Computer Communications 35 (2012) 970–979

Contents lists available at SciVerse ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

A Local Fast-Reroute mechanism for single node or link protection in hop-by-hop routed networks

Hui-Kai Su [*]

Dept. of Electrical Engineering, National Formosa University, Yunlin 632, Taiwan, ROC

ARTICLE INFO

Article history:
Received 22 March 2010
Received in revised form 13 February 2012
Accepted 15 February 2012
Available online 24 February 2012

Keywords:
Network protection
Network survivability
Fast reroute
Network routing
Internet protocol

ABSTRACT

Network survivability has become one of the most important QoS (Quality of Service) parameters in IP network-based applications, particularly with regard to real-time multimedia applications. IP-based protection that enable recovery from failure in just a few milliseconds can provide greater network resilience than traditional routing recovery or other lower-layer recovery technologies. This paper proposes an IP protection scheme, called IP Local Fast-Reroute (IPLFRR), for single node or link protection. This scheme works in an intra-area routing domain, providing a simple and efficient solution to improve the survivability of IP networks. Unlike MPLS Fast-Reroute, which requires an extra MPLS layer and related protocols, the proposed scheme is applicable to a network employing conventional IP routing and forwarding. Moreover, our mechanism is capable of preventing service disruptions and packet loss caused by the transient loops that normally occur during reconvergence of the network following a failure. Because the backup next-hops are predetermined, service interruption can be limited to a few milliseconds, which is on par with the failure detection time. Simulation results show that IPLFRR is capable of improving network survivability, following the failure of a single node or link.

1. Introduction

The internet (IP network) is a hop-by-hop routed network. The recent maturation of the internet has seen all-IP solutions applied in numerous communication networks. For real-time broadband multimedia applications, network availability is one of the important QoS (Quality of Service) parameters in IP transport networks. A set level of service must be guaranteed, regardless of the scale, duration, and type of failure. The two main approaches used to improve network resilience in the IP layer are *IP restoration* and *IP protection*. IP restoration attempts to find a new route by which to restore connectivity once a failure has occurred [1], e.g., Interior Gateway Protocol (IGP) routing recovery. IP protection, the intention of which is to achieve rapid recovery from failure (in just a few milliseconds), is based on fixed and predetermined failure recovery, where the selection of the next-hop is performed in conjunction with the identification of a backup for the next-hop. However, IP protection differs from the mechanisms of lower-layer failure recovery, such as a SONET Protection Switch or MPLS fast re-route techniques, due to the distinct routing characteristics of packet-switching networks and circuit-switching networks. In IP networks, the packet forwarding information is aggregated within the next-hop; therefore, the concept of a backup path is unable to deal with the affected packets when a link or node failure occurs.

Since the ARPANET was first established, IP networks have had the feature of restoration. Recently, many protection and restoration schemes have been provided in the lower layers in IP networks, e.g., SONET APS (Automatic Protection Switching) and MPLS Fast-Reroute [2]. Due to its distributed and connectionless architecture, an IP network is much more difficult to protect than connection-oriented networks. However, present networks are unable to satisfy the critical requirements of the growing number of real-time multimedia applications. There are three key reasons.

The first reason is that current approaches to IP restoration take too long. The speed and volume of transmissions have increased, leading to an increase in packet loss when a link or node fails. Recovery times are depicted in Fig. 1. In a typical link-state routing protocol, the time to recover encompasses failure detection, propagation of the failure information, and convergence to new routes. Failure detection time depends on the physical layer or the hello routing protocol. When failure is detected on the physical layer, it may take only a few milliseconds. Propagation delay and flooding delay are the key determinants of the propagation of failure information, typically consuming 10 ms to 100 ms per hop. Finally, an SPF (shortest path first) algorithm computes the new routes and installs them into the routing table; however, total convergence time may be up to several tens of seconds depending on network size.

[*] Tel.: +886 5 6315619; fax: +886 5 6315609.
E-mail address: hksu@nfu.edu.tw

0140-3664/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2012.02.007

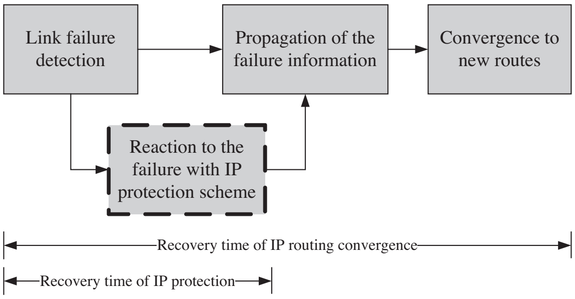
Link failure detection
Propagation of the failure information
Convergence to new routes
Reaction to the failure with IP protection scheme
Recovery time of IP routing convergence
Recovery time of IP protection

Fig. 1. The recovery times of IP routing convergence and IP protection.

