v6ops Working Group G. Van de Velde
Internet-Draft Cisco Systems
Expires: August 16, 2008 J. Brozowski
Comcast Cable
S. Miyakawa
NTT Communications
February 13, 2008

CPE Default Route Detection
<draft-vandevelde-v6ops-cpe-default-route-detection-00.txt>

Status of this Memo

Copyright Notice

Abstract

When the CPE (Customer Premisses Equipment) device is a routed IPv6 device, then detection automation of the upstream connectivity (i.e. the default-route) has not been uniformly described. There are many CPE vendors, and they may have many technologies to achieve this goal. This document provides an overview of the problem space, while

identifying various options within the solution space.

Table of Contents

1. Introduction

A Service Provider (SP) providing IPv6 connectivity to customer networks may want to automate provisioning of IPv6 prefixes and other configuration information to reduce errors and human interaction towards CPE devices. An available tool to achieve this goal is DHCP-PD [1]. DHCP-PD allows for both automated assignment of IPv6 prefixes and of configuration parameter allocation to a customer network.

Where DHCP-PD [1] typical delivers information about the allocated address space to a customer network combined with other configuration parameters, it does not provide information to the customer network about the upstream connectivity through the SP.

This document will provide a problem definition to help the CPE detect its upstream connectivity while providing insight about the potential solution space.

2. Problem statement

If assumed that a customer network is comprised of at least one CPE where the CPE is providing network connectivity (routed) to nodes on the customer network. In this case the CPE is assumed to be more than just a single host or node. It is also assumed that the CPE device is dynamically allocating network and configuration information through DHCP-PD. The CPE may segment received address space and allocate it towards the various interfaces available to the CPE. Techniques for the sub-allocation of delegated IPv6 address space is out of scope for this document.

If the customer network consists out of multiple routers hierarchically organized then only the CPE performing DHCP-PD with the SP network can be used to obtain an parent prefix from which sub-allocations can be derived. Additional care needs to be taken to distribute the through DHCP-PD received IPv6 address space on the CPE amongst the set of customer routers. These techniques and procedures (i.e. hierachical DHCP services) are outside the scope of this document.

Whereas the CPE directly connected to the SP has awareness of the Service Provider allocated address space it is not made dynamically aware of the upstream path to install upstream routing entries, specifically the default route for the customer network. The following sections outline techniques that can be used to obtain and populate (default-)route information in the CPE.

3. Alternatives for Default Route Detection

3.1. Manual Route Configuration on the CPE

The administrator of the CPE may have out-of-band awareness of the default gateway. In this case the administrator may configure routes manually on the CPE. However, even if this option may seem trivial, it is open to human mistakes and requires human action. Hence, it is not a preferenced method of operation for fully automated CPE provisioning.

3.2. Routing protocol between CPE and upstream router

If the CPE has routing capabilities then routing information can be exchanged between CPE and the SP access router. A dynamic routing protocol can be used to achieve this. This solution can be useful if the service provider router has a limited set of CPE's connected. This is due to scalability and possible state-maintenance which tend to require significant amount of bandwidth and processing power. This option will seldomly be useful for home networks where there are often large volumes of devices that connect to a single service provider access router.

3.3. Extension of DHCPv6 with a default-router option

Currently there is no option specified for DHCPv6 to identify the default-router that may be used by the device. If this option were available then it could be used by the CPE to detect its default-router and populate the required routing information on the CPE. Specification of this DHCPv6 option and device behavior to acquire and populate the same is out of scope for this document.

3.4. CPE has both Router and Host functionality

RFC4861 [2] section 6.2.7. Router Advertisement Consistency defines the behavior of routers related to the processing of Router Advertisement messages. It is specified that routers are to inspect router advertisement messages to validate the contents of the same relative to the link. RFC4861 [2] also indicates that any additional behavior beyond this related to the router is out of scope for the RFC.

Further, section 6.3.4. Processing Received Router Advertisements of RFC4861 [2] specifies host behavior relative to the processing of router advertisements. Specifically, the detection and installation of default routes is clearly specified.

Since a CPE can in essence be both router and host. The text in

RFC4861 [2] does not clearly specify how such a device should be expected to behave related to the processing of router advertisements specifically related to the installation of default routes.

A CPE device that is acting as a host and router may listen to Router Advertisements from the SP network and process them as a host to identify/detect its default-router. In addition this default-router information can be used to install routes on the CPE towards external upstream services and devices. This option can provide a scalable solution for (default-)route detection and population on CPE's based upon received Router Advertisement messages. This mechanism does not require any protocol changes or additional traffic on the wire. However, the behavior of the CPE relative to the processing of Router Advertisements requires additional specification.

4. IANA Considerations

There are no extra IANA consideration for this document.

5. Security Considerations

If a CPE device acts as both Router as Host then it will inherit the secruity for both Host as Router as specified in RFC4861 [2]. For the remaining there are no additional security considerations for this document.

6. Acknowledgements

Concept thinking has been done with Ralph Droms, Bernie Volz, Eric Levy-Abegnoli during IETF70.

7. References

7.1. Normative References

7.2. Informative References

[1] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, December 2003.

[2] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

Authors' Addresses

Gunter Van de Velde
Cisco Systems
De Kleetlaan 6a
Diegem 1831
Belgium

Phone: +32 2704 5473
Email: gunter@cisco.com

John Jason Brzozowski
Comcast Cable
1800 Bishops Gate Boulevard
Mt. Laurel,   NJ 08054
USA

Phone: +1 609 377 6594
Email: john_brzozowski@cable.comcast.com

Shin Miyakawa
NTT Communications
Tokyo,
Japan

Phone: +81-3-6800-3262
Email: miyakawa@nttv6.jp

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).