A New Traffic Engineering Approach for IP Networks

Ljiljana Adamovic and Martin Collier
Research Institute for Networks Communications Engineering (RINCE)
Dublin City University, Dublin 9, Ireland
e-mail: {ljiljana, collierm}@eeng.dcu.ie

Abstract

MPLS has received considerable attention as a protocol for transporting IP packets while providing traffic engineering. It requires label distribution, which represents a significant overhead when processing connectionless traffic. This paper describes a new protocol called subIP which efficiently provides connectionless service to IP traffic while remaining the simplicity of MPLS packet forwarding. When used in conjunction with a concept called multiple topology routing, which allows multiple routes to be obtained using standard shortest path routing algorithms, it allows best effort traffic to be flexibly routed across a network domain.

1 Introduction

With the intensive growth of the Internet there is a need for introducing control of traffic routes in IP networks in order both to improve the network utilization and to provide different types of service to the customers. This type of traffic control is called traffic engineering. In general, current proposals for traffic engineering are:
- optimizing link weights in link-state routing protocols in order to cause better traffic distribution with connectionless IP routing [2],
- introducing connection-oriented services with a protocol, such as MPLS [1], and balancing the traffic among established explicit paths based on various criteria.

In this paper we present a new approach. Different virtual topologies are derived from the actual network topology determined by an external entity, such as a network management system or a human operator. They are distributed and used by subIP, a new forwarding protocol proposed in this paper for balancing the connectionless traffic in order to improve network utilization.
subIP adopts ideas from both IP and MPLS. As with MPLS, subIP should be implemented below the IP layer. It adds a 4 byte subIP header between the data link header and the IP header to each IP packet. It may thus may be considered as a new version of the MPLS protocol. However, it provides connectionless service similar to IP. A subIP area has no more than 256 routers where each router has a unique 1 byte long subIP address. While traversing the area each packet carries the subIP address of the last area router to be visited on its way to the destination, the area destination router. Packet forwarding through the area is based on interpretation of this address.
The subIP routing tables are calculated based on the area topology information distributed by the existing routing protocol and the virtual topology information distributed by the subIP Control Message Protocol (sCMP), which is an integral part of subIP. For each topology defined each router calculates shortest paths for the area destination. The value of the *control* field in the subIP header determines which of the topologies should be used on packet forwarding. This concept allows balancing the traffic among shortest paths of different topologies, which may not be the shortest paths in the actual area topology.
subIP is simple. It simplifies and speeds up IP routing and improves network utilization with multiple topology routing. It provides better performance than MPLS connectionless hop-by-hop routing and may be expanded to support MPLS explicit routing. With a new subIP hierarchical addressing scheme and virtual paths established by MPLS there is a prospect of building multiple hierarchy networks with geographically significant addresses, which would significantly simplify traffic engineering.
In this paper we discuss subIP implementation within an autonomous system (AS) implementing the OSPF link-state routing protocol [5]. It may also be applied for networks implementing the IS-IS routing protocol [6], due to the similarity of the two protocols.
Since subIP adopts ideas from both IP and MPLS, a brief overview of the two protocols is given in section 2. The subIP protocol is described in section 3. Multiple topology routing is presented in section 4. Further network developments are discussed in section 5. The paper is summarized in section 6.

2 Existing Protocols

Apart from multiple topology routing which is explained in section 4, the subIP ideas are based on concepts of existing protocols IP and MPLS. We give a short overview of the two protocols in this section. For the MPLS forwarding concept the implementation of a label distribution protocol, such as CR-LDP or RSVP-TE is obligatory. The protocol stack is given in Fig. 1.

As will be discussed in the paper, more flexible protocol

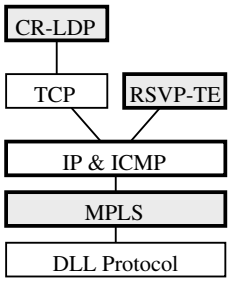


Figure 1: Protocol Relationship

structure can be provided with subIP.

