Building MPLS VPNs with QoS Routing Capability[1]

Peng Zhang, Raimo Kantola

Laboratory of Telecommunication Technology,
Helsinki University of Technology
Otakaari 5A, Espoo, FIN-02015, Finland
Tel: +358 9 4515454 Fax: +358 9 4512474
Email: {pgzhang@tct.hut.fi, raimo.kantola@tct.hut.fi}

Abstract. Recently MPLS is used for building up VPNs in IP backbone, called MPLS VPNs. In this paper, we discuss issues on finding routes with QoS requirements (i.e., QoS routing) in MPLS VPNs. We first present background on MPLS VPNs as well as QoS routing. Then we discuss both the benefits and problems resulted from introducing QoS routing into MPLS VPNs. We particularly present an architecture of MPLS VPNs with QoS routing capability, on which we discuss some important issues on running QoS routing in MPLS VPNs.

1. Introduction

With the rapid development of the Internet, there arise great interests in the deployment of Virtual Private Networks (VPNs) across IP networks. Many preliminary works have been done in this area. For example, a framework for IP based VPNs is proposed in [1], in which various types of VPNs, their respective requirements and mechanisms for implementations are discussed; An approach for building core VPN services in a service provider's MPLS backbone is presented in [2]; An extension to CR-LDP for VPNs is proposed in [3] by adding an optional VPN-ID TLV to CR-LDP label request message to identify the VPN that the request is meant for. In these documents, MPLS is believed to be a key technology for building up VPNs (i.e., MPLS VPNs) due to a number of reasons as follows.

- MPLS offers fast forwarding capability;
- MPLS connects sites through setting up label switch paths (LSPs) on which traffic engineering can be applied;
- MPLS provides supports for various L2 protocols, e.g., ATM, Frame Relay, etc.;
- MPLS supports signaling protocols, which can facilitate fast configurations of VPNs;
- MPLS is capable of scaling into very large networks.

Meanwhile, QoS is regarded as a key element of any VPN services. For example, services with stable and good qualities in terms of bandwidth and delay are expectedly offered in VPNs. Among various mechanisms of traffic engineering (e.g.,

[1] This work is supported by IPANA project which is carried out in Helsinki University of Technology.

S. Rao and K.I. Sletta (Eds.): INTERWORKING 2000, LNCS 1938, pp. 292-301, 2000.

traffic scheduling, resource management), QoS routing is one of the enhancing mechanisms for deploying quality classes into the IP networks[4]. The general objective of QoS routing is to improve the efficient utilization of network resources and to provide flexibility in support for various services. Therefore, QoS routing is expectedly used in MPLS VPNs. However, there still lacks insensitive study on this topic.

In this paper, we investigate the issues of QoS routing in MPLS VPNs. In particular, we present an architecture of MPLS VPNs with QoS routing capability as well as some methods for operating QoS routing in MPLS VPNs.

The remainder of this paper is organized as follows. In section 2, we describe the background on MPLS VPNs and QoS routing. In section 3, we discuss the benefits and problems resulted from introducing QoS routing into MPLS VPNs. We present and describe an architecture of MPLS VPNs with QoS routing capability in section 4. In section 5, we present and discuss some issues on operating QoS routing in MPLS VPNs. Some conclusions are given in the final section.

2. Background on MPLS VPNs and QoS Routing

In this section, we give the general information on MPLS VPNs and QoS routing. We describe the definitions and current status of some components as follows.

2.1 VPNs

A VPN is a set of sites which are attached to a common network (i.e., backbone), applying a set of specific policies (e.g., addressing, security, etc). VPN services are widely used for interconnecting sub-divisions of an organization or a company in multiple areas. VPNs are meant for sharing resources within VPNs.

