by forming an attachment circuit with the customer edge router so it is and an AToM pseudowire connection is formed with the other provider edge router so AToM is an edge technology. The attachment circuit can support any layer 2 encapsulation. AToM is used as layer 2 point to point service which is known as virtual private wire service.



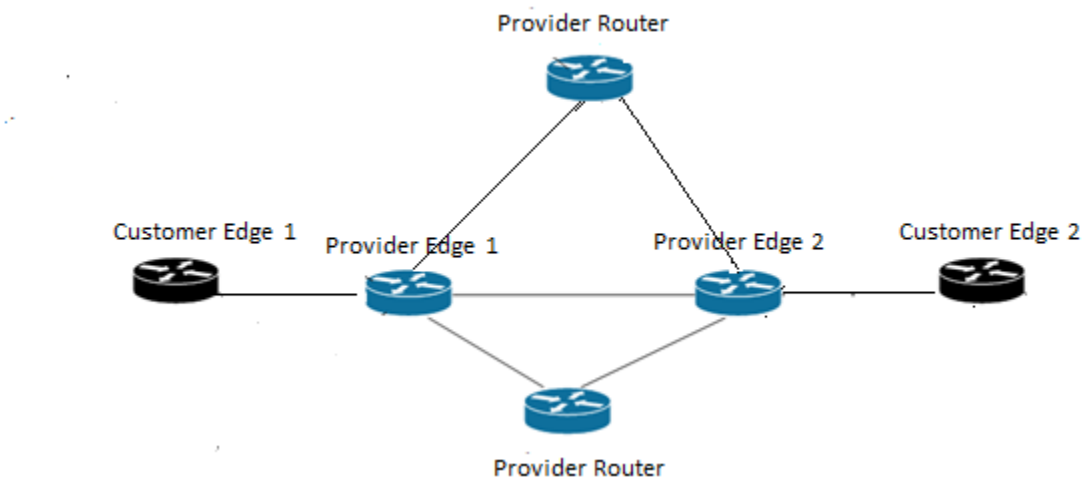
A pair of multiprotocol label switching label switched path forms the Atom pseudowire. Since a label switched path is formed in one direction so in order to have connection in both directions, two label switch paths are required which have to working in the opposite direction to form an pseudowire. There are many ways by which the label can be distributed in the multiprotocol label switching but ATOM uses Label Distribution Protocol for distributing labels. For establishing ATOM pseudowires two types of label distribution protocol sessions are used which is targeted label distribution protocol session and the other is non targeted label distribution protocol session.

The non-targeted label distribution protocol session uses label distribution protocol basic discovery for distribution of labels for tunnels between the provider edge router and directly connected provider router. The distribution of labels and the management of labels for the tunnels is done according to the topology of the multiprotocol label switching network which can made up by combining downstream on demand label distribution mode with unsolicited downstream label distribution mode or independent label switch path mode with ordered label switch path mode or liberal label retention mode with conservative label retention mode. The distribution of labels and the management of labels for the tunnels doesn't depend upon the ATOM as well as pseudowires emulation.

The targeted label distribution protocol session uses extended discovery mechanism for distribution of labels between the provider edge routers. These provider edge routers send targeted hellos messages to each other and therefore these sessions are called as targeted label distribution protocol sessions. Targeted

label distribution protocols are used for distribution of pseudowire labels in the ATOM. Unsolicited downstream label distribution mode can be used for pseudowire emulation over multiprotocol label switching as specified according to the engineering task force. In order to improve the performance as well as convergence time it is recommended to use independent label switch path mode along with liberal label retention mode for the signaling of pseudowires.

Procedure for the establishment of the AToM pseudowire is explained in the following steps: -



a) An attachment circuit is formed between customer edge router 1 and provider edge router 1 by provisioning a pseudowire.

b) Provider edge router 1 will form a label distribution protocol session by sending a targeted hello to the provider edge router 2 and both the provider edge routers will exchange keep alive messages in order to complete the formation of the session establishment.

c) After the session has been established between the both provider routers they can now exchange the label bindings for pseudowires emulation.

d) A local pseudowire label which will be allocated by the provider edge router 1 when the attachment circuit which is connected with the provider edge router 1 goes up. The pseudowire label generated by the provider edge

router will be generated according to the pseudowire ID which was provisioned for that pseudowire.

e) The pseudowire label will be encoded by the provide edge router into the table of TLV whereas the pseudowire ID will be encoded by the provider edge router into the table of forwarding equivalence class and provider edge router 1 will forward both the label bindings to the provider edge router 2 in the form of label mapping messages.

f) Provider edge router 2 will receive this label mapping from the provider edge router 2 and decode the pseudowire label from the table of TLV and pseudowire ID from the table of forwarding equivalence class.

g) An attachment circuit is formed between customer edge router 2 and provider edge router 2 by provisioning a pseudowire.

h) A local pseudowire label which will be allocated by the provider edge router 2 when the attachment circuit which is connected with the provider edge router 2 goes up. The pseudowire label generated by the provider edge router will be generated according to the pseudowire ID which was provisioned for that pseudowire.

i) The pseudowire label will be encoded by the provide edge router into the table of TLV whereas the pseudowire ID will be encoded by the provider edge router into the table of forwarding equivalence class and provider edge router 2 will forward both the label bindings to the provider edge router 1 in the form of label mapping messages.

j) Provider edge router 1 will receive this label mapping from the provider edge router 2 and decode the pseudowire label from the table of TLV and pseudowire ID from the table of forwarding equivalence class.

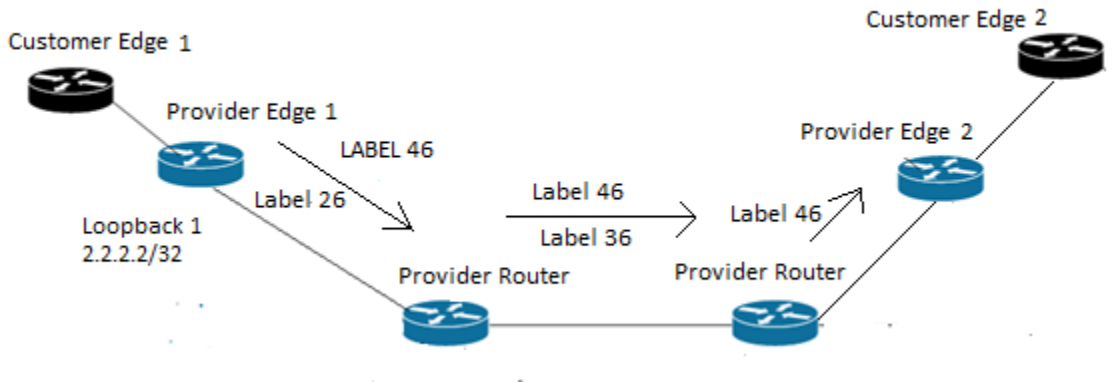
k) The pseudowire will be considered established after both provider edge router 1 and provider edge router 2 have exchanged the pseudowire labels with each other and pseudowire ID has been validated by checking the parameters for that particular pseudowire ID.

In case the attachment circuit on one of the provider edge 1 routing is not working, the provider edge router 1 will send a label withdraw message to the provider edge

router 2 so that it can pseudowire labels which were sent to provider edge router 1 can be withdrawn.

FORWARDING OF PACKETS IN AToM

In order to forward data in AToM, two labels are required. The first label is known as tunnel label which is responsible for identifying the tunnel in which the customer frames are being sent from one provider edge router to another edge router. Also, many pseudowires can be multiplexed into a single tunnel so in order to identify these pseudowires one more label is used which is known as VC or PW label. The customer edge router 1 will send a frame to the provider edge router 1and these frames will be forwarded to the egress label switch router along with two labels i.e. tunnel label and VC label.



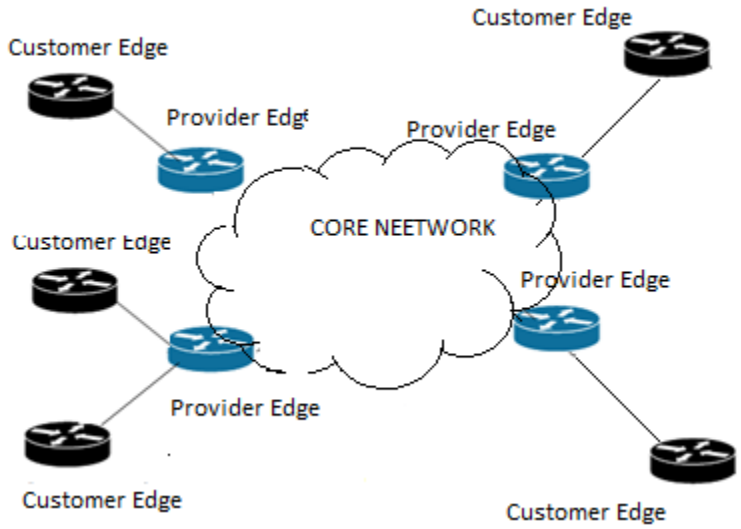
In this figure, label 46 is the VC label and label 26 as well as label 36 is the tunnel label. A targeted label distribution protocol session is set up which is used for advertising the VC labels between both the provide edge router 1 and router 2. The bottom label in the label stack will contain the VC label and at the top label in the label stack is the tunnel label. The egress attachment circuit which is present on the egress provider router is identified with the help of VC label and tunnel label is used for directing the intermediate label switch routers on how to forward the frames to the egress label switch routers. The VC label which is 46 is pushed on the frame by the ingress provider edge router 1 and then tunnel label is pushed. The tunnel label provides help in identifying the remote provider edge router and is also associated with the interior gateway protocol prefix. The packet is forwarded hop by hop according to the labels specified on the tunnel label and the packet will reach provider router. The tunnel label will be removes as the packet reaches egress provider edge router due to the result of penultimate hop popping. In the label forwarding information base provider edge router will find the VC label and

that VC label will be removed and the frame will be forwarded to the correct attachment circuit. The provider routers are not aware of VC label so no extra label distribution protocol is needed on the provider router.

USE OF LABEL DISTRIBUTION PROTCOL IN VPLS

The virtual private LAN service is a layer 2 virtual private network which is used for providing multipoint connectivity and is also used for providing broadcast capability. In virtual private LAN service, the point to point peer relationship has been removed as the customer edge routers are able to communicate with each other as if they are attached with the LAN but it has same architecture as the other layer 2 virtual private network where the customer edge routers are connected to the provider edge routers and the private edge routers are connected to each other through pseudowires. The pseudowires that are used in the point to point layer 2 connectivity is same to the pseudowires which are used in the virtual private LAN service. The difference in the behavior of point to point and multipoint is determined the way the data is forwarded in the layer 2 architecture.

As virtual private LAN Service offers transparent LAN services it is considered useful by the service providers as well as the enterprises.

