

*A Comparison Of MPLS Traffic Engineering  
Initiatives*



Robert Pulley  
&  
Peter Christensen

# *Need for MPLS*



- Problems in today's network
- QoS and CoS requirements
- Need for Resource Reservation
- Why not RSVP
- MPLS Goals

# *Traffic Engineering*



- Maximize Bandwidth Utilization
- Spread the network traffic across network
- Ensure available spare link capacity for re-routing traffic on failure
- Meet policy requirements imposed by the network operator

# *Outline*



- Label Distribution Protocol (LDP)
- Constraint-based Routing LDP (CR-LDP)
- Traffic Engineering with RSVP (TE – RSVP)
- Comparison of CR-LDP and TE-RSVP

# *Comparison - Hop-by-Hop vs. Explicit Routing*



- Hop by Hop
  - Each LSR chooses next hop on Shortest path basis
  - Similar to IP routing(No overhead)
  - E.g LDP
- Explicit routing
  - A single router, generally the ingress LER, specifies several or all of the LSRs in the LSP
  - Provides functionality for traffic engineering and QoS
  - E.g. CR-LDP, TE-RSVP

# *Label Distribution Protocol*



LDP uses four classes of messages

- Discovery Messages
- Session Messages
- Advertisement Messages
- Notification Messages

# *Discovery Messages*



- Used to announce and maintain the presence of an LSR in a network
- Basic Discovery- is used to discover directly connected neighbors
- Extended Discovery- is used to discover non-directly connected neighbors

## *Discovery Messages(Contd)*



- Basic: LSR multicasts HELLO message periodically to a well known port on “all routers on this subnet” multicast group
- All routers listen to this group to learn all LSRs with direct connection(Hello Adjacency)
- Extended: A targeted Hello is sent to a specific address rather than to the multicast group
- The only message that runs over UDP



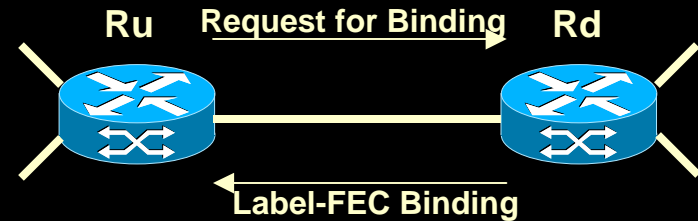
## *Session, Advertise, Notification*



- **Session:** used to establish, maintain and terminate sessions between LDP peers
- **Advertise:** create, change and delete label mappings for FECs.
- **Notification:** Used to provide advisory information and to signal error information
- All the above messages run over TCP

## *Label Distribution Methods*

- Unsolicited Downstream Label Distribution
- Downstream on Demand Label Distribution



Rd and Ru are said to have LDP adjacency

## *Label Distribution Methods(contd)*

### Unsolicited Downstream Label Distribution

- Rd discovers a 'next hop' for a particular FEC
- Rd generates a label for the FEC and communicates the binding to Ru
- Ru inserts the binding into its forwarding tables

### Downstream on Demand Label Distribution

- Ru recognizes Rd as its next-hop for an FEC
- A request is made to Rd for a binding between the FEC and a label
- If Rd recognizes the FEC and has a next hop for it, it creates a binding and replies to Ru

# *Distribution Control*



- **Independent LSP Control**

Each LSR makes independent decision on when to generate labels and communicate them to upstream peers

- **Ordered LSP Control**

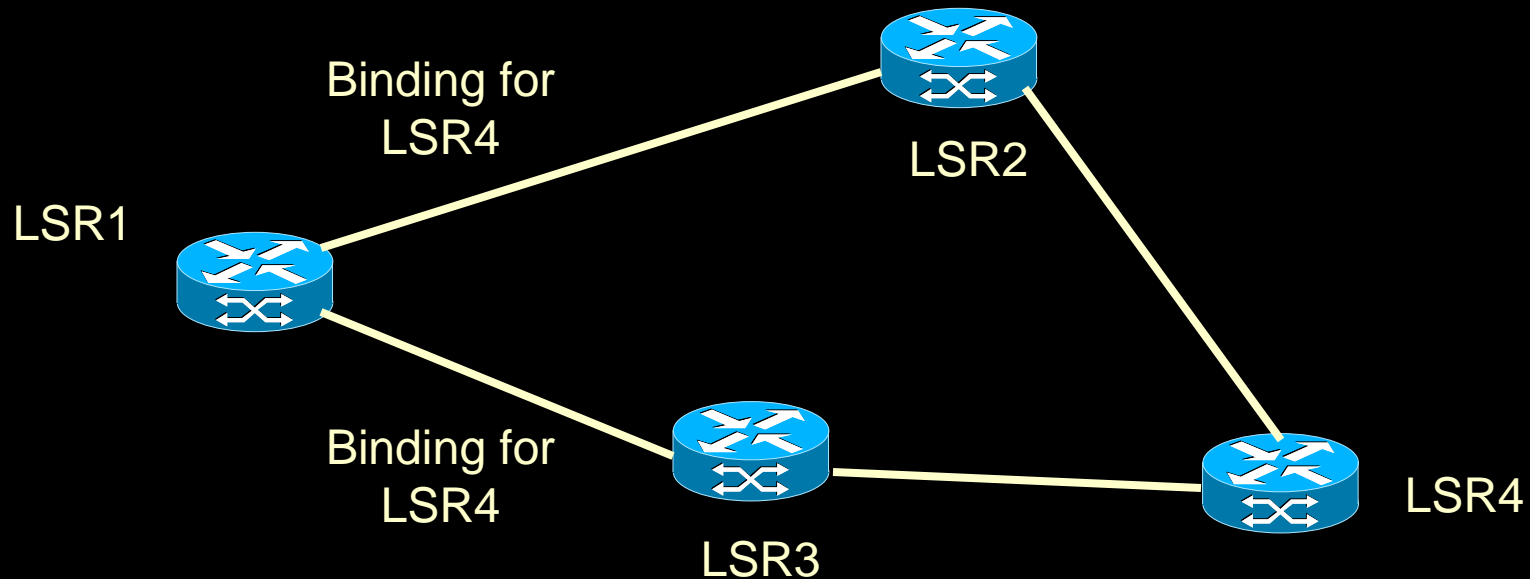
Label-FEC binding is communicated to peers if:

- LSR is the 'egress' LSR to particular FEC
- label binding has been received from upstream LSR

