POSSIBILITIES OF THE RESOURCE RESERVATION PROTOCOL FOR INCREASING THE CAPACITY AND RELIABILITY OF TRAFFIC TRANSMISSION BETWEEN SWITCHING SYSTEMS

DOI: 10.36724/2072-8735-2023-17-2-49-55

Irina V. Stepanova,
Moscow Technical University of Communications and Informatics, Moscow, Russia, **w515iv@mail.ru**

Knaj Nouma,
Moscow Technical University of Communications and Informatics, Moscow, Russia,
Romyana27g@gmail.com

Manuscript received 15 January 2023;
Accepted 20 February 2023

Keywords: *Multi Protocol label Switching MPLS, QoS based on MPLS, Label Edge Routers, Resource Reservation Protocol, MPLS Traffic Engineering, switching systems, tunnel protection mechanisms*

As a research task, the authors define the features of the use of the resource reservation protocol (RSVP) in modern networks of MPLS (Multi protocol label switching) technology, which provides an increase in the throughput of delay-sensitive voice and video traffic. The RSVP protocol allows you to transfer requirements for the level of Quality of Service (QoS) with reference to data flows. Internet and service providers are facing a new challenge with some real-time or mission-critical applications because these applications have different requirements in latency, bandwidth, jitter and packet loss. On the Internet, we have a so-called self-similar traffic flow, so there is a huge need for traffic management to run real-time applications efficiently. In traditional IP networks, some channels are congested and others remain underutilized due to the destination-based forwarding paradigm. The article discusses the characteristics of the RSVP protocol. The use of RSVP of three reservation styles is considered, as well as an extension of RSVP that supports better QoS, the establishment of explicit routable paths (LSP) with or without reservation, the possibility of LSP redirection. The benefits of segment routing (SR) are discussed in giving the network operator more control over the network, simplifying the network, and supporting class of service. It also discusses the protection mechanisms for MPLS-TE tunnels to provide failover.

Information about authors:

Irina V. Stepanova, *Associate Professor, Lecturer of the Department of Communication Network and Switching Systems, Ph.D. MTUCI, Moscow, Russia,*

Knaj Nouma, *Student MTUCI, Damascus, Syrian Arab Republic*

Для цитирования:
Степанова И.В., Кнаж Нума. Возможности протокола резервирования ресурсов для повышения пропускной способности и надежности передачи трафика между системами коммутации // T-Comm: Телекоммуникации и транспорт. 2023. Том 17. №2. С. 49-55.

For citation:
Stepanova I.V., Knaj Nouma (2023) Possibilities of the resource reservation protocol for increasing the capacity and reliability of traffic transmission between switching systems. *T-Comm*, vol. 17, no.2, pp. 49-55. (*in Russian*)

Introduction

Internet and service providers are facing a new challenge with some real-time or mission-critical applications because these applications have different requirements in latency, bandwidth, jitter and packet loss. On the Internet, we have a so-called self-similar traffic flow, so there is a huge need for traffic management to run real-time applications efficiently. In traditional IP networks, some channels are congested and others remain underutilized due to the destination-based forwarding paradigm.

IP (Internet Protocol) was not designed to support QoS, rather it was designed for education and research, but the network must carry a large amount of traffic and still has limited resources, so it is important to allocate and optimize the available resources. Allocating or scheduling network resources based on required QoS to optimize the use of our network resources called as traffic management.

MPLS provides a solution by providing a connection-oriented fabric on top of an existing IP-based network to maintain the required QoS for these applications. Traffic engineering in MPLS considers resource usage, which makes it more efficient to design routes based on separate flows or different flows between the same endpoints.

MPLS TE shifts traffic from overused to idle or underused links, avoiding congestion, packet loss, ensuring data delivery, optimizing resource usage, so no more links, no more capital expenditures with the ability to provide new services that generate higher revenue.

The use of MPLS technology supports faster routing at the backbone level, which will lead to a significant increase in the performance of the entire network, such as expanding the range of applications and services provided, increasing the income of network operators. Thus, the efficient use of network resources provides a better user experience.

1. Ch acteristics of the Resource Reservation Protocol

RSVP is a signaling control protocol that is used to convey QoS requirements for a specific data stream or streams. It is not a routing protocol but works with other routing protocols such as IP. Therefore, the implementation of RSVP in an existing network does not result in a transition to a new routing protocol. A host can use the RSVP protocol to request specific requirements for a particular application, data stream, or streams (Fig. 1).

The router uses RSVP to establish and then maintain the state of all nodes along the path of a particular flow in order to provide the requested resources. When working with the IP protocol, RSVP processes the data stream, rather than each packet individually, to ensure that resources are reserved for that stream along its route.