Although VPN services have appeared for a few years, constructing VPNs across IP backbone is a relatively new topic [1]. There are two different methods to construct VPNs across IP backbone, i.e., CPE (Custom Premises Equipment) based and network based. Most current VPN implementations are based on CPE equipment. VPN capabilities are being integrated into a wide variety of CPE devices, ranging from firewalls to WAN edge routers. On the other hand, there is also significant interest in ‘network based VPNs’, where the operation of the VPN is outsourced to an Internet Service Provider (ISP), and is implemented on network as opposed to CPE equipment. This method attracts both customers seeking to reduce support costs and ISPs seeking new revenue sources. In this paper, we discuss QoS routing in network based VPNs. However, most of the methods presented in this paper can also apply to CPE based VPNs.

2.2 MPLS

MPLS integrates a label swapping framework with network layer routing [5]. Its basic idea involves assigning short fixed length labels to packets at the ingress to an MPLS cloud (based on the concept of forwarding equivalence classes) and making forwarding decisions accroding to the labels attached to packets throughout the interior of the MPLS domain. Thousands of papers on MPLS have been presented in various aspects including traffic engineering and implementations. MPLS is regarded as a key technology for realizing Differentiated Services (DiffServ) networks.

2.3 MPLS VPNs

VPNs are built up by using MPLS. A MPLS VPN can consists of that are from the same enterprise or from different enterprises and these sites may attach to the same service provider or to different service provider. If more than one different service providers are used, the bilateral or multilateral agreements should be pre-determined.

Moreover, MPLS based VPNs provide the following benefits [6].

- A platform for rapid deployment of additional value-added IP services, including intranets, extranets, voice, multimedia, and network commerce;
- Privacy and security are equal to layer-2 VPNs by constraining the distribution of a VPN's routes to only those routers that are members of that VPN, and by using MPLS for forwarding;
- Easy management of VPN membership and rapid deployment of new VPNs;
- Increased scalability with thousands of sits per VPN and hundreds of VPNs per service provider;
- Scalable any-to-any connectivity for extended intranets and extranets that encompass multiple businesses.

2.4 QoS

The QoS requirements for a service are generally clarified by a set of parameters such as bandwidth, delay and so on. Offering QoS guaranteed or assured services in the Internet is becoming more and more attractive. Great efforts have been devoted to this field in various aspects, e.g., traffic scheduling, resource management, QoS routing, etc[7].

2.5 QoS Routing

Constraint based routing, a general term of QoS routing, selects routes according to not just a single metric (e.g., hop count) but also additional routing metrics (e.g., bandwidth and delay) and administrative policies (e.g., access authentication). In particular, QoS routing provides support for alternate routing, for instance, if the best existing path cannot admit a new flow, the associated traffic can be forwarded in an adequate alternate path. QoS routing algorithms can prevent traffic shifting from one

path to another "better" path only if the current path meets the service requirements of the existing traffic. A framework for QoS routing in the Internet is presented in [8]. QoS routing has been introduced into OSPF as described in [9]. A large number of routing algorithms are summarized in [4]. Some mechanisms for operating inter-domain QoS routing in DiffServ networks are presented in [10].

2.6 QoS Routing in MPLS VPNs

MPLS supports explicit paths and alternative paths so that QoS routing can be naturally used in MPLS VPNs. QoS routing might be used in such cases as finding routes for connecting a number of sites into a VPN or setting up paths for sessions within VPNs. QoS routing is also believed to be one of the key components for supporting QoS in MPLS VPNs.

3. Benefits and Problems of QoS Routing in MPLS VPNs

QoS routing determines routes under the knowledge of network resource availability, as well as the requirements of flows. As a result, the performance of applications is guaranteed or improved in comparison with that without QoS routing. Meanwhile, QoS routing optimizes the resource usage in the network by improving the total network throughput. QoS routing is likely used for constructing an efficient and high performance MPLS VPNs. These benefits might be achieved in a number of ways as follows.

- QoS routing selects feasible routes by avoiding congested nodes or links;
- If workload exceeds the limit of existing paths, QoS routing offers multiple paths for transferring additional traffic;
- If a link or node failure occurs, QoS routing selects alternative paths for quick recovery without seriously degrading the quality.