Used for explicit routing

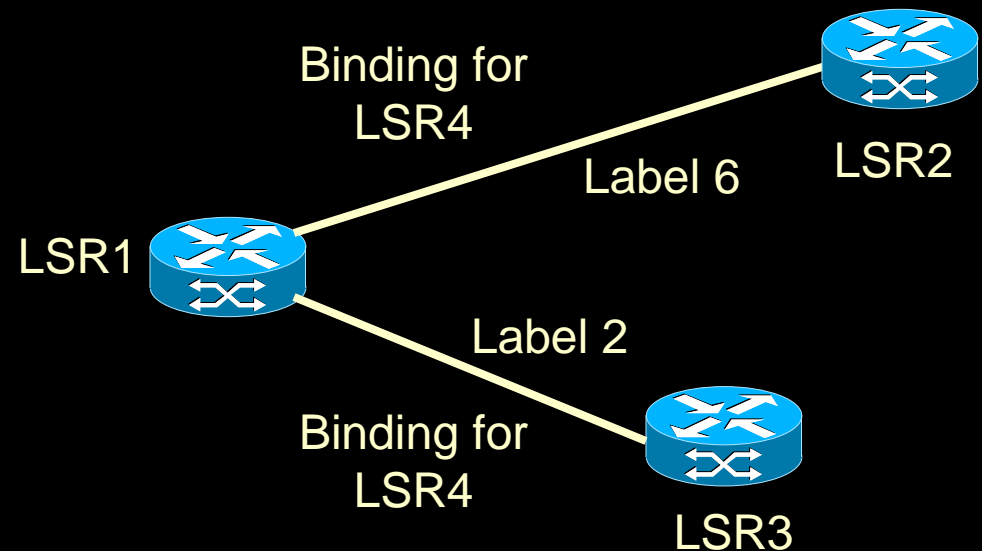
## *Label retention methods*

- Liberal Label Retention
- Conservative Label Retention



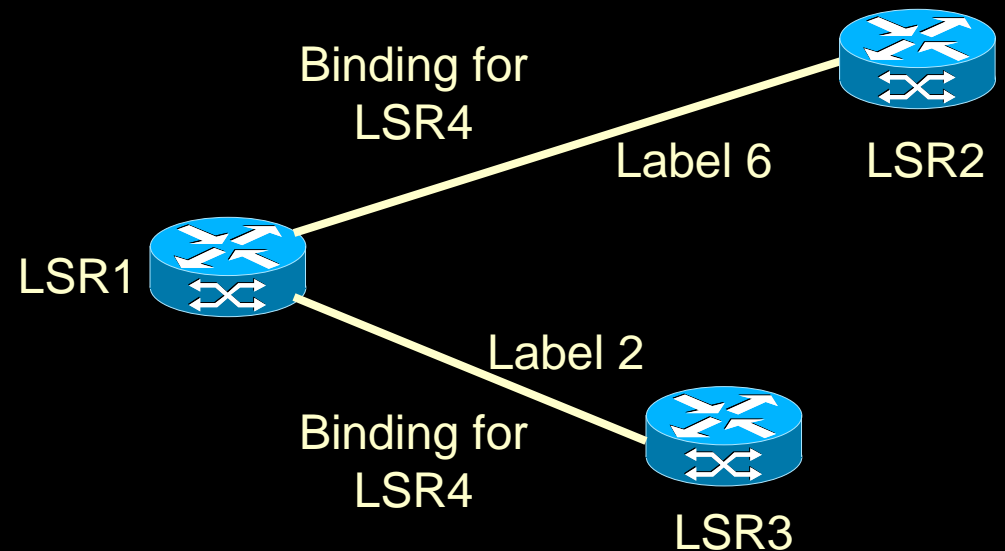
## *Liberal Retention Mode*

- LSR maintains bindings received from LSRs other than the valid next hop
- If the next-hop changes or on link failure, it may begin using these bindings immediately
- May allow more rapid adaptation to routing changes
- Requires an LSR to maintain many more labels

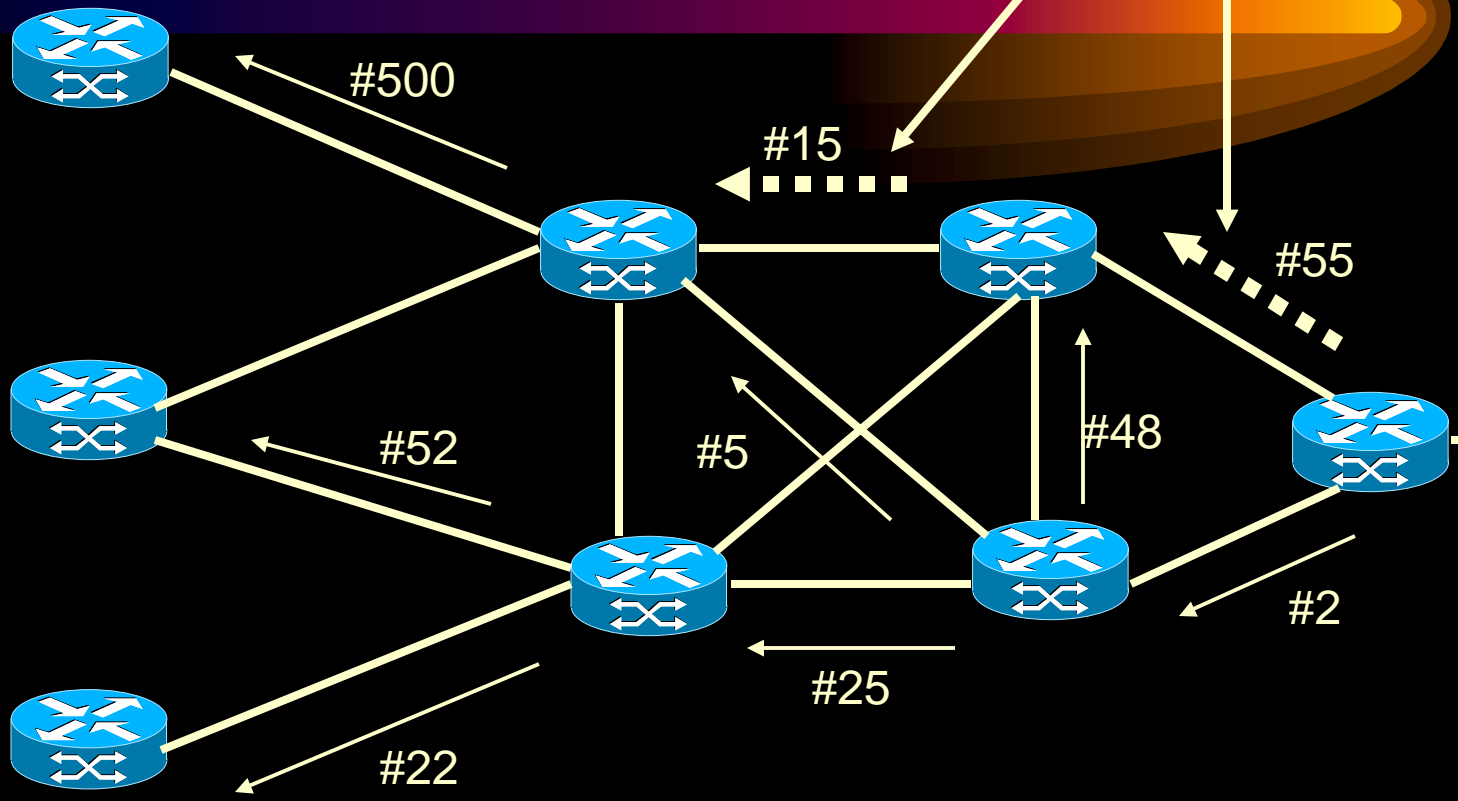


## *Conservative retention Mode*

- LSR only maintains bindings received from valid next hop
- If the next-hop changes, or on link failure binding must be requested from new next hop
- Restricts adaptation to changes in routing
- Fewer labels must be maintained by LSR