RSVP was developed by the IETF and can be used for label distribution and end-to-end QoS. An enhanced version of RSVP (RSVP-TE Traffic Engineering) is suitable for extending an MPLS network with end-to-end resource reservation with support for automatic signaling and LSP configuration with traffic engineering. RSVP has the ability to control the flow of data. A sequence of data from a single source, identified by a destination address, a destination port, and a protocol identifier, is called a data stream. A data stream consists of sessions that represent certain individual QoS requirements.

RSVP parses the available routing table at each node in a given data stream to begin session establishment, and then sends (the sending application) "path messages" to the destination (destination) IP address. The receiver, after receiving the path message, sends a "Reserve-Request Message" to reserve the necessary path and resources, the request must be transmitted via RSVP, since it can go through all nodes on the route. The sending application receives a "reservation request message" that lets it know all the reserved resources it needs. Thus, having reserved resources, you can start sending application data packets.

In an end-to-end guarantee, the application must meet the minimum latency and/or minimum bandwidth requirement. It is the responsibility of the packet scheduler to allocate the resources needed to carry the data link layer data flow issued by each interface. At each node, a decision is made locally in a mechanism called access control to decide whether the QoS requirement can be met at that node or not.

For the admission control mechanism, an upstream reservation request message is sent by RSVP at each node. Thus, upon receipt of an admission control request, other parameters (packet classifier and packet scheduler) are set by RSVP to achieve QoS. Otherwise, if the mechanism requesting admission control fails, an error message will be sent.

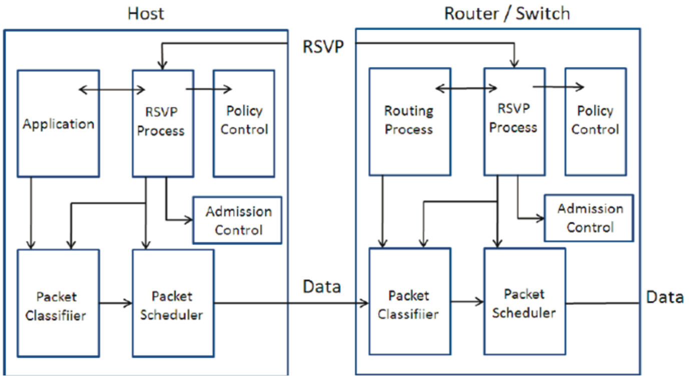


Fig. 1. RSVP in HOST and ROUTER

2.1. Analysis of the features of the RSVP Messages protocol

RSVP uses the following message types to establish a data flow or remove information associated with a reserved resource and report an error.

1-Path Messages: The sender host sends a path message periodically to update the state of the path along downstream routes (unicast and multicast). Path messages must follow the same data flow application path so that the router knows exactly the state of that path, the previous and next hops in that session.

All of this information provides an overview of the specified end-to-end path to be used when sending the upstream reservation request message.

2-Resv message: after receiving the path message, the recipient sends messages about the reservation of the necessary resources.

3-Path break message: Path break messages help maintain network performance by freeing up resources.

4-Resv break message: opposite of resource request message used to release all resources allocated by the receiver.

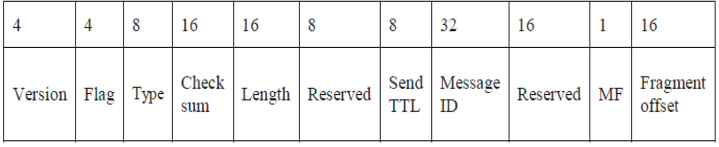
5-Error Messages: Two types of error messages.

Path error message: Messages about a problem with path parameters.

Resv error message: There is a problem with the required resources, this message is sent from the receiver to all receivers that should be on the data flow path.

6-Resv message acknowledgment: Can be sent by the recipient to confirm whether a reservation has already been made or not.

An RSVP message consists of a common header (32-bit words) and the following fields (Fig. 2).



4	4	8	16	16	8	8	32	16	1	16
Version	Flag	Type	Check sum	Length	Reserved	Send TTL	Message ID	Reserved	MF	Fragment offset

Fig. 2. RSVP message format

– Vers on: 4-bit field, the version number of the protocol;

– F ags: 4-bit field (not yet defined);

– essage type: 8 bits (can have six possible values);

– Checksum: 16 bits, to indicate the standard TCP/IP checksum for RSVP;

– Length: 16 bits, representing the size of the packet in bytes;

– Send TTL: 8 bits, the lifetime value of the message;

– Message ID: 32 bits, provides a label that is shared by all fragments of a single message from a given RSVP hop;

– Extra fragment (MF): 1 bit, reserved for the message;

– ragment Offset: 24 bits represent the offset bytes for the message.

2.2. RSVP object field structure

Important information representing the content of RSVP messages can be carried by RSVP objects. This information is important in traffic engineering because it can be used for LSP signaling (Fig. 3).

