Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: January 17, 2013

T. Tsou, Ed.
Huawei Technologies (USA)
T. Murakami
IP Infusion
S. Perreault
Viagenie

July 16, 2012

Port Set Definition Algorithms Analysis
draft-tsou-softwire-port-set-algorithms-analysis-02

Abstract

This memo analyses the some port set definition algorithms which encodes port set infomation into IPv6 address so as to support stateless IPv4 to IPv6 transition technologies, e.g. 4rd-U and MAP.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on January 17, 2013.

Copyright Notice

Table of Contents

1. Introduction

Some stateless IPv4 to IPv6 stransition technologies are invented by the industrial to provide IPv4 network service through IPv6 network, which also support IPv4 address sharing via port sets. These technologies can significantly simplify the implementation of the border router and reduce resource requirement.

In these solutions, a port set is assigned to each CPE, and can be calculated by a port set ID in conjunction with some other parameters; for any port number, the corresponding port set ID can also be derived, that means, the mapping algorithm must be reversible. When the CPE needs to send an IPv4 packet, it can map an IPv4 packet into an IPv6 packet, either by translation or encapsulation, the IPv4 address and port set ID will be embedded into an IPv6 address; when the BR receive the IPv6 packet, it will decapsulate it. When the BR need to forward an IPv4 packet to the CPE, it will first derive the port set ID from the port, and then map the IPv4 packet into an IPv6 packet.

In order to support these technologies, some port set definition algorithms are worked out. It may be useful to analyse the characteristics of these algorithms for better understanding and to choose a proper algorithm for different needs.

A good port set definition algorithm must be reversible, easy to implement, and should be able to define non-continuous or random port sets for better security, be able to exclude the well known ports, 0 ~ 1023 or 0 ~ 4095, etc.

This memo will analyse the following characterics:

- Port set type: continuous, non-continuous, random
- Stateless: yes or no
- Security: security level, continuous port set provides common security, random port set provides good security.
- Implementation: implementation complexity, performance, etc.
- Friendliness for NAT44: comply with NAT44 or not
- Sharing ratio: maximum, minimum sharing ratio
- Revert calculation from port number to PSID at BR.

- Exclude well known ports

2. Terminology

BR: Border Router.

CPE: Customer Premise Equipment.

GMA: Generalized Modulus Algorithm.

MAP: Map Address and Port.

PSID: Port Set ID, one of the key parameters used to derived a set of ports.

3. Various types of algorithms

Currently, the port set definition algorithms can be classified into three categories: GMA style, Mask/Value style and cryptographical style.

3.1. GMA style algorithms

Currently there are three sets of draft support GMA style algorithm: MAP [I-D.ietf-softwire-map-01], 4rd-U [I-D.ietf-softwire-4rd-02] and, but they are not exactly all the same.

3.1.1. MAP

In MAP [I-D.ietf-softwire-map-01], a port set can be defined by the following parameters:

R: sharing ratio;

P: PSID;

M: maximum number of contiguous ports.

To derive a port from the port set, the following equation can be used:

Port = R * M * j + M * P + i

j is port range index: j = (4096 / M) / R to ((65536 / M) / R) - 1, if the port numbers (0 - 4095) are excluded.

i is the port index in a sub port set, i = 0 to M-1;

To derive the PSID from a given port:

PSID = (floor(Port/M)) % R, where % is the modulus operator.

Parameter M is to generate non-continuous ports sets, rather than a single continuous port set, which brings better sercurity. If M=1, a single continuous port set is defined.

PSID will be encoded in the IPv6 address, as shown in Figure 1 and Figure 2.