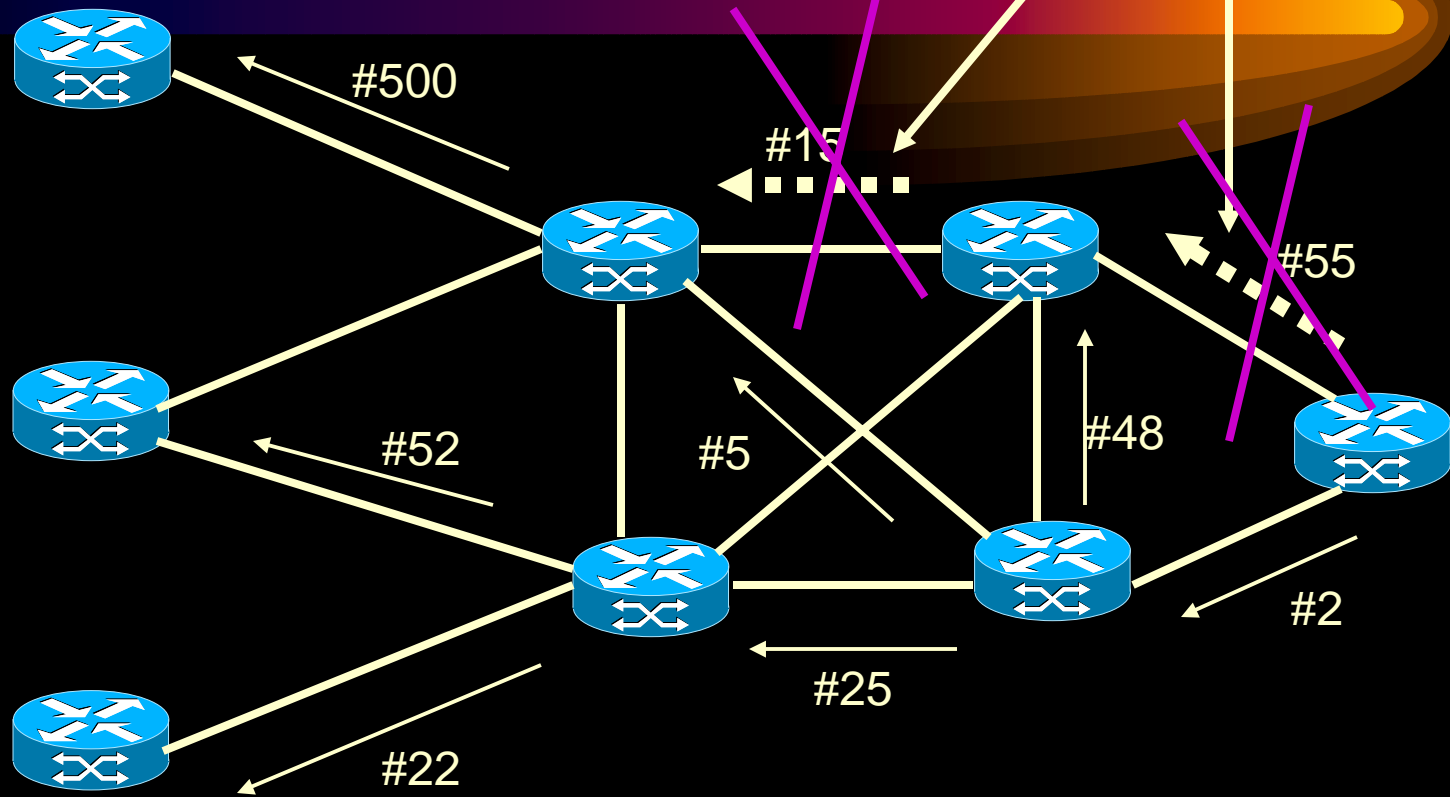
Labels are kept



Liberal Retention mode



Labels are released

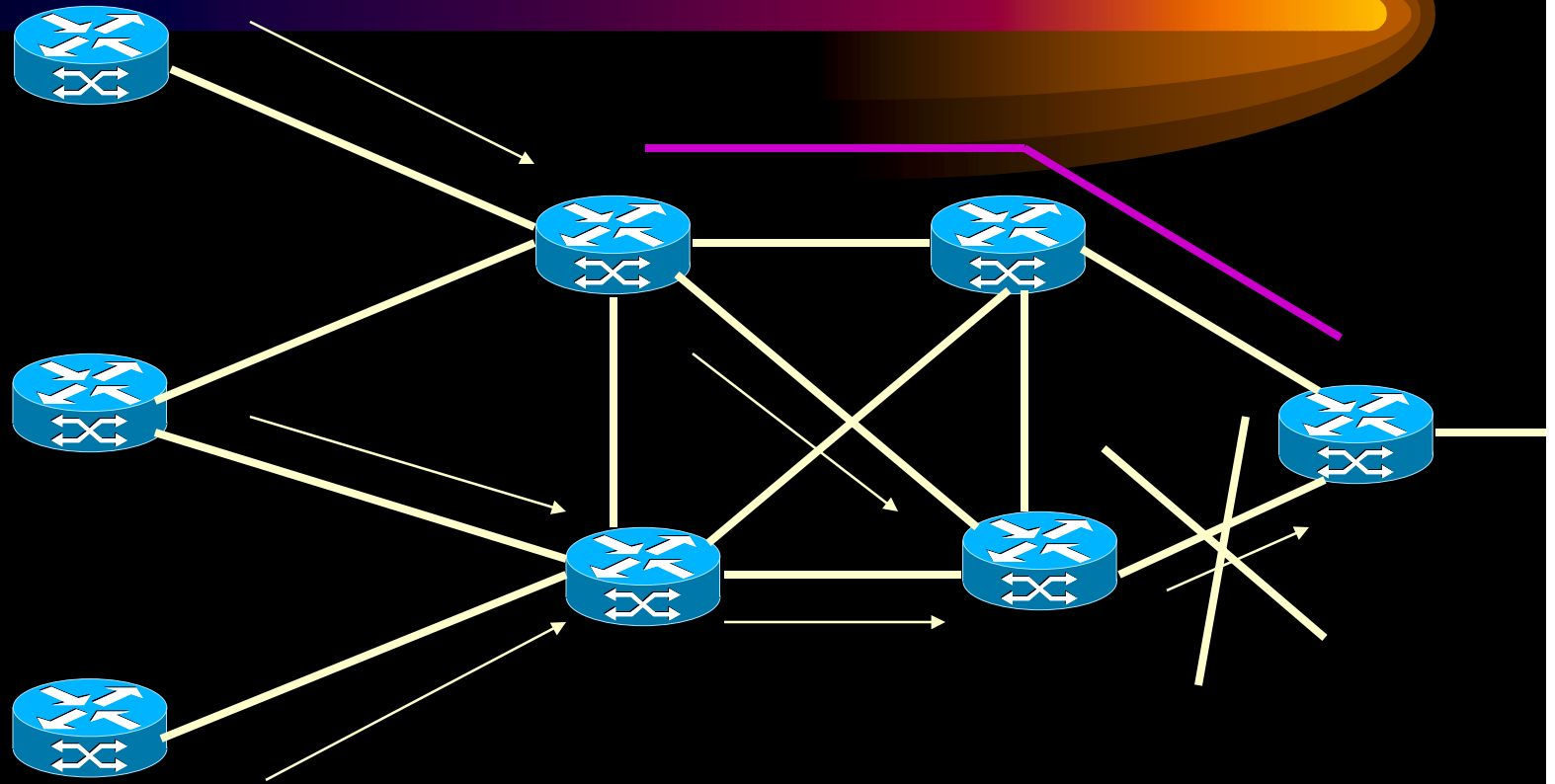


Conservative Retention mode

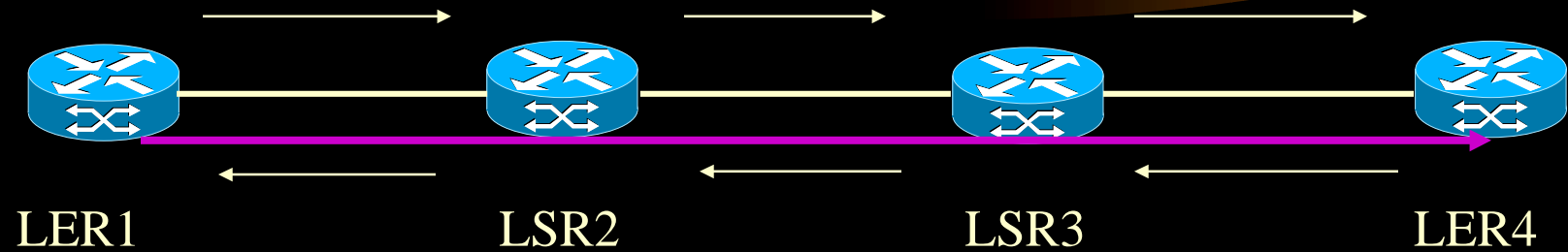
## *Constrained Based Routed LDP (CR-LDP)*

- It uses LDP messages with a modified version
- Explicit path is set
- It can co-exist with the pure LDP
- Introduces additional constraints..new parameters..for traffic regulation

# *LDP Similar to IP*



## *Explicit Setup using CR-LDP*



### Advantages of Explicit Routing

- Operator has routing flexibility
- Can use routes other than shortest path
- Traffic engineering