2.1 IP

The Internet Protocol (IP)[4] is the core of the data exchange in the Internet. It provides connectionless, best-effort delivery of datagrams through the network. It also provides fragmentation and reassembly of long packets, if necessary, for transmission through *small packet* networks.

The IP routes packets through the network based on the interpretation of the destination address in the IP header. The information distributed by a routing protocol is used by routers for calculating shortest paths towards the reachable destinations. The results are stored in routing tables and each table entry contains a destination address prefix, next hop to reach the destination and the cost of the path to the destination. On packet forwarding a router finds in its routing table the longest prefix matching the packet's destination address and forward the packet towards the next hop associated with the found longest prefix.

The IP header is at least 20 bytes long. In general, the fields of concern for packet forwarding are: *Source Address* and *Destination Address*, the 4 byte IP addresses of the source and destination of the packet and the 1 byte *Time to Live* (TTL) field, which contains the number of hops a packet may take on its way to a destination. The TTL field is decremented with each hop of the packet. If zero is reached the packet is discarded and a message is sent back to the sender. The purpose of the field is to prevent packets from looping endlessly due to topology changes or in the case of some error.

To provide endnodes with feedback about the problems in the network IP uses the Internet Control Message Protocol (ICMP) [7]. Typically it reports errors in the processing of datagrams, such as *destination unreachable*, *parameter problem*, etc. ICMP is an integral part of IP. Its messages are sent in the data portion of an ordinary IP packet, with the protocol field in its IP header identifying it as an ICMP packet.

IP routing along shortest paths may cause congestion on some network links while longer not used path exists. Current IP implementations do not provide balancing the traffic among paths of different costs. The traffic may though be balanced among multiple paths of equal cost using ECMP algorithm[3].

2.2 MPLS

Multiprotocol Label Switching (MPLS)[1] is a forwarding protocol implemented below the network layer protocol. Its forwarding procedure is based on labels. The two neighboring nodes negotiate about a number, the *label* to be used on forwarding an IP packet with certain characteristics. The label has local significance. It is stored in the MPLS header added to each packet when it enters an MPLS domain before it is forwarded. At subsequent hops through the domain the label is used as an index into a table which specifies the next hop and a new label to replace the old one before forwarding the packet to its next hop. There is no IP header examination nor longest prefix match table lookup while the packet is traversing the MPLS domain. The scheme is conceptually very similar to ATM cell switching.

The labels are distributed by a separate label distribution protocol, such as CR-LDP or RSVP-TE, which is thus necessary for MPLS operation. Some routing protocols (e.g. BGP) have been extended so that they also distribute the labels, though not OSPF. For establishing label switched paths (LSPs) MPLS defines two types of routing: hop-by-hop and explicit routing. Hop-by-hop routing provides the same paths within the MPLS domain as when IP routing is used. To accomplish it each MPLS router independently assigns a label to each address prefix in its routing table. When the network topology changes the paths are recalculated and new labels need to be assigned and distributed. Since packet forwarding is based on labels, this prolongs the time the network is operating with inconsistent forwarding information and decreases network stability. Alternatively, a router may keep all the labels received from the neighbors assigned for each address prefix, which allows for quicker adaptation to routing changes, but requires many more labels to be maintained [1]. The paths established using explicit routing are determined based on some criteria by the ingress domain routers and labels are distributed along the path on setup.

The MPLS header is shown in Fig. 2. It is 4 bytes long, most commonly encapsulated between the data link header and the network layer header. Beside the label, it contains 3 experimental bits not yet defined, a 1 bit (S) top of the label stack indication and 8 bits of Time To Live (TTL) field.