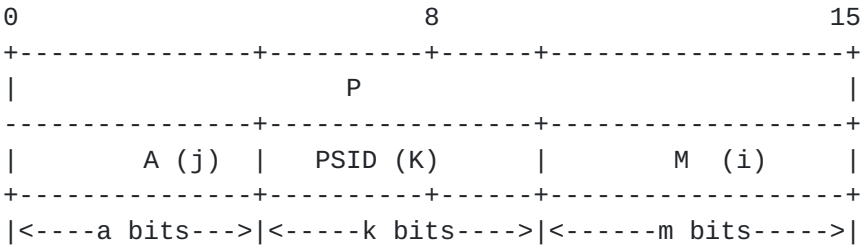

Figure 1: Bit representation

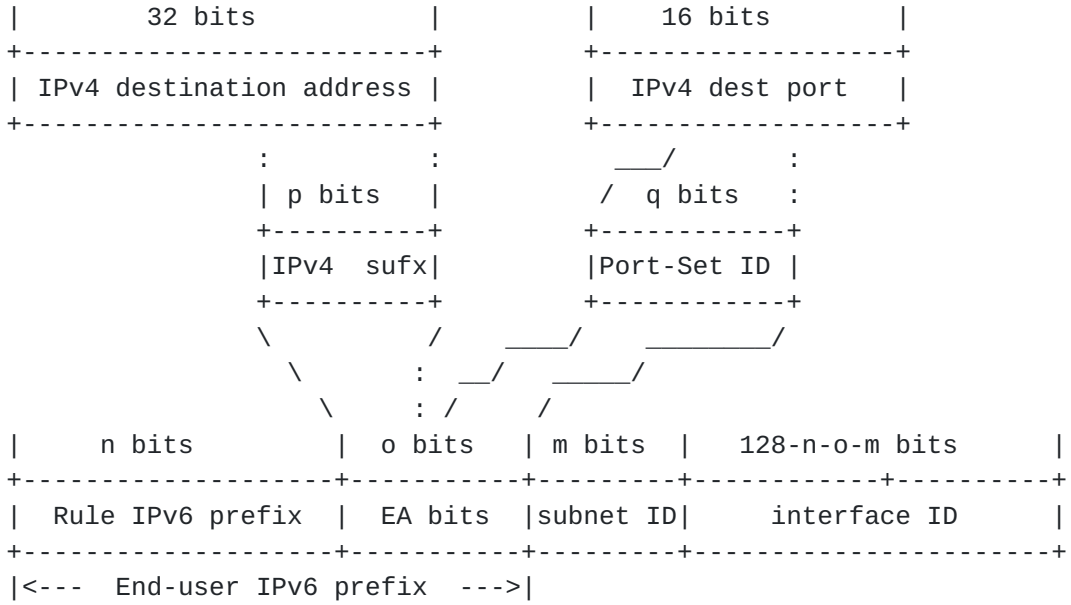

Figure 2: Deriving of MAP IPv6 address

3.1.2. 4rd-U

In 4rd-U [I-D.ietf-softwire-4rd-02], PSID itself is sufficient for defining a port set, as shown in Figure 3.

To derive the PSID from a given port, it only needs to take out the PSID bits from the 16bit port number.