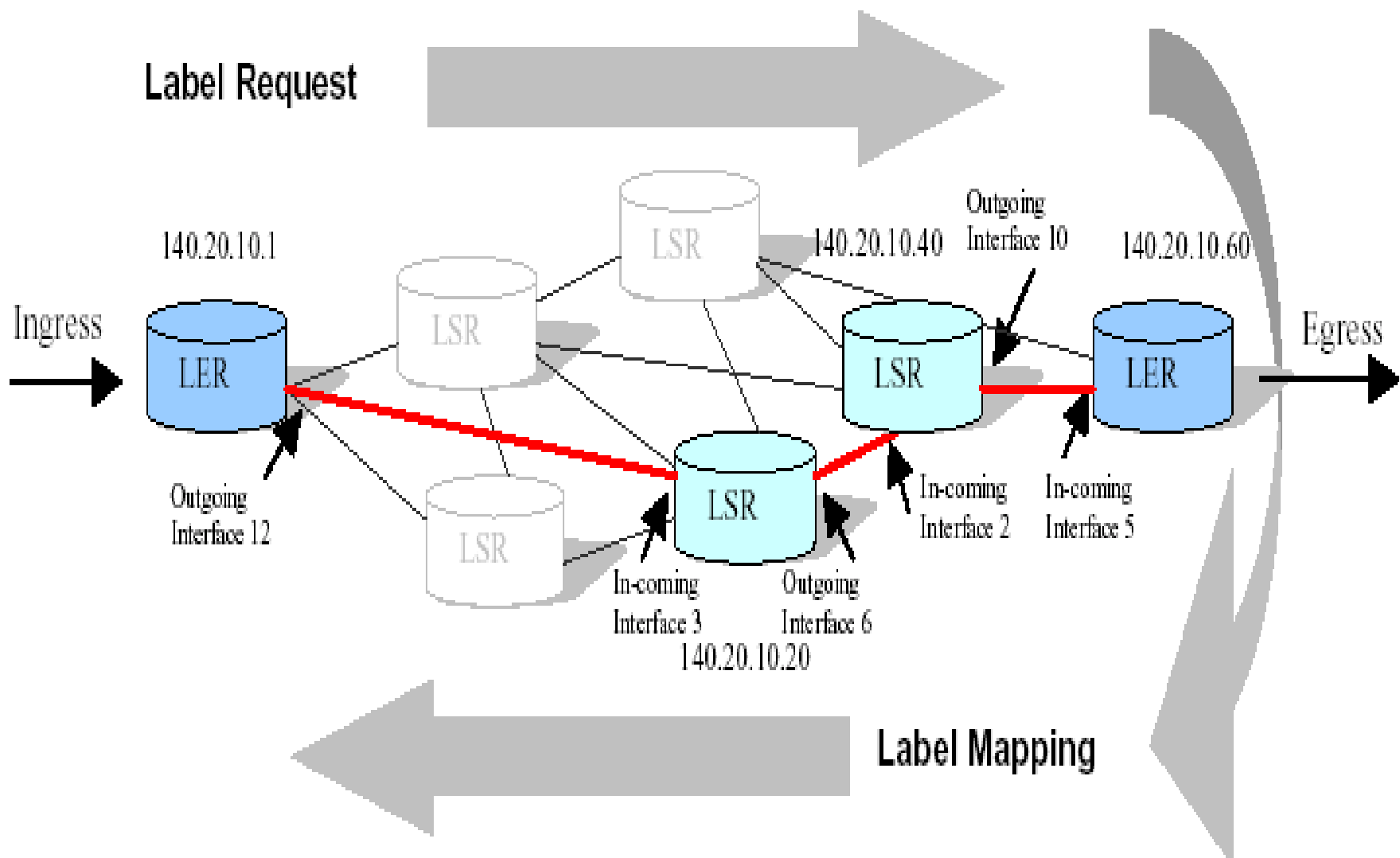


Figure 2: Example of a Strict Explicitly Routed CR-LDP LSP

## *Strict and Loose Explicit Routes*

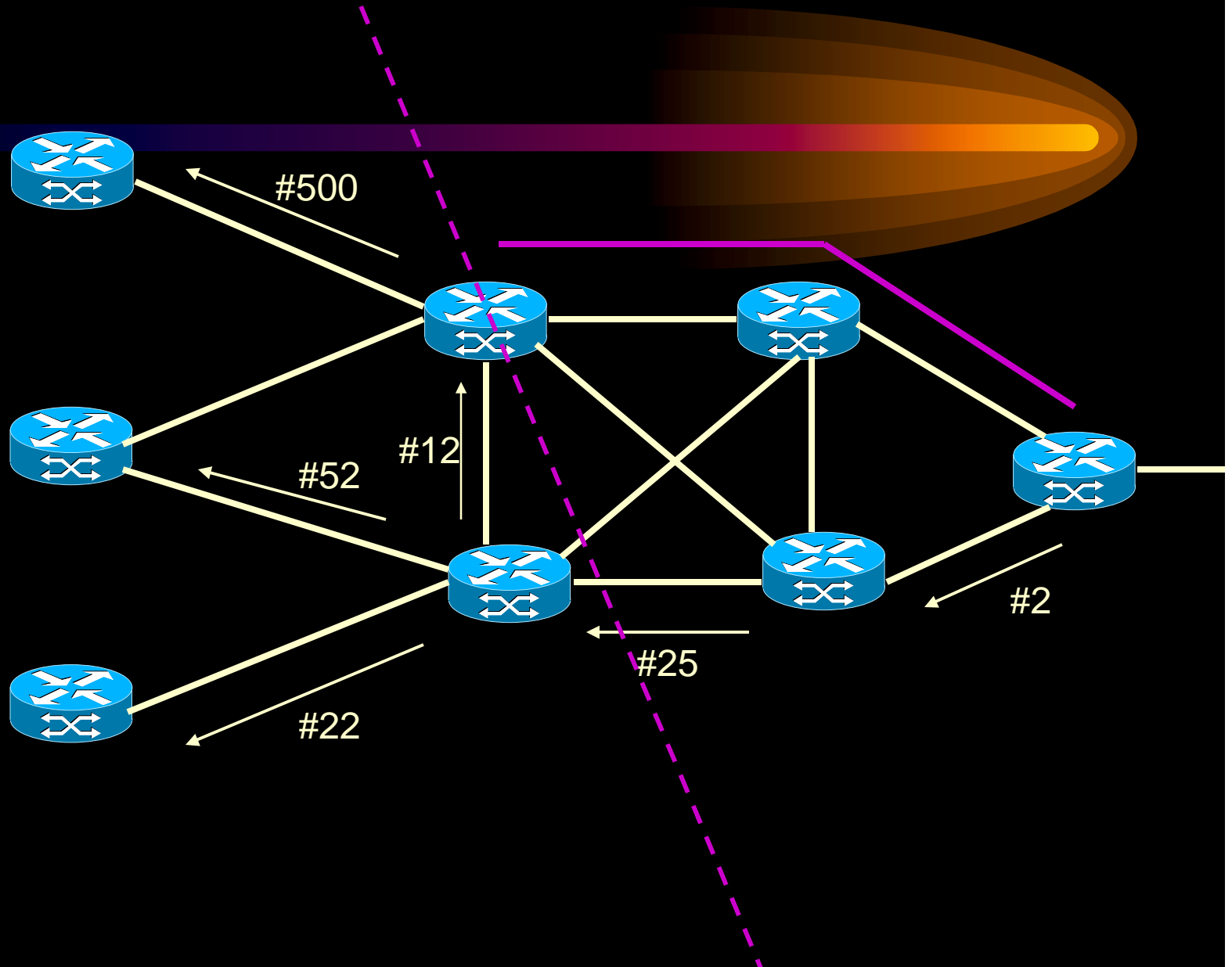


- **Strict ER-LSP:** Specifies list of nodes using actual address of each node to traverse.
- **Loose ER-LSP:** Specifies list of nodes to act as one of the ‘abstract’ nodes to traverse.

# *Hard State*



# *LDP/CR-LDP Internetworking*





# *CR-LDP Traffic Engineering*



- QoS and Traffic parameters
- Path Preemption
- Path Re-optimization
- Failure Notification
- Loop Detection