Any link or node failure in a routed network disrupts the delivery of traffic until the network routes re-converge on the new topology. Packets may be dropped or enter a loop if their forwarding paths traverse the failed component. Such disruptions often last several tens of seconds or longer, and approximately 54% of network failures exceed 1 min [1]. Most applications have been constructed to tolerate short-time failures, but such disruptions are intolerable for interactive real-time applications and non-interactive real-time streaming applications, such as Voice over IP (VoIP), Video on Demand (VoD), and P2P streaming applications. The jitter buffer (or playout buffer) in real-time applications is designed to address packet jitter and network congestion in IP networks and can tolerate only a brief transport disruption, e.g., 200 ms to 450 ms for VoIP, and 1 s to 30 s for VoD. Therefore, IP restoration alone appears incapable of providing adequate network survivability for real-time applications; protection mechanisms are also needed. IP protection is capable of preserving the flow of data during IP restoration. This limits the period of disruption to the time required for failure detection and the reaction of the IP protection mechanism, such that IP restoration can be performed as usual. Finally, after the IGP converges, packets can be delivered according to the new route.

The second reason that present networks are unable to satisfy the requirements of real-time multimedia applications is their inability to detect failures occurring in higher layers, despite the fact that lower-layer protection and restoration may work faster than IP protection. For example, an optical protection mechanism can protect against link failures but not against failure of an IP router or forwarding software. By contrast, higher-layer entities may be able to protect against lower-layer failures if there is an alternate route between communicating entities.

The third reason is that traditional IGPs incur packet loops and losses due to transient loops or micro loops [3]. With IGPs, each time the network topology changes, some of the routers modify and update their Forwarding Information Base (FIB) to take into account the new topology. Each change in topology causes a convergence phase. During this phase, routers may have transient inconsistencies in their FIBs, which often cause packet loops and losses, even if the reachability of the destination is not compromised following the change in topology. Packet losses and transient loops are also caused by link down events resulting from maintenance operations, even if this operation is predictable and not urgent. Thus, IP protection mechanisms are necessary to enhance the availability of IP networks.

This paper proposes an *IP Local Fast-Reroute (IPLFRR)* mechanism, with two algorithms for node protection and link protection, IPLFRR-N (IPLFRR for Node protection) and IPLFRR-L (IPLFRR for Link protection), in an intra-area routing domain. The underlying concepts can be found in [4,5]. Our mechanism provides simple, effective protection of IP networks. Unlike MPLS Fast-Reroute, the proposed mechanism is applicable to networks employing conventional IP routing and forwarding with the ability to prevent service disruptions and packet loss caused by the transient loops that commonly occur during the re-convergence of the network following a failure. In addition, additional control protocols or enhanced routing protocols are not required, such that current link-state routing protocols will suffice. The candidates for backup next-hop are pre-determined when IP routing converges. In the event that a node or a link fails, the detection by an adjacent node allows local rerouting of the packets to the backup next-hop. Because the backup next-hop has been determined beforehand, the interruption to service can be limited to a few milliseconds. In simulations, only backup next information for each destination needed to be calculated and extra control messages were unnecessary. Simulation results show that most failures were recovered efficiently.

The remainder of the paper is organized as follows. In Section 2, we introduce related studies dealing with the protection of IP networks. The IP Local Fast-Reroute framework is introduced in Section 3. In Section 4, details of the underlying mechanism, and the IPLFRR algorithms for node protection and link protection are explained. In Section 5, we present simulations of network resilience. Finally, Section 6 provides our conclusions.

2. Background

This paper focuses on IP network protection; however, improvements in IP network resilience in the lower layers can be found in [1,6–10], e.g., SONET/SDH protection, optical network protection, and MPLS Fast-Reroute. Convergence of IP routing can also be enhanced using a novel router architecture, an incremental SPF algorithm, and schemes to prioritize and update IP network prefixes [11].

The issue of IP protection has been discussed since 2002, when a scheme for the precomputation of the second shortest paths was introduced in [11]. In this scheme, the minimum-cost path of each node to every other node in the network is computed. An alternate path is computed only if the primary path becomes unusable due to a failure. An alternative is for each node to anticipate the failure and precompute feasible backup routes to all other nodes. When the primary route fails, the packets are quickly rerouted to the second shortest path; however, in practice it has been difficult to provide an efficient and fast rerouting service capable of avoiding looping.

An IP Fast-Reroute (IPFRR) framework [12,13] and loop-free alternate selection scheme [14] were proposed by the *IETF Routing Area Working Group*. IPFRR is compatible with current link-state routing protocols, such as OSPF and IS–IS. The IPFRR framework introduces three mechanisms to repair paths: equal cost multi-paths (ECMP), loop-free alternate paths (LFAP), and multi-hop repair paths. ECMP and LFAP are the simplest methods to repair paths and are considered sufficient for approximately 80% of failures. Multi-hop repair paths are considerably more complex [15], requiring extra control protocols or enhanced routing protocols. It is anticipated that approximately 98% of failures could be repaired using this method.

Thus, IP protection schemes can be divided into two types: local and global. LFAP [14] is a local IP protection scheme, in which the packets affected by a failure in a link or node are rerouted directly to the backup next-hop. Local IP protection schemes are simple to implement; however, the protection performance depends on network topology. By contrast, global IP protection schemed are capable of 100% protection for the network; however, complex calculation and complicated algorithms are required. Global schemes typically use multiple routing configurations [16], Not-via address [17,18] or IP tunnels [19,20].

The proposed mechanism falls under the class of local IP protection, in which IPLFRR-L is equivalent to schemes involving loop-