Adding QoS Protection in Order to Enhance MPLS QoS Routing

Jose L Marzo *, Eusebi Calle *, Caterina Scoglio**, Tricha Anjali**

(*) Broadband Comm. and Distributed Systems
Institut d'Informàtica i aplicacions (IiiA)
Universitat de Girona, 17071 Girona, SPAIN
e-mail: {marzo, eusebi}@eia.udg.es

(**) Broadband and Wireless Networking Lab
School of Electrical and Computer Engineering
Georgia Institute of Technology, Atlanta, GA 30332, USA
e-mail: {caterina, tricha}@ece.gatech.edu

Abstract—**In this paper, a method for enhancing current QoS routing methods by means of QoS protection is presented. In an MPLS network, the segments (links) to be protected are pre-defined and an LSP request involves, apart from establishing a working path, creating a specific type of backup path (local, reverse or global). Different QoS parameters, such as network load balancing, resource optimization and minimization of LSP request rejection should be considered. QoS protection is defined as a function of QoS parameters, such as packet loss, restoration time, and resource optimization. A framework to add QoS protection to many of the current QoS routing algorithms is introduced. A Backup Decision Module to select the most suitable protection method is formulated and different case studies are analyzed.**

Keywords- QoS routing, network protection, MPLS.

I. INTRODUCTION

An initial design of a network may not be satisfactory due to changes in offered load, traffic characteristics etc. Network resources also vary due to resource reservations and topology changes (such as node or link failures). A new, dynamic traffic-engineering plane needs to be triggered. One important part of designing a QoS network concerns the reliability of the network. This reliability can be provided with fault management mechanisms, applied at different network levels and time scales. MPLS provides a fast restoration method to recover from failures by establishing an Label Switched Path (LSP) as a backup path. With these backups, traffic can always be redirected in case of a failure. MPLS also provides faster and more efficient fault detection and recovery activation than other network protocols or technologies. Several approaches defining a "fast restoration" framework have been proposed by IETF ([1], [2] and [3]).

A crucial aspect in developing a fault management system is the creation and routing of "backup LSPs". In this paper, we analyze the use of MPLS as a suitable means to provide QoS and fast restoration. We propose a method that considers periodic updates of network information as opposed to the use of dynamic on-line routing by some other methods ([4], [5], [6] and [7]). These methods balance the network load, optimize resources and minimize the request rejection ratio. However, they do not include the provision of a fault tolerant routing mechanism and QoS protection, as defined in Table I. We propose an enhanced routing mechanism, which provides QoS protection using a Backup Decision Module (BDM), to meet the above objectives.

TABLE I
QOS ROUTING & QOS PROTECTION OBJECTIVES

QoS routing	**QoS protection**
Load-balancing optimization	***Minimizing Packet losses***
Resource optimization	***Resource optimization***
Minimizing request rejection	***Minimizing restoration times***

In section II we introduce MPLS fault management methods. The next section discusses some proposed QoS routing methods, and QoS protection capabilities. In section IV, we propose a framework to incorporate QoS protection into these schemes. Section V describes BDM and different case studies are analyzed in section VI.

II. MPLS FAULT MANAGEMENT METHODS

Protection methods follow a cycle, from fault identification to LSP recovery. This cycle involves the development of various components:

a) A method for selecting the working and protection paths,
b) A method for bandwidth reservation in the working and protection paths,
c) Once the paths are created, a method for signaling their setup,
d) Mechanisms for fault detection and notification (such as transmitting a Fault Indication Signal (FIS)).

* This work was partially supported by the Spanish Research Council (CICYT) under contract TEL-99-0976. The work of Caterina Scoglio and Tricha Anjali was supported by NASA Goddard and Swales Aerospace.

0-7803-7802-4/03/$17.00 © 2003 IEEE

e) Finally, a switchover mechanism to move traffic from the Working Path (WP) to the protection path.

In [1], a Path Source LSR (PSL) is defined as the node responsible for the switchover function once the failure is identified. The Path Merge LSR (PML) is the node where the working and backup paths merge into a single outgoing LSP.

Main MPLS fault management methods

We describe three fault management algorithms in detail and then present a multilevel MPLS protection scenario that combines the main features of these methods.

a) Global backup

In this model (see Fig. 1(a)), an ingress node is responsible for path restoration when the FIS arrives. This requires an alternative, unconnected backup path for each working path. The ingress node is where the protection process is initiated, irrespective of the failure location along the working path.