# *CR-LDP Traffic Engineering (Contd)*

## *CR-LDP Traffic Parameters*

0	1	15	31
U	F	Traffic Para TLV	Length
Flags		Frequency	Reserved
Peak Data Rate			
Peak Burst Size			
Committed Data Rate			
Committed Burst Size			
Excess Burst Size			

## *CR-LDP Traffic Engineering(Contd)*

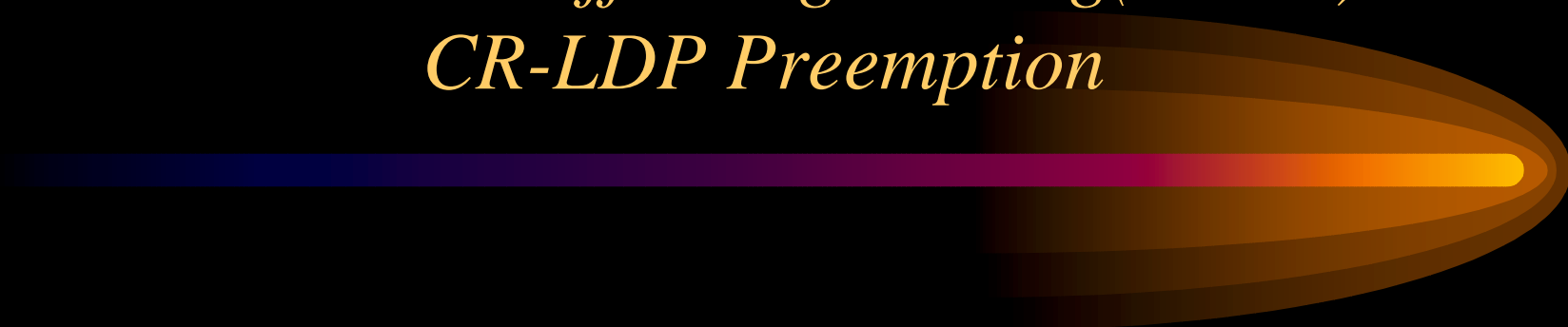
### *CR-LDP Traffic Parameters*



- Peak Rate – Maximum rate at which traffic should be sent to CR-LDP
- Committed Rate – The rate that the MPLS domain commits to be available to the CRLSP
- Excess Burst Size – Measures the extent by which the traffic sent on CR-LSP exceeds the committed rate
- Frequency – constraints delay