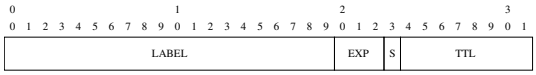


Figure 2: The MPLS Header

The concept of the label stack allows packets to carry more than one label while traversing the network. Each

label is placed in a separate MPLS header and the headers are organized as a *label stack*. Processing of the labelled packet is always based on the label of the top header. This is used when tunelling packets through a nested MPLS domain [1].
The TTL field in the MPLS header has the same meaning as in the IP header. It is copied from the IP header when the packet enters the MPLS domain and decremented at each hop along the label switched path. If its value reaches zero somewhere along the path, the packet is discarded. When the packet leaves the domain the TTL field is copied back to the packets IP header.
Initially, the main goal of MPLS was to speed up packet forwarding by implementing simple and fast switches within the MPLS domain that forward packets based on short labels placed in a new MPLS packet header. With the emergence of fast longest prefix match algorithms that sped up IP forwarding, the justification for MPLS in IP networks now is its use in balancing the traffic among explicit paths in order to increase network utilization.

3 subIP

subIP provides connectionless packet forwarding in an area with no more than 256 routers. Its routing concept is the same as IP routing. It does not provide packet fragmentation and reassembly, unlike IP. The subIP should be implemented bellow the IP in the layered protocol architecture (Fig. 3), and it adds a 4 byte header to each

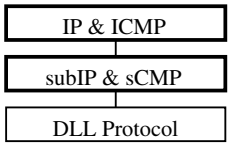


Figure 3: Layered Protocol View

IP packet between the data link and IP header, same as MPLS. However, due to a different routing concept it does not require a label distribution protocol, unlike MPLS.
A unique per subIP area 1 byte subIP router address is assigned to each area router, which bounds the subIP area size to 256 routers. When a packet enters the area the ingress router determines the last area router on the packet's way to the destination, the egress area router, based on the IP destination address in packet's IP header and the information collected by a routing protocol. The ingress and the egress router may be considered as the source and destination of the packet within the subIP area. The ingress router stores the subIP addresses of the source (its own address) and destination (egress) area routers in the subIP header of the packet. The forwarding concept through the area is now the same as in IP routing. Based on the subIP area topology information each area router calculates shortest paths to the routers within the area using the existing shortest path algorithms. The results are stored in routing tables where each table entry contains area destinations, next hops along the path and the cost of the path to reach those destinations. Since only the area routers are considered as destinations (up to 256 routers) and the destinations are identified with 1 byte subIP addresses, the routing tables are small. At each hop the routing table entry containing the destination subIP address in the packet's subIP header determines the next hop of the packet. There is no IP header examination nor longest prefix match table lookup while the packet is traversing the subIP area.
The subIP area topology information is distributed to each area router by the existing routing protocol implemented in the area. In order to provide some control of the traffic routes, subIP also allows new virtual topologies to be distributed to all the area routers using its subIP Control Message Protocol (sCMP), which is an integral part of the subIP. Its messages are sent in the data portion after the subIP header, with the protocol field in subIP header identifying it as an sCMP packet (similarly to ICMP used with IP). The new topologies are derived from the actual subIP area topology. The area routers calculates shortest paths for all the defined topologies. The ingress area router controls which topology should be used on forwarding with *control* field of subIP header. This allows traffic balancing among shortest paths of different topologies. The multiple topology routing is discussed in section 4.
The subIP depends on the information collected by a routing protocol. We discuss its implementation in an autonomous systems (AS) implementing the OSPF [5] link state-routing protocol. The OSPF defines two hierarchy levels in an AS, areas that communicate over the second level backbone. Our subIP areas will be determined by the areas defined by the OSPF, including one subIP area for the backbone.

3.1 subIP Header

The format of the subIP header is shown in Fig. 4.
The *control* field is used for specifying the topology to be used on packet forwarding in multiple topology routing, explained in section 4. It may also be used in hier-