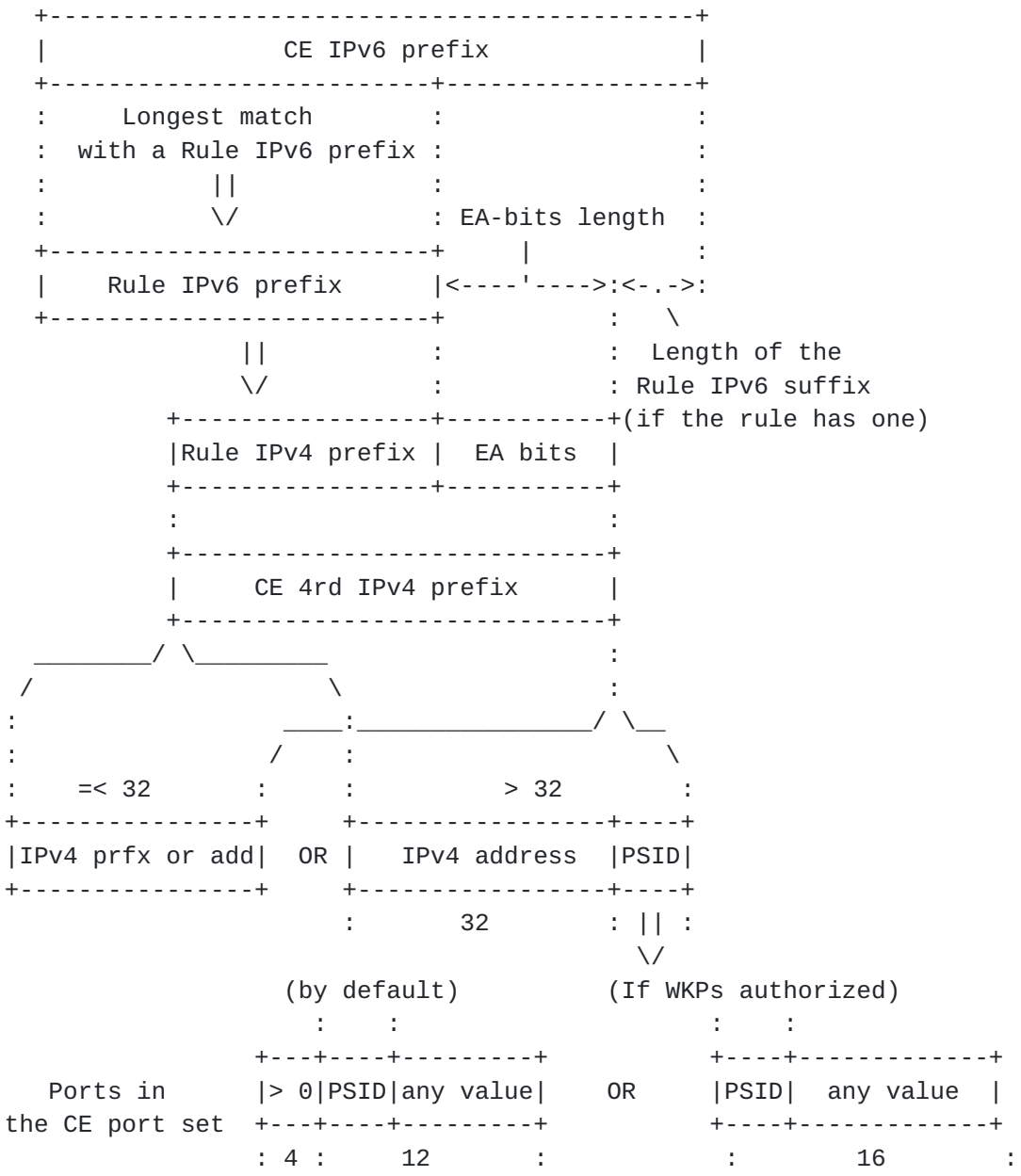

Figure 3: From CE IPv6 prefix to 4rd IPv4 address and Port set

3.1.3. Summary

Port set type	no-continuous
Stateless	yes
Security	good
Implementation	easy
Friendliness for NAT44	yes
Sharing ratio	up to 2^12
Revert calculation from port number to PSID at BR	yes
Exclude well known ports	yes, 0~1023 or 0~4095

1. 4rd-U is a parameter-free algorithm, which is different MAP; while MAP can provide more variation due to the extra parameter(s). From the port set definition point of view, MAP and 4rd-U provide the same level of security.

2. MAP support sharing ratio up to 2^16, although it may not be necessary.

3.2. Mask/Value style algorithms

[RFC6431] defines an IPCP option to allocate port set to CPEs, as shown in Figure 4.