However, these benefits of QoS routing also incur the cost of developing new routing protocols or extending the existing ones. Moreover, it potentially increases higher communication, processing and storage overheads. It brings out a number of problems as follows[8]:

- What kinds of resource information can be used for determining feasible routes?
- Which protocols are suitable for distributing route and resource information within domain or across multiple domains?
- How to select routes across multiple domains?
- How to balance the complexities and benefits of introducing QoS routing into the real networks?
- In which ways the cost of running QoS routing in MPLS VPN networks can be minimized?

Currently, there lacks deep and broad investigations on these problems although some work have already been carried on[9].

4. An Architecture for QoS Routing in MPLS VPNs

4.1 Architecture

We present the architecture as shown in Figure 1. A MPLS VPN is built up by connecting MPLS sites through tunnels across IP backbone. Each MPLS site has a Bandwidth Broker (BB), which is to exchange route and signaling information and to manage and maintain VPN networks.

A Central Bandwidth Broker (CBB) in IP backbone is likely used, however, not necessarily. If the IP backbone can provide QoS support, CBB performs similar functions as BBs in each MPLS site. BBs of each MPLS site can negotiate with the CBB in order to setup QoS guaranteed tunnels or sessions. CBB performs VPN management in a central way, for example, CBB determines the acceptance of a MPLS site into the MPLS VPN. CBB can be implemented in any router in IP backbone, or virtually in BB of a MPLS site.

Both BB and CBB have two major tasks related to route management:

- Finding routes for connecting a number of sites into a VPN;
- Setting up paths for sessions within VPNs.

The first task has a longer time scale than the second task. In this paper, we intend to focus on the second task.

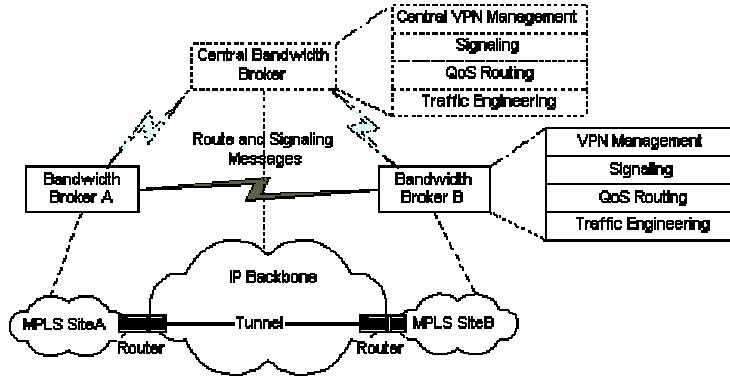

Fig. 1. An Architecture of MPLS VPNs with QoS Routing

Each bandwidth broker consists of a number of components, i.e., VPN Management, Signaling Protocol, QoS Routing and Traffic Engineering. VPN Management performs functions of management and administrative policies, e.g., addressing, access authentication, tunneling management, etc. Signaling Protocol is needed to setup tunnels between MPLS sites or sessions between applications of different MPLS sites. QoS routing is used for finding feasible routes for tunnels or sessions and for maintaining topology of MPLS VPNs. Traffic Engineering includes a

number of mechanisms (e.g., classifying, marking, shaping and queuing) for forwarding packets.

In practice, there are several candidates for implementing these components. For VPN Management, SNMP might be used; For Signaling Protocol, CR-LDP or Extended RSVP can be used; For QoS Routing, QOSPF or inter-domain QoS routing might be used; For traffic engineering, Integrated Service or Differentiated Service might be used.

The functions of these components can be understood by depicting the process of setting up a path for a flow with quantitative QoS requirements.

1. When a BB (or CBB) receives a request for a flow, it determines a set of possible routes and then selects a feasible route;
2. Once a path has been found, the BB (or CBB) assures that the flow follows the path;
3. The BB updates its local resource database and broadcasts the route and resource information to other nodes;
4. The BB marks the flow packets and polices the flow;
5. The BB monitors the link state to detect a link failure and performs rerouting in case link failure occurs.

4.2 QoS Routing Model

Since this paper focuses on QoS routing, we present an implementation of QoS routing component in Figure 2.