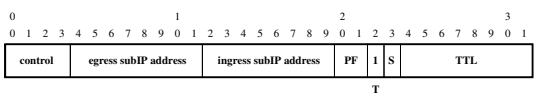


Figure 4: The subIP Header

archical networks to indicate the level of hierarchy.
The *egress subIP address* presents the subIP area router address of the egress area router. It is used for determining the next hop on packet forwarding.
The *ingress subIP address* presents the subIP area router address of the ingress area router. It may be used on sending an ICMP messages from within the area in order

to avoid determining the egress router (and thus longest prefix table lookup) on sending messages back to the source.
Both *ingress* and *egress subIP addresses* may be used as an ID of the ingress-egress flow aggregation, for balancing the traffic among equally shortest paths within the area, similar as in IP routing.
The *PF* field is the protocol field. It allows only 4 different protocol to be implemented *on top* of subIP. Two values of this field are reserved for the IP and subIP Control Message Protocol(sCMP).
The T (type of service) bit is set to 1 to indicate subIP connectionless service. If it is set to 1 it may indicate the MPLS connection-oriented service and the MPLS header, as will be discussed in section 5.
The S bit is the top of the label stack indication. It is used to allow sending more than one subIP header with one packet organized as a label stack, same as in MPLS.
The TTL field contains the number of hops a packet may take on its way to a destination. As in MPLS, it is copied from the packet's TTL field in the IP header when an IP packet enters the subIP area and decremented at each hop. If zero is reached the packet is discarded, else the field is copied back to the IP header TTL field when the packet leaves the area.

3.2 Addressing the Domain

Each router in a subIP area has a unique 1 byte subIP address. As shown in Fig. 5, the subIP network with new addresses underlies the existing IP network. While the IP addresses are assigned per router's interface, the subIP addresses are assigned per router and present a unique per area prefix of all the IP addresses of a router. In order to identify different subIP areas within a two level hierarchy AS, we assign a 4 byte hierarchical subIP AS router address to each AS router in the form *AS:backbone router:area:area router*, where, for simplicity, each byte represents a subIP address of the AS, backbone router, area and area router, respectively. The length of these addresses may depend on the number of areas and routers, as long as the backbone router address and the area router address are not more than 1 byte long. They are used on subIP forwarding within the backbone and an area, respectively. The new subIP

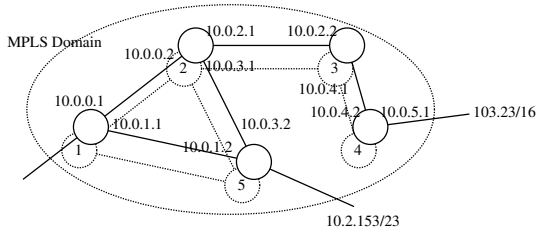


Figure 5: The subIP Addresses

address carried in the subIP header and the subIP routing concept allow exact match table lookup on packet forwarding through the domain. A similar approach is used in CLNP where a node has unique address per area and level 1 routing uses exact match table lookup [6].
Since the 4 byte subIP address uniquely identifies a router in the AS, the best and the most appropriate way to distribute subIP addresses is in the routing protocol messages as router IDs, if implementation allows. This ID is a 4 byte identifier of a router that sent the routing protocol message. Currently, one of the router IP addresses is set as router ID. Alternatively, a file containing mappings of the router IDs to the subIP addresses can be manually added to each router.

3.3 Determining the Egress Router

In subIP routing the ingress subIP area router needs to determine the last subIP area router on the packet's way to the destination, i.e. the egress area router. This may be done based on the packet's IP destination address in its IP header and the information gathered by the routing protocol. In our case, a subIP area matches an OSPF area and router ID in routing protocol messages is the subIP address of the router. Each link state advertisement (LSA) distributed by OSPF contains the ID of the router that sent it and is kept in the router link state databases [5]. subIP may thus expand the existing IP routing tables for each address prefix with the subIP area router address of the router that advertised it. For the routes generated from within an area (our subIP area) the egress router is the router that advertised the longest prefix matching the destination in the packets IP header. If there is more than one router advertising the prefix, the one that provides the shortest path is chosen. The cost of the path to a particular subIP area router may be found in the subIP forwarding tables, while the OSPF link advertisements contain the cost of the path towards a destination from the router advertising it. Table 1 is a simplified example of the ingress router subIP routing table for the subIP area given in Fig. 5. For a

Table 1: Address Advertisements

subIP area router who advertised	IP address prefix/mask
4	103.23/16
5	10.2.153/23

packet with destination address 10.2.153.178 by performing the longest prefix match lookup of the table it may be found that the subIP address of the router that has advertised it is 5 and that is the egress area router for this packet.
For the paths outside the subIP area the egress subIP router is the area border router (ABR) that provides the shortest path to a particular destination.

