Volume 3, Issue 6, June 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Analyzing Multi Protocol Label Switching Network

Ravindra Kumar Gupta*, Arvind Kumar Singh*, Pankaj Singh#, Omjeet Singh$,

** Sri Satyasai Institute of Science and Technology,Bhopal, India*

 # UCER, Allahabad, India

$HMFAMIET, Allahabad India

Abstract: Multiprotocol Label Switching (MPLS) is a differentiated and scalable framework introduced by IETF, which uses simple configuration & management to deliver end-to-end IP services. It enables the network devices to specify path based on Quality of Service (QoS) and bandwidth requested for those applications by changing the hop-by-hop paradigm. Fault tolerance is the ability of the system to respond gracefully to an unexpected hardware or software failure. By using fault recovery techniques we can make MPLS network fault tolerant. Traditional IP networks have many limitations such as routing tables, which can be complex and time consuming. These limitations affect the performance of the network in some applications of triple play services (i.e., voice, video and data) which may be delay sensitive applications. Thus, the main impetus behind Multi Protocol Label Switching (MPLS) technology proposed to speed up the traffic flow in the network using labels.

Keyword: MPLS, LSR, LSP, LER, FEC.

1. Introduction

Multi-Protocol Label Switching (MPLS) is growing in popularity as a set of protocols for provisioning and managing core networks. The networks may be data-centric like those of ISPs, voice-centric like those of traditional telecommunications companies, or one of the modern networks that combine voice and data. These networks are converging on a model that uses the Internet Protocol (IP) to transport data. MPLS overlays an IP network to allow resources to be reserved and routes pre-determined. Effectively, MPLS superimposes a connection-oriented framework over the connectionless IP network. It provides virtual links or tunnels through the network to connect nodes that lie at the edge of the network. A well-established requirement in telephone networks is that the network should display very high levels of reliability and availability. Subscribers should not have their calls dropped, and should always have access to their services. Downtime must consequently be kept to a minimum, and backup resources must be provided to take over when any component (link, switch, switch sub-component) fails. The data world is increasingly demanding similar levels of service to those common in the arena of telephony. Individual customers expect to be able to obtain service at all times and expect reasonable levels of bandwidth. Corporate customers expect the same services, but may also have data streams that are sensitive to delays and disruption. As voice and data networks merge they inherit the service requirements of their composite functions. Thus, modern integrated networks need to be provisioned using protocols, software and hardware that can guarantee high levels of availability. High Availability (HA) is typically claimed by equipment vendors when their hardware achieves availability levels of at least 99.999% (five 9s). This may be achieved by provisioning backup copies of hardware and software. When a primary copy fails, processing is switched to the backup. This process, called failover, should result in minimal disruption to the data plane. Network providers can supply the required levels of service to their customers by building their network from equipment that provides High Availability. This, on its own, is not enough, since network links are also prone to failure, and entire switches may fail. The network provider must also provide backup routes through the network so that data can travel between customer sites even if there is a failure at some point in the network. Multi-Protocol Label Switching (MPLS) is rapidly becoming a key technology for use in core networks, including converged data and voice networks. MPLS does not replace IP routing, but works alongside existing and future routing technologies to provide very high-speed data forwarding between Label-Switched Routers (LSRs) together with reservation of bandwidth for traffic flows with differing Quality of Service (QoS) requirements.

MPLS uses a technique known as label switching to forward data through the network. A small, fixed-format label is inserted in front of each data packet on entry into the MPLS network. At each hop across the network, the packet is routed based on the value of the incoming interface and label, and dispatched to an outwards interface with a new label value. The path that data follows through a network is defined by the transition in label values, as the label is swapped at each LSR. Since the mapping between labels is constant at each LSR, the path is determined by the initial label value. Such a path is called a Label Switched Path (LSP). MPLS may also be applied to data switching technologies that are not packet based. The path followed by data through the network is still defined by the transition of switching labels and so is still legitimately

called an LSP. However, these non-packet labels (such as wavelength identifiers or timeslots in optical networks) are only used to set up connections, known as cross-connects, at the LSRs. Once the cross-connect is in place all data can be routed without being inspected, so there is no need to place the label value in each packet. Viewed another way, the wavelength of timeslot is itself the label. At the ingress to an MPLS network, each packet is examined to determine which LSP it should use and hence what label to assign to it. This decision is a local matter but is likely to be based on factors including the destination address, the quality of service requirements and the current state of the network. This flexibility is one of the key elements that make MPLS so useful. The set of all packets that are forwarded in the same way is known as a Forwarding Equivalence Class (FEC). One or more FECs may be mapped to a single LSP.MPLS enhances the services that can be provided by IP networks, offering scope for Traffic Engineering, guaranteed QoS and Virtual Private Networks (VPNs).