As shown in this figure, this model consists of three functional blocks (i.e., Policy Control, Route Computation & Selection, and Routing Information Advertise and Update) and three tables (i.e., VPN topology database, tunnels & sessions table, and tunnels & sessions routing table).

Policy Control exerts specified policies on finding routes and exchanging routing information. Route Computation & Selection determines routes based on the knowledge of topology information and policy constraints.

Routes are computed and saved into tunnels & sessions table for data forwarding. The tunnels & sessions table is used to store information related to specific flows, in terms of traffic parameters, requirements for QoS, etc. Routing Information

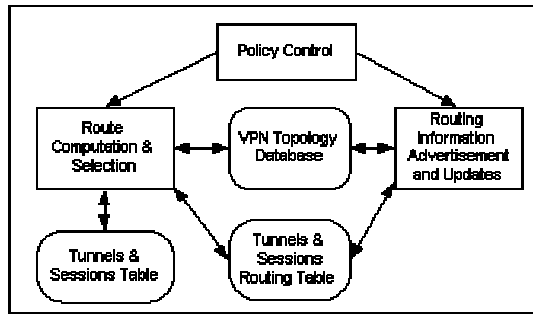

Fig. 2. An Implementation of QoS Routing

Advertisement and Update is in charge of broadcasting routing information (e.g., resource information, policy constraints, routes selected, etc) and updating local database when receiving VPN routing information from other sites.

Here, we introduce two simple routing algorithms: Lowest Cost (LC) algorithm and Widest Bandwidth (WB) algorithm[11].

Consider a directed graph *G=(N, E)* with numbers of nodes *N* and numbers of edges *E*, in which each edge *(i, j)* is weighted by two parameters, b_{ij} as the available bandwidth and c_{ij} as the cost. The cost is an additive parameter, e.g., hop number, delay, etc. Let $b_{ij} = 0$ and $c_{ij} = \infty$ if edge *(i, j)* does not exist in the graph.

Given any directed path $p = (i,j,k,\ldots,l, m)$, define $b(p)$ as the bottleneck bandwidth of the path, i.e., $b(p) = \min[b_{ij}, b_{jk},\ldots, b_{lm}]$, and define $c(p)$ as the sum of the cost, i.e., $c(p) = c_{ij} + c_{jk}+\ldots+ c_{lm}$. Given two nodes i and m of the graph and two constraints B and C. To LC algorithm, the QoS routing problem is to find a path p^* between i and m so that $b(p) \geq B$ and $c(p) \leq C$. To WB algorithm, the QoS routing problem is then to find a path p^* between i and m so that $b(p) \geq B$ and the path has the widest bandwidth, and if there are more than one widest paths the path with the lowest cost is selected. Let C_i be the estimated cost of the path from source node s to destination node t. Let B_i be the estimated bandwidth of the path from source node s to destination node t.

- LC algorithm

  Step 1: Set $c_{ij} = \infty$, if $b_{ij} < B$;

  Step 2: Set $L= \{s\}$, $C_i = c_{si}$ for all $i \neq s$;

  Step 3: Find $k \notin L$ so that $C_k = \min_{i \notin L} C_i$;

  If $C_k > C$, no such a path can be found and the algorithm terminates,

  If L contains node t, a path is found and the algorithm terminates.

  $L:=L \cup \{k\}$.

  Step 4: For all $i \notin L$, set $C_i:=\min[C_i, C_k+c_{ki}]$;

  Step 5: Go to Step 3.

- WB algorithm:

  Step 1: Set $b_{ij} = 0$, if $b_{ij} < B$;

  Step 2: Set $L = \{s\}$, $B_i = b_{si}$ and $C_i = c_{si}$ for all $i \neq s$;

  Step 3: Find set $K \subset L$ so that $B_K = \max_{i \in L} B_i$;

  Step 4: If K has more than one element, find $k \in K$ so that $C_i (s, \ldots, k, t) = \min_{i \in K} [C_{(s, \ldots, k, t)}]$. $L:= L \cup \{k\}$. If L contains all nodes, the algorithm is completed.