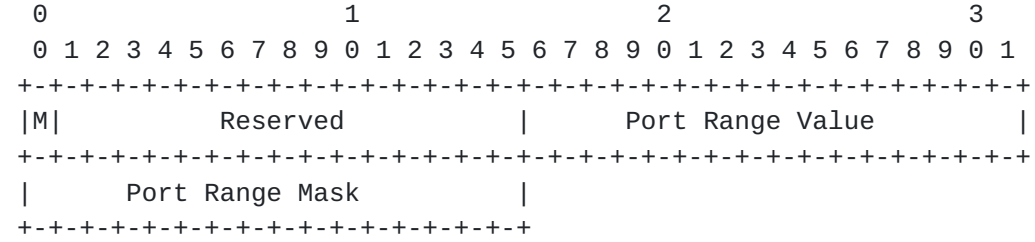

Figure 4: IPCP option format

The Port Range Value can be encoded in IPv6 address, similar as parameter PSID in other technologies, e.g. MAP [I-D.ietf-softwire-map-01].

To derive the Port Range Value from a given port, the port number should porform bit-and operation with the Port Range Mask.

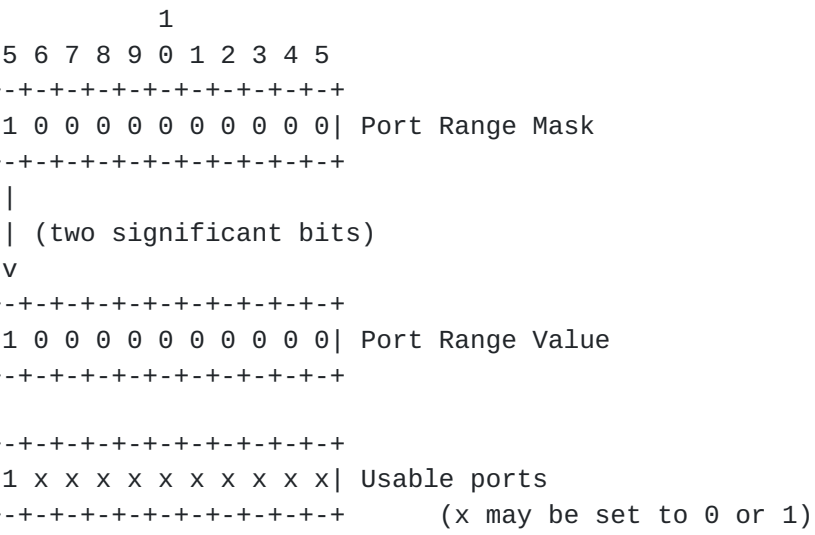

Figure 5: Example of Port Range Mask and Port Range Value

This alogrithm can have some kind of randomization effect by setting different number of bits and bits at different location in the Port Range Mask.

This algorithm may have a problem if the well known ports(0~1023 or 0~4096) need to be excluded, it is a bit difficult to achieve that. But if the operator do not have a specific usage for the well known ports, then it is OK to allocate those port to end users, just like other common ports. Some tests have done and prove that is OK.

Port set type	continuous, no-continuous
Stateless	yes
Security	good
Implementation	easy
Friendliness for NAT44	yes
Sharing ratio	up to 2^16
Revert calculation from port number to PSID at BR	yes
Exclude well known ports	difficult

```
       -------------------------------+----------------------------
```

3.3. Cryptographical style algorithms

The cryptographical port set definition algorithm introduced in [RFC6431] can provide very good security, but it is very difficult to derive the port set infomation, e.g. the starting point, from a given port. This algorithm can only be used in stateful scenarios, the BR must be operated in stateful mode.

In order to use this kind of algorithm in a stateless scenario, the algorithm must be reversible, that is, with some given information, it should be able to derive the port set information from a given port number.