The IP protocol itself is a routed protocol, carrying payload across IP domains toward a specific destination. The destination prefix and next-hop should be known ahead of time along each node across the most likely path to be taken by the network traffic. Within an organizational domain, populating routing table at each node is the responsibility of routing protocols like, Interior Gateway routing Protocol (IGP) or it can be done in conjunction with an Exterior Gateway routing Protocol (EGP). Routing protocols use IP as underlying communication protocol to exchange control plane information dynamically among different nodes for proper path setup. Routing protocols have their own transport layer mechanism to handle reliable transmission of their control messages. Whenever network statistics change, control information is exchanged among routing processes running at each intermediate node that are working in a coordinated fashion. Variable network statistics is one of the reasons for unordered packet delivery of IP packets to an end system or in severe situation lead to packet drop [2]. The reason behind these intricate situations is that different IP packets sharing a common source and destination may be forwarded along different paths. Network states might change as a result of link statistics update, or failure scenario. In both situations, nodes connected to affected interfaces first update this information in their database tables (which might not be the routing table) and advertise it to other neighbors participating in building up a snapshot of domain topology. Hence, it is the responsibility of each and every node to keep its database updated, so that an incoming IP packet may route in an optimal way. A topological information update requires a number of advertisements to be exchanged among participating nodes. In case of Distance Vector Routing Protocols (DVRP) like RIP (Routing Information Protocol) and EIGRP (Enhanced Interior Gateway Routing Protocol) the updated information is exchanged between the connected neighbors and they advertise only the known best paths reachable through them, resulting in distributed route calculation [2]. In Link State Routing Protocols (LSRP) like ISIS and OSPF an updated information is exchanged with each and every LSRP capable router [2] or a single designated router (centralized calculation), with the exception that ISIS exchange whole of its link states information updates in Link State Advertisements (LSA) while OSPF only advertise the local link information that is changed [6], [7]. Thus, different sizes of update advertisements need to be processed by a node running a specific or multiple routing protocols. In an IP network running LSRP, each IP capable node maintains LSDB (Link State Data Base) of all received LSA. Dijkstra's Shortest Path First (SPF) [7] is the algorithm used by the LSRP to calculate the cost of reaching a remote destination with minimal resources involved along the path. The LSDB must be synchronized among participating nodes. Every node has a consistent view of the network topology with synchronized LSDB. This synchronized LSDB is given as an input for the SPF calculation. Each node starts SPF algorithm by first considering itself as root node of a tree and then computes a cost to reach different nodes by populating the leafs, hence making the Shortest Path Tree. SPT once built at each participating nodes ultimately populates routing table also known as Routing Information Base (RIB). This SPF algorithm then runs on new incoming Link State Advertisement (LSA). A disadvantage of SPF calculation is that it's processing increases with the number of nodes involved in the routing process. To overcome this calculation load, the LSA updates are localized within small network portions. An LSRP domain is thus divided into different areas and mostly LSA is restricted within a defined area boundary. A summary of steps performed by different LSRP nodes to compute a common snapshot of topology in IP domain is provided by [4]:

IGP Convergence = D + O + F + SPT + RIB + DD

Where D is the link state update detection time, O is the time to originate LSA, F is the complete flooding time from node detecting the failure, SPT is shortest path tree computation time, RIB is the time to update Routing Information Base as result of SPT computation and DD is the time to distribute the FIB (Forwarding Information Base) update. The FIB is a topology driven database implemented in hardware. An entry in FIB corresponds to a RIB entry. FIB keeps an update copy of RIB entries in its cache to decrease lookup delay and increases device packet processing throughput. An LSA update triggers SPF calculation among the nodes and often results in traffic drop for the amount of time elapsed during link state topology convergence among participating nodes. This amount of elapsed time is critical for traffic with real time applications.

