Network Working Group
INTERNET-DRAFT
Updates: RFC 826

T.-S. Jou
IBM Corporation
February, 1999

Duplicate IP Address Detection Based on Gratuitous ARP
<draft-jou-duplicate-ip-address-02.txt>

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

To view the list Internet-Draft Shadow Directories, see http://www.ietf.org/shadow.html.

Copyright Notice

Abstract

The Address Resolution Protocol specifies the scheme to resolve the hardware address of a host by using its IP address. The hardware addresses are normally unique for each hardware module because they were assigned by manufacturers; but there is much less control on the uniqueness of IP addresses on a LAN. With the booming network popularity, the possibility of the same IP address being used on different hosts is increasing. The duplication may come from users' or network administrators' mistakes, or configuration errors on host addresses assigning programs such as BOOTP or DHCP servers. This document is to define an extension to the original ARP protocol to prevent a newly configured host from making much damage to a host that has been the owner of the same IP address. The solution is based on the de-facto gratuitous ARP packets with modification on a host's behavior when an address duplication is detected.

Acknowledgments

This document was first prepared while the author was an IBM employee. The initial idea was confirmed and tested with help from Lori Napoli and Sajay Khanna in IBM. Thanks also go to Mike Patton in MAP Network Engineering, Inc., for pointing out the security concerns.

1. Introduction

The Address Resolution Protocol, defined in RFC 826 [1], is used to determine a host's hardware address based on its network address. To adapt to the possible changes of the association between a hardware address and an IP address, two mechanisms are specified in the RFC:

(1) When a host receives an ARP packet and the sender IP address exists in its ARP table, the host should update the cached ARP entry with the sender hardware address in the packet.
(2) Each host ages away old ARP entries to allow changes on the network.

There are increasing number of hosts that are connected to networks and have IP addresses assigned, some of them dynamically, hence there are increasing number of possibilities that the same IP address is assigned to multiple hosts on a LAN. RFC 826 oversees this problem. Later in this document we can see the above mechanisms even causes catastrophic problems. If address duplication ever occurs, neither of the two hosts sharing the same address can be reliably reached by others because the unpredictable hardware address resolution on the shared IP address. This is especially a serious threat to a server that many clients depend on.

The problem can be avoided gracefully if following three conditions are achieved:

(a) The host that attempts to use a duplicate IP address can detect this address is being used by another host, and stop using this address immediately, possibly via turning down its interface.
(b) The host that originally owns the IP address notifies the the attempting host for the duplication, and then keep operating.
(c) The confusion caused by the second host's attempt can be reduced to minimum for all other hosts on the network.

A host running one of many latest TCP/IP implementations can generate a gratuitous ARP packet when any of its interfaces is configured, usually at booting time. The gratuitous ARP packet is an ARP request with both sender and the target IP address fields containing the

configured IP address. This de-facto behavior can be deployed to detect IP address duplication. After seeing the gratuitous packets, a

host following RFC 826 will send an ARP reply if the address is being configured on one of its interfaces. Due to the lack of standards, once the gratuitous ARP sender receives the unexpected ARP reply, the response varies. Most implementations can display warning messages on their consoles or to create error logs. Some implementation allows both hosts to keep using this IP address until the problem is corrected manually. Some other implementations disable the networking capability on both hosts and require both hosts to be reconfigured and possibly be rebooted. The latter implementation makes the hosts very vulnerable to configuration errors. The correct behavior should be that the host originally owns this IP address keeps operating, while error messages are reported to draw network administrator's attention. The host that attempts to use a duplicate IP address should stop operating on this address.

The problem cannot be fully solved without addressing Condition (c). Since a gratuitous ARP request is a link-layer broadcast packet, all hosts on the network will receive it. According to RFC 826, all hosts that have this IP address cached in their ARP tables will update the entry with the sender hardware address. This behavior originally is designed to allow a host that has just changed its hardware address (such as interface card is replaced) to be able to update others. However, this design results in these hosts not being able to reach the original IP address owner until their ARP entry expires, even if the gratuitous ARP sender stops using the address immediately. Since the gratuitous ARP packet just updated every host's ARP entry, the entry will be valid for the full ARP entry lifetime, normally 20 minutes.

As specified by RFC 826, the ARP reply from the original IP address owner is a unicast packet, hence the hosts with the ARP entry cached will not be aware of the occurrence of duplication. To correct the problem, this document specifies the reply of the gratuitous ARP to be a link-layer broadcast packet, hence Condition (c) can be achieved because all other hosts will be able to receive the ARP reply and change their cached entries back to destine to the original address owner. Even thought there is still a window of time that the cached entries are destined to the gratuitous ARP sender, the time period is much shorter than the ARP entry lifetime.

2. Discussion of an Alternative to Broadcast Reply

An alternative to replying with a broadcast ARP reply packet is to let the original address owner to send a gratuitous ARP packet again, which can correct other hosts' cached entries as well. However, if for whatever reason the host attempting to use the duplicate IP address chooses to continue operating, that host will reply with an

ARP packet. Once the original address owner receives the reply, it becomes a protocol dilemma whether to send another gratuitous ARP, which potentially can cause an infinite looping of ARP packets between the two hosts, or, to hand over the IP address to the new host, which violates Condition (b) we would like to achieve.