## *CR-LDP Traffic Engineering(Contd)*

### *CR-LDP Preemption*



- A CR-LSP carries an LSP priority. This priority can be used to allow new LSPs to *bump* existing LSPs of lower priority in order to steal their resources.
- This is especially useful during times of failure and allows you to rank the LSPs such that the most important obtain resources before less important LSPs.

## *CR-LDP Traffic Engineering(Contd)*

### *Preemption TLV*



- When an LSP is established its setupPriority is compared with the holdingPriority of existing LSPs.
- If holdingPriority < setupPriority(bump)
- If holdingPriority > setupPriority(retain)

## *CR-LDP Traffic Engineering(Contd)*



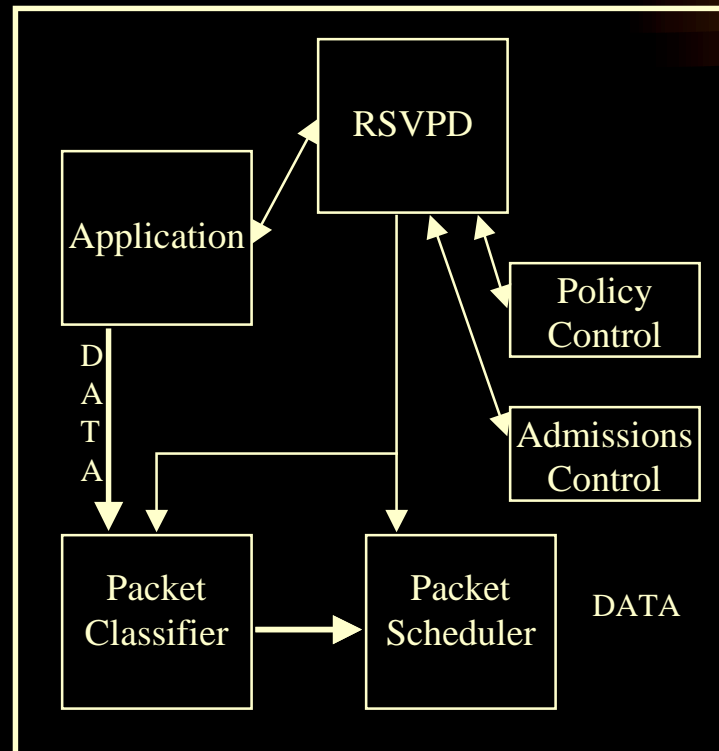
- **Path Re-optimization.**
  - Capable to re-path loosely routed LSPs.
  - Can use Route Pinning (even if better path available will not re-path)
- **Failure notification (uses notification messages of LDP)**
- **Multi-Protocol Support**
- **Loop Detection**
  - A Path Vector TLV contains a list of the LSRs that its containing message has traversed.
  - A Hop Count TLV contains a count of the LSRS that the containing message has traversed.

# *TE- RSVP*



- Resource Reservation Protocol(RSVP)
- RSVP Daemon
- RSVP Messages
- ER-RSVP (TE-RSVP)

# *RSVP Daemon*





## *RSVP Messages*

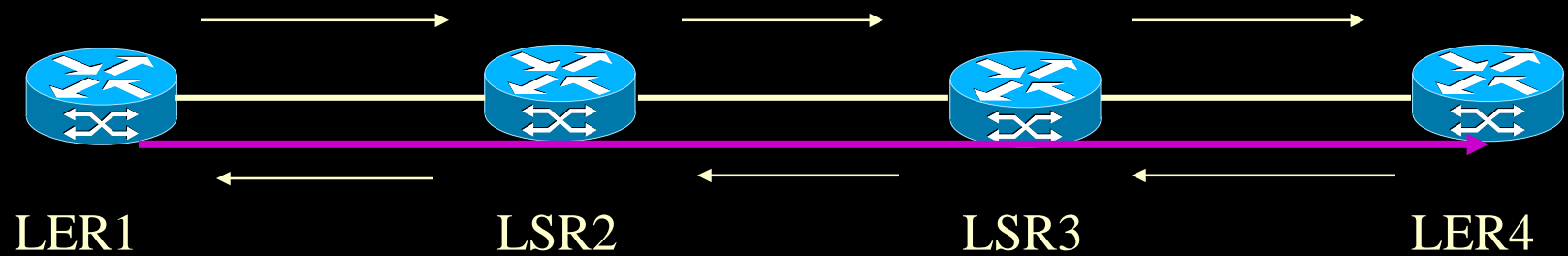
- ***Path Message***: Stores a “path state” in each node along the way that includes the previous hop’s unicast address. This unicast address is used to route reservation messages hop-by-hop in the reverse direction.
- ***Reserve Message***: Reservation messages are sent by receivers upstream towards the senders . As reservation messages travel up they maintain a reservation state in each node along the path.

## *RSVP Messages*



- **Error and Confirmation Messages:** If an error occurs during the Path/Reservation process, accordingly an error message is sent  
Confirmation message is used to inform it that the reservation was successful.
- **Teardown Message:** Explicit teardown is possible with this message