2. Motivation

MPLS (Multi Protocol Label Switching) is renowned in the service provider's network as one of the core protocols providing reliable, fast and efficient packet switching across a domain. It comes into play with increasing demand by customers for high service quality regarding their application requirements. The service providers consequently implement this cutting edge technology in their network domain to utilize and manage the resources in a cost effective flexible way, with a surety to stay in business for long time. MPLS provides its functionality in a way that the intermediate devices need not to re-process the network layer information, attached with each packet traversing the MPLS network. Despite label lookup at

each node, the intermediate nodes do forwarding decisions by just using the MPLS Label (more specifically the MPLS Header) attached to the labeled packet. This single piece of information (label) is easily implemented in hardware (as compared to network layer header information). MPLS brings the routing down to hardware level in a smooth fashion and below the network layer, thus acting as double edge sword lowering the latency inherited by packets across a domain [2]. The customers to a service provider network have no concern about the implemented technologies; they just desire guaranteed services through a provider's network. MPLS take this factor into account by reusing IP quality of service architecture for the applications running over it. More and more features are added to make the MPLS network architecture with the passage of time, making it a fault tolerant architecture to rely on. The main focus of this dissertation work is to study and analyze the fault tolerance mechanism inside IP and MPLS networks. It is likely that a reader of this dissertation will be able to figure out the operation of next generation networks and basis for the standards currently under development (like MPLS-TP) at IETF for convergence of data and voice/video over IP, using MPLS as underlying technology. The basic operation of an MPLS network is shown in the diagram below.

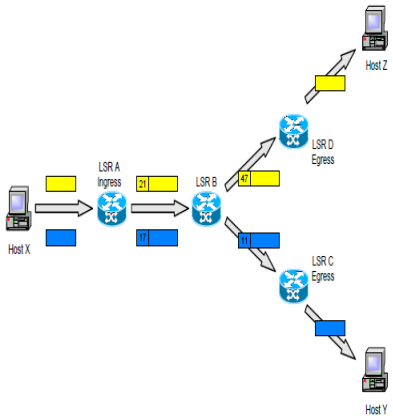

Figure 1.1: Two LSPs in an MPLS Network

3. Methodology for MPLS Network

For fault tolerance in MPLS networks there are several schemes and algorithms are developed, some of them are related to the domain of "Protection Switching" and some of them are "Rerouting". They are generally tested on major criteria's like, Recovery Time, Packet Loss and Multiple Fault Tolerance. Most important criteria we focused are multiple fault tolerance though it is very rare but has strong impact on the reliability of the network. The two major types of recovery schemes that are used for MPLS recovery are Protection Switching and Rerouting are being explained here along with some other aspects of MPLS networks.

3.1 Protection Switching

Protection switching is a recovery scheme in which recovery label switch path(s) are pre-computed or pre-established before a failure occurs on the working label switch path. When the fault occurs and Path Switch LSR (PSL) receives the Fault Identification Signal (FIS), PSL switches the traffic to the pre-established recovery path. As the recovery paths are pre-established so PSL immediately transfers the traffic on the backup path after receiving the FIS this makes protection switching faster than rerouting. Resources required for the establishment of recovery path are reserved. Protection switching pre-establishes a recovery path or path segment based on network routing policies, the restoration requirements of the traffic on the working path and administrative considerations.

3.2 Rerouting

Rerouting, a fault recovery technique where a recovery path is established on demand after a fault occurs. The recovery path can be based on fault information, network routing policies and network topology information. An advantage of fault recovery by rerouting is that it does not take up any backup resources in the network before the recovery path is signaled. The new paths may be based upon fault information, network routing policies, pre-defined configurations and network topology information. Thus, on detecting a fault, paths or path segments to bypass the fault are established using signaling. On the other hand rerouting has the disadvantage that resources may not be available at the time of computing recovery path that may leads to major failures.

3.3 Placement of Recovery Path

After the computation of recovery path or if the path is pre-computed by protection switching technique, path can be place locally or globally.

Local Repair, in local recovery, the recovery path selection or switching is done by a label switch router (LSR), which is nearest to the failed router or link. The main function of local repair is to fix the problem at the point of failure or within a very short distance from the failure for minimizing total packet loss and recovery time. In other words local repair aims to protect against a link failure or neighbor node failure and to minimize the amount of time required for propagation of failure signal. If a repair can be performed local to the device that detects the failure, restoration can be achieved faster. In local repair, the immediate upstream LSR of the failure is the LSR that initiates the recovery operation.