On the other hand, if the link-layer broadcast ARP reply is sent by the original address owner but for some reason the host attempting to use the duplicate IP address is still operating, those hosts that have the ARP entry cached will be able to keep communicating with the original address owner until their ARP entries expire. Since these entries are updated by the broadcast reply, they will remain valid for approximately the full entry lifetime. But those hosts that have to resolve this IP address will see undetermined results. However, if the duplication problem can be fixed in time, perhaps manually by the users or the network administrator, the proposed scheme still causes lesser damage to all hosts on the network.

3. The Solution

The implementation details of the solution is described in this section. The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

(1) A gratuitous ARP request packet MUST be generated in two situations:
   (i) when an IP address is being assigned to a working interface, and
   (ii) when an interface that has IP address assigned is being turned up from down.

   A gratuitous ARP packet on an Ethernet is defined as

```
48.bit Destination Address     = 0xffffffffffff (broadcast)
48.bit Source Address          = Hardware address of interface
16.bit Frame type              = 0x806 (ARP)
----------------------
16.bit Hardware type           = 0x1 (Ethernet)
16.bit Protocol Type           = 0x800 (IP)
 8.bit Hardware Address size   = 6
 8.bit Protocol Address size   = 4
16.bit Opcode                  = 1 (Request)
48.bit Sender Ethernet Address = Hardware address of interface
32.bit Sender IP Address       = Configured IP address
48.bit Target Ethernet Address = Don't care
32.bit Target IP Address       = Configured IP Address
```

(2) If a host receives an ARP request packet in which the target IP address and the sender IP address fields are the same and it matches the address of the receiving interface, it implies IP address duplication happens. The host MUST send a link-layer

broadcast ARP reply as defined below. The host SHOULD report, log, and/or display warning messages to indicate the detection of IP address duplication.

```
48.bit Destination Address     = 0xffffffffffff (broadcast)
48.bit Source Address          = Hardware address of interface
16.bit Frame type              = 0x806 (ARP)
----------------------
16.bit Hardware type           = 0x1 (Ethernet)
16.bit Protocol Type           = 0x800 (IP)
 8.bit Hardware Address size   = 6
 8.bit Protocol Address size   = 4
16.bit Opcode                  = 2 (Reply)
48.bit Sender Ethernet Address = Hardware address of interface
32.bit Sender IP Address       = Local IP address
48.bit Target Ethernet Address = Sender Addr in Request packet
32.bit Target IP Address       = Local IP Address
```

(3) Within a small time period after a host sends a gratuitous ARP packet, if the host receives an ARP reply with both sender IP address and the target IP address fields match the address of the receiving interface, it MUST stop using this address. If this is the only address of the interface, the interface MUST be turned down. If there are multiple IP addresses assigned to the interface, the implementation can choose to only remove the affected address and keep the interface operating with other assigned addresses. The host SHOULD report, log, and/or display messages to indicate the error. If such a reply packet is received outside the time period, the host SHOULD only report, log, and/or display messages, but keep operating with the address.

4. Backwards Compatibility

The hosts with this solution implemented can coexist with other hosts that do not have it implemented. The implementation is trivial and the overhead is very limited. Since one of the primary functions to fully solve the problem is that the second host stops using the duplicate IP address, the problem addressed here cannot be completely avoided unless all hosts on the network follow this document. However, because many existing TCP/IP implementations generate gratuitous ARP packet, as well as error reporting when duplication occurs, running hosts with this solution implemented can increase the chance of catching the error at earlier stage and reduce the possible damage made by an error.

5. Security Considerations

The proposed solution can decrease the impact when a user, either fraudulently or simply by mistake, configures a host with an existing

IP address on the LAN. Nevertheless, the proposed solution is mainly designed to prevent configuration errors, not for malicious attacks. If a hacker can fabricate and transmit ARP packets on a LAN, these packets can easily confuse all hosts on the LAN and to sabotage any

network operations. Preventing malicious attacks within a LAN is sophisticated, and is out of the scope of this document.

A new security concern introduced by the proposed scheme is by having a requirement to disable an interface when a suitable ARP reply is seen. To limit the vulnerability from attacks and network errors, as described in Step (3) of the solution, this disabling SHOULD only happen if the reply is received within some time period of sending out a gratuitous ARP request. A RECOMMENDED default period is 3 seconds, which is long enough to cover normal operations.

6. Reference

[1] Plummer, D., "An Ethernet Address Resolution Protocol", STD 37, RFC 826, MIT, November 1982.

7. Author's Address

Tyan-Shu Jou
Torrent Networking Technologies Corporation
3000 Aerial Center Parkway
Suite 140
Morrisville, NC 27560
U.S.A.

Phone: (919) 468-8466 x233
Email: tsjou@torrentnet.com

8. Full Copyright Statement