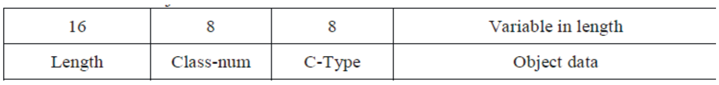
An object consists of a fixed-length header and a variable-length data field with a maximum length of 65,528 bytes.

– Length: 16 bits defines the total length of the object (must be a multiple of 4).

– lass-num: 8 bits define the class of the object, e.g., session.

– C-type: The 8-bit field represents the unique object type for each class-num. It can correspond to different types of Internet address families, such as IPV4 and IPV6.

– bject data: contains the id data of the class-num and c-type fields. Both can be used to define a unique object.



16	8	8	Variable in length
Length	Class-num	C-Type	Object data

Fig. 3. RSVP Object Field Structure

2.3. Soft state RSVP

In the soft state of RSVP, each router updates RSVP messages that change dynamic routing and group membership. A periodic stream of path messages and soft-state reservation update messages helps to avoid timeouts.

If there are no update messages before the timeout expires, the soft reservation state will be deleted. Path break messages and Resv break messages can also remove the soft state reservation.

The router's state will change if new path messages are received. This end-to-end change is propagated by RSVP and to report the new path, a reservation request message will be sent to reserve resources on the new path**.**

2.4. RSVP reservation style capabilities

RSVP reservation styles can be defined by the option included in the reservation request messages. In its turn reservation style define how to select sender by the receiver of Path message and how to treat reservation from different sender within the same session.

There are two reservation styles: – Distinct reservation.
– hared reservation.

1-Distinct reservation: Each uplink router performs a distinct reservation on an individual basis.

2-Shared reservation: a common reservation is shared among multiple senders.

Also in order to select the sender there are two ways:

1. Explicit sender – a list of prospective senders will be created;

2. Wildcard sender – the entire sender will be selected which can then participate.

In RSVP there are three styles of reservations defined by the combination described above.

1-Fixed filter (FF): in Fixed Filter a separate reservation is allocated to only one sender and cannot be used by other senders. The reservation will be treated as a total reservation or the sum of all resources required by the sender. A fixed filter is used by unicast applications such as video applications.

2-Wildcard filter (WF): we can use one total reservation for all wildcard senders, regardless of their number. A single reservation can be sufficient for all senders, because at any given time only a few senders can transmit, so there is no need to split the reservations.

3-Shared Explicit (SE): between explicit senders, the recipient can set a common explicit reservation. Thus, a certain amount of bandwidth is set for a group of users.

2.5. Explicit Routing Implementation Options (RSVP extension)

RSVP extension support explicit routing, which based the requirement of QoS and Class of service. RSVP extension can install explicit routed LSP with or without reservation, rerouting LSPs and loop detection. To support better QoS, RSVP extension creates LSP tunnel to implement QoS along the tunnel and in the case of node failure or congestion in an LSP path, then the tunnel can be routed manually or automatically which ensure the reliability of delivery.

RSVP can associate RSVP flow with labels by employing downstream label assignment on router and host to support MPLS and RSVP. The most important feature of RSVP extension is explicit routing support, in explicit routing a path through IP network can be defined and controlled from source to destination to minimize the end-to-end delay, maximize throughput of network and enhance traffic performance characteristic, which is helpful when talking about traffic oriented application.

In Path messages, EXPLICIT_ROUTE is incorporating to carry a sequence of nodes which compose the route a packet will follow in a network. Depending on network state and QoS requirement, the network administrator specifies these paths which play an important role in traffic engineering.

2.6. Organizing LSP Tunnels

In an MPLS domain, an upstream router sends a request for label reassignment from the downstream router in an RSVP path message (the RSVP object field here is LABEL_REQUEST) to a specific IP address, depending on the available routing information on each router. Once the RSVP path message is received at a particular destination IP address, a Reservation-request message is sent in the upstream direction to reserve the path and resources required for data transmission, and it passes through all nodes (Fig. 4).

To provide label reassignment information for this session, LABEL_REQUEST queries the intermediate LSR. Receipt of the reservation-request message by the sending application, gives it an overview of all the reserved resources, then by simply reserving the resources, the sending application can start sending data packets. In case of failure in providing the label reattachment process at any node on the path, the unknown object class is sent in Path error messages to the sender of the path message. The error message is sent thanks to the QoS traffic management that is implemented for a particular data stream.