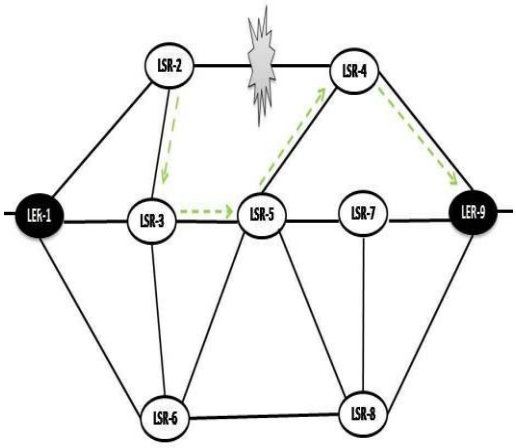

Figure 1.2: Local Repair.

Global Repair, in global recovery the alternative backup path selection is done by Protection Switch LSR. There is an alternative LSP that is pre-established or computed dynamically from ingress to egress routers. Ingress router is the entry point of MPLS network and Egress router the end point of MPLS Network. In other words global repair protect against any link or node failure on a path or on a segment of a path. In global repair the Point of Repair (POR) is distant from the failure and needs to be notified by a FIS. Recovery path is completely disjoint from the working path. This has the advantage that all links and nodes on the working path are protected by a single recovery path and having the disadvantage that a FIS has to be propagated all the way back to the ingress LSR before recovery can start.

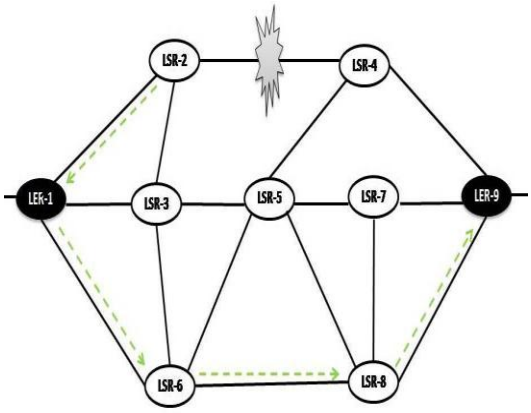

Figure 1.3: Global Repair.

3.4 Traffic Engineering

MPLS is today mostly used for traffic engineering and I will therefore start by describing what traffic engineering is and why traffic engineering is needed. In a sense, IP networks manage themselves. A host using the Transmission Control Protocol (TCP) adjusts its sending rate according to the available bandwidth on the path to the receiver. If the network topology should change, routers react to changes and calculate new paths to the destination. This has made the TCP/IP Internet a robust communication network. But robustness does not implicate that the network runs efficiently. The interior gateway protocols used today like OSPF and ISIS compute the shortest way to the destination and routers forward traffic according to the routing tables build from those calculations. This means that traffic from different sources passing through a router with the same destination will be aggregated and sent through the same path. Therefore a link may be congested despite the presence of under-utilized link in the network. And delay sensitive traffic like voice-over-IP calls may travel over a path with high propagation delay because this is the shortest path while a low latency path is available.

