

Network Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: September 5, 2009

N. Ward  
Braintrust Ltd.  
March 4, 2009

IPv6 Autoconfig Filtering on Ethernet Switches  
draft-nward-ipv6-autoconfig-filtering-ethernet-00

### Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on September 5, 2009.

### Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (<http://trustee.ietf.org/license-info>). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

### Abstract

Many ethernet switch vendors provide features for filtering IPv4 address assignment services - i.e. DHCP, Bootp. This document describes what is necessary for a switch to provide the same level of

Internet-Draft

IPv6 Autoconfig Filtering

March 2009

filtering for IPv6, as a standard on which operators can base equipment selection decisions.

Requirements Language

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](#) [[RFC2119](#)].

Table of Contents

- [1.](#) Introduction . . . . . [3](#)
- [2.](#) Protocols . . . . . [3](#)
  - [2.1.](#) Router Advertisements . . . . . [4](#)
  - [2.2.](#) DHCPv6 Replies . . . . . [4](#)
- [3.](#) Filtering . . . . . [5](#)
  - [3.1.](#) Requests . . . . . [5](#)
- [4.](#) IANA Considerations . . . . . [5](#)
- [5.](#) Security Considerations . . . . . [5](#)
- [6.](#) Acknowledgements . . . . . [6](#)
- [7.](#) Normative References . . . . . [6](#)
- Author's Address . . . . . [6](#)

## 1. Introduction

IPv6 provides several ways of assigning addresses to IPv6 capable hosts. These are the prefix field in Router Advertisement (RA) messages, and stateful DHCPv6. In IPv4, we can filter DHCP and Bootp servers in ethernet switches, allowing only our authorised configuration servers to provide autoconfiguration information to hosts. Few ethernet switches provide similar functionality for IPv6 autoconfiguration services, and many hosts already listen for RA messages and then subsequent to receiving and RA message either configure addressing statelessly, or statefully with DHCPv6.

This represents a problem for many networks, for which the only solution at present is to filter out all IPv6 packets from their ethernet network.

This document describes how to filter RA and DHCPv6 messages so that autoconfiguration can be provided only by authorised hosts and/or switch ports.

## 2. Protocols

In order to filter IPv6 packets, some level of understanding of the IPv6, ICMPv6 and UDP protocols is required by the switch. The following fields are analysed so need to be understood by the switch:

- 1) Ethertype in the ethernet header (always 0x86DD)
- 2) Source MAC address in the ethernet header
- 3) Destination MAC address in the ethernet header
- 4) Version in the IPv6 header (always 6)
- 5) Source IPv6 address in the IPv6 header

- 6) Destination IPv6 address in the IPv6 header
- 7) Next-header in the IPv6 header
- 8) Type and Code in the ICMPv6 header
- 9) UDP source port
- 10) UDP destination port

[2.1.](#) Router Advertisements

Router advertisement messages SHOULD only be sent by routers, and so should enter a switch only from a port with a router, and/or from a router's link-local IPv6 address or ethernet MAC address. Router advertisements can be sent unsolicited (periodically) to multicast IPv6 and MAC addresses, or solicited (on demand) to a specific MAC and IPv6 destination.

The characteristics of a router advertisement message are:

Field	Value
Source MAC Address	Router's MAC address
Destination MAC Address	33:33:00:00:00:01 for unsolicited, a host's MAC address for solicited
Source IPv6 Address	Router's IPv6 link-local address
Destination IPv6 Address	FF01::1 for unsolicited, an address in FE80::/64 for solicited
Next-header	58
ICMPv6 Type	134
ICMPv6 Code	0

Unique to router advertisements is the ICMPv6 type, 134.

## 2.2. DHCPv6 Replies

DHCPv6 reply messages SHOULD only be sent by DHCPv6 servers and relays, and so should only enter a switch from a port with a DHCPv6 server or relay, and/or from a DHCPv6 server or relay's link-local IPv6 address or ethernet MAC address.

The characteristics of a DHCPv6 reply message are:

Field	Value
Source MAC Address	DHCPv6 server or relay's MAC address
Source IPv6 Address	DHCPv6 server or relay's link-local IPv6 address
Destination IPv6 Address	An address in FE80::/64
Next-header	17
UDP source port	547

Ward

Expires September 5, 2009

[Page 4]

---

Internet-Draft

IPv6 Autoconfig Filtering

March 2009

UDP destination port	546
----------------------	-----

Unique to DHCPv6 replies is the UDP source and destination ports, 547 and 546 respectively.

## 3. Filtering

An ethernet switch MUST be able to be configured to filter Router Advertisement and DHCPv6 reply messages under one or both of the following conditions:

- a) The source MAC address is not configured to belong to a router, or DHCPv6 server or relay.
- b) The source IPv6 link-local address is not configured to belong to a router, or DHCPv6 server or relay.
- c) The ethernet frame was not received on a port configured to as authorised to receive these messages.

### [3.1.](#) Requests

It may be desirable for a switch to only transmit Router Solicitation and DHCPv6 request messages out a port if it is configured as a port having a router, DHCPv6 server or relay. Comment is sought for this.

## [4.](#) IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

## [5.](#) Security Considerations

This document describes filtering features for ethernet switches, so improves security of IPv6 auto configuration in switched ethernet environments.

It is unknown if this document introduces any security issues.

Ward

Expires September 5, 2009

[Page 5]

---

Internet-Draft

IPv6 Autoconfig Filtering

March 2009

## [6.](#) Acknowledgements

Discussion on the NANOG mailing list.

## [7.](#) Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

### Author's Address

Nathan Ward  
Braintrust Ltd.

Level 1, 206 Symonds St.  
Auckland, 1010  
NZ

Phone: +64-21-431675  
Email: [nward@braintrust.co.nz](mailto:nward@braintrust.co.nz)