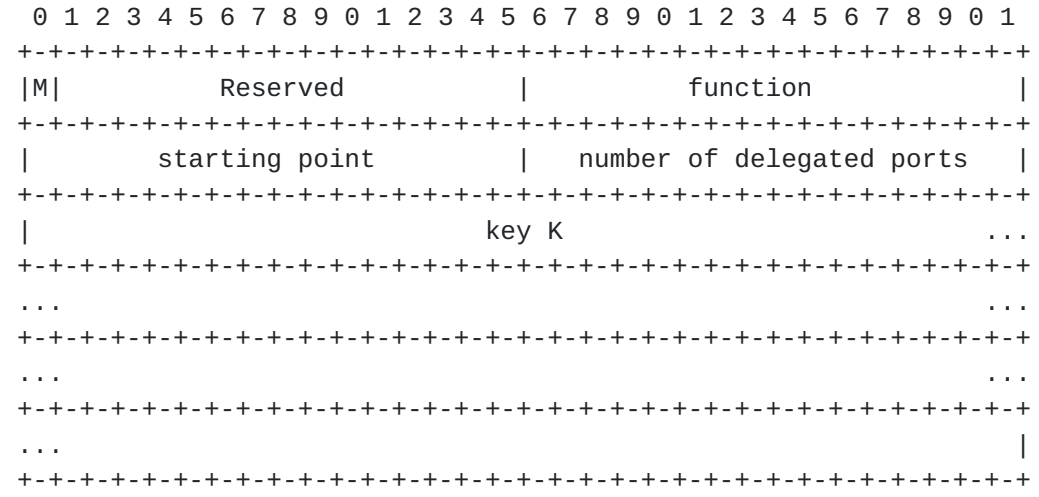

Figure 6: Format of the Cryptographically Random Port Range Option

Port set type	continuous, no-continuous
Stateless	No *
Security	Very good
Implementation	difficult
Friendliness for NAT44	yes
Sharing ratio	up to 2^16
Revert calculation from port number to PSID at BR	No *
Exclude well known ports	difficult

* It may be possible to find a cryptographic algorithm which can be reversed, e.g. define a reversible one-to-one mapping algorithm. But that is out the scope of this memo. If strong security is required, it may be worth giving this topic further study.

4. Conclusion

TBD.

5. IANA Considerations

This memo includes no request to IANA.

6. Security Considerations

The port set should be as random as possible, in order to make it difficult to predict what the next port will be used, to avoid some potential TCP attack [RFC6056].

7. References

7.1. Normative References

[I-D.ietf-softwire-4rd-02]
Despres, R., Penno, R., Lee, Y., Chen, G., and S. Jiang,

"IPv4 Residual Deployment via IPv6 - a unified Stateless Solution (4rd) (Work in progress)", Jan 2012.

[I-D.ietf-softwire-map-01]
Troan, O., Dec, W., Li, X., Bao, C., Zhai, Y., Matsushima, S., and T. Murakami, "Mapping of Address and Port (MAP) (Work in progress)", Jun 2012.

[RFC6056] Larsen, M. and F. Gont, "Recommendations for Transport-Protocol Port Randomization", BCP 156, RFC 6056, January 2011.

[RFC6431] Boucadair, M., Levis, P., Bajko, G., Savolainen, T., and T. Tsou, "Huawei Port Range Configuration Options for PPP IP Control Protocol (IPCP)", RFC 6431, November 2011.

7.2. Informative References

[I-D.bsd-softwire-stateless-port-index-analysis]
Boucadair, M., Skoberne, N., and W. Dec, "Analysis of Port Indexing Algorithms", Sept 2011.

Authors' Addresses

Tina Tsou (editor)
Huawei Technologies (USA)
2330 Central Expressway
Santa Clara CA 95050
USA

Phone: +1 408 330 4424
Email: tina.tsou.zouting@huawei.com

Tetsuya Murakami
IP Infusion
1188 East Arques Avenue
Sunnyval
USA

Email: tetsuya@ipinfusion.com

Simon Perreault
Viagenie
246 Aberdeen
Quebec, QC G1R 2E1
Canada

Phone: +1 418 656 9254
Email: simon.perreault@viagenie.ca
URI: http://viagenie.ca