# *Explicit Path using RSVP*



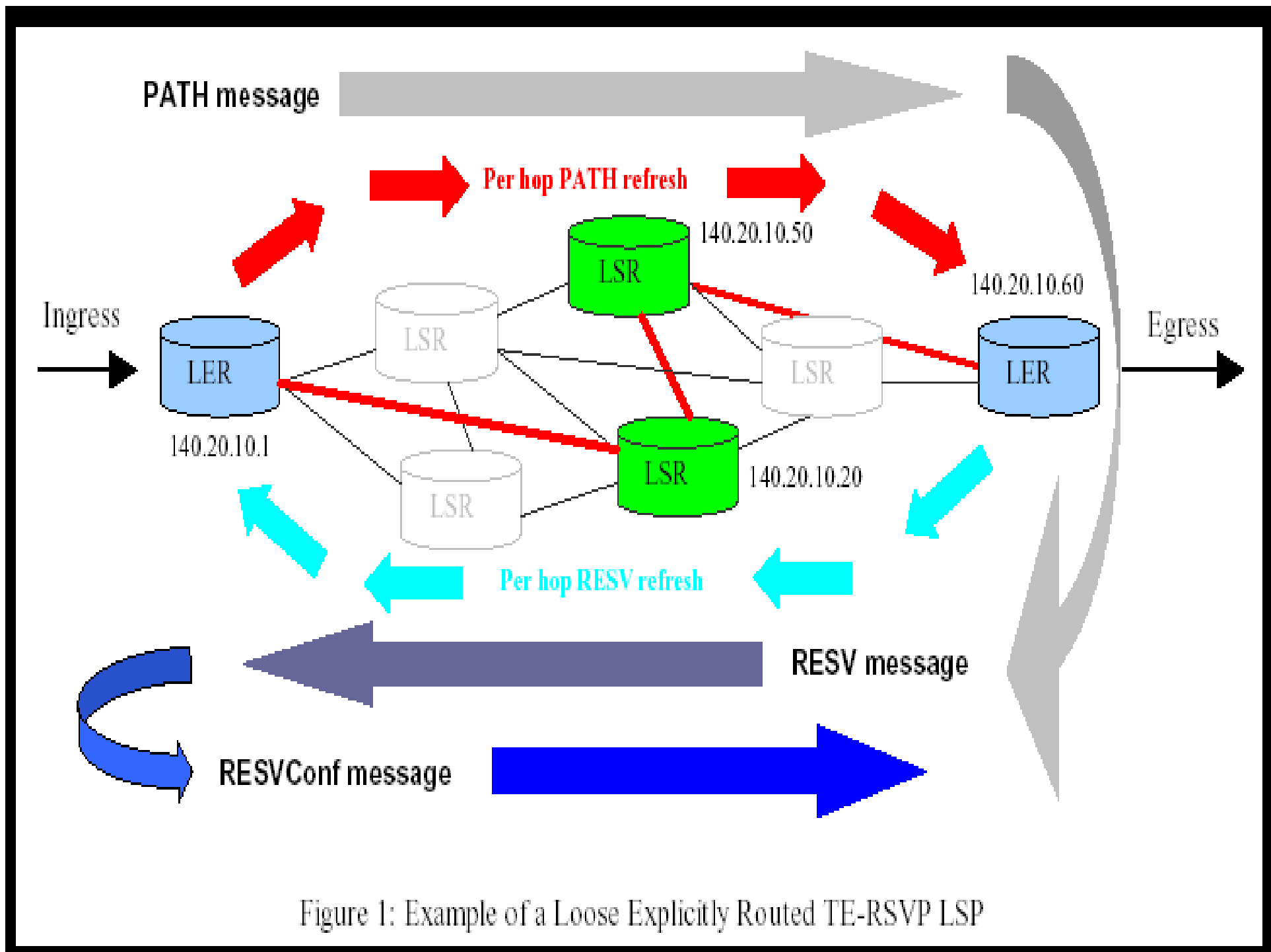
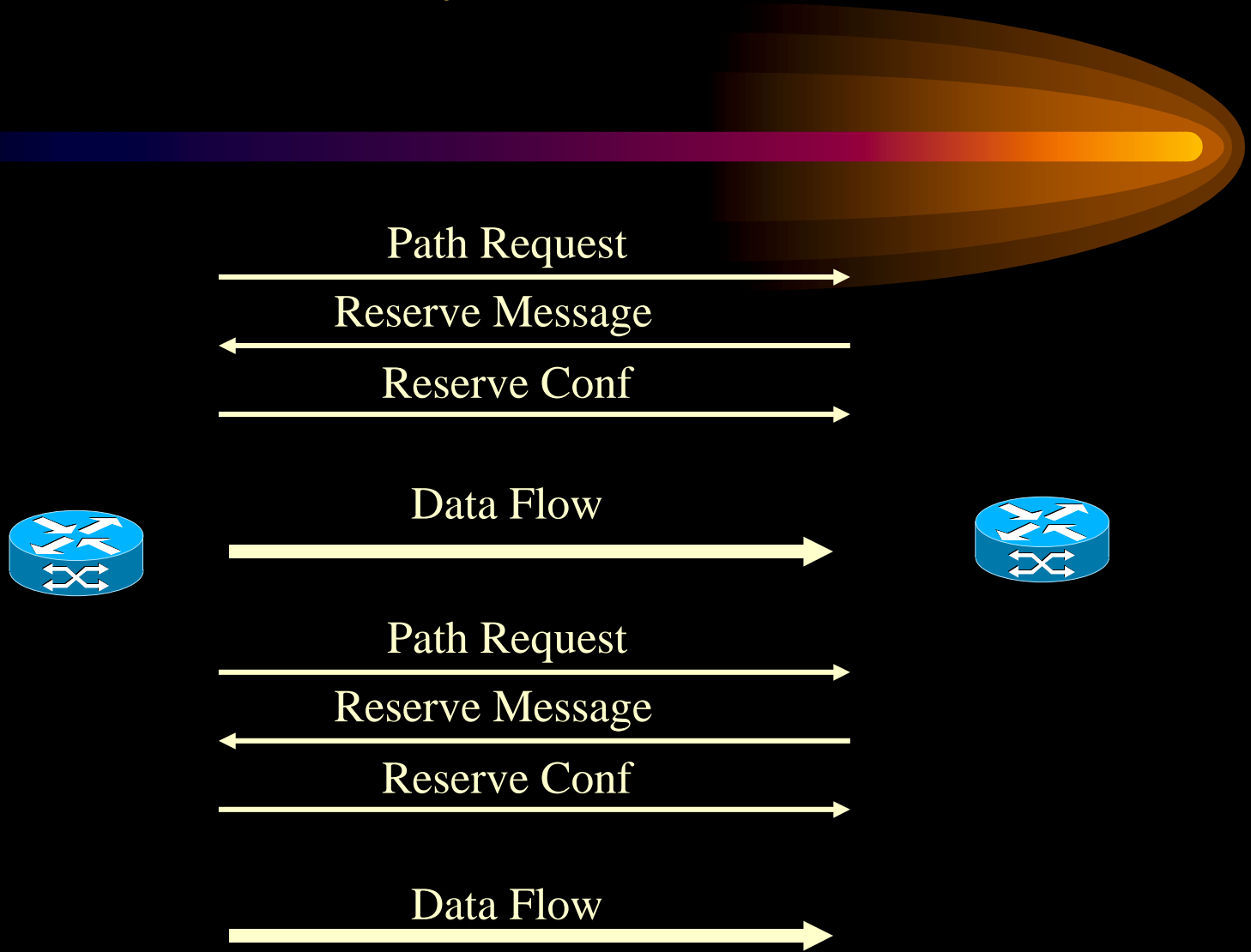