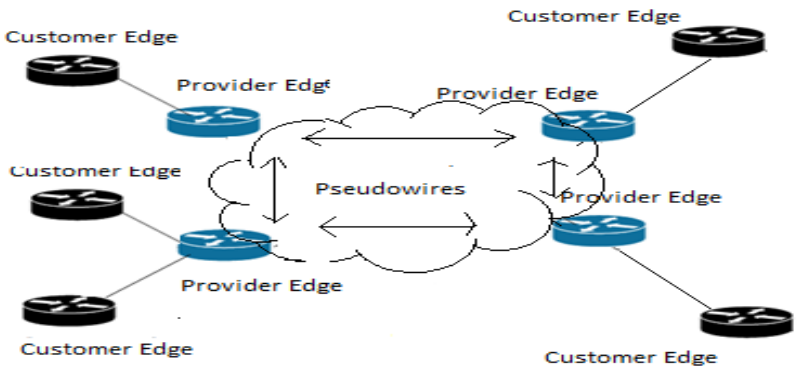


According to this figure the provider edge routers will behave like a virtual switch so that the customer edge routers can be visualized as if they are on an Ethernet network with a single bridge. The connection between customer edge router and provider edge router can be through the direct links or it can be through the access network. To get full connectivity for the customers by using few connections the

virtual private LAN service allows only single link between provider edge router and customer edge router for transmitting packets to the other customer edge routers. The other advantage of using virtual private Lan service is that once the provide edge routers have been provisioned then only the provider edge routers needs to be reconfigured if the customer edge router is removed, added or relocated. Also forwarding between the attachment circuit and pseudowire on a provider edge router is no longer done on the basis of one to one mapping but on the basis of layer 2 forwarding table which is dynamically populated.

By using the learning process, the mac address and next hop interfaces are populated in the forwarding table. The forwarding table is used by the provider edge router for determining the outgoing path and these outgoing path are taken from the destination MAC address. If an unknown MAC address is received by the provider edge router that frame will be duplicated as well as forwarded to all the ports in the Lan segment. A collection of ports which could be belonging to the same VLAN is the LAN segment and during configuration it must be specified that a particular port belongs to which virtual private LAN service instance so that in case of unknown MAC destination the frames will be forwarded on those ports only which belong with that instance.

The functionality of the Ethernet switch is emulated by the virtual private LAN service. Before the Ethernet frames are forwarded in the network they receive two labels which is virtual circuit label and the tunnel label. The forwarding of the Ethernet frame is done in the same way as in the AToM networks. The responsibility of the virtual circuit label is for indicating the virtual circuit to which the frame will belong and the virtual label is always at the bottom of the label stack. The tunnel label is responsible for forwarding of the frames from the ingress provider edge router to the egress provider edge route and the tunnel label is always present at the top of the tunnel stack.

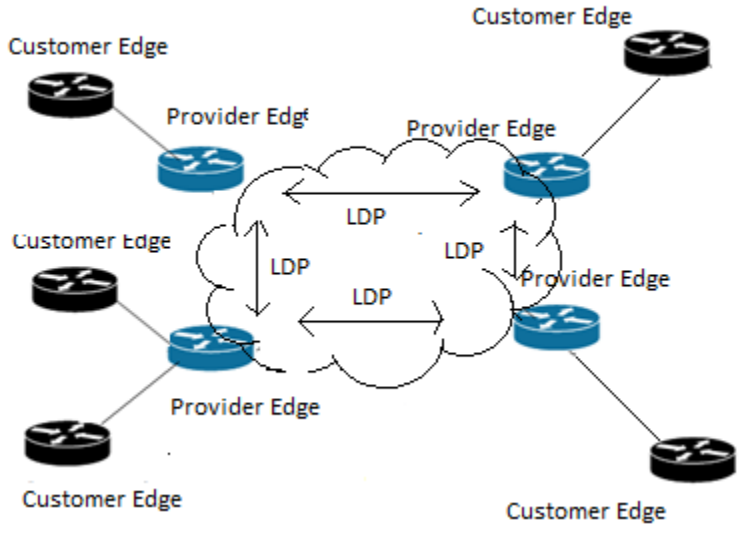


In this figure, there is one virtual private LAN service instance and all the provider edge routers are connected with that instance. This customer is using several sites and all these sites have been connected with the provider edge router. As seen above all the provider edge routers are connected with each other via pseudowires to carry the frames between each other and in order to carry the frames in both the direction there will be need of two label switch path for every pseudowire.

VIRTUAL PRIVATE LAN SERVICE NETWORK SIGNALING

For each virtual private LAN service instance a full mesh of pseudowires is required between the provider edge routers and the neighbor of the provide edge router must be specified i.e. for one virtual private LAN service instance all the remote provide edge routers needs to be specified. A targeted label distribution protocol session will be formed with all the other provide edge routers in a full mesh for the signaling and the advertisement of the virtual circuit label between each pseudowires of the provider edge routers. Therefore, to establish pseudowire for all virtual private LAN service instance a single label distribution protocol can be used between two provider edge routers.

After the establishment of the label distribution protocol session between the provider edge routers, pseudowires will be created so that the virtual switches can be interconnected with each other and that too in full mesh deployment. On the provider edge router if the virtual private LAN service instance is given for a VLAN interface then

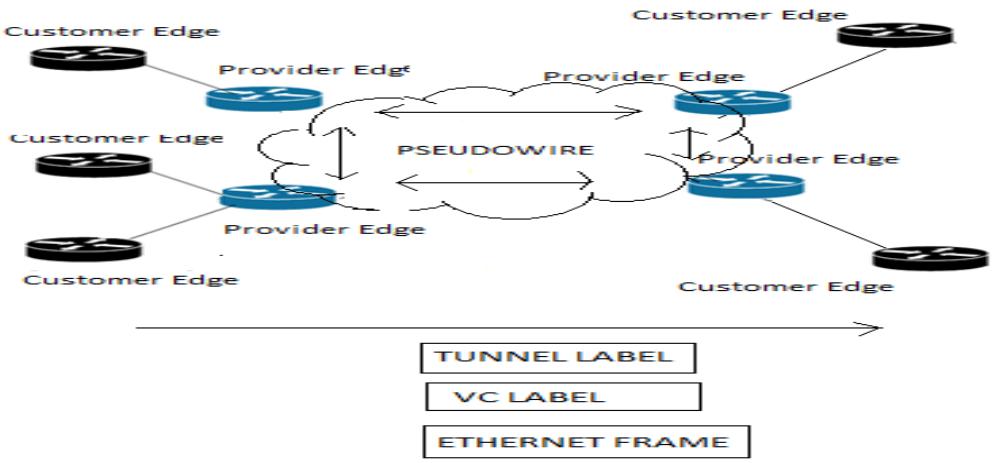


a virtual circuit ID will be issued and this virtual circuit ID is the same as the virtual private network ID. The virtual circuit ID is present between the pseudowire of the two provider edge routers and the virtual circuit label is different for every pseudowire.

DATA PLANE OF VIRTUAL PRIVATE LAN SERVICE

On the Ethernet frame two labels are imposed which are tunnel label and virtual circuit label. The tunnel label is at the top of the label stack and the responsibility of tunnel label is to identify the label switch path to which the frame belongs which is used in forwarding the frames from one provider edge router to the another provider edge router. The virtual circuit label is the label that is at the bottom of the label stack and the responsibility of the virtual circuit label is to identify the pseudowires between the two provider routers and the virtual circuit label is used by the egress provider edge router for determining the attachment circuits in order to forward the frames.

The Ethernet frame is transported without the 802.1 Q tag as the tag is removed before the frame has to be forwarded. A MAC table is built by the provider edge router and Ethernet frames are forwarded according to this MAC table from the Ethernet port and from the pseudowires. The configuration of provider router and the label distribution protocol which is used for signaling the pseudowires forms the control plane. A virtual forwarding instance is made up of control plane as well as data plane information and is used for forwarding frames to the attachment circuits. Label distribution protocol is used for population the virtual forwarding instance with the label information of virtual circuit and membership of virtual circuit.



In the above diagram the two labels i.e. tunnel label which is at the top of the label stack and virtual circuit label which is at the bottom of the label stack is shown along with Ethernet frame as they are forwarded in the network.

USE OF LABEL DISTRIBUTION PROTOCOL IN MPLS TE WITH VPN

Multiprotocol label distribution switching with traffic engineering is used by the service providers for the effective spreading of the traffic in the network. It also helps in avoiding links which are underutilized or links which are overutilized. The bandwidth and attribute of the link like delay is considered by the traffic engineering and the traffic engineering has capability to automatically adapt with the changes in the bandwidth and attributes of the link.

In these network if the head end router has the knowledge regarding the topology of the network and regarding the bandwidth on all the links, the head end router has the capability to calculate the most efficient route through the network. In order to establish label switch path from end to the other multiprotocol label switching needs to be activated on the routers.

Any network that has label switch routers can use the traffic engineering. The routing protocol used traffic engineering end points is the link state routing protocol so that the head end label switch router has the knowledge regarding the bandwidth and the link attributes. Every router in the network which are present in the same area build a state of link and then share that links with each other so that they information regarding the topology for that area which helps the head end label switch router in deploying traffic engineering on that label switch path by using source based routing. This path is called as multiprotocol label distribution switching with traffic engineering tunnel. As the label switch path is unidirectional so is the traffic engineering tunnel. The traffic engineering tunnel has to be signaled which is known as resource reservation protocol and the configuration for the tunnel is only on the one end which is the head end label switch router and not on the other end of the tunnel which is the tail end label switch router.

With the help of traffic engineering, tunnels can be created in the multiprotocol label switching virtual private network between the two provider edge routers for passing all the traffic through the tunnel so that the congestion can be avoided and so that more control can be enforced on the traffic which is passing through that tunnel.