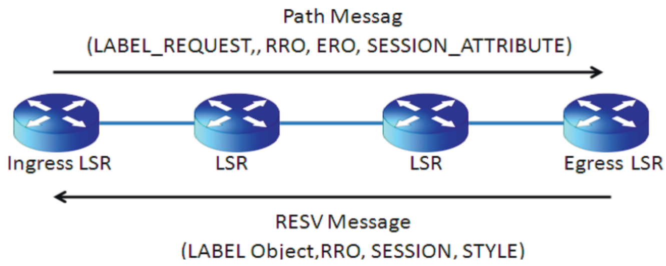

Path Messag
(LABEL_REQUEST,, RRO, ERO, SESSION_ATTRIBUTE)
Ingress LSR
LSR
LSR
Egress LSR
RESV Message
(LABEL Object,RRO, SESSION, STYLE)

Fig. 4. Resource Reservation in RSVP

2.7. Using Constraint Based Routing (CBR)

Constraint based routing is an important QoS (Quality of Service) routing method for defining an explicit path in an MPLS domain. With CBR, parameters such as delay, bandwidth, number of hops and QoS are satisfied, allowing to optimize network performance, avoid congestion, load and obtain optimum data delivery (Fig. 5).

Link state routing protocols such as OSPF do not propagate label attachment information unlike distance vector routing protocols such as RIP and IGRP, which are suitable for passing label attachment information because they pass their information to routers that are not directly connected.

MPLS explicit routes are predefined routes through the MPLS domain instead of the selected routes on each router in the routing hop-by-hop. These explicit routes in the router using OSPF and BGP routing protocols. Tags carry information on which explicit route (or LSP) the tagged packet should follow.

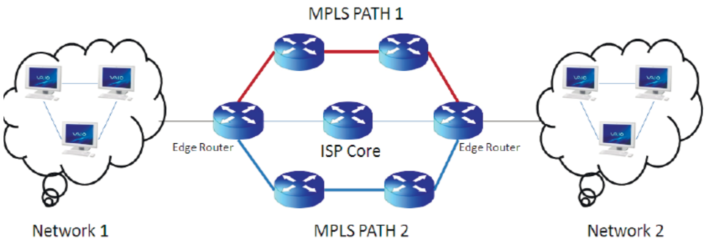


Fig. 5. TE in an MPLS network using explicit routing

MPLS has the flexibility to support CBR, defining explicit routes based on available bandwidth, packet priority, policy-based server directives, or operator whims.

CD-LDP (Constraint based routing LDP), a derivative of LDP, is used to configure explicit routing LSPs by network managers to manage sensitive traffic. After path definition, signaling protocols (LDP, RSVP) are used to establish (ER-LSPs) Explicitly Routed label Switched Pathes in the MPLS domain from incoming to outgoing node (underutilized links will be used as ER-LSPs), and RSVP-TE is also used to handle MPLS TE requirements.

3. MPLS Traffic Engineering

The traditional IP-based network forwarding method has disadvantages of choosing the least-cost paths due to Interior Gateway Protocols IGPs, many routers in our network will prefer this least-cost path causing over-utilization, congestion and packet drops in this path.

Using traffic engineering allows to distribute the load through underutilized and idle path, but this require the full overview of the network topology and resources availability to establish paths which provide the QoS characteristics or TE tunnels (Fig. 6).

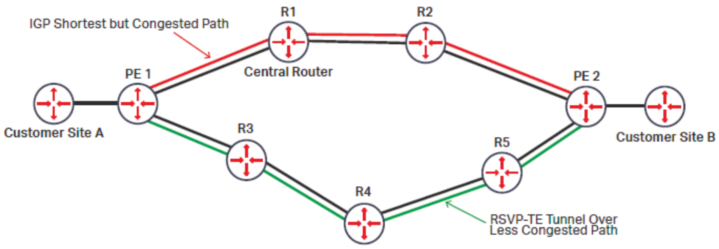

IGP Shortest but Congested Path
R1
R2
Central Router
PE 1
PE 2
Customer Site A
Customer Site B
R3
R5
R4
RSVP-TE Tunnel Over Less Congested Path

Fig. 6. Using traffic engineering in MPLS

In MPLS network, collected overview information using Open Shortest Path First (OSPF) and other IGPs protocol like Intermediate System to Intermediate System (IS-IS) help the ingress routers to establish various, distinct paths between two edge routers in MPLS domain, which can be used by TE tunnels to forward packets based on the labels this is called MPLS Traffic Engineering.

MPLS TE drives traffic from over utilized to idle or underutilized links avoiding congestion, packet drop, ensuring data delivery, optimization resources utilization, so no more links no more CAPEX with the ability to provide new services which bring a higher revenue.

4. Traffic Engineering Mechanisms

There are two mechanisms:

1-Resource Reservation Protocol _ Traffic Engineering (RSVP-TE).

2-Segment Routing (SR).

here two needed definitions to simplify the process:

Headend Router –The upstream, transmit end of a tunnel – the router originates and maintains the traffic engineering LSP.

Router – The downstream, receive end of a tunnel – the router terminates the traffic engineering LSP originating from the Headend router.