This method has the advantage of setting up only one backup path per working path, and is a centralized protection method, which means only one LSR has to be provided with PSL functions. On the other hand, this method has a high cost (in terms of time) as the FIS is sent to the ingress node. Furthermore, it implies higher packet losses during the switchover time.

b) Reverse backup

The main feature of this method is to reverse traffic close to the point of failure, back to the source switch (ingress node) of the path being protected via a Reverse Backup LSP (see Fig. 1(c)). As soon as a failure is detected, the LSR at the ingress of the failed link, reroutes incoming traffic to the backup LSP sending it in the opposite direction, back to the ingress node. Haskin [2] proposes to pre-establish the reverse backup path making use of the same nodes of working path, simplifying the signaling process.

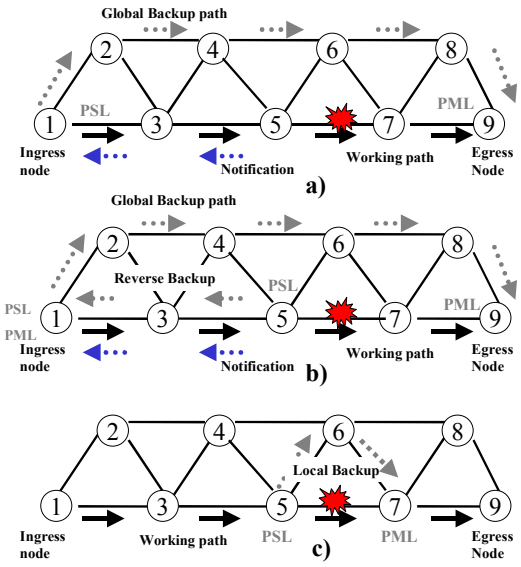

Fig 1 . MPLS protection methods (a) Global (b) Reverse (c) Local

This method, like the local repair method, is especially good for loss sensitive traffic. Another advantage is simplified fault indication, since the reverse backup transmits the FIS to the ingress node and the recovery traffic path at the same time. One disadvantage is poor resource utilization. Two backups per protected domain are needed. Another drawback is the time taken to send the fault indication to the ingress node, similar to the global repair model.

c) Local backup

With this method, restoration begins at a point much closer to the fault (see Fig. 1(b)). It is a local method and does not necessarily involve the ingress node. The main advantage is that it offers a faster restoration time than the global repair model, as well as significant reduction in the packet loss.

On the other hand, every LSR requiring protection has to be provided with a switchover function (PSL). A PML needs to be provided too. Another drawback is maintenance and creation of multiple backups (one per protected domain). This can lead to low resource utilization and increased complexity. An intermediate solution establishes local backups only for segments with high reliability requirements.

III. QoS Routing and Fault Management

The easiest way to find a path between a source and a destination is to select the shortest path. If the distance is measured in terms of the number of hops, this algorithm is called a Minimum Hop Algorithm.

QoS routing algorithms, such as Widest Shortest Path (WSP), Shortest Widest Path and Dynamic Alternative Path ([8] and [9]), have two objectives: minimize the number of hops (to maximize the resource utilization) and maximize the available bandwidth (to balance the network load). Minimum Interference Routing Algorithm (MIRA) [10] also considers path request rejection minimization. MIRA is based on the max-flow computation and minimum interference. It also takes into account specific MPLS characteristics (for instance, MIRA has apriori knowledge of the ingress-egress nodes). Other suggestions for providing QoS are based on mathematical preprocessing such as multi-commodity flow [4] or integer programming computations [5], [6] and [7].

Although these schemes consider setting up a backup path, it is usually a secondary objective. In some of these proposals (such as MIRA), the backup path is reduced to the possibility of re-routing in case of a network fault. Other proposals (such as [4], [8] and [9]) do not consider any protection scheme. Normally, they apply a global protection scheme that can be dynamic or pre-established, but no further QoS parameters for the backup path are taken in consideration.

A scheme offering a working path and a global backup path with QoS guarantees (bandwidth guarantees) is given in [6]. If both the paths are not available, the path request is rejected. In [7] the proposal is enhanced by adding local backup schemes.

