Problems in the Information Dissemination of the Internet Routing

ZHAO YiXin (赵邑新), YIN Xia (尹霞) and WU JianPing (吴建平)

Department of Computer Science, Tsinghua University, Beijing 100084, P.R. China
E-mail: dan.zhao@intel.com

Received June 11, 2001; revised August 2, 2002.

Abstract Internet routing is achieved by a set of nodes running distributed algorithms — routing protocols. However, many nodes are resistless to wrong messages or improper operations, unable to detect or correct them. Thus a wrong message or an improper operation can easily sweep almost the whole Internet. Such a fragile Internet routing comes from the features of these algorithms and protocols. Besides, the strategies taken by the network equipment manufacturers and administrators also are of important influence. When determining the options or selections in the implementation/operation, they always pay more attention to the expense of a single node or a single area and make some simplifications in implementations and configurations while caring less about the influence on the whole network. This paper tries to illustrate such a scheme is not reasonable at all and suggests the consideration from the view of the overall optimization. From three typical cases involved in the Internet routing, a general model is abstracted, which makes the results significative for more Internet related aspects. This paper evaluates the complexity of the theoretical analysis, then acquires the effect of error information on the whole network through the simulation on the Internet topology. It is shown that even very little error information can incur severe impact on the Internet. And it will take much more efforts of downstream nodes to make remedies. This result is intuitively revealed through the comparisons in the charts and the visual presentations. Then a hierarchical solution to establish the upgrade plan is given, which helps to upgrade the nodes of the network in a most efficient and economical way.

Keywords Internet routing, information dissemination, distance vector algorithm, BGP-4, flap damping

1 Introduction

One of the features of the Internet is the employment of distributed algorithms. Each router executes its own instances of such algorithms, such as routing protocols. All these routers cooperate with each other to get their own results and provide information for others. High performance and robust Internet routing is the key factor for the Internet application and performance. However, nodes in the Internet routing are always resistless to wrong messages or improper operations. Our work tries to reveal such a condition and gives some preliminary analysis about the reasons, then suggests solutions for establishing efficient network upgrade plan.

The original motivation starts from our discussion with router developers and network administrators. As to some implementation selections (e.g., data structures and algorithms to advertise routes) and the operation options (e.g., enable/disable route flap damping in routers), we found they cared more about the overhead of a single node or a single area, which we hesitate to agree with. Therefore, we decided to do something to see what the whole Internet will be like if something wrong happens. First, we study three familiar cases involved in the Internet routing: the distance vector algorithm in the routing protocol, the AS_PATH composition of BGP-4 (Border Gateway Protocol, Version 4)\[1\] and the route flap damping\[2\]. We want to see if some node fails to do some operation and/or generates some wrong messages, and how other nodes in the network will be affected. Besides the features of related algorithms and protocols, such failures often come from incorrect implementations or configurations, sometimes from very subtle mistakes in codes or settings. If some wrong message (or some improper operation) appears, the
first question is whether it is detectable? If so, can the wrong message be corrected or can the operation be remedied? Anyway, we want to see that how many nodes may be affected even if there are some nodes that can (and would like to) detect the errors and correct them. Based on these three cases, a common model is acquired, which can be applied in more fields related to the Internet, such as evaluating the spread of a virus on the Internet, upgrading the software/hardware, etc.

Originally, we planned to theoretically analyze the effect. However, practical work and analysis show it is a very complicated problem. Then we resorted to the simulation. We use inet\textsuperscript{3} program to generate an Internet topology and further observe how wrong messages can affect other nodes. With comparisons and visual presentations it reveals that things are not good at all. When determining the options and selections, developers and administrators should be more cautious about the expense of a single node or a single area versus the overhead of the whole network. As to how to upgrade the network in a most efficient and economical way, a hierarchical solution is provided.

Large amount of efforts has been taken to study the Internet routing. These efforts range from the routing protocol design to the test and the analysis of the Internet routing. RIP (Routing Information Protocol), OSPF (Open Shortest Path First) and BGP-4\textsuperscript{[1]} are three main routing protocols exploited in the Internet. The former two are used inside Autonomous Systems (AS). BGP-4 is the only widely exploited inter-AS routing protocol. Besides, there are routing protocols from ISO and some network equipment manufacturer. In order to assure the correctness and high performance of routing protocol implementations, the protocol test is exploited.\textsuperscript{[4]} presents the test of IP routing protocols with the test environment generated by a software tool SOCRATES.\textsuperscript{[5]} summarizes the research and the practice on routing protocol test we have performed so far.

The rest of this paper is organized as follows. Section 2 presents three cases from which we start our discussion. Section 3 is a preliminary analysis. Then in Section 4 some definitions are given and more analysis is done. Section 5 introduces the general model and the failed attempt for the theoretical analysis. Section 6 explains our simulation study and analyzes the result. Section 7 gives our hierarchical algorithm to establish the most efficient upgrade plan. Finally, conclusive remarks are presented.

2 Three Cases Involved in the Internet Routing

The Internet may be the most complicated distributed system. It is a packet-switching network that enables its attached computers to exchange information by sending data packets to each other. The correct and effective delivering of data packets is done by routing, that is, routers select the best route from the source to the destination. The needed routing information is collected and processed dynamically by routing protocols running on each router. Each routing protocol is a kind of distributed algorithm. Each router runs a separate instance of such an algorithm. Routers cooperate with each other, accomplishing their own jobs and providing information for others. It is just the cooperation among routers and the information exchange that support the performance and the application of the Internet. And the quality of each node may affect other nodes and even the whole Internet.

However, routers in the Internet always only talk with their neighbors. After processing the received information, these routers often transfer it to all neighbors except the sources. Thus the information is transmitted hop by hop through the Internet. There are hundreds thousands of routers in the Internet. It is highly possible that some of them fail to function properly due to the implementation or the configuration. Thus they perform some improper operations. Or some wrong information will be generated and transmitted in the Internet. "Only talking with neighbors" makes it more difficult to detect errors or further correct them. What we concern is, when there are really some improperly behaving routers, how the Internet will be affected. And in order to detect the generated wrong information, what overhead will be taken (especially compared with the minimal expense in a non-error environment)?

The Internet is always depicted as a graph \( G = (V, E) \). \( V \) is the set of vertices (e.g., routers) and \( E \) is the set of edges (e.g., links). For each \( v \in V \), the neighbor set of \( v \) is \( N(v) = \{v_j | (v_i, v_j) \in E \} \). A message sent from \( v_i \) to \( v_j \) is denoted as \( m_{ij} \). ASs can also be regarded as vertices if we only concern the AS level routing. Here we will take a look at these three cases involved in the Internet routing.

Case 1. Calculating the shortest path with a distance vector algorithm.

Suppose \( D(v, d) \) is the shortest metric from router \( v \) to destination \( d \).