4.1. Resource Reservation Protocol traffic Engineering (RSVP-TE):

In order to reserve resources along the path from sender to receiver in IP network we use RSVP protocol. To reserve path via RSVP-TE, the Headend router checks the availability of needed resources along the path in an MPLS domain, sending RSVP PATH message.

Receiving request by Tailend router and in the case of resources availability Then RSVP RESERVATION message is sent by Tailend router to confirm the reservation, then an LSP is assigned to a TE tunnel. So the Headend router can then start traffic transmitting through tunnel based on the resource requirements (Fig. 7).

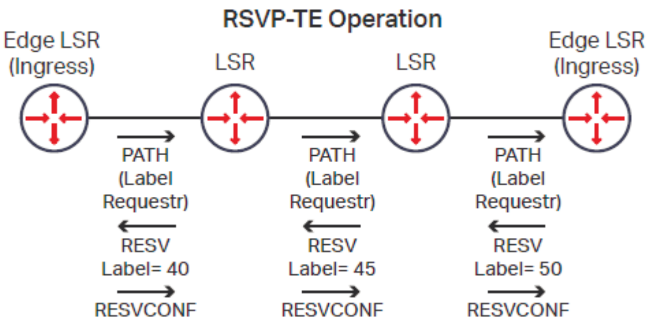


Fig. 7. RSVP-TE Functionality

4.2. Segment Routing (SR):

In SR technology with packet forwarding the path of traffic is determined by the source, does not depend on hop-by-hop signaling and is formed from a set of segments (Fig. 8).

Here, the labels are called segments, with two types of segments:

– n de segment;

– djacency segment.

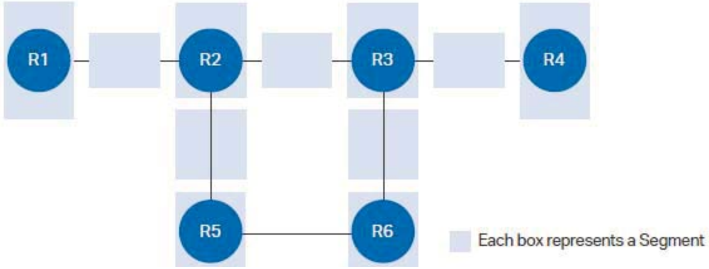


Fig. 8. Segmental routing domain represented in segments

The node segment must advertise throughout the network as it represents the shortest path to destination. Adjacency segment is a link between two adjacent nodes. Within SR domain, a local segment identifier (SID) is assigned for each node by network operators (Fig. 9).

To create a tunnel in SR domain a single segment or a set of segment can be used to reach the destination. In the SR domain below the path from source A to destination Z contains: node segment (from A to C), CO link as an adjacent segment (from C to O), node segment (from O to Z).

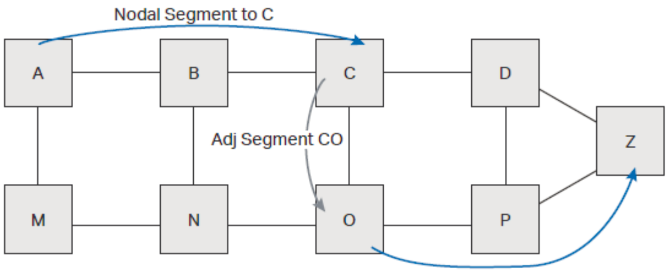


Fig. 9. Source routing using segments

When the network operator uses SR, it have more control on the network as SR support Class of Service TE (CoS). For example the operator can direct traffic over any path based on the state of network and still taking into account the requirements of traffic, like sending data over a normal or high latency path and voice data or video conferencing data over a low latency path. SR allow to simplify the network because SR does not need signaling or labels distribution protocols, SR works with fewer labels and fewer overhead at each node of the network.

SR overcomes the disadvantages of RSVP-TE so the network has more scalability and faster convergence time to sub 50 milliseconds by enabling Fast-Re-Route (FRR) technology in any topology.

5. MPLS-TE tunnel protection mechanisms

To provide a recovery from failure MPLS-TE provide two mechanisms:

1-End-to-End protection (using a secondary path).

2-Local protection (using MPLS FRR).

5.1. End-to-End Protection:

From its name the recovery is for the entire LSP, here we have two LSP, primary LSP to carry traffic and secondary as a backup when the primary fails, the two are different in order to avoid the single point of failure (Fig. 10).

When primary LSP failed, failure detection mechanisms inform the Headend router taking advantages of RSVP signaling and IGP protocols, so the Headend router switches sending to secondary, as still the primary failed, but once the primary recovered the traffic will be switched back to it.