When two provide edge routers have two traffic engineering tunnels which are both in opposite direction and when the vpnv4 routes border gateway protocol next hop

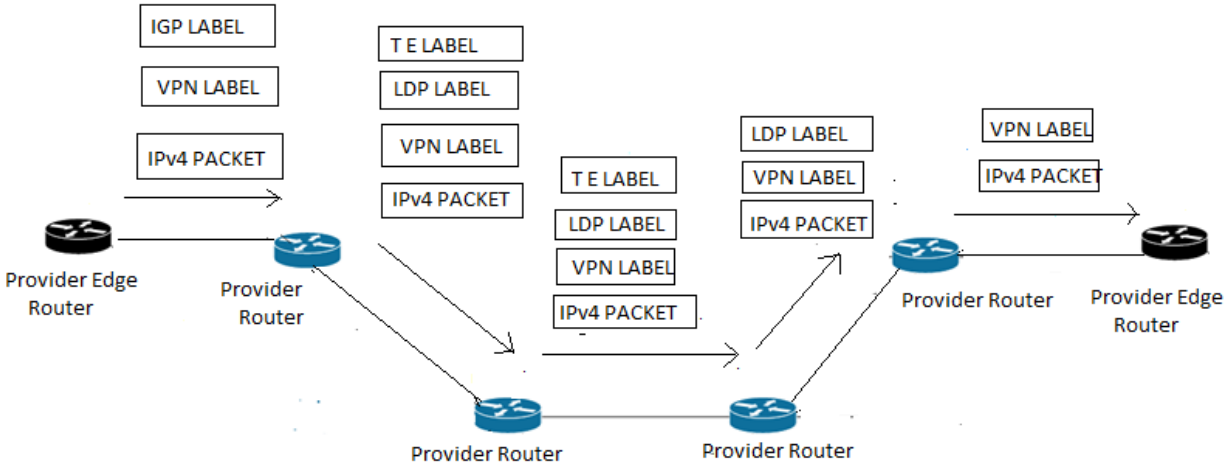
is toward the tunnels it will result in the VRF traffic going through the traffic engineering tunnel. There are two labels associated with the packet which is TE label and VPN label. The TE label is present at the top of the label stack whereas the VPN label is at the bottom of the label stack. All the VRF traffic will flow over the tunnel if label distribution protocol is not enabled and all the provider routers have traffic engineering enabled on them as the traffic will never get to the egress provider edge router because the traffic has only VPN label with them. If the provider edge routers are present at the head end label switch router as well as at the tail end label switch router there is no need of label distribution protocol but the label distribution protocol is enabled in the traffic engineering tunnel when the provider router is behaving as the tail end label switch router instead of the provider edge router because if the label distribution protocol is not enabled the packets will become unlabeled which will result in the loss of VPN label as well as IGP label. The packets will not be forwarded to the correct VRF interface if the VPN label is lost and if the IGP label is lost the packets will not be able to reach the egress provider edge router as the packet could be lost or it could be dropped since IP lookup for the destination IP address will not be correct. Also the provider routers will not have any knowledge regarding the IP VF routes. Therefore, for the packets to be able to reach the provider edge routers it is very important that label distribution protocol is running between the provider routers.

The label distribution protocol session must be enabled between the head end label switch router and tail end label switch router. The implicit null label will be received by the upstream label switch router which is sent by the tail end label switch router for that label switch path. In case of the provider edge router as the tail end router it will be okay as at the penultimate hop router one labelled will be removed and the packet with the VPN label will arrive at the egress provider edge router but this is not the case when provider router is behaving as the tail end label switch router as it will cause a problem. Since the implicit null label will be received by the upstream label switch router which is sent by the tail end label switch router for that label switch path and at the penultimate hop router one labelled will be removed and the packet with the VPN label will arrive at the egress provider router which will drop that packet or the packet will be forwarded to a wrong location as it could be forwarded to a different label switch path having the same label. The solution for above problem is that label distribution protocol session should be activated between the head end router and tail end router which can be done in two ways: -

a) Label distribution protocol should be enabled on the tunnel interfaces and two tunnels requirement both in opposite direction to each other between the provider edge router and provider router.

b) A label distribution protocol session which is targeted session between the provider edge router and provider router.

By using the first method two tunnels will be formed between the routers which are operating in opposite direction and on the tunnel interfaces label distribution protocol is enabled which will result in formation of label distribution protocol session consisting of targeted session between the head end label switch router and tail end label switch router automatically. By using the second method the targeted label distribution protocol session is setup between the tail end router and on the head end router. Also on the tunnel interface of the head end router multiprotocol label switching need to be enabled. By using both the solutions the result will be same i.e. the label distribution protocol will be advertised by the targeted label distribution protocol session from the tail end label switch router to the head end label switch router.



In the above figure, the label has been shown that are passing the network in the traffic engineering tunnel. As seen above the virtual private network packet consists of three labels which are traffic engineering label, label distribution protocol label and virtual private network label. The packet arrives with two label at the end of the tail end label switch router of the traffic engineering tunnel which is the label distribution protocol label and virtual private network label. In the figure, a traffic engineering tunnel is shown where a provider edge router works as the tail end label switch router and the targeted label distribution protocol session has been established between both the tunnels which will result in the packet being labelled with the label distribution protocol and an additional label is added on top of that packet which is the traffic engineering label before the packet will be switched out.

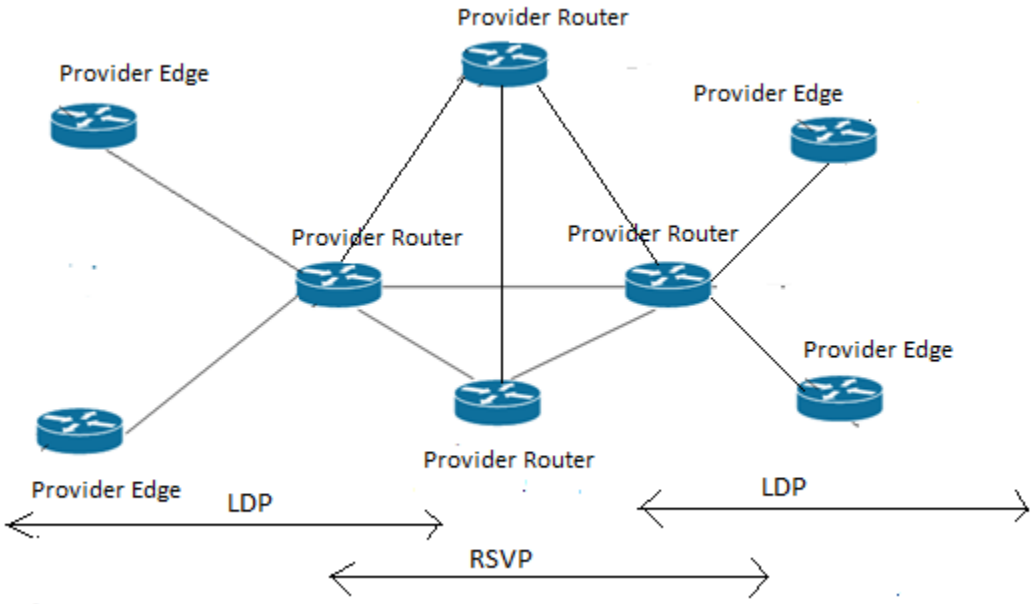
USE OF LABEL DISTRIBUTION PROTOCOL IN RSVP

The benefit of using label distribution protocol over resource reservation protocol is that different types of traffic such as IPv4, IPv6, unicast as well as multicast can be converged and then be transported across the layer 2 and layer 3 virtual private networks. It provides connectivity which is flexible that can be used for accommodating different topologies as well as protocols and if there are multiple providers using label distribution protocol over resource reservation protocol, secure internetworking can be provided. The benefit of using resource reservation protocol tunnels is that the traffic can be controlled as the customer wants as it supports engineering of traffic, guarantee of bandwidth and redundant capability for link as well as nodes. The number of label switch path required can be reduced by using resource reservation protocol which affects the protocols as the requirement for the resources gets reduced and for the routers also thereby reducing the convergence time. In label distribution protocol over resource reservation protocol the network disruption time is minimal and also the rollout is very cost effective as the label switch path which is built from the tunnels which are point to point and is connected with the neighbors that are directly connected. These tunnels do not provide end to end connectivity but only till the next hop and that is why label distribution protocol is running over these tunnels. The directly connected neighbors are connected with these sessions and therefore when a new router is added it will have both resource reservation protocol and label distribution protocol sessions. Thus the responsibility of label distribution protocol is to advertise the labels for the addresses which are new whereas the resource reservation protocol label switch paths are connected only with the next hop.

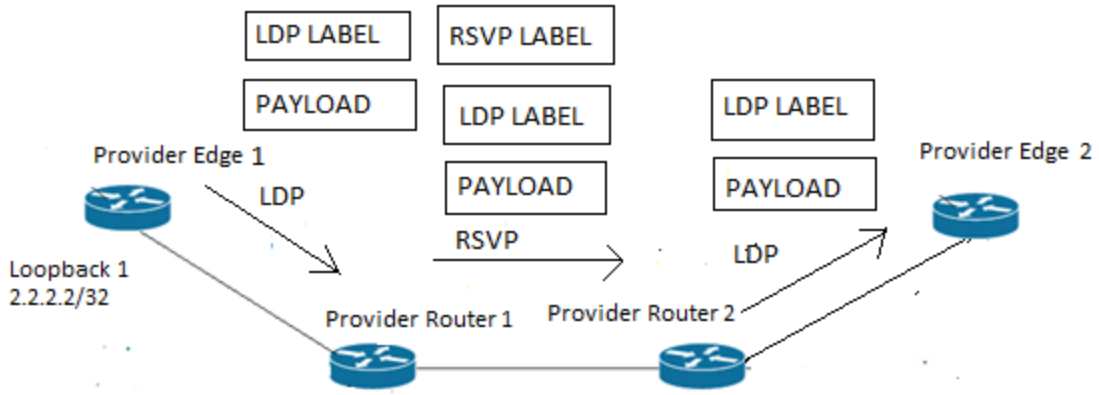
By enabling label distribution protocol over resource reservation protocol full mesh of resource reservation protocol label switch path can be established between the provider edge routers and label distribution protocol is also used simultaneously for its simplicity. Another benefits of using label distribution protocol over resource reservation protocol are label distribution protocol can be easily configured than resource reservation protocol. Traffic engineering, Quality of service, link and node services are some of the capabilities which is offered by the resource reservation protocol and in case the provide edge router is not compatible with the resource reservation protocol traffic engineering, label distribution protocol over resource reservation protocol can be used in that case for controlling the traffic.

The main concept of the label distribution protocol over resource reservation protocol is that on the core routers of the network resource reservation protocol is running and on the edge routers the label distribution protocol is running. The traffic which consists of label distribution protocol is then encapsulated inside the tunnels

consisting of the resource reservation protocol. The responsibility of provider router in this network is to just switch labels with the help of resource reservation protocol to ensure that the fast failover is maintained in the network. The interaction with the other networks, customers is the responsibility of the provider edge routers. The label distribution protocol is running on all the edges routers which goes up to the core routers and the label distribution protocol traffic is encapsulated with the help of tunnels which are present within the core routers. Therefore, all the edge routers have the label distribution protocol connectivity within the network and the core routers are running the resource reservation protocol which has the benefit of providing traffic engineering and quick failover services. The good thing about this network is that resource reservation protocol is not required everywhere as it is very resource intensive and label distribution protocol can be used which is not so resource intensive label protocol.



In this figure, we can see that the resource reservation protocol tunnel engineering is running on the core network which helps in maintaining fast failover and on the edges of the network label distribution protocol is running which consumes very less resources in the network.



In this figure the two provider routers which are connected with each other have a label distribution protocol session and are running both the label distribution protocol and resource reservation protocol on them. When the packet which has to be sent to the provider edge router 2 is forwarded from the provider edge router 1 the label distribution protocol label is put on top of the packet and it is sent to the provider router 1. At the provider router 1, an additional label is put on that packet which is resource reservation protocol label and is forwarded through the traffic engineering tunnel to the provider router 2. At provider router, the resource reservation protocol label is removed and the packet is forwarded by using the label distribution protocol to the provider edge router 2. At the provider edge router 2, the label distribution protocol is removed and the packet is forwarded to the customer edge router.