IV. QoS Protection Routing

Having reviewed several current alternatives for constructing paths with QoS, we realized that protection in general, not to mention QoS protection, was in most cases a secondary consideration. An analysis of a combination of QoS routing and QoS protection has not been explored enough in recent literature. In [7] and [11], the utilization of more than a single protection method is introduced; however, no QoS protection (as defined in this paper) is considered, i.e. there is no QoS protection metric evaluation. We propose to achieve this QoS protection in such a way that it is a transparent feature and not necessarily activated all the time, depending on the desired degree of protection. In this section, we introduce our algorithm for adding this QoS protection.

We propose an algorithm formed by modules to manage a network. Our algorithm is divided in different computational modules to achieve scalability and transparency for the method. The algorithm is shown in Fig. 2.

The current network state is represented by the Network State Graph *NSG (N, L, R, P)*, where *N* is the set of nodes, L is the list of physical links, R denotes the remainder (residual) link capacity and P corresponds to the link protection needs. The link protection needs (*P*) are assigned, with apriori knowledge of protection segment, via network administrators (depending on their own experience, fault records, etc.). A way is to mark links with their fault probability. In the following, protected segments are marked with binary labels (0 or 1). in order to simplify the formulation and computation.

A LSP request is defined by (*i, e, t, c*) where *i* is the ingress node, *e* is the egress node, *t* is the traffic class (for instance, in DiffServ *t* can be: *EF, AF1, AF2* or *BE*) and *c* corresponds to the bandwidth requirements. This LSP request activates our algorithm. First, the Graph Weight Computation Module that processes the *NSG* is applied.

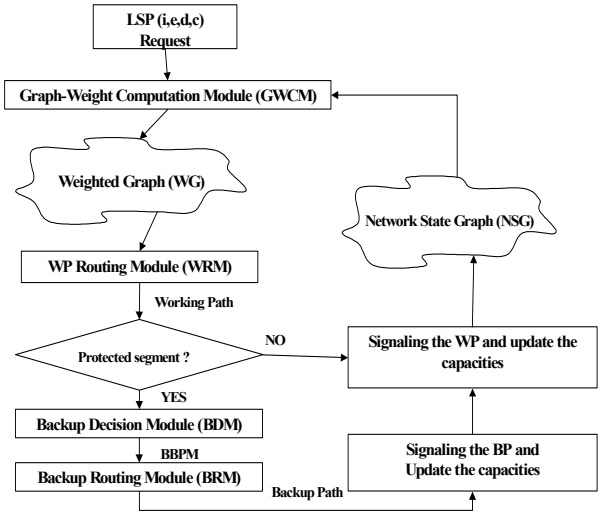

Fig 2. Our QoS Protection Routing Algorithm

The Graph Weight Computation Module (GWCM)

In this phase, two computations are carried out:

a) Reducing the links that do not meet the bandwidth requirements (*C*).
b) Assigning weights to the remaining links. This weight labeling can be based on different QoS objectives (see Table 1). These weights can be computed according to residual bandwidth or using other more complex policies (such as the criticality in MIRA). More than one QoS requirement can be combined.

The result is the Weighted-Graph *WG (N, L, R, P, W)*, which is defined in same way as the *NSG*, but with the added weight *W* for each link, which is computed in this phase.

The Working Path Routing Module (WRM)

Once the Weighted-Graph is obtained, a new LSP (Working Path) can be routed by a simple shortest path routing (SPR) scheme considering the weights (*W*). The nature of GWCM and this WRM are not significant in this proposed scheme, furthermore, our method is independent of them. Most of the current QoS routing algorithms finish at this point. When protection is needed (*P* contains protected segments in the WP), we add two new components, BDM and BRM, as shown in Fig. 2.

The Backup Decision Module (BDM)

In this module, a QoS Protection (QoSP) metric is computed to decide which backup method is the most suitable for this WP. The output of this module is the Best Backup Protection Method (BBPM), i.e. global backup, a reverse backup or a local backup. As BDM is the major contribution of this framework, Section V provides a complete description of this module and Section VI presents a case study.

The Backup Routing Module (BRM)

As in the case of the WRM, this module routes a Backup Path using a SPR computation. Depending on the value computed by the BDM (BBPM) just the most suitable backup routing is triggered.

