COMPARISON OF PACKET-SWITCHING AND LABEL-SWITCHING FOR ROUTING IN VPN-BASED NETWORKS

Nader F. Mir  
Department of Electrical Engineering  
San Jose State University  
San Jose, California 95192, U.S.A  
nader.mir@sjsu.edu

Devang K. Doshi  
Department of Electrical Engineering  
San Jose State University  
San Jose, California 95192, U.S.A  
doshi.devang@yahoo.com

Maulik B. Gandhi  
Department of Electrical Engineering  
San Jose State University  
San Jose, California 95192, U.S.A  
gandhimb@gmail.com

ABSTRACT

The contribution of this paper is to study Virtual Private Networks (VPNs) and compare them under two different types of conditions. One type of VPNs is supported by regular Internet Protocol version 4 (IPv4) and the other type by multi-protocol label switching (MPLS). The comparison will be in terms of CPU and bandwidth usage. We will show that MPLS is a better choice compared with IPv4 in terms of packet processing capability and bandwidth usage. We will show that MPLS technology is scalable in terms of CPU processing and bandwidth usage. The MPLS and IPv4 VPNs are simulated over the NS2. The comparison is made between MPLS and IPv4 networks in terms of bandwidth usage by applying routing protocol details and CPU usage for each technology. Various network performance parameters are compared with the help of trace file generated from the simulations of the MPLS and IP networks. The project achieved far better results for MPLS when compared to IPv4 network.

KEY WORDS

Label Switching, VPNs, IPv4, Routing in Computer Networks

1. Introduction

Due to the many new bandwidth greedy applications, it is very much required to build scalable and economical networks. Every day new voice and multimedia applications are being developed and getting deployed. Internet applications include online games, movies, video conference, Pod cast lectures and VoIP communication, and so on. All these applications require huge amount of bandwidth in the backbone network to work smoothly. These bandwidth greedy applications put extra strain over the existing Internet structure. Apart from extra strain over the network, there are many challenges to transport the traffic over the Internet with differentiating class of services. To decrease the delay in the network, there is a need for high speed switching of the data packets. With the evolution of IPv6 and IPv4 still in place, it is essential to have these two networks be compatible. To find solutions to all these challenges is a tough situation which the service providers are facing today.

Multi-protocol label switching (MPLS) [1][2] is one solution to the mentioned problems. With MPLS, the scalability of the network increases and the delay decreases. MPLS supports the transfer of multiprotocol data. MPLS employs traffic engineering techniques to effectively implement peer-to-peer VPNs [3][4]. The division of MPLS controlling and forwarding applications has given rise to multilayer, multiprotocol interoperability between layer 2 and layer 3 [2][7]. MPLS makes use of small labels instead of IP address to forward packets. The label has local meaning between two routers.

In the remaining portion of this paper, we present VPNs of types label switching or packet switching networks and compare the results of their performance.

2. Use of Label Switching

MPLS has helped in removing dependencies on layer2 and layer 3 of TCP/IP suite. The forwarding of packet is simplified with less delay. One can have multiple packets with the same label. With the help of RSVP one can get better scalability of multicast VPN service [6][8].

MPLS routers are known as label switched routers. The routers on the edge of the network called ingress Label Switched Routers (LSRs) forward packets coming from customer site into the core MPLS network. The routers on the edge forward the data from core of the MPLS network to the customer site are known as egress LSRs. The routers that are in the core of MPLS networks are known as core LSRs [3]. Border Gateway Protocol (BGP) packets update for least cost path entries of the routing table. The routing of the packets will be label based. The ingress LSRs check the IP address and attach appropriate label. The core LSR replaces an incoming label with outgoing label with the help of forwarding table. The egress LSR removes the label and forwards the IP data packet to appropriate destination with help of IP routing table as shown in Figure 1.

A label contains the forwarding information of the packet. Router A makes the decision based on the label of incoming
packet. The core LSR forwarding table swaps the incoming label (5) with outgoing label (8) as seen in Figure 2. The outgoing label indicates the output port from which the packet needs to be forwarded. Labels also help in providing quality of service information. Based on the labels the packets can be stored at appropriate quality of buffer depending on the size and service time by the traffic classifier as shown is Figure 2.

Label switched paths (LSPs) are unidirectional predefined connections according to the network topology. LSP is always defined between ingress and egress LSRs. Each LSP acts as if it is a tunnel. MPLS network can realized as virtually fully connected network. In Fig. 3, the LSP for IP packet 1 will be <LSR1, LSR3, LSR5, LSR7>.

In MPLS, group of packets are forwarded in the same way depending on their destination and route. This group of packets belongs to the same FEC. As one can see in Fig. 3. IP packet 1 coming from LSR1 going to LSR3 has label 31 and IP packet 2 coming from LSR2 going to LSR3 has label 32. But, when both these packets leave LSR3 they will have same label 51 as they have the same destination and same path.