3.4 sCMP

The subIP Control Message Protocol (sCMP) is a protocol used with subIP for collecting information from the network. An sCMP message may be very short, placed in the next label stack entry or longer, placed in the data portion sent after the subIP header. However, the messages cannot be longer than the MTU per path since subIP does not provide fragmentation and reassembly. For example, the minimal MTU within the domain may be the maximal packet size.

An advantage of the sCMP messages is that they are simple to send. In order to send a message back to the ingress router of the received packet, a subIP area router may copy the address of the packet's ingress router from the subIP header of the received packet. This address is now the *egress subIP address* in the subIP header of the message, while the *ingress subIP address* is the subIP address of the area router sending the message.

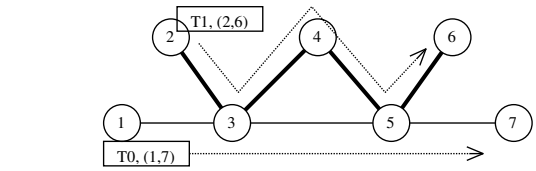
subIP provides means for balancing the traffic within a subIP area using multiple topology routing, described in section 4. sCMP is used to distribute the required topology and control information. Other sCMP messages may also be defined. For example, a short sCMP message indicating congestion indication on a particular subIP link is useful for better traffic distribution decisions.

4 Multiple Topology Routing

The concept of shortest paths routing used both in subIP and IP may cause congestion on particular links while a longer unused path exists. Currently IP only provides traffic balancing among multiple paths of equal cost. However, subIP also provides traffic balancing among multiple paths of different costs in order to avoid congestion along shortest paths.

The subIP shortest paths routing is based on the topology information collected by a routing protocol (in our case OSPF). Since each router has the same topology information, the calculation of the shortest path between two nodes gives the same result at any node in the same routing domain. We may thus define several virtual topologies based on the physical topology information collected by the routing protocol and distribute it to all the area routers. For example, this information may contain a bit mask matrix or a list of links that should be omitted from the full topology before shortest path calculations for each defined topology. The subIP addressing scheme allows its compact presentation. Each topology will be marked as a different level topology and each area router will have a separate next hop field in its routing table for each topology. The 4 bit *control* field in the subIP header, set by the ingress router, will be used to indicate which of the defined topologies should be used on packet forwarding.

A simplified example is given in Fig. 6. The physical area topology is marked as T0 and its next hop field in the routing table is NextHop0. In our T1 topology information we indicated that link 3-5 should be pruned before shortest path calculations. Using a shortest path algorithm each area router determines the next hops for the area destinations for this topology and stores them as NextHop1 in the routing table. In the given example the router R3 will find different next hops for destination R6 and R7 for the two topologies. A received packet will be routed according to the NextHop0 if the *control* field in its subIP header is set to 0 and according to the NextHop1 if this field is set to 1. By assigning packets to



R3 Routing table

Address	Next Hop 0	Next Hop 1
6	5	4
7	5	4

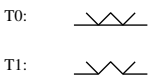


Figure 6: Multiple Topology Routing

different topologies the ingress routers balance the traffic in the domain. In the given example the ingress router R2 forward packets to the egress R6 along the topology T1, while the ingress router R1 sends packets to the egress router R7 along the topology T0. Alternatively, each ingress router may split its traffic to these destinations by performing a finer traffic aggregation based on the address prefix in routing tables.