  Step 5: For all $i \notin L$, set $B_i:= \max[B_i, \min[B_k, b_{ki}]]$;

  Step 6: Go to Step 3.

Both algorithms first eliminate the link whose available bandwidth is below the required bandwidth and produces a new graph. Then, the former calculates path with the lowest cost by using Dijkstra's algorithm while the latter calculates the path with the widest bandwidth by using a variation of Dijkstra's algorithm.

The other important topic of QoS routing is cost. The cost of QoS routing includes three parts, that is, storage cost, computation cost and distribution cost. Usually, it mainly depends on the distribution cost. Therefore, the updating algorithm of route and resource information is very important. Here, we briefly present two updating algorithms as follows.

- The first algorithm, called Period Based algorithm (PB), performs update periodically.

- The second algorithm, called Threshold Based algorithm (TB), performs update when the variation of available bandwidth of the link exceeds a configured threshold.

5. Issues on Running QoS Routing in MPLS VPNs

In this section, we present and discuss some issues on running QoS routing in MPLS VPNs in the following subtopics.

- Distributing label and VPN attributes

In MPLS VPNs, labels and VPNs attributes (e.g., label ID, VPN ID, etc) can be distributed and maintained by using QoS routing protocols. Extensions to BGP for carrying label and VPN attributes in MPLS VPN are proposed in [2, 12]. One can construct different kinds of VPNs, by setting up the Target and Origin VPN attributes.

For example, label distribution can be piggybacked in the BGP Update message by using the BGP-4 Multiprotocol Extensions attribute[13]. The label is encoded into the NLRI field of the attribute. Label mapping information is carried as part of the Network Layer Reachability Information (NLRI) in the Multiprotocol Extensions attributes.

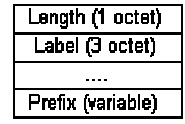

Fig. 3. Format of NLRI for label distribution in BGP-4

The Network Layer Reachability information is encoded as one or more triples of the form <label, length, prefix> as shown in Figure 3. The Length field indicates the length in bits of the address prefix plus the label(s); The Label field carries one or more labels; The Prefix field contains address prefixes followed by enough trailing bits to make the end of the field fall on an octet boundary.

The other alternative uses signaling protocol for distributing label and VPN attributes.

- Distributing route and topology information

QoS routing can be used for maintaining VPN topology within VPN. It is used for understanding not only the topology information but also resource states in VPNs, in which deliberate control and management can be applied. The resource states can be clarified with a number of parameters, e.g., bandwidth, delay, etc.

For example, BGP-4 can be extended for supporting traffic engineering[14]. The BGP update message will contain a new Optional Transitive attribute called TE Weight. The traffic engineering weights act as a cost or distance function, describing the quality of a path to a destination network in traffic engineering terms. Each TE Weight type could be:

- Maximum Bandwidth Available
- Maximum Number of IGP Hops

- Maximum Transit Delay
- Color
- Etc.

Therefore, the routes with quality information are distributed, then BGP Route Selection process is extended to select routes on the basis of the TE weights.

- Finding feasible routes

There are a number of algorithms for finding QoS routes in a single domain[4]. The two routing algorithms presented in section 4.2 are very promising and expectedly used in the real network because of their simplicities. On the other hand, both algorithm use *bandwidth* as the key parameter because in many cases *bandwidth* dominates the quality of service.

Moreover, some mechanisms for operating inter-domain QoS routing are proposed in [10]. In this case, Figure 4 illustrates the main functions and the procedures for setting up paths across domains. Signaling entity (SE) is a signaling agent of a MPLS site, while routing entity (RE) is a routing agent of a MPLS site running inter-domain QoS routing protocols. SE's functions include outgoing and incoming parts. The outgoing part collects QoS requests from interior routers and determine to initiate path setup requests; The incoming part processes path setup requests from other SEs. SE queries its local RE for external routes, and RE replies SE with next hops or whole routes. Note that the *path setup request* message usually contains the specifications of the flow and the requirements for QoS.