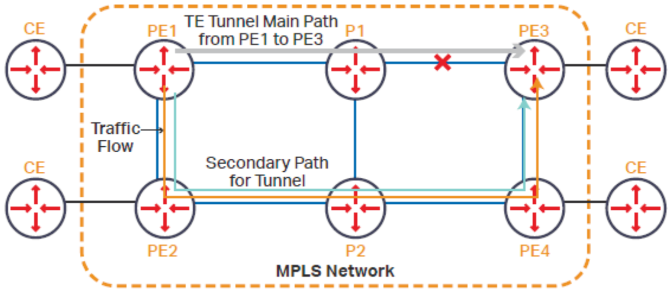

CE
PE1
TE Tunnel Main Path from PE1 to PE3
P1
PE3
CE
Traffic Flow
Secondary Path for Tunnel
CE
CE
PE2
P2
PE4
MPLS Network

Fig. 10. End to end protection with a secondary path

End-to-End protection use three methods:

1 – Full strict hop LSP paths.

2 – Shared Risk Link Group (SRLG).

3 – Admin Group.

Full strict hop LSP ensure the difference between Primary and secondary LSP, overlap between them is not allowed along the path from source to destination so the failure of one path does not affect the other. In large network this configuration adds more complexity to network (Fig. 11).

Shared Risk Link Group (SRLG) uses a set of links within a common fiber, so if the any links in this group failed the other links may fail too as they share the same risk.

In MPLS, the recovery mechanism ensures to choose the primary and secondary LSP from different SRLG.

Admin Group similarly to SRLG where the primary and secondary LSPs do not use links from same Admin group.

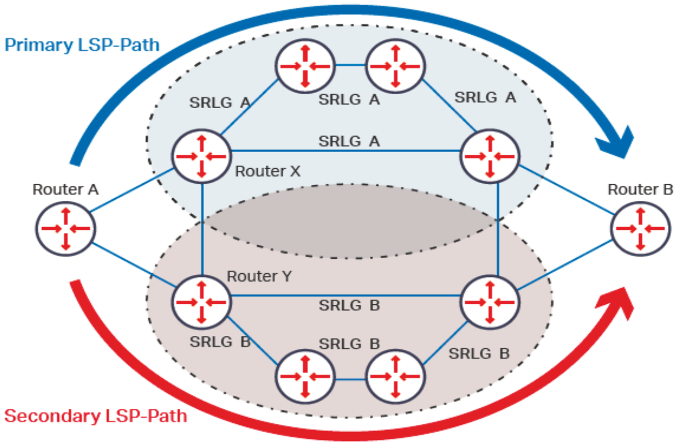


Fig. 11. End to End protection (Path Diversity) in SRLG

5.2. Local protection (MPLS Fast Reroute):

MPLS FRR contains two protection methods – link protection and node protection (Fig. 12).

End to End protection mechanism has a fast recovery method as a secondary LSP is pre-established. However, MPLS Fast Reroute is a recovery mechanism from either node or link failure of MPLS TE tunnels.

FRR mechanism bypasses the node or link failure while Headend routers establish a new LSP (end to end). FRR is a fast local protection as the action takes place close to the point of failure and the recovery in less than 50 milliseconds with a minimal packet loss with no need to the overhead of creating end to end backup LSP. two basic terms in MPLS FRR:

Point of Local Repair (PLR): point is a router located at the beginning of new backup LSP, which will be created after the downstream node/link failure. This router will have a new task of notifying the Headend router abut error and failure of primary LSP.

Merge Point (MG): is a router located at the end of the new backup path, merging it into the original LSP.

Link Protection: In a link protection mechanism, only the failed link along the LSP will be bypassed.

The new backup tunnel will be known as Next-Hop backup tunnel (NHOP) because the backup tunnel will end at the next hop after the point of failure.

There are two task for PLR when a link fails, first is to swap the labels, push the new backup label, and reroute the traffic along the backup path to the MP, where the traffic.

Second is to notify the Headend router in the case of any failure in LSP.

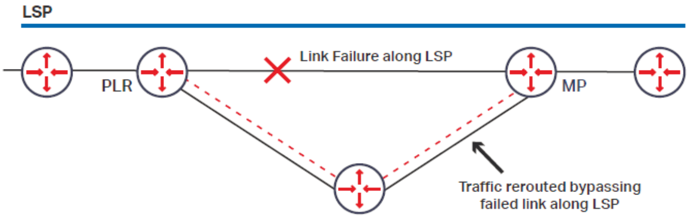


Fig. 12. MPLS protection-link FRR

In a node protection mechanism, only the failed downstream router will be bypassed so the backup LSP ends two hops away from the PLR so it is called next-next-hop (NNHOP) backup tunnels. here we notice that node protection mechanism provide protection against node and link failure (Fig. 13).