ADVANTAGES OF USING LABEL DISTRIBUTION PROTOCOL

The main advantages of using label distribution protocol are: -

a) There is no need of the additional signaling protocol if the label distribution protocol is already running on the network.

b) During the forwarding of the packet few labels are put on top of the packet which are very important requirement in the older hardware requirements which have limitations in handling label stacks which are deep.

c) Label distribution protocol is simple to configure as compared with the other signaling protocols.

d) Label distribution protocol is uses less resources as compared to the other signaling protocols.

e) A lower time bound was imposed on the convergence time of label distribution protocol by the interior gateway routing protocol convergence time bound which used to result several hundred milliseconds of traffic loss. However, it was rectified with the by the addition of fast reroute capabilities to the label distribution protocol and the convergence time has reduced below resource reservation protocol fast reroute time.

DISADVANTAGES OF USING LABEL DISTRIBUTION PROTOCOL

The main drawback with label distribution protocol is that since for routing it needs to rely on interior gateway protocols it can have same complications such as: -

a) The label switch path which are established by the label distribution protocol has to follow the shortest path created by the interior gateway protocol so if there is a change in the path of the interior gateway protocol, the label switch path will also undergo a change rather than following a path which is predefined.

b) The scope of the label switch path which are established by the label distribution protocol is same as the scope of interior gateway protocol. So, it is impossible by the label switch path to cross autonomous boundaries with the label distribution protocol.

c) In interior gateway protocols traffic can be looped or can be blackholed during the event of reconvergence and these properties have been inherited by the label distribution protocol since it relies on interior gateway protocols for decisions which are based in routing.

d) A traffic loss can occur in the case of loss of synchronization between the label distribution protocol and the interior gateway protocol.

e) Label distribution protocol cannot be used for controlling the traffic as per the needs of the customer.

SECURITY THREATS FACED BY LABEL DISTRIBUTION PROTOCOL

Some of the threats faced by the label distribution protocol are: -

a) Spoofing

b) Privacy of label distribution

c) Denial of service

SPOOFING

The spoofing attack can be carried on two types of label distribution protocol communication which is: -

a) Discovery exchange

b) Session communication

DISCOVERY EXCHANGE

In order to maintain and establish label distribution protocol session, label switch routers send hellos to each other periodically. In order to create a new hello adjacency or in order to refresh the existing one a receipt of the hello is needed. A session can be terminated if a hello packet is spoofed for an adjacency as it can result the adjacency to time out. This can happen when a small hold time is specified in the hello which is spoofed as the receiver will except the hello at the time specified in the hold time while the sender will send hello at the time which was agreed previously.

This threat can be mitigated by using the following methods: -

a) Label switch routers should accept hellos on those interfaces that are connected directly.

b) The hellos which have not been addressed for the all the routers on the multicast group should not be accepted and should be ignored.

In case the label switch routers are not directly connected and want to establish label distribution protocol session they can use the help of extended hello messages. The threat of spoofing in case of extended hellos can be mitigated by the label switch router by filtering the hello messages and by accepting only those hello messages which have been originated at the source which has been

permitted according to the information in the access list.

SESSION COMMUNICATION

Transmission control protocol MD5 signature option is used by the label distribution control protocol in order to provide authenticity and integrity for the session messages but now a days TC 5 is considered weak for providing authentication and it should be replaced with a stronger hashing algorithm but as of now no such transmission control protocol option is available. So, label distribution protocol can use any technique for transmission control message digest until any technique which is stronger than MD5 is specified and has been cleared for implementation.

PRIVACY

No mechanism has been provided in the label distribution protocol to protect the privacy for label distribution. The security required by the label distribution protocol is same as the security required by the routing protocols. Label distribution protocol provides mechanism by which it has ensured that the messages are authenticate and integrity have been maintained which is as good as the security of the routing protocols. As the labels are carried without any security in the packet the privacy would not be able to protect the packet against the spoofing attack. Also without having the knowledge to which forwarding equivalence class, the label has been bound it is still possible that a spoofing attack can take place. Therefore, privacy cannot help label distribution protocols in the case of label spoofing. So in order to avoid the spoofing attack, it is important that only the label switch routers that are trusted can label the data packets and the label switch routers have properly learned the labels before putting the labels on the packet.

DENIAL OF SERVICE

There are two targets where the denial of service attack can take place which are: -

a) User datagram protocol port used for label distribution protocol discovery

b) Transmission control protocol port used for label distribution protocol session establishment

USER DATAGRAM PORT USED FOR LABEL DISTRIBUTION PROTOCOL DISCOVERY

The threat for the denial of service attack can be addressed by the label switch router administrator the hellos is exchanged between the peers which are connected directly and can be trusted that they will not be initiating the denial of service attack. As the interior peers are under the direct control of the administrator the interfaces to the interior peer will not be any threat but the interfaces to the exterior peers will represent a threat since they are not under the control of the administrator and this threat can be reduced by the administrator by connecting the exterior peers to only those label switch routers which trust that the exterior peers will not initiate a hello attack.

However, the more serious threat is the denial of service attack by the used of extended hellos. The solution for this threat is using access list for filtering the extended hello by defining only those addresses with whom the extended discovery is permitted but it has a downside as label switch router resources are required for carrying out filtering.

If there is an environment where multiprotocol label switching cloud has been identified which can be trusted, the interior label switch routers can be protected by the edge label switch routers against the denial of service attack by using the extended hellos as extended hellos which are origination outside the multiprotocol label switching cloud can be filtered and only those extended hellos will be accepted which are originating at the addressed which are permitted according to the access list. The only downside with this solution is that at the edges resources will be consumed.

TRANSMISSION CONTROL PROTOCOL PORT USED FOR LABEL DISTRIBUTION PROTOCOL SESSION ESTABLISHMENT

A label distribution may be a target of denial of service attack just like other protocols that use transmission control protocol and label distribution protocol is equally vulnerable to these attacks as are the other protocols. However, it can be mitigated as following: -

a) For the establishment of session, the label switch router should avoid using promiscuous transmission control protocol listening and should be listening only that are specified for the discovery of peers as packets can be dropped early during processing because it will hard for them to match with connections that are existing or those connections which are in progress.

b) By using MD5 option also helps in mitigating the denial of service attack since the SYN segment will be accepted if and only if the checksum is valid but the checksum must be computed by the receiver before deciding to discard a SYN segment which is perfect.

c) If there is an environment where multiprotocol label switching cloud has been identified which can be trusted, the interior label switch routers can be protected by the edge label switch routers against the denial of service attack by using the extended hellos as extended hellos which are origination outside the multiprotocol label switching cloud can be filtered and only those extended hellos will be accepted which are originating at the addressed which are permitted according to the access list.

NEW ADVANCEMENT IN LABEL DISTRIBUTION PROTOCOL

MULTIPOINT LABEL DISTRIBUTION PROTOCOL

Point to multipoint (P2MP) and multipoint to multipoint (MP2MP) are the extensions to the label distribution protocol in multiprotocol label switching networks. These extensions are also known as multipoint label distribution protocol and label switch path for the point to multipoint and multipoint to multipoint is constructed by not relying on any other multicast tree construction protocol. Multipoint label switch path can be used for various applications like with IP multicast or provide support in layer 3 virtual private network for multicast.

Multiprotocol label distribution protocol is used to provide support in multicast virtual private network and is used for forwarding and routing of the multicast packets. By using multicast virtual private network, the service provider can transparently connect its network and there is no change in the way the network is administered and also there is no change in the connectivity.

LINK MANAGEMENT PROTOCOLS

A new mechanism is under development by the internet engineering task force which is known as generalized multiprotocol label switching (GMPLS) which is used in the networks for establishing connections related to the light paths. Generalized multiprotocol switching is an extension of multiprotocol switching which has been designed to improve the fast switching in IP based networks. The

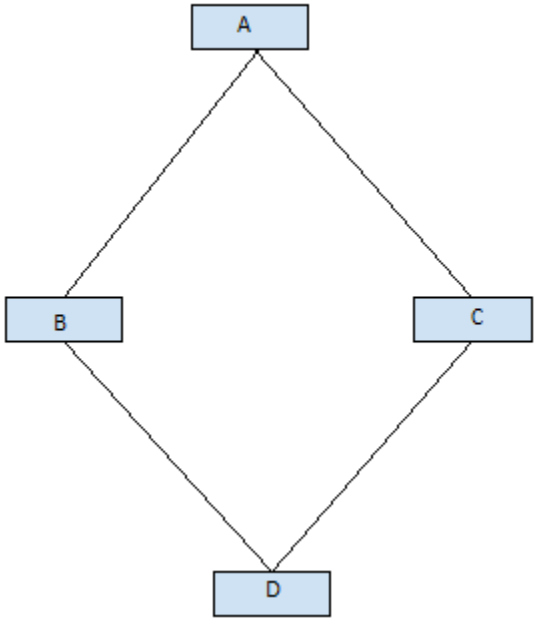
internet engineering task force is doing much work so that it can be able to change the existing protocols so that it can provide support to generalized multiprotocol label switching and the internet engineering task force has proposed some modifications to open shortest path first, constraint based resource reservation protocol and resource reservation protocol. The generalized multiprotocol switching is used to provide switching for networks which consists of time, wavelength, space as well as for packet and therefore known as multiprotocol lambda switching. The number of parallel links between nodes have been increased with the use of generalized multiprotocol switching which is useful in photonic network as between pair of nodes there are hundreds of parallel links existing in the network. The another advantage of using generalized multiprotocol switching is that it provides support for fault detection, fault isolation and incase he network goes down it has the shortest downtime as network can be switched to alternate channels.

So, in order to support the generalized multiprotocol label switching a new protocol was introduced which is link management protocol. Link management protocol has been developed as the extension to the label distribution protocol and is used for providing management and configuration to the optical networks. It also provides fault isolation and manages traffic engineering link. In present scenario it will be used to control channel connectivity and to verify if the data bearing channels have a physical connectivity or not. It will be used to check the information regarding the links i.e. connection of the links and will be used for managing any failure in the link. The main advantage of using link management protocol is that in both opaque as well as transparent channel it can pinpoint the location of the localized failure even if any encoding scheme has been used. It uses channel management and link property correlation as the core functions. To maintain and establish the channel between the nodes is the responsibility of the channel management and synchronization of properties of the link is the responsibility of the link property correlation.

LOOP FREE ALTERNATIVE

Loop free alternative has a main goal of reducing convergence time thus reducing the packet loss when a router in topology fails. This technique works on the logic of choosing pre calculated backup next hops that are used in case of network failure until the network converges. The best way to avoid packet loss is that the router that is adjacent to the failed router will invoke a repair path. The traffic will be forwarded through this repair path until the network converges and the new next

hop are installed in the network with just one condition that the routing protocol to be used should be Link state routing protocol. Usually when a link fails and network connectivity is lost to one or more prefixes the routing with link failure signals its neighbors for the new next hop for affected prefixes to be recomputed but this usually takes hundreds of milliseconds thus leading to packet loss. Now with fast reroute can reduce this failure time of hundreds of milliseconds to 10s of millisecond by pre computing the alternate next hop path thus switching to alternate hop in case of network failure.