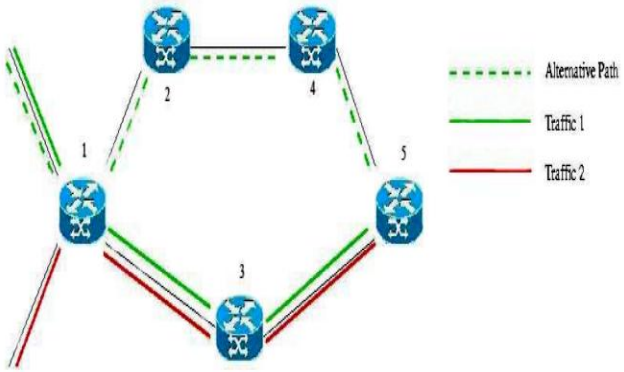

Figure 1.4 Traffic engineering

As illustrated in the above figure the shortest path from router 1 to 5 is the path (1-3-5). All traffic passing through router 1 with destination router 5 (or another router with router 5 in the shortest path) will travel through this shortest path if the shortest path algorithm is used for forwarding in this network. Although there is an alternative path (1-2-4-5) available that could be used to distribute traffic more evenly in the network. Traffic engineering is the process of controlling how traffic flows through a network to optimize resource utilization and network performance. Traffic engineering is basically concerned with two problems that occur from routing protocols that only use the shortest path as constraint when they construct a routing table. The shortest paths from different sources overlap at some links, causing congestion on those links. The traffic from a source to a destination exceeds the capacity of the shortest path, while a longer path between these two routers is under-utilized. As we will see later MPLS can be used as a traffic engineering tool to direct traffic in a network in a more efficient way then original IP shortest path routing. MPLS can be used to control which paths traffic travels through the network and therefore a more efficient use of the network resources can be achieved. Paths in the network can be reserved for traffic that is sensitive, and links and router that is more secure and not known to fail can be used for this kind of traffic.

The true benefit of deploying MPLS inside a network lies in traffic engineering. Traffic engineering (TE) is the process to steer traffic around a network, while maintaining requirement that the path taken will be an optimal path for the network traffic that belongs to a particular class. This optimal path is not along the IGP shortest path for all time. Strictly speaking traffic engineering (TE) is a form of congestion avoidance mechanism, to avoid congestion from occurring along the best path (shortest path) which carries all traffic. TE is used as the congestion may results by inefficient mapping of traffic streams onto network resources. TE used to avoid long term congestion; it has nothing to do with short term congestion caused by busty traffic. TE is a process in its own, used to measure, analyze network behavior and be applied to traffic pattern to achieve certain goals. In data communication world, TE provides an integrated approach to engineer traffic at layer 3 of OSI. TE hence controls the path along which data flows.

Traffic engineering using MPLS integrates label swapping framework with network layer routing. Incoming IP packet gets classified at the ingress and is assigned a label corresponding to a destination. Traffic engineering label is assigned to this labeled packet to further define the circuit to be taken for labeled packet across the network. TE thus provides benefits similar to overlay model but without separate layer-2 network architecture as provided by ATM or Frame Relay. MPLS-TE further enhances the IP-DiffServ architecture, as it is not mostly preferred to send different applications traffic, having diverse characteristics along the same path and treated in the same way. Such TE is not possible in IP network with flexibility like this, as it is provided by MPLS enabled network. IP routing is destination based and each node along the path independently follows the least cost principle to get traffic around network as quickly as possible. The only possibility with IP traffic engineered network is to manipulate the link cost so that a specific link lies along the least cost path for a specific traffic. But, manipulation is not a solution for larger networks as topology changes more often. Manipulation may result in suboptimal routing across a network domain, and besides getting more from a network the operators are paying more for using metric manipulation. The difference between network engineering and traffic engineering is [13]:

Network Engineering: The process of manipulating network to suit for a traffic requirement, results in installing new infrastructure as required depending upon traffic flows.

Traffic Engineering: The process of manipulating traffic to better utilize deployed network resources. MPLS TE, attempts to take the best of connection oriented traffic approach and merge it with IP routing. [RFC-2702] layouts the requirement for traffic engineering but gives rise to the so called "Fish Problem" [8, 13], shown in figure 3.1. Consider all links being equal cost for IP routing traffic flowing from source A or B will always take the path C-G-D There is no way to utilized the C-E-F-D path unless the link metric along that path is manipulated and makes ECMP or better than primary link. This is partial solution for network traffic originating from A or B, what if traffic is also originated from E or G; this leads to suboptimal scenario using IP capabilities in providing true TE. MPLS switching follows source based path. In MPLS network, head end has the capability to decide a path through the network for a particular FEC. For specific application traffic, head-end C

decides either to use LSP along the path C-G-D or LSP along the path C-E-F-D. MPLS-TE decouples the routing and forwarding [16]. The building block for MPLS-TE involves RSVP-TE and CR-LDP [8] [11] [14]. CR-LDP stands for Constraint Routing LDP, i.e. the original LDP protocol with new constraints across the network links, to be taken into account while calculating the path for an LSP. RSVP-TE is tweaked version of RSVP signaling protocol.