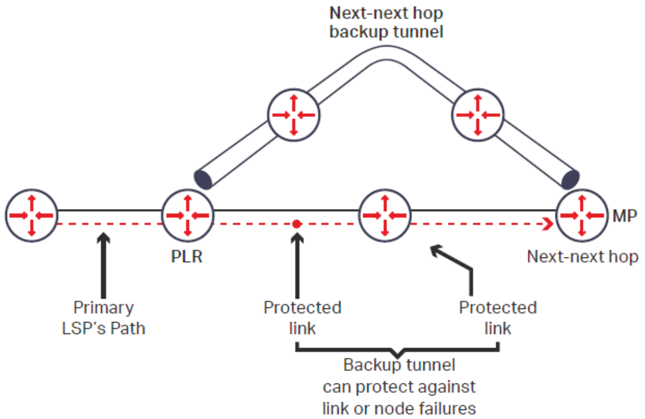


Fig. 13. MPLS Protection-Node FRR

However in link or node protection, many other additional option can be used to ensure flexibility and reliability of MPLS-TE tunnels so the delivery of data is not affected by downtime: detour and facility backup (1:N):

– de our or one-to-one protection: a separate backup path is assigned for only one LSP.

– Facility backup (1:N) or many-to-one protection: here many LSPs share the backup tunnel.

Conclusion

1) MPLS TE allows traffic to be directed from overused to idle or underused links, avoiding congestion and optimizing resource usage.

2) SVP is a signaling control protocol that signals QoS requirements for certain data flows. RSVP was developed by the IETF and can be used for end-to-end marking and QoS distribution. A host can use RSVP to query specific application requirements for specific data flows from the network, and then keep up for all hosts along a specific path.

3) he most important feature of the RSVP extension is explicit routing support. With explicit routing, a path through an IP network can be defined and controlled from source to destination to minimize end-to-end delay, increase network throughput, and improve traffic performance characteristics. This is important for voice-oriented applications.

4) The use of segment routing gives the network operator more control over the network because the SR supports the TE service class, so the operator can route traffic to any path depending on the state of the network, and still consider traffic requirements/ Such as sending data through the normal path or the path with high latency, and voice or video conferencing data along a low latency path.

5) SR allows to simplify the network because SR does not require signaling protocols or label distribution, SR works with fewer labels and less overhead at each network node. SR overcomes the shortcomings of RSVP-TE so the network has greater scalability and faster convergence time to less than 50 milliseconds by enabling Fast-Re-Route (FRR) technology in any topology.

6) To provide failover, MPLS-TE provides two mechanisms: end-to-end protection (using a secondary path) and local protection (using MPLS FRR). In End-to-End Protection: Recovery for the entire LSP, here we have two LSPs, a primary LSP to carry traffic and a secondary LSP as a backup in case the primary fails, these two are different to avoid a single point of failure.

7) The end-to-end protection mechanism has a fast recovery method because the secondary LSP is pre-installed. However, MPLS Fast Reroute is a mechanism to recover from node or link failure of MPLS TE tunnels. The FRR mechanism bypasses a node or link failure while the head-end routers establish a new LSP (end-to-end). FRR is fast local protection because action occurs close to the point of failure and recovery takes less than 50 milliseconds with minimal packet loss and no need for an end-to-end redundant LSP.

References

1. S.N. Step ov (2015) Teletraffic Theory: Concepts, Models, Applications. Moscow: Hot Line – Telecom. 868 p. (Theory and Practice of Infocommunications Series).

2. I.V. St anova, Knaj Nouma (2022) Analysis of the capabilities of MPLS technology for managing traffic in communication networks. *T-Comm*. Vol. 16, No. 5, pp. 63-68.

3. Srinivas Vegeshna (2003) Quality of service in IP networks. Fundamental principles of quality of service functions in Cisco networks: Translated from English. Moscow: Williams Publishing House. 368 p.

4. I.V. Stepa va, M.O.A. Abdulvasea (2017) Use of perspective technologies for development of the distributed corporate communication networks. *T-Comm*. Vol. 11. No. 6, pp. 10-15.

5. E.A. Kucheryaviy (2004) Traffic management and quality of service in the Internet. SPb: Nauka i tekhnika. 336 p.

6. V.Yu. Dear (2014) Multiservice communication networks. Transport networks and access networks. Moscow: Bris-M. 189 p.

7. A.P. Pshenichnikov (2019) The theory of teletraffic. Moscow: Hotline – Teleco .

8. V.O. Tikhv sky, V.A. Koval, G.S. Bochechka (2017) IoT/M2M networks: technologies, architecture and applications. Moscow: Media Publisher. 320 p.

9. M. Krayushin (2014) Quality control in IP networks. *Journal of network solutions LAN*. No. 1, pp. 1-8. Publishing House "Open Systems".

10. A.P. Pshenichniko E.K. Patenchenkova (2019). Infocommunication networks. Moscow: MTUCI.

11. V.A. Mochalov (2014) Principles of construction and operation of sensor communication networks. Moscow: MTUCI. 54 p.

12. M. Zakhvatov (2011) Guide to creating virtual private networks (VPN) based on MPLS technology – Cisco Systems.

13. I.V. Stepanova (2011) Issues of building and designing systems for wireless broadband access technologies Wi-Fi and Mesh. M.: MTUCI. 115 p.