For example, in the current figure without lop free alternative the path that router A chooses to reach D is through C and that will be the only path that router A will compute and only path that will be stored. With the help of loop free alternative, the router A will also install a backup path that is path through B to reach D. This path will be used until the shortest path first is run again and the topology converges. One of the criteria for choosing a loop free alternative is that a neighbor can find loop free alternative if and only if: -

Distance of neighbor to destination < Distance of Neighbor to source + Distance of source to destination

There is also a chance of loop formation in the topology because if more than one link fails even after providing node protection then there is a chance of traffic loss.

The only way to avoid looping is by using downstream paths. There are two ways by which loop free alternative can be used. One of the protecting techniques is node protecting and second protecting technique is link protecting but the best is to choose the third option that is the combination of both i.e. node and link protecting loop free alternative.

There are some rules that should be taken care of when applying loop free alternative, some of them are: -

a) Loop free alternative should not be used in backbone area with virtual links unless all area border routers are connected to each other in a mesh.

b) If an area has more than one alternative area border router, then for the inter area routes the loop free alternative should not be used.

ALTERNATE NEXT HOP CALCULATION

In a link state routing protocol, the alternate backup next hop is calculated that is part of shortest path first calculation but in order for a loop free alternative be calculated for a destination the following has to be taken care of:

a) Shortest distance from source to destination which is distance 1.

b) Shortest distance from the source router neighbor to destination which is distance 2.

c) Shortest distance from source router neighbor to itself which is distance 3.

d) Distance 1 is available when SPF algorithm is run and distance 2 and distance 3 is calculated by perspective of source router neighbors.

So, the alternate next hop can be loop free during the link failure if they follow this condition which is: -

Distance of neighbor to destination < Distance of Neighbor to source + Distance of source to destination

NODE PROTECTION ALTERNATE NEXT HOP

Suppose S is the primary neighbor and D is the destination. H is the alternate next hop which is protecting the neighbor S against the node failure and H is loop free

with respect to both S and D then for backup next hop to protect against node failure the following condition must be true: -

Distance (H to D) < Distance (H to S) +Distance (S to D)

If this condition is not met, then Node protection cannot be provided.

USING ALTERNATE NEXT HOP

The backup next hop will be used in case there is a failure in the primary next hop and the traffic will be diverted to the backup next hop. After the failure has been detected the router will: -

a) The failure primary next hop will be removed.

b) For the next hop which has failed the loop free alternative will be calculated and will be installed.

Also other next hops can be removed if the router believes that they got affected by the failure even though it may not be visible at that time and the alternate next hop will be used only for the shortest path.

REQUIREMENT FOR LFA IN LABEL DISTRIBUTION PROTOCOL

In label distribution protocol the traffic will follow the path which is provided according to the interior gateway protocol and therefore the label distribution protocol will also follow the loop free alternatives that is provided according to the interior gateway protocol. In label distribution protocol the labels that are installed in the forwarding plane should be available before the occurrence of the failure which means that the labels must be distributed by the label switch router for forwarding equivalence class irrespective if the neighbor is upstream or not. Also label retention mode must be used by the label distribution protocol as to retain labels for neighbors that are not primary and label distribution protocol should be using the downstream unsolicited mode so that the labels should be distributed to downstream routers. So, if all these conditions are met then label distribution protocol can be used for providing the loop free alternate.

ADVANTAGES OF USING LOOP FREE ALTERNATIVE

a) By using loop free alternative fast convergence time can be provided and there is no need for the additional configuration in the interior gateway protocol as well as no other protocol is needed.

b) Loop free alternative can be deployed as router by router and therefore there is no need for any change in the protocol.

c) Since backup paths can be precomputed as well as installed in the data plane therefore it is possible to achieve a sub 50ms repair time.

d) Loop free alternative offers independent implementation of the prefix.

e) There is a fixed repair time with the loop free alternative as the repair time depends on failure detection time as well as on the time required to activate the behavior for the loop free alternative.

f) In loop free alternative link as well as node protection can be provided together without any difference in the operation.

g) In the current network the loop free alternative does not require any another virtual layer of topology.

h) The loop free alternative helps in saving money as compared to multiprotocol label switching traffic engineering as staff is required for the operation and maintenance of these network entities.

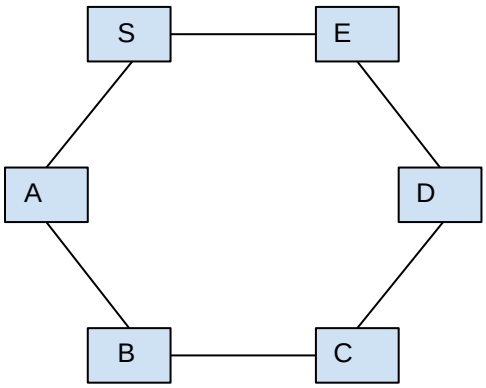
i) The per prefix mode of loop free alternative allows for simpler and more efficient capacity planning.

Loop free alternative is an important protection alternative for the multiprotocol label switching networks. The major advantage of using loop free alternative is the simplicity by which it can be implemented and the other greatest factor is that it is possible to integrate loop free alternative with the default interior gateway protocol behavior as well as there is also no need to upgrade the network for using the loop free alternative. The only disadvantage of using loop free alternative is that it depends upon the topology of the network i.e. with each topology the loop free alternate will change.

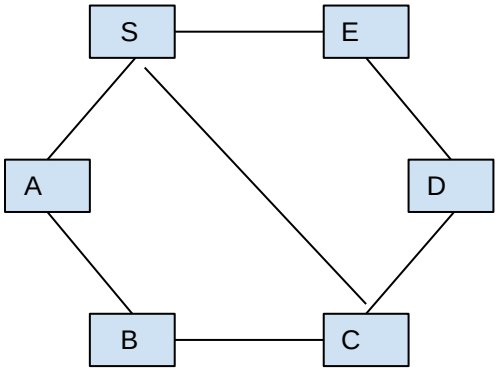
ADVANCEMENT IN LOOP FREE ALTERNATIVE

The original loop free alternative cannot be used to provide connectivity failover in ring as well as square based topologies. In order to provide protection in ring as well as square based topologies a new version of loop free alternative is used which is the remote loop free alternative. The loop free alternative cannot be used in this case because of the following condition: -

Distance of (neighbor to destination) < Distance of Neighbor to source + Distance of source to destination.



For example, in the above case the normal loop free alternative cannot work. The loop free alternative can only work for node C if there is an equal cost to reach S from both sides but for D and E protection with the help of loop free alternative is not possible. The logic behind the remote loop free alternative is that S will form a tunnel to remote end point which in turn is going to be remote loop free alternative to reach another node in the network. The nodes will be divided among two spaces which will be P space and Q space with respect to a link. But the remote loop free alternative will be chosen on the basis of common end point in these two Spaces.



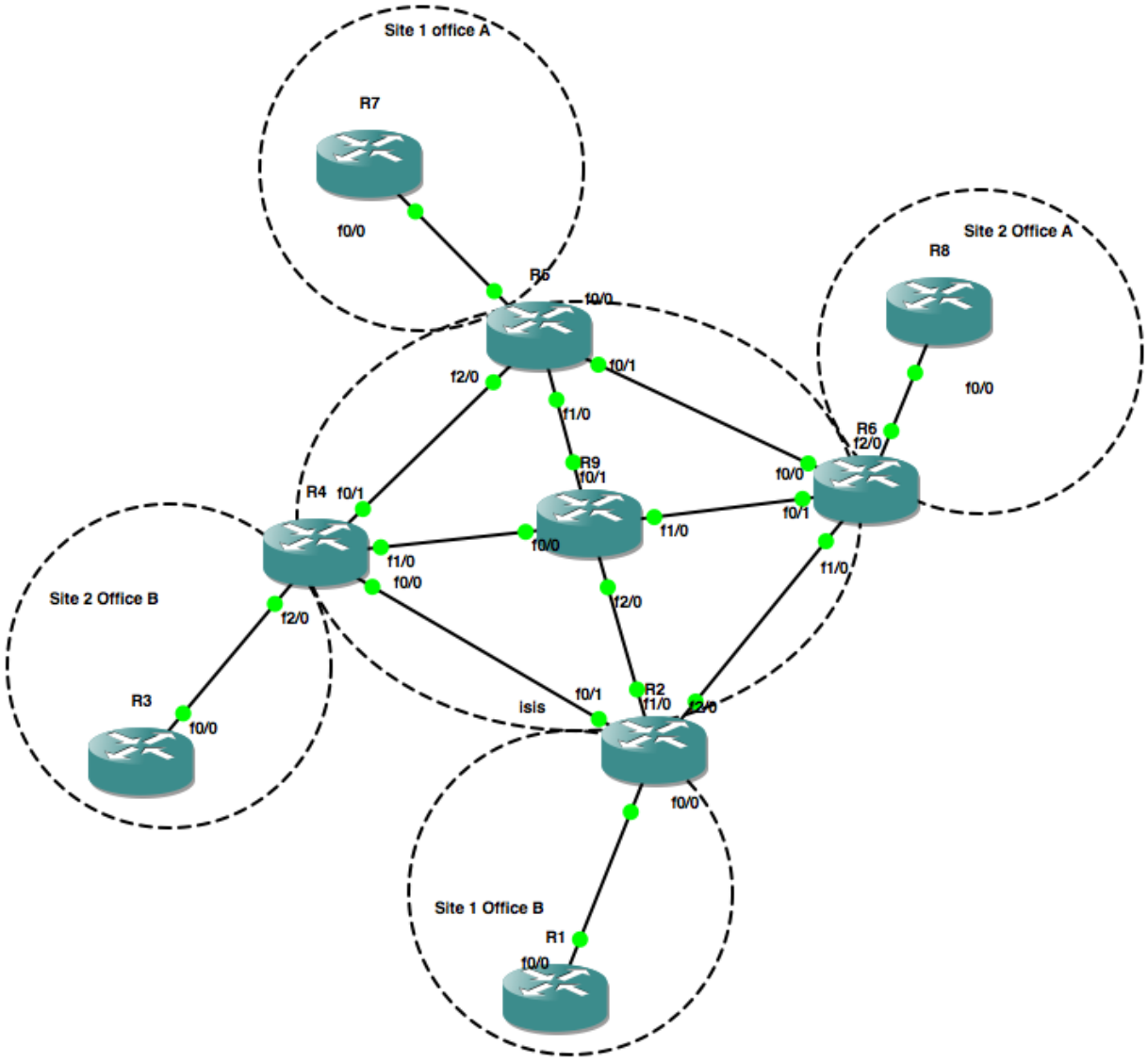
The tunnel which has been formed in the above figure can only be used for repairing traffic and cannot be used with the normal traffic. But the operation that are associated with the administration and maintenance of the traffic can be traversed through the tunnel. Suppose in above topology the SE link is a protected link then the neighbor of S that is loop free alternative is used if it does not traverse the link SE but if this is not possible then S will initiate a tunnel to the remote neighbor in order to provide connectivity in case of failure.