Different topologies and traffic distribution are determined by an external entity, such as a network management system or a human operator, to achieve certain traffic engineering goals. Generally, a new topology is defined rarely and distributed rarely. However, distribution of the new topology information does not disrupt the current network routing. Once the information is distributed throughout the subIP area, the same external entity may trigger the use of the new topology on packet forwarding by sending a message to one or more edge area routers. This also provides some control of the edge routers in traffic balancing. Within the area a packet received with non-0 *control* field in its subIP header will trigger routing table calculations for a particular virtual topology and it may be timed out when no more subIP headers with non-0 *control* fields are detected. The ingress LER may assign packets to different topology levels based on their egress address or a finer traffic aggregation may be applied based on the address prefix in the table of address advertisements or packet destination address. For the control message exchange cCMP is used as discussed in section 3.4.

Defining different topologies can be kept simple and used only to avoid congestion in the network, but there are also prospectives for more sophisticated traffic engineering techniques, which requires further study. Link

utilization, congestion or failures in a certain period of time, for example in peak hours, are some of the factors that can be considered on defining a new topology. A separate topology may also be defined for the inter-AS traffic and the intra-AS traffic. Since subIP does not provide fragmentation and reassembly, it may be useful to define a topology based on the MTU size of links so that regardless of basic topology changes a long packet cannot be routed to a link that cannot transmit it.
The advantages of the multiple topology routing approach are:

- it has **centralized approach** for determining area routes based on an area-wide view of the topology and traffic, rather than the local views at each router
- distributing the network feedback information to a single router instead of a number of edge routers introduces **less protocol overhead** and also simplifies the operation of the edge routers
- it supports **route pinning**, which allows the movement of some traffic from one path to another without disrupting the paths for other traffic
- **backup paths** may be included in a new topology, which allows faster rerouting in the event of a network failure, and also the physical network topology is always available as a backup for the edge routers

The disadvantages of the presented approach are:

- recalculating shortest paths for a number of topologies on topology changes may slow down routing in bigger networks, although the time required for calculations may be reduced by modifying the shortest path algorithms so that the paths are calculated in parallel

The implementation of subIP in IP networks may thus lead to better network utilization. The advantage of this approach comparing to optimizing link weights in routing protocols is in providing route pinning. Comparing to the approach of balancing the traffic among explicit routed paths, multiple topology routing requires simpler management. In the former case the number of explicit routes that needs to be established and maintained is in general, proportional to N^2, where N is the number of domain routers. The number of new topologies defined in the latter case cannot be grater than 16, which is determined by the 4 bit *control* field in subIP header. This is though a trade off with providing better quality of service (QoS). Still, to achieve satisfying QoS per path similar traffic engineering techniques need to be applied throughout the Internet. Simple multiple topology routing may thus be a good transient solution before the conditions for implementing more sophisticated traffic engineering techniques are globally fulfilled.

5 Further Developments

subIP may be extended with the MPLS connection-oriented service. The change required in the current MPLS header in order for it to inter-operate with subIP is that one of the three experimental bits (T) needs to be reserved to distinguish the two protocols. In the MPLS

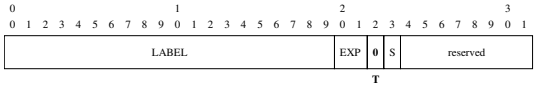


Figure 7: The Modified MPLS Header

header it should be set to 0. Given that the connectionless service is provided by subIP instead of MPLS hop-by-hop routing, this change may also allows the TTL field of the MPLS header to be redefined. In general, the TTL field is used with connectionless service to prevent packets from looping. Since with connection-oriented services loops cannot occur, in this case the ingress router may process the TTL field in the IP header of the packet by reducing it for the hop count of the explicit route (or an estimate of the path length). This will prevent packets that need more hops through the area than are allowed entering the area, there will be no TTL processing at each hop and the TTL field may be used for other purposes, such as defining different types of traffic, which is indicated in Fig. 4 by marking the field as *reserved*.
subIP can support a new protocol, independent of IP, as long as the maximum packet size of the protocol does not exceed the minimum subIP area MTU. This may be a new routing and signaling protocol to be used for explicit route establishment and distribution of the new subIP topology information (sLDP) (Fig. 8). A protocol