A local backup can be computed using a SPR between the nodes a and b: SPR (*a, b*); where *a, b* are the first and last node of the protected segment (see Fig. 3). A global backup can be computed using a SPR (*i,e*) and finally a reverse backup can be computed by adding a SPR (*a,i*) to the global backup.

Signaling WP and BP Modules

Once the working and the backup routes are decided, a signaling method can be used to create both paths. RSVP-TE and CR-LDP are two possible methods for signaling the paths with the QoS (Bandwidth) requirements. Therefore, the *NSG* is updated with the new residual capacities.

V. The Backup Decision Module (BDM)

In this module, a QoS Protection (*QoSP*) metric value is computed to decide which backup method is the most suitable for each request. According the design criteria this module is

independent of the routing method to be applied by BRM. Once the WP is routed, the input information is:

N	Number of links of the WP
NP	Number of the protected links of the WP
C	Bandwidth required by the LSP request.
D	Distance (*i,a)*. Number of links between ingress node *(i)* and PSL node *(a),* (see fig. 3).
PT_FIS	Propagation Time of the FIS.
MHN	Max. Hop Number allowed for a working or global/reverse backup path (*i,e*).
MHN_LB	Max. Hop Number allowed for a local path (*a,b*).

In this scenario, Packet Loss (*PL*) depends on the distance *D(i,a)* from the failure location to the node responsible for the recovery, and on the requested capacity of the connection. The product distance by capacity provides an upper limit for packet loss.

$$PL = D(i, a) * C * PT\_FIS$$

The Restoration Time (*RT*) depends on the distance as well as on the latency of links (*PT_FIS*). We ignore the time it takes for fault detection since it affects all the methods equally.

$$RT = D(i, a) * PT\_FIS$$

Finally, the Resource Consumption (*RC*) is evaluated differently for the repair method used. For simplicity, we use the allocated bandwidth as the metric. For the global method, resource consumption (RC_G) depends on the number of links in the backup path. In the reverse repair method, the resources (RC_R) are the sum of the RC_G plus the resources required for the reverse path (*N-D(a,i))*C*. A particular case is when, using the Haskin mechanism [2], resource consumption is *2*N*C*. Resource consumption for local repair method (RC_L) depends on *C* and the number of protected links *NP*, which ranges from 2 to *MHN_LB*. Therefore, RC for the different methods is evaluated by:

$RC_G = N' * C$, where $N' \in [N, MHN]$

$RC_R = RC_G + (N - D(a,i)) * C$

$RC_L = NP * NL' * C$, where $NL' \in [2, MHN\_LB]$

The general QoSP function (*f*) can be expressed as:

$$QoSP = f(PL, RT, RC) \quad (1)$$

We propose a function *f* as a weighted sum combining the above protection parameters:

$$QoSP = \alpha * PL^N + \beta * RT^N + \lambda * RC^N \quad (2)$$

Protection parameters are heterogeneous in nature, *PL* is expressed in terms of number of packets, *RT* in seconds and *RC* in bits/s (bandwidth), hence they must be normalized. A lineal function can be applied in order to range them from 0 (best QoSP case) to 1 (worst QoSP case). Therefore, PL^N, RT^N and RC^N corresponding normalized values are obtained.

The traffic class of the LSP request (*t*) should be also considered. The protection requirements of the Diffserv (DS) traffic classes can be characterized as in Table II.

TABLE II

DS QoS PROTECTION REQUIREMENTS AND α, β and λ ASSIGNMENTS

Traffic Class	QoS requirements	α	β	λ
EF	*Very low PL and RT*	*0,5*	*0,45*	*0,05*
AF1	*Very low PL*	*0,5*	*0,3*	*0,2*
AF2	*Low PL*	*0,33*	*0,33*	*0,33*
BE	*No requirements*	*0,05*	*0,05*	*0,9*

α, β, λ weight values are defined based on DS traffic characteristics [12]. For instance for a EF service *α, β,* which affect *PL* and *RT* are large in relation with *λ,* which affects *RC,* in order to guarantee EF service performance. Similar policy is applied to the reminded traffic classes. Values shown in Table II are based in our heuristic criteria, they should be more accurately tested in further experimentation.