The tunnels which can be used for the remote loop free alternative can vary for example in case of the multiprotocol label switching, the label stack can be used for provide the tunnel by having a targeted label distribution protocol session on the both sides of the tunnel endpoint. In multiprotocol label switching, this task is simple because the tunnel formation which requires that the label will be attached and encapsulation will also be provided is done with the help pf label distribution protocol and whereas the decapsulation will be done at the end i.e. by the penultimate hop router.

SECTION B

LAB

LAB 1: LABEL DISTRIBUTION PROTOCOL WITH ISIS



RI

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!

```
hostname R1
!
boot-start-marker
boot-end-marker
no ip icmp rate-limit unreachable
ip cef
!
!
no ip domain lookup
!
multilink bundle-name authenticated
!
!
!
archive
log config
 hidekeys
!
!
ip tcp synwait-time 5
!
!
interface Loopback1
ip address 1.1.1.1 255.255.255.255
!
interface FastEthernet0/0
ip address 12.1.1.1 255.255.255.0
duplex auto
speed auto

!
router ospf 1
log-adjacency-changes
network 1.1.1.1 0.0.0.0 area 0
network 12.1.1.1 0.0.0.0 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
control-plane
!
```

```
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
end
```

R2

```
!

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
ip vrf site1
rd 65000:1
route-target export 65000:1
route-target import 65000:1
!
no ip domain lookup
!
```

```
mpls label protocol ldp
multilink bundle-name authenticated
!
!
!
!
archive
log config
 hidekeys
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface Loopback1
ip address 2.2.2.2 255.255.255.255
ip router isis
!
interface FastEthernet0/0
ip vrf forwarding site1
ip address 12.1.1.2 255.255.255.0
ip ospf 1 area 0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 24.1.1.2 255.255.255.0
ip router isis
duplex auto
speed auto
mpls ip
!
interface FastEthernet1/0
ip address 29.1.1.2 255.255.255.0
ip router isis
duplex auto
speed auto
mpls ip
!
interface FastEthernet2/0
ip address 26.1.1.2 255.255.255.0
ip router isis
```

```
duplex auto
speed auto
mpls ip
!
router ospf 1 vrf site1
log-adjacency-changes
redistribute bgp 65000 subnets
!
router isis
net 49.0001.2222.2222.2222.00
is-type level-2-only
!
router bgp 65000
no synchronization
bgp log-neighbor-changes
neighbor 5.5.5.5 remote-as 65000
neighbor 5.5.5.5 update-source Loopback1
no auto-summary
!
address-family vpnv4
 neighbor 5.5.5.5 activate
 neighbor 5.5.5.5 send-community extended
exit-address-family
!
address-family ipv4 vrf site1
 redistribute ospf 1 vrf site1
 no synchronization
exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
mpls ldp router-id Loopback1 force
!
!
control-plane
!
!
!
!
line con 0
```

exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
end

R3

!

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
!
multilink bundle-name authenticated
!
!
!
!
!
archive

```
log config
 hidekeys
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface Loopback1
ip address 3.3.3.3 255.255.255.255
!
interface FastEthernet0/0
ip address 34.1.1.3 255.255.255.0
duplex auto
speed auto

!
router ospf 2
log-adjacency-changes
network 3.3.3.3 0.0.0.0 area 0
network 34.1.1.3 0.0.0.0 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
!
!
!
control-plane
!
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
```

```
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
end
```

R4

```
!

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R4
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
ip vrf site2
rd 65000:2
route-target export 65000:2
route-target import 65000:2
!
no ip domain lookup
!
mpls label protocol ldp
multilink bundle-name authenticated
!
archive
log config
 hidekeys
```

```
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface Loopback1
ip address 4.4.4.4 255.255.255.255
ip router isis
!
interface FastEthernet0/0
ip address 24.1.1.4 255.255.255.0
ip router isis
duplex auto
speed auto
mpls ip
!
interface FastEthernet0/1
ip address 45.1.1.4 255.255.255.0
ip router isis
duplex auto
speed auto
mpls ip
!
interface FastEthernet1/0
ip address 49.1.1.4 255.255.255.0
ip router isis
duplex auto
speed auto
mpls ip
!
interface FastEthernet2/0
ip vrf forwarding site2
ip address 34.1.1.4 255.255.255.0
ip router isis
ip ospf 2 area 0
duplex auto
speed auto
mpls ip
!
router ospf 2 vrf site2
log-adjacency-changes
redistribute bgp 65000 subnets
```

```
!
router isis
net 49.0001.4444.4444.4444.00
is-type level-2-only
!
router bgp 65000
no synchronization
bgp log-neighbor-changes
neighbor 6.6.6.6 remote-as 65000
neighbor 6.6.6.6 update-source Loopback1
no auto-summary
!
address-family vpnv4
 neighbor 6.6.6.6 activate
 neighbor 6.6.6.6 send-community both
exit-address-family
!
address-family ipv4 vrf site2
 no synchronization
exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
!
mpls ldp router-id Loopback1
!
!
control-plane
!
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
```

```
line vty 0 4
login
!
!
end
```

R5

```
!

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R5
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
ip vrf site1
rd 65000:1
route-target export 65000:1
route-target import 65000:1
!
no ip domain lookup
!
mpls label protocol ldp
multilink bundle-name authenticated
!
!
!
archive
log config
 hidekeys
!
```

```
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface Loopback1
ip address 5.5.5.5 255.255.255.255
ip router isis
!
interface FastEthernet0/0
ip vrf forwarding site1
ip address 57.1.1.5 255.255.255.0
ip ospf 1 area 0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 56.1.1.5 255.255.255.0
ip router isis
duplex auto
speed auto
mpls ip
!
interface FastEthernet1/0
ip address 59.1.1.5 255.255.255.0
ip router isis
duplex auto
speed auto
mpls ip
!
interface FastEthernet2/0
ip address 45.1.1.5 255.255.255.0
ip router isis
duplex auto
speed auto
mpls ip
!
router ospf 1 vrf site1
log-adjacency-changes
redistribute bgp 65000 subnets
!
router isis
net 49.0001.5555.5555.5555.00
```

```
is-type level-2-only
!
router bgp 65000
no synchronization
bgp log-neighbor-changes
neighbor 2.2.2.2 remote-as 65000
neighbor 2.2.2.2 update-source Loopback1
no auto-summary
!
address-family vpnv4
 neighbor 2.2.2.2 activate
 neighbor 2.2.2.2 send-community extended
exit-address-family
!
address-family ipv4 vrf site1
 redistribute ospf 1 vrf site1
 no synchronization
exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
!
mpls ldp router-id Loopback1 force
!
!
control-plane
!
!
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
```

```
login
!
!
end
```

R6

```
!

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R6
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
ip vrf site2
rd 65000:2
route-target export 65000:2
route-target import 65000:2
!
no ip domain lookup
!
mpls label protocol ldp
multilink bundle-name authenticated
!
!
!
!
archive
log config
```

```
 hidekeys
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface Loopback1
ip address 6.6.6.6 255.255.255.255
ip router isis
!
interface FastEthernet0/0
ip address 56.1.1.6 255.255.255.0
ip router isis
duplex auto
speed auto
mpls ip
!
interface FastEthernet0/1
ip address 69.1.1.6 255.255.255.0
ip router isis
speed 100
full-duplex
mpls ip
!
interface FastEthernet1/0
ip address 26.1.1.6 255.255.255.0
ip router isis
duplex auto
speed auto
mpls ip
!
interface FastEthernet2/0
ip vrf forwarding site2
ip address 68.1.1.6 255.255.255.0
ip ospf 2 area 0
duplex auto
speed auto
!
router ospf 2 vrf site2
log-adjacency-changes
redistribute bgp 65000 subnets
!
```

```
router isis
net 49.0001.6666.6666.6666.00
is-type level-2-only
!
router bgp 65000
no synchronization
bgp log-neighbor-changes
neighbor 4.4.4.4 remote-as 65000
neighbor 4.4.4.4 update-source Loopback1
no auto-summary
!
address-family vpnv4
 neighbor 4.4.4.4 activate
 neighbor 4.4.4.4 send-community both
exit-address-family
!
address-family ipv4 vrf site2
 redistribute ospf 2 vrf site2
 no synchronization
exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
!
mpls ldp router-id Loopback1 force
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
```

```
login
!
!
end
```

R7

```
!

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R7
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
!
multilink bundle-name authenticated
!
!
!
!
!
!
archive
log config
 hidekeys
!
!
!
!
ip tcp synwait-time 5
```

```
!
!
!
!
interface Loopback1
ip address 7.7.7.7 255.255.255.255
!
interface FastEthernet0/0
ip address 57.1.1.7 255.255.255.0
duplex auto
speed auto
!
!
router ospf 2
log-adjacency-changes
network 7.7.7.7 0.0.0.0 area 0
network 57.1.1.7 0.0.0.0 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
end
```

R8

```
!
```

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R8
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
!
multilink bundle-name authenticated
!
!
!
archive
log config
 hidekeys
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface Loopback1
ip address 8.8.8.8 255.255.255.255
!
interface FastEthernet0/0
ip address 68.1.1.8 255.255.255.0
speed 100
full-duplex
!
```

```
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
router ospf 2
log-adjacency-changes
network 8.8.8.8 0.0.0.0 area 0
network 68.1.1.8 0.0.0.0 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
end
```

R9

```
!