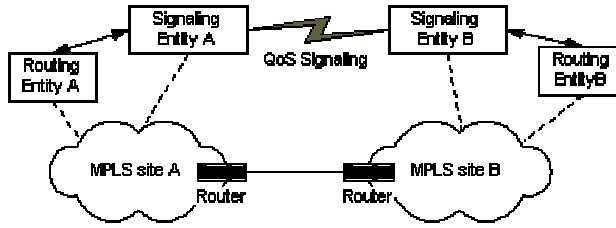

Fig. 4. Setting up paths across domain

We present five mechanisms for operating QoS routing across domains [10]:

1. SE based - crankback
2. SE based – flooding
3. Cache based Routing
4. *D*-hop resource routing
5. RE based source routing

For brevity, we just describe the first mechanism as follows.

When SE receives a *path setup request* message from an upstream SE, it first requests its local RE for next hop. If RE replies a non-blank next hop, SE checks if there is enough available resource on the link to that hop. If yes, SE adds itself to route list of the path and sends a request to that hop. If no, it requests the local RE for next hop again. If SE has queried RE for *K* times, SE sends a *path setup failure* message upstream. Here, *K* is a given constant. If SE receives a *path setup failure* message from downstream SE, it also requests its local RE for next hop again. A

feasible route will be found until the request reaches the destination. In this case, resource reservation is proceeded downstream.

This mechanism does not require RE to understand the global resource information, that is, there is no need for global topology and resource information database. As a result, advertising and updating resource information can be avoided. The current inter-domain routing protocol (i.e., BGP) can be directly used, except minor modifications on interface with SE.

6. Conclusions

MPLS is likely used in VPNs due to its distinguished merits, e.g., fast forwarding, tunneling, etc. QoS routing is naturally used in MPLS VPNs for providing feasible routes with considerations on QoS constraints. QoS routing is beneficial for developing QoS guaranteed MPLS VPNs across IP networks. In this paper, we investigate both benefits and problems when introducing QoS routing into MPLS VPNs. Particularly, we present an architecture of MPLS VPNs with QoS routing capability and discuss some issues on running QoS routing in MPLS VPNs. However, there are still a great number of open research problems concerning QoS routing in MPLS VPNs, e.g., methods of advertising and updating resource information, algorithms of computing routes, etc.

References

1. B. Gleeson, et al: A Framework for IP Based Virtual Private Networks. IETF RFC2764 (2000)
2. K. Muthukrishnan, et al: Core MPLS IP VPN Architecture. IETF Draft (2000)
3. P. Houlik, et al: Extensions to CR-LDP for VPNs. IETF Draft (2000)
4. Chen, S., Nahrstedt, K.: An Overview of Quality of Service Routing for Next-Generation High-Speed Networks: Problems and Solutions. IEEE Networks, Vol. 12, No. 6 (1998) 64-79
5. R. Callon, et al: A Framework for MPLS. IETF Draft (1999)
6. Cisco VPN Solution Center: MPLS Solution User Guide. Chapter 1 (1999) page 3-4
7. S. Blake, et al: An Architecture for Differentiated Services. IETF RFC2475 (1998)
8. E. Crawley, et al: A Framework for QoS-based Routing in the Internet. IETF RFC2386 (1998)
9. G. Apostolopoulos, et al: QoS Routing Mechanisms and OSPF Extensions. IETF RFC2676 (1999)
10. P. Zhang, R. Kantola: Mechanisms for Inter-Domain QoS Routing in Differentiated Service Networks. Accepted by QoS of future Internet Services (QofIS'2000). Berlin (2000)
11. Z. Wang and J. Crowcroft: Quality of Service Routing for Supporting Multimedia Applications. IEEE JSAC, Vol.14, No.7 (1996) 1228-1234
12. P. Houlik, et al: Carrying Label Information in BGP-4. IETF Draft (2000)
13. T. Bates, et al: Multiple Extensions for BGP-4. IETF RFC2283. (1998)
14. B. Abarbanel, S. Venkatachalam: BGP-4 Support for Traffic Engineering. IETF Draft (2000)