4. Aims and Objective

The main goal of this work is to understand the IP network resilience to a failure situation inside an internet realm. Network resource failure leads to traffic drops in worst condition and results in initiating new calculation around a failed resource. This will analyze IP network capabilities in handling such failure situation in accordance with the MPLS network architecture. An analysis using study of various facts was carried out to understand the impact of MPLS technology on the traditional IP networks.

5. Summary

I described the basics of MPLS and explained some of the properties of MPLS that can be used for traffic engineering. The main property of MPLS that makes it useful for traffic engineering is the possibility to compute a path from source to destination that is subject to a set of constraints, and forward traffic along this path. Forwarding traffic along such a path is not possible with best effort IP routing, since the IP forwarding decision is made independently at each hop, and is based solely on the packet's IP destination address. MPLS can easily achieve to forward traffic along an arbitrary path. The explicit routing capabilities of MPLS allow the creator of the LSP to do the path computation, establish MPLS forwarding state along the path, and map packets into that LSP. Once a packet is mapped onto an LSP, forwarding decisions are based on the label, and none of the intermediate hops makes any independent forwarding decisions based on the packet's IP destination.

References:

1. Had .M, Geo .C, Pap .M, Vass .V "A Haybrid Fault- Tolerant Algorithm for MPLS Networks", *WWIC 2008, LNCS 5031*, pp. 41-52, 2008.
2. Jack Foo. "A Survey of Service Restoration Techniques in MPLS Networks".
3. Alar .V, Tak .Y.L, Mar J.C, Gue L.G, "MPLS/IP Analysis and Simulation for the Implementation of Path Restoration Schemes".
4. Johan Martin. Thesis on "MPLS Based Recovery Mechanisms", 2005.
5. CISCO. Multiprotocol Label Switching CICSO.
6. Ahn .G, Chun .W, "Design and Implementation of MPLS Network Simulator Supporting LDP and CR-LDP". The *Proceedings of the IEEE International Conference on Networks (ICON'00).*
7. Kaur .G, Kumar .D, "MPLS Technology on IP Backbone Network", *International Journal of Computer Applications (0975-8887)*, 2010.
8. Sharma .V "Framework for Multi-Protocol Label Switching (MPLS)-based *Recovery", RFC-3469*, Ferruary 2003.
9. Andersso .L "LDP Specification", *RFC-5036*, October 2007.
10. Rosen .E "Multiprotocol Label Switching Architecture", *RFC-3031*, January 2001.
11. Shew .S "Fast Restoration of MPLS Label Switched Paths", *draft-shew-lsp-restoration-00*, October 1999.
12. Qiu .Y, Che .J, Gu .J, Xin .X "A Simulation for MPLS Global Recovery Model", *First International Conference on Intelligent Networks and Intelligent Systems, IEEE* 2008.
13. Alo .S, Aga .A, Nou .A"A Novel Approach for Fault Tolerance in MPLS Networks", IEEE 2006.
14. Thomas H. Cormen et al., "Introduction to Algorithms," Second Edition, MIT Press, 2001
15. G. Ahn, J. Jang, and W. Chun, "An Efficient Rerouting Scheme for MPLS-Based Recovery and Its Performance Evaluation," Telecommunication Systems, Vol. 19, No. 3, 2002
16. Alouneh .S, A. En-Nouaary .A, and Agarwal .A: MPLS security: an approach for unicast and multicast environments. Annales des Télécommunications, Vol. 64, No.5-6, pp. 391-400, 2009.
17. Hundessa .L and Pascual J. D., "Optimal and Guaranteed Alternative LSP for Multiple Failures," in Proceeding ICCCN 2004, Chicago, USA, Oct 2004, pp. 59- 64.
18. Alouneh .S, En-Nouaary .A, Agarwal .A, "A Multiple LSPs Approach to Secure Data in MPLS Networks", Journal of Networks, Vol 2, Issue 4, pp 51-58, August 2007.
19. Farrel .A et al. "Crankback Signaling Extensions for MPLS Signaling" draft-iwata-mpls-crankback-07.txt October 2003
20. Harrison .E, Farrel .A, Miller .B Protection and restoration in MPLS networks"
21. Data Connection White Paper October 2001
22. Sharma .V, Hellstrand .F "Framework for Multi-Protoco Label Switching (MPLS)-based Recovery" IETF, RFC 3469 February 2003