MPLS is very helpful in implementing different applications. One such application of MPLS is in implementing Virtual Private Networks. MPLS VPNs are based on peer models. In IP based VPNs one had different tunneling on IP backbone. This type of overlay networks used to be a burden on the networks. In MPLS VPN, the service provider network acts as a peer to the Customer edge router. The peering is not between two Customer Edge (CE) routers. As a result, the number of peers a CE router has is constant irrespective of the number of total VPN sites. This helps in managing thousands of sites within that particular VPN. If a new site needs to be added the service provider just needs to connect the site with a Provider Edge (PE) router. Also, in MPLS, every data packet is associated with a particular Label Switched Path. Every LSP exists only between ingress LSR and egress LSR. At each PE router the forwarding table is configured for a particular input port. Thus the each particular VPN will have its unique input port. This will protect from any unwanted data.

LDP is used to distribute label bindings amongst the LSRs. Any ingress LSR will identify all its neighbors. The upstream LSR will assign Forwarding Equivalence Class (FEC) based on the destination. The upstream LSR will request the downstream LSR for a label binding. The downstream LSR will send the binding label and the upstream LSR will construct the forwarding table consisting of the Destination, out label and output port. Core LSR will only have in label and corresponding out label and output port. The egress LSR will have the in label and the corresponding IP Destination and the output port from which the packet should be forwarded.
directed to VPN from coming at any other port of the VPN [2]. As the routing happens with the help of label there is less delay in the switching of the packets.

3. Simulation VPNs and Results

For the simulation purposes, we have used network simulator tool NS2. Network Simulator 2 is a discrete event network simulator. It is written in C++/OTcl/Tcl [5]. It is used very much in routing protocols, multicast and ad-hoc networking. Network Simulator 2 supports both wired network and wireless network simulation [5]. Figure 4 shows the topology created for the MPLS and IPv4 networks.

The simulation is run for 40 seconds. Host A sends different sizes of data packets to Host C, while Host B sends different sizes of data packets to Host D for different simulation instances. The network characteristics are set as Link Delay = 10ms, Link Bandwidth = 3Mb, Burst time = 3 seconds and Idle rate = 2 seconds. With these characteristics, the simulations were run for different packet sizes of 100B, 300B, 500B, 800B, 1000B, 3000B and 6000B.

The data for both MPLS and IP networks are collected. All the network characteristics like delay, number of packet loss and number of routing packets are found out using the trace files and .awk scripts. The very first observation of simulation is that the throughput is the same for 1000 bytes, 3000 bytes and 6000 bytes because the maximum transfer unit is 1000 bytes. So the 3000 bytes and 6000 bytes of data packets are fragmented and sent as 1000 bytes of data packets. The number of routing packets in IPv4 network is around 1757, almost double of the number of MPLS routing packets which is 927. Thus MPLS networks also help in saving the bandwidth.

Figure 5 shows a comparison between the maximum delay in MPLS and in IP network. The X-axis represents the packet sizes in bytes. The Y-axis represents the maximum delay in seconds. Results improve as the packet size increases. Although there was not much of difference between the maximum delay of MPLS and IP networks, Figure 6 shows there is considerable difference in the minimum delay between the two networks. MPLS has far better results.

Figure 7 shows the average delay of the data packets in the MPLS and the IP networks. With the help of AWK scripts, the delay of every packet was added and divided by the total number of packets. Again the Figure clearly shows better result for the MPLS VPN.

Figure 8 shows the number of lost packets that we experience during the simulation of both the networks. The X-axis represents the packet size while the Y-axis represents the number of packets lost. As the number of data packets generated is more when the packet size 100 bytes it
experiences the most loss. But the total byte lost in the network is almost constant for different sizes of data packets. Figure shows that packet loss in IPv4 network is more than MPLS network.

Figure 9 presents the maximum throughput (data size of the packet / minimum delay) of the MPLS and IP networks. The X-axis represents the packet size while the Y-axis represents the throughput (Kbytes/second). As in all other cases, MPLS is better than IP when the network throughput is considered.

4. Conclusion

This paper studied various VPNs in terms of CPU usage and bandwidth usage. MPLS is a better choice compared with IPv4 network in terms of packet processing and bandwidth usage. Peer-to-peer VPN does not provide isolation and Overlay networks do not provide scalability. MPLS is better VPN in terms of scalability, packet processing and packet loss. The paper compares MPLS network and an IPV4 network using network simulation tool NS2. Results are analyzed using Figures and tables. The analysis of the trace files, which are generated by the simulations; helps in proving the advantages of an MPLS model over an IP network. The traffic characteristics and network parameters are kept same for both the networks. The difference in results between the networks is based on technologies. The various test cases are generated based on different packet size. The simulations were run with different sizes of data packets to show the consistency of MPLS based VPNs over IPv4 networks. The results of the simulation clearly shows that MPLS based networks have less minimum delay, maximum delay and average delay. The better results of MPLS for delay prove faster processing of the packets. Number of packets generated by IP routing protocols are more than the MPLS LDP. Thus, less bandwidth is consumed in MPLS networks for routing of packets. Also we see that the number of packets lost is more in IP network than in MPLS network. It has the advantages of a peer-to-peer model. MPLS VPNs are better scalable, easy to manage and provide good security. MPLS VPNs have all benefits that the service providers are looking for at this point of time.

References