14. I.V. Stepa a (2017) Principles of organization of communication systems with fixed and mobile access. Moscow: MTUCI. 104 p.

15. D. Adami (2009) New ns2 Module for Modeling MPLS Networks with point-to-multipoint LSP support", International Conference on IEEE Communications (ICC 2009), Dresden, Germany, June 2009, pp. 1-5.

ВОЗМОЖНОСТИ ПРОТОКОЛА РЕЗЕРВИРОВАНИЯ РЕСУРСОВ ДЛЯ ПОВЫШЕНИЯ ПРОПУСКНОЙ СПОСОБНОСТИ И НАДЕЖНОСТИ ПЕРЕДАЧИ ТРАФИКА МЕЖДУ СИСТЕМАМИ КОММУТАЦИИ

Степанова Ирина Владимировна, *Московский технический университет связи и информатики, Москва, Россия,* **w515iv@mail.ru**
Кнаж Нума, *Московский технический университет связи и информатики, Москва, Россия,* **romyana27g@gmail.com**

Аннотация

В качестве исследовательской задачи авторы определяют особенности использования протокола резервирования ресурсов Resource Reservation Protocol (RSVP) в современных сетях технологии Multi-protocol label Switching (MPLS), обеспечивающего увеличение пропускной способности чувствительного к задержкам голосового и видео трафика. Протокол RSVP позволяет транслировать требования к уровню качества обслуживания (QoS) применительно к потокам данных. В статье рассматриваются характеристики протокола RSVP. Рассматривается использование в RSVP трех вариантов резервирования, а также расширение RSVP, поддерживающее лучшее QoS, установление явных маршрутизируемых путей (LSP) с резервированием или без него, возможность перенаправления LSP. Обсуждаются преимущества сегментной маршрутизации (SR), которые дают сетевому оператору больший контроль над сетью, упрощают сеть и поддерживают класс обслуживания. Также обсуждаются механизмы защиты туннелей MPLS-TE для обеспечения аварийного переключения.

Ключевые слова: *многопротокольная коммутация по меткам MPLS, QoS на основе MPLS, пограничные маршрутизаторы, протокол резервирования ресурсов MPLS, инжиниринг трафика в MPLS, механизмы защиты туннелей.*

Литература

1. Степанов С.Н. Теория телетрафика: концепции, модели, приложения. М.: Горячая линия – Телеком, 2015. 868 с.
2. Степанова И.В., Кнаж Нума. Анализ возможностей технологии MPLS по управлению трафиком в сетях связи // T-Comm: Телекоммуникации и транспорт, 2022. Т. 16. № 5. С. 63-68.
3. Srinivas Vegeshna. Quality of service in IP networks. Fundamental principles of quality of service functions in Cisco networks. M.: Williams Publishing House, 2003. 368 c.
4. Stepanova I.V., Abdulvasea M.O.A. Use of perspective technologies for development of the distributed corporate communication networks // T-Comm, 2017. Vol. 11, No. 6. C. 10-15.
5. Кучерявый Е.А. Управление трафиком и качество обслуживания в Интернете. СПб: Наука и техника, 2004. 336 с.
6. Диар В.Ю. Мультисервисные сети связи. Транспортные сети и сети доступа. М.: Брис-М, 2014. 189 с.
7. Пшеничников А.П. Теория телетрафика. М.: Горячая линия – Телеком, 2019.
8. Тихвинский В.О., Коваль В.О., Бочечка Г.С. IoT/M2M сети: технология, архитектура и приложения. М.: Медиа Паблишер, 2017. 320 с.
9. Крабшин М. Контроль качества в IP-сетях // Журнал сетевых решений LAN, 2014. №1. С. 1-8.
10. Пшеничников А.П., Патенченкова Е.К. Инфокоммуникационные сети. М.: МТУСИ, 2019.
11. Мочалов В.А. Принципы построения и работы сетей сенсорной связи. М.: МТУСИ. 2014. 54 с.
12. Захватов М. Руководство по созданию виртуальных частных сетей (VPN) на основе технологии MPLS. Cisco Systems, 2011.
13. Степанова И.В. Вопросы построения и проектирования систем для технологий беспроводного широкополосного доступа Wi-Fi и Mesh. МТУСИ, 2011. 115 с.
14. Степанова И.В. Принципы и оорганизация систем связи с фиксированным и мобильным доступом. МТУСИ, 2017. 104 с.
15. Adami D. New ns2 Module for Modeling MPLS Networks with point-to-multipoint LSP support // International Conference on IEEE Communications (ICC 2009), Dresden, Germany, June 2009, pp. 1-5.