                Requirements for Address Selection Mechanisms

Status of This Memo

Abstract

   There are some problematic cases when using the default address
   selection mechanism that RFC 3484 defines. This document describes
   additional requirements that operate with RFC 3484 to solve the
   problems.

Table of Contents

1. Introduction

   Today, the RFC 3484 [RFC3484] mechanism is widely implemented in
   major OSs. However, in many sites, the default address-selection
   rules are not appropriate, and cause a communication failure. The
   problem statement (PS) document [RFC5220] lists problematic cases
   that resulted from incorrect address selection.

   Though RFC 3484 made the address-selection behavior of a host
   configurable, typical users cannot make use of that because of the
   complexity of the mechanism and lack of knowledge about their network
   topologies. Therefore, an address-selection autoconfiguration
   mechanism is necessary, especially for unmanaged hosts of typical
   users.

   This document contains requirements for address-selection mechanisms
   that enable hosts to perform appropriate address selection
   automatically.

2. Requirements of Address Selection

   Address-selection mechanisms have to fulfill the following eleven
   requirements.

2.1. Effectiveness

   The mechanism can modify RFC 3484 default address-selection behavior
   at nodes. As documented in the PS [RFC5220], the default rules
   defined in RFC 3484 do not work properly in some environments.
   Therefore, the mechanism has to be able to modify the address-
   selection behavior of a host and to solve the problematic cases
   described in the PS document.

2.2. Timing

   Nodes can perform appropriate address selection when they select
   addresses.

   If nodes need to have address-selection information to perform
   appropriate address selection, then the mechanism has to provide a
   function for nodes to obtain the necessary information beforehand.

   The mechanism should not degrade usability. The mechanism should not
   enforce long address-selection processing time upon users.
   Therefore, forcing every consumer user to manipulate the address-
   selection policy table is usually not an acceptable solution. So, in
   this case, some kind of autoconfiguration mechanism is desirable.

2.3. Dynamic Behavior Update

   The address-selection behavior of nodes can be dynamically updated.
   When the network structure changes and the address-selection behavior
   has to be changed accordingly, a network administrator can modify the
   address-selection behavior of nodes.

2.4. Node-Specific Behavior

   The mechanism can support node-specific address-selection behavior.
   Even when multiple nodes are on the same subnet, the mechanism should
   be able to provide a method for the network administrator to make
   nodes behave differently. For example, each node may have a
   different set of assigned prefixes. In such a case, the appropriate
   address-selection behavior may be different.

2.5. Application-Specific Behavior

   The mechanism can support application-specific address-selection
   behavior or combined use with an application-specific address-
   selection mechanism such as address-selection APIs.

2.6. Multiple Interface

   The mechanism can support those nodes equipped with multiple
   interfaces. The mechanism has to assume that nodes have multiple
   interfaces and makes address selection of those nodes work
   appropriately.

2.7. Central Control

   The address-selection behavior of nodes can be centrally controlled.
   A site administrator or a service provider could determine or could
   have an effect on the address-selection behavior at their users'
   hosts.

2.8. Next-Hop Selection

   The mechanism can control next-hop-selection behavior at hosts or
   cooperate with other routing mechanisms, such as routing protocols
   and RFC 4191 [RFC4191]. If the address-selection mechanism is used
   with a routing mechanism, the two mechanisms have to be able to work
   synchronously.

2.9. Compatibility with RFC 3493

   The mechanism can allow an application that uses the basic socket
   interface defined in RFC 3493 [RFC3493] to work correctly. That is,
   with the basic socket interface the application can select
   appropriate source and destination addresses and can communicate with
   the destination host. This requirement does not necessarily mean
   that OS protocol stack and socket libraries should not be changed.

2.10. Compatibility and Interoperability with RFC 3484

   The mechanism is compatible with RFC 3484. Now that RFC 3484 is
   widely implemented, it is preferable that a new address selection
   mechanism does not conflict with the address selection mechanisms
   defined in RFC 3484.

   If the solution mechanism changes or replaces the address-selection
   mechanism defined in RFC 3484, interoperability has to be retained.
   That is, a host with the new solution mechanism and a host with the
   mechanism of RFC 3484 have to be interoperable.

2.11. Security

   The mechanism works without any security problems. Possible security
   threats are described in the Security Considerations section of this
   document.

3. Security Considerations

3.1. List of Threats Introduced by New Address-Selection Mechanism

   There will be some security incidents when combining the requirements
   described in Section 2 into a protocol. In particular, there are 3
   types of threats: leakage, hijacking, and denial of service.

   1. Leakage: Malicious nodes may tap to collect the network policy
       information and leak it to unauthorized parties.

   2. Hijacking: Nodes may be hijacked by malicious injection of
       illegitimate policy information. RFC 3484 defines both a source
       and destination selection algorithm. An attacker able to inject
       malicious policy information could redirect packets sent by a
       victim node to an intentionally chosen server that would scan the
       victim node activities to find vulnerable code. Once vulnerable
       code is found, the attacker can take control of the victim node.

   3. Denial of Service: This is an attack on the ability of nodes to
       communicate in the absence of the address-selection policy. An
       attacker could launch a flooding attack on the controller to
       prevent it from delivering the address selection policy
       information to nodes, thus preventing those nodes from
       appropriately communicating.

3.2. List of Recommendations in Which Security Mechanism Should Be
      Applied

   The address selection mechanism should be afforded security services
   listed below. It is preferable that these security services are
   afforded via use of existing protocols (e.g., IPsec).

   1. Integrity of the network policy information itself and the
       messages exchanged in the protocol. This is a countermeasure
       against leakage, hijacking, and denial of service.

   2. Authentication and authorization of parties involved in the
       protocol. This is a countermeasure against Leakage and
       Hijacking.

4. Normative References

   [RFC3484] Draves, R., "Default Address Selection for Internet
              Protocol version 6 (IPv6)", RFC 3484, February 2003.

   [RFC3493] Gilligan, R., Thomson, S., Bound, J., McCann, J., and W.
              Stevens, "Basic Socket Interface Extensions for IPv6", RFC
              3493, February 2003.

   [RFC4191] Draves, R. and D. Thaler, "Default Router Preferences and
              More-Specific Routes", RFC 4191, November 2005.

   [RFC5220] Matsumoto, A., Fujisaki, T., Hiromi, R., and K. Kanayama,
              "Problem Statement for Default Address Selection in
              Multi-Prefix Environments: Operational Issues of RFC 3484
              Default Rules", RFC 5220, July 2008.

Authors' Addresses

   Arifumi Matsumoto
   NTT PF Lab
   Midori-Cho 3-9-11
   Musashino-shi, Tokyo 180-8585
   Japan

   Phone: +81 422 59 3334
   EMail: arifumi@nttv6.net

   Tomohiro Fujisaki
   NTT PF Lab
   Midori-Cho 3-9-11
   Musashino-shi, Tokyo 180-8585
   Japan

   Phone: +81 422 59 7351
   EMail: fujisaki@nttv6.net

   Ruri Hiromi
   Intec Netcore, Inc.
   Shinsuna 1-3-3
   Koto-ku, Tokyo 136-0075
   Japan

   Phone: +81 3 5665 5069
   EMail: hiromi@inetcore.com

   Ken-ichi Kanayama
   INTEC Systems Institute, Inc.
   Shimoshin-machi 5-33
   Toyama-shi, Toyama 930-0804
   Japan

   Phone: +81 76 444 8088
   EMail: kanayama_kenichi@intec-si.co.jp