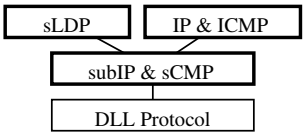


Figure 8: A New Routing and Signaling Protocol

implemented *on top* of subIP introduces less protocol overhead since the IP header is not included in protocol messages and also shorter area addresses may be used on defining paths. It also provides better network modularity.
While in MPLS the importance of explicit routing is emphasized in order to provide traffic balancing in an MPLS domain, we emphasize its importance in establishing virtual paths in order to build an arbitrary network topology. Together with the new addressing scheme that may be introduced by subIP it may be a step towards a multiple hierarchy network with hierarchical addresses with geographical significance which would

significantly simplify traffic engineering. A number of ASs may be grouped into a new subIP hierarchy level where the similar approach of routing applied within an AS may be introduced. However, the routing between the ASs is controlled with an Exterior Gateway Protocol, such as BGP, which is conceptually different from OSPF and additional topology and addressing information needs to be distributed in order to implement subIP, which is for further study.

6 Conclusion

In this paper we present a new approach for optimizing network utilization within an AS. It is based on the subIP protocol proposed in the paper.

subIP is a modification of the MPLS protocol which provides connectionless service similar to IP. It basically divides the Internet into small areas with local short subIP router addresses. The IP routing concept is then applied within the areas based on the new addresses. The new information is distributed in the 4 byte subIP packet header. Since subIP requires smaller forwarding tables and uses fast exact match table lookup on forwarding, it provides simpler and faster packet forwarding than IP.

Similar to MPLS hop-by-hop routing, subIP routes packets along the same path as IP. However, as opposed to MPLS hop-by-hop routing, the subIP concept does not require a label distribution protocol, which reduces protocol overhead and simplifies the protocol. The reaction of the protocol on topology changes is faster since forwarding tables are calculated based on available topology information, while the MPLS approach may introduce latency for redistributing the labels. The subIP also requires smaller forwarding tables and does not require label swapping on forwarding.

The disadvantage of the subIP is that it bounds the area size to 256 routers. Still, in view of future multiple hierarchy networks with small interconnected domains which provides better scalability and simpler management, this area size is acceptable.

The concept of traffic balancing within the area provided by subIP is based on defining different area topologies based on the physical area topology. The calculation of the shortest paths within the area based on the new topology information, but consistent at each area router, may give different results than calculations based on the physical topology. Using the *control* field of subIP, traffic is thus balanced among shortest paths belonging to different topologies. Some of the advantages of the approach are centralized control, route pinning and providing backup routes. It is also simple and may lead to a better network utilization.

The paper discusses subIP implementation in an AS implementing the OSPF routing protocol. Its new addressing scheme and the MPLS explicit routing which may provide virtual paths and thus arbitrary network topology may be a good step towards a new multiple hierarchy network with addressing scheme with geographical significance. This would significantly simplify traffic engineering. However, the subIP implementation with conceptually different exterior gateway routing protocols requires further study.

References

[1] R. Callon E. Rosen, A. Viswanathan. RFC 3031: Multiprotocol Label Switching Architecture, January 2001.

[2] Bernard Fortz, Jennifer Rexford, and Mikkel Thorup. Traffic engineering with traditional IP routing protocols. *IEEE Communications Magazine*, pages 118–124, October 2002.

[3] C. Hopps. RFC 2992: Analysis of an Equal-Cost Multi-Path Algorithm, November 2000.

[4] Information Sciences Institute. RFC 791: Internet Protocol, September 1981.

[5] J. Moy. RFC 2328: OSPF Version 2, April 1998.

[6] Radia Perlman. *Interconnections: Bridges, Routers, Switches and Internetworking Protocols, Second Edition*. Addison Wesley, September 2001.

[7] J. Postel. RFC 792: Internet Control Message Protocol, September 1981.