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
```

```
no service password-encryption
!
hostname R9
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
!
mpls label protocol ldp
multilink bundle-name authenticated
!
!
!
!
!
archive
log config
 hidekeys
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface Loopback1
ip address 9.9.9.9 255.255.255.255
ip router isis
!
interface FastEthernet0/0
ip address 49.1.1.9 255.255.255.0
ip router isis
duplex auto
speed auto
```

```
mpls ip
!
interface FastEthernet0/1
ip address 59.1.1.9 255.255.255.0
ip router isis
duplex auto
speed auto
mpls ip
!
interface FastEthernet1/0
ip address 69.1.1.9 255.255.255.0
ip router isis
duplex auto
speed auto
mpls ip
!
interface FastEthernet2/0
ip address 29.1.1.9 255.255.255.0
ip router isis
shutdown
duplex auto
speed auto
mpls ip
!
router isis
net 49.0001.9999.9999.9999.00
is-type level-2-only
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
```

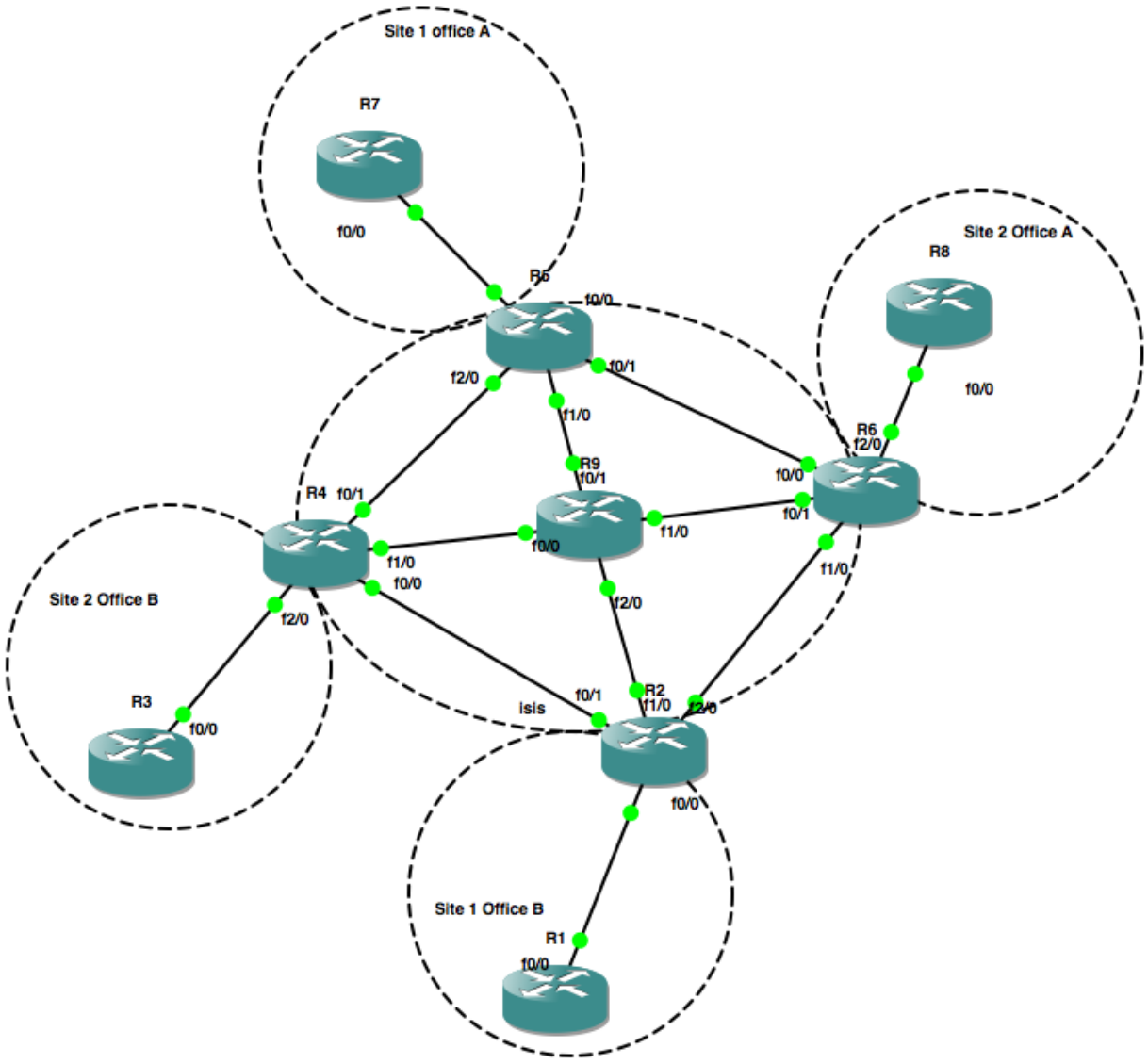
logging synchronous
line vty 0 4
login
!
!
end

```
R1#ping 7.7.7.7 source 1.1.1.1 repeat 300

Type escape sequence to abort.
Sending 300, 100-byte ICMP Echos to 7.7.7.7, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!....!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 98 percent (296/300), round-trip min/avg/max = 56/95/392 ms
R1#
```

The link between the router R2 and the router R9 was shut down during the ping between R1 to R7 and as see from the result there was a loss of four ping and then the network converged again.

LAB 2: LOOP FREE ALTERNATIVE



R1

!

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec

```
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
!
multilink bundle-name authenticated
!
!
!
!
archive
log config
 hidekeys
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface Loopback1
ip address 1.1.1.1 255.255.255.255
!
interface FastEthernet0/0
ip address 12.1.1.1 255.255.255.0
duplex auto
speed auto

!
router ospf 1
log-adjacency-changes
network 1.1.1.1 0.0.0.0 area 0
network 12.1.1.1 0.0.0.0 area 0
!
ip forward-protocol nd
!
```

```
!
no ip http server
no ip http secure-server
!
!
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
end
```

R2

```
!

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
ip vrf site1
rd 65000:1
route-target export 65000:1
route-target import 65000:1
```

```
!
no ip domain lookup
!
mpls label protocol ldp
multilink bundle-name authenticated
!
]
!
archive
log config
 hidekeys
!
!
ip tcp synwait-time 5
!
!
!
!
interface Loopback1
ip address 2.2.2.2 255.255.255.255
ip router isis
!
interface FastEthernet0/0
ip vrf forwarding site1
ip address 12.1.1.2 255.255.255.0
ip ospf 1 area 0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 24.1.1.2 255.255.255.0
ip router isis
duplex auto
speed auto
mpls ip
!
interface FastEthernet1/0
ip address 29.1.1.2 255.255.255.0
ip router isis
duplex auto
speed auto
mpls ip
!
interface FastEthernet2/0
ip address 26.1.1.2 255.255.255.0
ip router isis
duplex auto
speed auto
mpls ip
!
router ospf 1 vrf site1
```

```
log-adjacency-changes
redistribute bgp 65000 subnets
!
router isis
fast-reroute remote-lfa level-2 mpls-ldp
net 49.0001.2222.2222.2222.00
is-type level-2-only
!
router bgp 65000
no synchronization
bgp log-neighbor-changes
neighbor 5.5.5.5 remote-as 65000
neighbor 5.5.5.5 update-source Loopback1
no auto-summary
!
address-family vpnv4
 neighbor 5.5.5.5 activate
 neighbor 5.5.5.5 send-community extended
exit-address-family
!
address-family ipv4 vrf site1
 redistribute ospf 1 vrf site1
 no synchronization
exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
mpls ldp router-id Loopback1 force
!
!
control-plane
!
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
```

!
end

R3

!

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
!
multilink bundle-name authenticated
!
!
!
!
archive
log config
 hidekeys
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface Loopback1
ip address 3.3.3.3 255.255.255.255
!
interface FastEthernet0/0

```
ip address 34.1.1.3 255.255.255.0
duplex auto
speed auto

!
router ospf 2
log-adjacency-changes
network 3.3.3.3 0.0.0.0 area 0
network 34.1.1.3 0.0.0.0 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
end
```

R4

```
!

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R4
!
boot-start-marker
boot-end-marker
!
```

```
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
ip vrf site2
rd 65000:2
route-target export 65000:2
route-target import 65000:2
!
no ip domain lookup
!
mpls label protocol ldp
multilink bundle-name authenticated
!
!
!
archive
log config
 hidekeys
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface Loopback1
ip address 4.4.4.4 255.255.255.255
ip router isis
!
interface FastEthernet0/0
ip address 24.1.1.4 255.255.255.0
ip router isis
duplex auto
speed auto
mpls ip
!
interface FastEthernet0/1
ip address 45.1.1.4 255.255.255.0
ip router isis
duplex auto
speed auto
mpls ip
!
```

```
interface FastEthernet1/0
ip address 49.1.1.4 255.255.255.0
ip router isis
duplex auto
speed auto
mpls ip
!
interface FastEthernet2/0
ip vrf forwarding site2
ip address 34.1.1.4 255.255.255.0
ip router isis
ip ospf 2 area 0
duplex auto
speed auto
mpls ip
!
router ospf 2 vrf site2
log-adjacency-changes
redistribute bgp 65000 subnets
!
router isis
fast-reroute remote-lfa level-2 mpls-ldp
net 49.0001.4444.4444.4444.00
is-type level-2-only
!
router bgp 65000
no synchronization
bgp log-neighbor-changes
neighbor 6.6.6.6 remote-as 65000
neighbor 6.6.6.6 update-source Loopback1
no auto-summary
!
address-family vpnv4
 neighbor 6.6.6.6 activate
 neighbor 6.6.6.6 send-community both
exit-address-family
!
address-family ipv4 vrf site2
 no synchronization
exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
!
```

```
mpls ldp router-id Loopback1
!
!
control-plane
!
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
end
```

R5

```
!

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R5
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
ip vrf site1
rd 65000:1
route-target export 65000:1
route-target import 65000:1
!
```

```
no ip domain lookup
!
mpls label protocol ldp
multilink bundle-name authenticated
!
!
!
archive
log config
 hidekeys
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface Loopback1
ip address 5.5.5.5 255.255.255.255
ip router isis
!
interface FastEthernet0/0
ip vrf forwarding site1
ip address 57.1.1.5 255.255.255.0
ip ospf 1 area 0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 56.1.1.5 255.255.255.0
ip router isis
duplex auto
speed auto
mpls ip
!
interface FastEthernet1/0
ip address 59.1.1.5 255.255.255.0
ip router isis
duplex auto
speed auto
mpls ip
!
interface FastEthernet2/0
ip address 45.1.1.5 255.255.255.0
ip router isis
duplex auto
speed auto
mpls ip
!
```

```
router ospf 1 vrf site1
log-adjacency-changes
redistribute bgp 65000 subnets
!
router isis
fast-reroute remote-lfa level-2 mpls-ldp
net 49.0001.5555.5555.5555.00
is-type level-2-only
!
router bgp 65000
no synchronization
bgp log-neighbor-changes
neighbor 2.2.2.2 remote-as 65000
neighbor 2.2.2.2 update-source Loopback1
no auto-summary
!
address-family vpnv4
 neighbor 2.2.2.2 activate
 neighbor 2.2.2.2 send-community extended
exit-address-family
!
address-family ipv4 vrf site1
 redistribute ospf 1 vrf site1
 no synchronization
exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
!
mpls ldp router-id Loopback1 force
!
!
control-plane
!
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
```

```
line vty 0 4
login
!
!
end
```

R6

```
!