Reverse and local repair methods avoid packet loss (as shown in section II), hence these losses can be considered negligible. Local method minimizes the restoration time, and thus it can be ignored with respect to the other methods (inverse and global). Considering the characteristics of the protection methods, as explained above, we obtain the expressions shown in the following table:

TABLE III

QoS PROTECTION METHODS COMPUTATION

Method	QoS_Protection (QoSP)
$QoSP_{Global}$	$\alpha * PL^N + \beta * RT^N + \lambda * R_G{}^N$
$QoSP_{Local}$	$\lambda * R_L{}^N$
$QoSP_{Reverse}$	$\beta * RT^N + \lambda * R_R{}^N$

Computing the QoSP values (Table III) the Best Backup Protection Method (BBPM), which is the minimum QoSP, is selected according to:

$$BBPM = \min(QoSP_{Global}, QoSP_{Reverse}, QoSP_{Local})$$

Therefore, just one routing method is triggered instead of computing all three, leading to reduction in computation cost.

VI. CASE STUDY OF THE BDM

All the following experiments calculate the expression *(2)* for QoSP to search the best method to apply according to the QoS requirements of the request. Different scenarios are considered with varying traffic classes (EF, AF1, AF2, BE), required bandwidth, number of segments to be protected in the WP and the distance of the first node of the protected segment. To simplify, in a multiple protected segment scenario, we

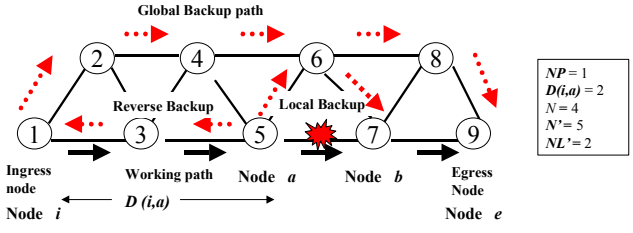

Fig 3 . Illustrative example

assume concatenated segments and a single distance measure. The values of α, β, λ are assigned according to Table II.

*Case 1: QoSP and bandwidth influence (*EF, NP=6, D(i,a)=2*)*
For this experiment, we consider that *NP*, the number of segments to protect, is 6 and the distance to the initial node (D(*i,a*)) is 2. Fig.4(a) shows the QoSP values for different bandwidth requirements (*C*). For EF requests, BDM gives priority to the local method, which ensures that the requirements for PL and RT will be reached. The second option is the reverse method, although the difference between the two methods increases with the required bandwidth, since it affects *PL*. The greater the bandwidth request, the worse is the packet loss in case of a failure.

*Case 2: QoSP and distance influence (*EF, C=400, NP=2*)*
For this experiment, we consider that NP is 2 and the BW is constant. Fig.4(b) shows the QoSP values for different distances D(i,a). As expected, BDM selects the local backup method as the first option that best suits the characteristics of *EF* traffic. More interesting is that the second option varies according to the distance. For short distance, a global backup is suggested, with lesser resource consumption than the reverse method. For larger distances (2 or larger in figure 4(b)), reverse backup is better. This is because in case of *EF* traffic, RT and PL are crucial, in comparison to resource consumption.

