Design Issues of Fault Tolerant Mechanism for Dynamic Host Configuration

Hideo Kodaka

School of Information Science,
Japan Advanced Institute of Science and Technology

February 13, 1998

Keywords: Dynamic Host Configuration, network partitioning, cooperative system, fault tolerance, pessimistic strategy, mutual agreement.

A Dynamic Host Configuration(DHC) is a mechanism that dynamically configures hosts which are connected to a network. The DHC system consists of servers and clients: servers centrally manage an address pool (a collection of information for configuration) and deliver specified information to clients, called "services". These clients dynamically configure their own hosts based upon the information received from the server. This paper focuses on one of the more widely accepted implemented mechanisms, Dynamic Host Configuration Protocol(DHCP). In the current state of DHCP technology, however, it is not fully capable for the DHCP server to equip a mechanism that shows tolerance of some failures. The client does not obtain configuration parameters from the server when that server fails or when a network partitioning occurs between the server and the client. Therefore, the client fails to be connected to a network.

The purpose of this research is to improve the fault tolerance of DHCP servers by means of analyzing the failures which cause interruption of services. This paper focuses on two failures and attempts to newly define them as follows:

1. network partitioning:
   caused by a failure of the underlying communications substrate, when two systems that could previously communicate cannot do so then after

2. permanent server failure:
   when a server permanently fails to respond to requests from clients

Moreover, the proposed system aims at tolerating these two failures when they occur simultaneously or sequentially even if one of the failures does not recover.

Even though it is possible for the servers in the existing DHCP to be redundant, it is mandatory not to overlap network addresses as a resource in each address pool managed by each server. In recent research, unlike the aforementioned, there is a proposed framework that a set of DHCP servers work together and share a synchronized address pool in order to allow a client to continue to use the same network address even if the server who initially offered the client the temporary use of its address is unavailable for some reason. However, with this proposal, the existing DHCP can not sufficiently tolerate diverse failures that occur on a network because it is thought to respond to only one failure from the original server.

On the assumption that the partitioning and permanent server failure have occurred, there exists two problems in the existing mechanism of cooperative DHCP servers. One is that each server in a server group defined as multiple cooperative servers keeps the address pool which was shared before the failures occurred. It is possible for servers to allocate the same network address to two or more clients. Secondly, it is very difficult for a group consisting of more than three servers to completely come to a consensus among the group, so called a "complete consensus". It does not mean to obtain authority of an address, so that servers can not allocate network addresses to clients.

A policy for fault tolerance is "pessimistic strategies" in this paper. During partitioning, each partition makes the worst case assumptions about what is occurring in other partitions, and operates under pessimistic assumptions. Based on this policy, it then analyzes what sort of appropriate behavior is necessary for a partitioned group while some failures occur. This policy emphasizes avoiding contradiction of data concerning authority of network addresses.

The above problems can be solved by following two methods:

1. A server can obtain authority of addresses by means of "mutual agreement" ,whereby the server consents the other server among the same group. Because only one message is exchanged between the two servers, it does not lead to vague agreement. That is why this method is very useful.

2. By means of restructuring an address pool, it was possible for each of the two servers to centrally manage explicit regions within the address pool. Then, two servers give mutual agreement in order to reserve some addresses before they can allocate an address to the clients.

This paper concludes that the proposed DHCP servers

- are capable to tolerate permanent server failures and network partitioning,
- exclusively manage authority of network addresses among the group, and finally,
- keep the loss of resources including network addresses to a minimum when some failures occur.