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R6
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
ip vrf site2
rd 65000:2
route-target export 65000:2
route-target import 65000:2
!
no ip domain lookup
!
mpls label protocol ldp
multilink bundle-name authenticated
!
!
archive
log config
 hidekeys
!
!
!
!
ip tcp synwait-time 5
!
```

```
!
!
!
interface Loopback1
ip address 6.6.6.6 255.255.255.255
ip router isis
!
interface FastEthernet0/0
ip address 56.1.1.6 255.255.255.0
ip router isis
duplex auto
speed auto
mpls ip
!
interface FastEthernet0/1
ip address 69.1.1.6 255.255.255.0
ip router isis
speed 100
full-duplex
mpls ip
!
interface FastEthernet1/0
ip address 26.1.1.6 255.255.255.0
ip router isis
duplex auto
speed auto
mpls ip
!
interface FastEthernet2/0
ip vrf forwarding site2
ip address 68.1.1.6 255.255.255.0
ip ospf 2 area 0
duplex auto
speed auto
!
router ospf 2 vrf site2
log-adjacency-changes
redistribute bgp 65000 subnets
!
router isis
fast-reroute remote-lfa level-2 mpls-ldp
net 49.0001.6666.6666.6666.00
is-type level-2-only
!
router bgp 65000
no synchronization
bgp log-neighbor-changes
neighbor 4.4.4.4 remote-as 65000
neighbor 4.4.4.4 update-source Loopback1
no auto-summary
!
```

```
address-family vpnv4
 neighbor 4.4.4.4 activate
 neighbor 4.4.4.4 send-community both
exit-address-family
!
address-family ipv4 vrf site2
 redistribute ospf 2 vrf site2
 no synchronization
exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
mpls ldp router-id Loopback1 force
!
!
control-plane
!
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
end
```

R7

```
!

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R7
!
boot-start-marker
```

```
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
!
multilink bundle-name authenticated
!
archive
log config
 hidekeys
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface Loopback1
ip address 7.7.7.7 255.255.255.255
!
interface FastEthernet0/0
ip address 57.1.1.7 255.255.255.0
duplex auto
speed auto
!
!
router ospf 2
log-adjacency-changes
network 7.7.7.7 0.0.0.0 area 0
network 57.1.1.7 0.0.0.0 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
control-plane
!
!
```

```
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
end
```

R8

```
!

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R8
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
!
multilink bundle-name authenticated
!
!
!
!
archive
log config
 hidekeys
!
```

```
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface Loopback1
ip address 8.8.8.8 255.255.255.255
!
interface FastEthernet0/0
ip address 68.1.1.8 255.255.255.0
speed 100
full-duplex
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
router ospf 2
log-adjacency-changes
network 8.8.8.8 0.0.0.0 area 0
network 68.1.1.8 0.0.0.0 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
```

```
!
end
```

R9

```
!

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R9
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
!
mpls label protocol ldp
multilink bundle-name authenticated
!
!
!
!
archive
log config
 hidekeys
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface Loopback1
ip address 9.9.9.9 255.255.255.255
ip router isis
```

```
!
interface FastEthernet0/0
ip address 49.1.1.9 255.255.255.0
ip router isis
duplex auto
speed auto
mpls ip
!
interface FastEthernet0/1
ip address 59.1.1.9 255.255.255.0
ip router isis
duplex auto
speed auto
mpls ip
!
interface FastEthernet1/0
ip address 69.1.1.9 255.255.255.0
ip router isis
duplex auto
speed auto
mpls ip
!
interface FastEthernet2/0
ip address 29.1.1.9 255.255.255.0
ip router isis
shutdown
duplex auto
speed auto
mpls ip
!
router isis
fast-reroute remote-lfa level-2 mpls-ldp
net 49.0001.9999.9999.9999.00
is-type level-2-only
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
!
line con 0
exec-timeout 0 0
privilege level 15
```

```
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
end
```

```
R1#ping 7.7.7.7 source 1.1.1.1 repeat 300

Type escape sequence to abort.
Sending 300, 100-byte ICMP Echos to 7.7.7.7, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 99 percent (299/300), round-trip min/avg/max = 55/92/395 ms
R1#
```

Here also the link between the router R2 and the router R9 was shut down during the ping between R1 to R7 but in this case loop free alternative was used and as seen from the result there was a loss of just two pings as compared to the loss of four ping in the earlier case and then the network converged again.

This proves the benefit of using free loop alternative as the speed by which network has converged has improved as compared with the network which was not using the loop free alternative.

SECTION C

CONCLUSION

USE AND NEED OF MULTIPROTOCOL LABEL SWITCHING

I am going to discuss the need why do we need multiprotocol label switching in the network and where is the multiprotocol label switchng used. Let me answer the first question i.e. why do we need multiprotocol label switching and the answer is that before the beginning of multiprotocol label switching, ATM and fame relay were the two important protocols for wide area network but there were many problems with the integration of protocols like IP over frame relay and ATM due to which multiprotcol label switching was introduced.Multiprotcol label switching can be used for carrying various topologies like IPv4, IPv6 as well as layer 2 protocols and that too just by adding label to the packets.Therfore, in order to switch multiple protocols very easily multiprotocol label switching was introduced. The other benefits of using multiprotocol label switching is that it provides featurelike traffic engineering which can be used for controlling the traafic according to the needs of the customer.The second question is where can the multiprotocol label switching can be used. The multiprotocol label switching is mostly used by the large enterprises as well as the service providers as they can have more control over the traffic and also have control over the services to be delivered to the customers. Another advantage of using multiprotocol label switching is that it can be used for carrying both data as well as voice and therefore is a scalable wide area network.The use of multiprotocol label switching has resulted in good revenue to the service provider.

USE AND NEED OF LABEL DISTRIBUTION PROTOCOL

I am going to discuss why is label distribution protocol used and where do we need the label distribution protocol. The answer for the first question i.e. why label distribution protocol is used as we know label distribtion protocol is a signalling protocol and it is used for the distribution as well as exchange of the label mappings. So in the lab it was used to exchange labels between the label switch routers as the packets are forwarded by using the label switching therefore label distribution protocol is needed for that as no another signaling protocol provides the functionality which label distribution protocol can provde. Now, the second question i.e where the label distribution protocol is used. Label distribution protocol will be used to provide support to the label switch router and label switch router is a router that provides support to the multiprotocol label switching.So wherever label switch router is being used label distribution protocol will be used for switching and distributing the labels within the label switch routers present in the multiprotocol label switcing network.There are other signalling protocols also like the resorce reservation protocol. However it is used

to provide support to the traffic engineering. So , basically it depends upon the needs of the customer and the topology.

USE AND NEED OF INTERMEDIATE SYSTEM TO INTERMIEDIATE SYSTEM

Intermediate system to intermediate system is an interior gateway routing protocol which uses the link state routing protocol regarding the decisions for the routing ans uses the Dijkstra's algorithm to find the shortest path in the network which is same as open shortest path first. Label distribution supports both the intermediate system to indermediate system and open shortest path first as interior gateway protocols to be used in multiprotocol label switching network. The use of interior gateway protocol in the label distribution protocol is that the label switched path through the multiprotocol switching network can be established only by using the interior gateway routing protocols such as intermediate system to indermediate system and open shortest path first along with the label distribution protocol. Therefore, label distibution protocol depends upon the interior gateway protocol for the ip forwarding and for setting up the shortest path through the network. Therefore interior gateway protocols play a very important role because if the label distribution protocols and interior gateway protocols are not synchronized it can result in the loss of packets.

The second question is why Intermediate system to intermediate system is preferred over open shortest path first as interior gateway protocol by service providers in the large networks. The reason for this is the convergence time in Intermediate system to intermediate system is less as compared to open shortest path first as the shortest path for the routes will not be calculated in Intermediate system to intermediate system until the link there is an impact on the route if there is a change in the link and also unlike open shortest path first there is no need to run Dijkstra's algorithm on all the network destination in case a new link state advertisement is received but only the link state database will be scanned and those routes will be picked which are present in the database. Another advantage of using Intermediate system to intermediate system is that it routes intermediate systems instead of networks which doesnot affect it performance in case there are large number of networks. Therefore, it uses less resources and memory as comapred to opem shortest path first.

USE AND NEED OF FREE LOOP ALTERNATIVE

The use of free loop alternative is to provide a way by which the packet loss can be reduced in an enviorment that supports multiprotocol label switching networks if there is a single failuer in the link or the node. By using the loop free alternative a 10 seconds of milli seconds convergence time can be achieved automatically by using a alternative path which has to be loop free and it can also work with interior gateway protcols like Intermediate system to intermediate system and open shortest path first. The requirement for using loop free alternative is that to forward traffic it must not use any failed elemrnt or protecting node and no loops must be formed while using loop free alternative. The advantage of using loop free alternative is that it can be used on any interface if and only if that interface is behaving as the primary path.

SECTION D

BIBLIOGRAPHY

http://www.cisco.com/c/en/us/products/ios-nx-os-software/multiprotocol-label-switching-mpls/index.html

http://www.dummies.com/how-to/content/types-of-label-switching-routers.html

http://www.cisco.com/c/en/us/td/docs/ios/12_4t/12_4t2/ftldp41.html

https://en.wikipedia.org/wiki/Label_Distribution_Protocol

http://ipcisco.com/mpls-label-distribution-protocol-ldp-part-1/

https://en.wikipedia.org/wiki/Constraint-based_Routing_Label_Distribution_Protocol

http://networkshorizon.blogspot.ca/2012/01/constraint-based-routing-ldp-cr-ldp.html

http://www.juniper.net/documentation/en_US/junos13.2/topics/concept/mpls-notification-messages.html

http://tools.ietf.org/html/rfc5036#section-3.5.1

http://www.juniper.net/techpubs/en_US/junos14.1/topics/concept/mpls-notification-messages.html

http://routingnull0.com/2015/11/15/mpls-l3vpns-part-1/

http://blog.hoff.geek.nz/2013/11/08/ldp-over-rsvp/

http://tools.ietf.org/html/rfc3031

http://routingnull0.com/2015/11/15/mpls-l3vpns-part-1/

http://tools.ietf.org/html/rfc5036#section

http://blog.hoff.geek.nz/2013/11/08/ldp-over-rsvp/

http://www.exzaktec.com/2009/10/ldp-rsvp-te-both/

http://searchnetworking.techtarget.com/definition/GMPLS

https://tools.ietf.org/html/rfc6388

https://tools.ietf.org/html/draft-ietf-mpls-lmp-02

http://www.rfc-editor.org/rfc/rfc4209.txt

http://www.cisco.com/c/en/us/td/docs/ios/iproute_isis/configuration/guide/15_1s/irs_15_1s_book/irs_ipv4_lfafrr.pdf

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_isis/configuration/15-sy/irs-15-sy-book/irs-ipv4-lfafrr.html

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_pi/configuration/xe-3s/iri-xe-3s-book/iri-ip-lfa-frr.html

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_isis/configuration/15-s/irs-15-s-book/irs-rmte-lfa-frr.html#GUID-85C9A452-689E-414E-855F-C3DA6C33C6B0

http://etherealmind.com/loop-free-alternate-routes/

http://www.juniper.net/documentation/en_US/junos12.3/topics/topic-map/isis-ldp-synchronization.html

https://learningnetwork.cisco.com/thread/57624

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_isis/configuration/15-s/irs-15-s-book/irs-rmte-lfa-frr.html

http://www.juniper.net/documentation/en_US/junos15.1/topics/concept/isis-node-link-protection-understanding.html

http://www.juniper.net/documentation/en_US/junos15.1/topics/concept/is-is-remote-lfa-for-ldp-tunnels-overview.html