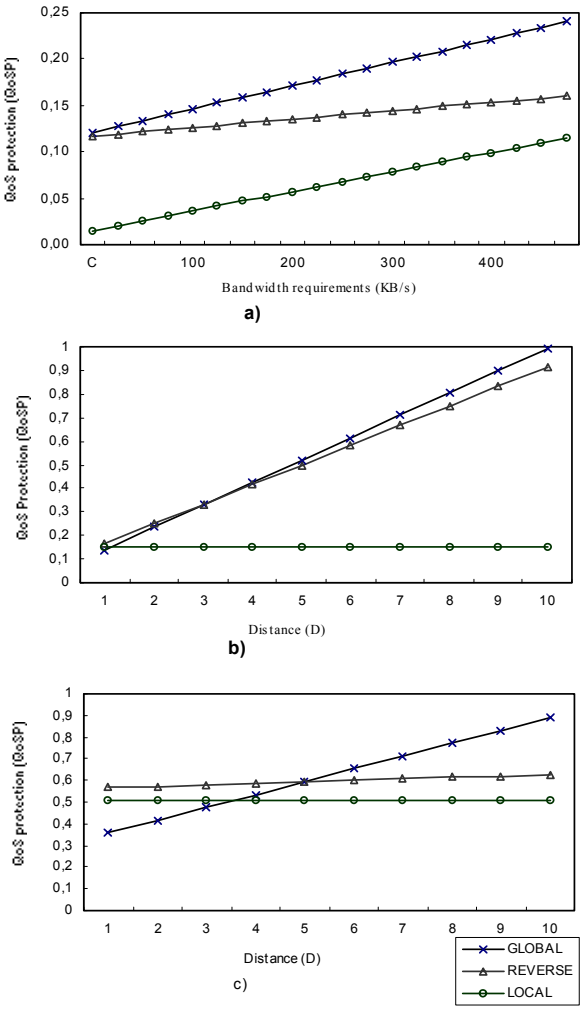

Fig 4. BDM case studies (a) QoSP and Bandwidth (b) QoSP and distance EF, C=400, NP=2 (C) QoSP and distance AF2, C=400,NP=5.

*Case 3: QoSP and distance influence (*AF2, C=400, NP=5*)*
Figure 4(c) shows the influence of the distance with a high number of segments to protect (NP=5). For shorter distances, the global method is chosen, providing a complete working path protection with values of PL and relatively adequate RT. However, for larger distance (D≥4) the local backup (low PL and RT) is the method of choice. If the distance is greater than 5, we see that the second option of the BDM is the reverse backup and the global method becomes the worst choice.

CONCLUSIONS

In this paper, a new QoS protection scheme is proposed that extends previous work in QoS routing and MPLS protection mechanisms. We have also proposed a new framework for achieving such QoS protection. The final result is a transparent and flexible method that addresses this lack of QoS protection. A Backup Decision Module (BDM) is introduced in the framework as the crucial element. An analysis of different cases shows that the BDM can select the most suitable backup method for each LSP request, thus avoiding expensive evaluations. The proposed framework does not require a complete change of current QoS routing proposals. It also allows Internet Service Providers to set a degree of protection for their MPLS backbones according to their needs.

REFERENCES

[1] V. Sharma, B.M. Crane, S. Makam, K. Owens,C. Huang, F. Hellstrand, J. Weil, L. Andersson, B. Jamoussi, B. Cain, S. Civanlar, A. Chiu. "Framework for MPLS-Based Recovery". (Work in progress) Internet Draft draft-ietf-mpls-recovery-frmwrk. Jul 2001.

[2] D. Haskin, R. Krishnan "A Method for Setting an Alternative Label Switched Paths to Handle Fast Reroute". (Work in progress) Internet Draft draft-haskin-mpls-fast-reroute. Nov 2000.

[3] S. Makam, V. Sharma, K. Owens, C. Huang "Protection/Restoration of MPLS Networks", (work in progress) Internet Draft draft-makam-mpls-protection. Oct 1999.

[4] S. Subhash, M. Waldvogel, P. Warkhede. "Profile-Based Routing: A New Framework for MPLS Traffic Engineering". Proceedings of QofIS'01.

[5] M. Kodialam, T.V. Lakshman, "On-line Routing of Guaranteed Bandwidth Tunnels", Seventh IFIP Workshop on Performance Modeling and Evaluation of ATM/IP Networks, June 1999.

[6] M Kodialam T. V. Lakshman. "Dynamic routing of bandwidth guaranteed tunnels with restoration", Proceedings of IEEE Infocom 2000.

[7] M. Kodialam, T.V. Lakshman. "Dynamic Routing of Locally Restorable Bandwidth Guaranteed Tunnels using Aggregated Link Usage Information". Proceedings of IEEE Infocom 2001.

[8] R. Guerin, D. Williams, A. Orda. "QoS Routing Mechanisms and OSPF Extensions". Proceedings of IEEE Globecom 1997.

[9] Q. Ma and P. Steenkiste. "On Path Selection for Traffic with Bandwidth Guarantees". Proceedings of IEEE Conf. of Network Protocols 1997.

[10] M. Kodialam, T.V. Lakshman. "Minimum Interference Routing with Applications to MPLS Traffic Engineering". Proceedings of IEEE Infocom 2000.

[11] E. Calle, T. Jové, P. Vilà, J.L. Marzo. "A dynamic multilevel MPLS protection domain". Proceedings of DCRN'2001. Budapest, Hungary

[12] F. Le Facheur et al. "Requirements for support of Diff-Serv-aware MPLS traffic engineering". IETF draft June 2001 (work in progress) < draft-ietf-tewg-diff-te-reqts-01.txt>