Figure 1: Example of a Loose Explicitly Routed TE-RSVP LSP

# *Soft State*



# *RSVP Traffic Engineering*



- QoS and Traffic parameters
- Failure Notification
- Loop Detection
- Multi Protocol Support
- Path Preemption

## *Discussion*



- Label Switching
- Scalability
- Security and Reliability
- Data Aggregation
- Other Minor Differences

# *Label Switching*



- LSRs assign a label, corresponding to a LSP, to each IP datagram as it is transmitted towards the destination.
- Thereafter, at each corresponding hop, the label is used to forward the packet to its next hop.
- Both CR-LDP and RSVP create LSPs by first sending label requests through the network hop-by-hop to the egress point.
- End result of both the signaling protocols is to establish an internal “cross-connect” from the ingress interface to the egress interface inside the LSR.



# *Scalability*



- Least amount of time should be spent at a router in receiving and processing frames.
- Label Switching decreases the time required to analyze each IP datagram.
- Additional overhead is incurred while creating, maintaining and destroying information needed to establish LSPs, but it is minimal compared to IP header processing.
- CR-LDP setup is referred to as “hard state”. Hence all information is exchanged only at setup time.

## *Scalability (contd)*

- RSVP on the other hand is referred to as “soft state”.
- After initial LSP setup, refresh messages must be exchanged periodically between peers for notification that connection is still desired.
- If refresh messages are not exchanged, a timer senses the connection to be dormant and deletes the state information, returns the label and reserved bandwidth to the resource pool.
- “Soft-state” refresh overhead is one of the weaknesses of RSVP and hence RSVP is not scalable.

## *Scalability (contd)*

- To reduce the volume of “chatter” between two nodes, an RSVP node can group a number of RSVP refresh messages into a single message. This is called bundling.
- In addition, the Message ID and Message Ack objects can be used to detect changes in refresh state.
- If a peer router receives a refresh message with an unchanged Message ID, it assumes that the refresh state is identical to the previous message.
- This reduces time spent in exchanging information between peers but does not eliminate computing time required to generate and process the refresh messages.

## *Scalability (contd)*

- CR-LDP had the advantage of hard state for scalability but has its own challenges.
- Once two LDP peers discover each other, a TCP/IP session is established between them for exchange of messages to maintain and establish LSPs.
- All LSPs associated with a particular session have to be destroyed if the TCP session is torn down or fails.
- The impact of this can be substantial if a large number of LSPs have been previously established.
- RSVP tunnel is a separate entity onto itself, so a change in the session is local to itself.

## *Security and Reliability*

- MPLS separates the routing decisions and forwarding of the data.
- Once the path has been established, the frame is no longer promoted to the upper layers.
- Hence there is minimal chance that unauthorized individuals will be able to “sniff” or redirect the flow from its intended destination.
- CR-LDP uses a TCP/IP connection which offers a reliable and secure connection between peers. It also offers timely error notification in case of communication failure between peers.

## *Security and Reliability (contd)*

- RSVP on the other hand uses UDP and “raw” IP datagrams to communicate between peers.
- This makes it vulnerable to security attacks and does not enable fast recovery.
- IPSec and other encryption or authentication schemes can be used to guarantee valid path and reserve messages, but “spoofing” attacks can impair the performance of RSVP.
- Connection failure can only be detected after a TE-RSVP neighbor fails to receive a refresh message from one of its peers.

## *Data Aggregation*

- In CR-LDP, each FEC is specified as a set of packets that are mapped onto a corresponding LSP.
- An IP address prefix describing an entire subnet can be designated as the “destination” of the LSP or FEC. So, all traffic destined for that subnet can travel through a single LSP.
- Differentiated services can be provided in CR-LDP by assigning a certain set of traffic parameters to each packet as it travels through the network.
- RSVP on the other hand, was initially designed to offer reserved bandwidth capabilities to a single IP address.

## *Other Minor Differences*

- In CR-LDP, after discovery, each LDP peer submits its type and range of labels to be used to establish LSPs. If there is no set of labels that intersect, the session is torn down.
- In RSVP, there is no negotiation of label space. If the network is large, the effort for configuring labels can be considerable.
- Both support the concept of “loosely” routed paths and route pinning.
- In CR-LDP route pinning can take place only at setup time, RSVP can set up pinning by modifying PATH messages.



# Summary

## Similarities between TE-RSVP and CR-LDP

Characteristics	CR-LDP	TE-RSVP	Comments
Initiate Setup	Label Request Message	PATH Message containing LABEL_REQUEST object.	
Setup Accomplished	Mapping Message	RESV Message	
Differentiated Services Defined	DIFF-SERV_PSC TLV	DIFFSERV_PSC object	Both contain the DiffServ Code point or DSCP information and included in the setup request message – see row 1
Support for point to multipoint LSPs	No	No	Yet to be defined by the IETF.
Source Route Capability	Carried in Explicit Route List TLV	Carried in EXPLICIT_ROUTE object	Specify route used to setup switched path.

## Summary (contd)

### Differences between CR-LDP and RSVP

Characteristics	CR-LDP	TE-RSVP	Comments
Development Stage	New	Old with extensions being added, support for legacy networks.	RSVP objects being modified to be used in a MPLS environment
Signaling Transport	UDP for discovery, TCP for sessions	Raw IP datagrams or UDP encapsulation for message exchange	Non-deterministic failure detection with RSVP. TCP failure can have catastrophic impact on LSP's with CR-LDP.
Connection State	Hard State	Soft State	Soft State said to be non-scalable, RSVP to support aggregation of refreshes – also known as refresh reduction.
Reliability	Failure produces proactive signaling action	Dependant on soft state timer response to detect failure.	Non-deterministic failure detection with RSVP.
Manageability	LSR, LDP, TE MIBs	Modified RSVP and LSR MIBs	
Extensibility	Vendor Specific, opaque and experimental TLVs	Experimental Objects	Very similar in function
Scalability	Hard State connections reduce session signaling overhead	Requires Refresh reduction, aggregation to minimize Soft State overhead.	
Interoperability	Well defined support for most transports, ATM, Frame Relay, Ethernet	Tunneling through ATM network must be manually configured.	

## *Conclusion*



- Both CR-LDP and TE-RSVP provide very similar functionality for establishing traffic engineered label switched paths.
- LDP is new, while RSVP has operational experience.
- Extensive enhancements have been made to RSVP in order to support the needs of MPLS.
- MPLS traffic engineering should evolve into a single entity that combines the best of TE-RSVP and CR-LDP.