Deploying IPv6 in University Campus Network - Practical Problems

Tomas Podermański
Brno University of Technology
tpoder@cis.vutbr.cz

Matěj Grégr
Brno University of Technology
igregr@fit.vutbr.cz

Abstract

IPv4 addresses are still running out. Global IPv4 address pool administered by IANA organization is depleted together with IPv4 pool of APNIC Routing Registry. This situation pushes organizations to think about IPv6 transition. Unfortunately IPv4 and IPv6 are incompatible protocols which raise new security issues and problems with user monitoring and accounting. The article shares experiences of deploying IPv6 on the university campus network and describes the most significant troubles that we have been faced with. It describes and compares differences in first hop security in IPv6 and IPv4 networks. Issues connected with user addressing, accounting and monitoring are also discussed. The experience is mainly based on the deployment of IPv6 on the campus network at Brno University of Technology which is one of the biggest universities in the Czech Republic.

Keywords:

IPv6, Security, Accounting

1 Introduction

It is now a few months since IANA has run out of IPv4 addresses. Large ISPs have usually reserved some address pool for the future, but requesting new IPv4 addresses from LIRs will be much more difficult and probably impossible. Unfortunately there are more and more devices, which require an Internet connection – smart phones, PDAs, netbooks etc. One solution for the ISP to meet their requirements is to use NAT. This works well for basic connectivity, but causes difficulties to many applications. There are also scenarios where large ISPs will trade with their unallocated IPv4 addresses. However both of them can be considered as only short term solutions.

The only perspective solution is deploying IPv6. IPv6 is not compatible with IPv4 so the networks will have to run both protocols, until all services are available on IPv6. Deploying IPv6 brings many new issues. Techniques for IPv6 address assignment implemented differently in various operating systems (OS) can be one of the examples. Missing implementations of security tools (RA Guard, SEND etc.) is also a serious issue. The new feature - privacy extensions [1], makes user's identification more difficult. This behavior is desired to ensure user privacy, however it is in contradiction with a unique user identification in a local network which is necessary for a network administrator. New ways to deal with this feature needs to be developed. Transition techniques raise security problems [7]. Improperly configured operation systems sending rogue Router Advertisement can cause network malfunctioning [2]. These are other examples of problems that network administrators are facing. New ways to manage IPv6 network needs to be found.

This article assembles experience with deploying IPv6 at the campus network at Brno University of Technology (BUT) that is one of biggest universities in the Czech Republic. The network was built up as the result of cooperation amongst other universities placed in Brno and Czech Academy. The campus network connects together several institutions (University faculties, research Institutions, Czech Academy, high schools) placed on over 20 locations in different parts of Brno. Each location is connected at least with two optical cables from two independent directions to achieve maximum reliability of the network. The total length of the optical cables is over 100km.

The core of the network is based on 10 Gb/s Ethernet technology using HP ProCurve and Extreme Networks devices. OSPF and OSPFv3 routing protocols are used as the interior routing protocol. External connection to the National Research and Education

Network (NREN) that is run by CESNET is provided over two 10Gb/s lines with BGP and BGP+ routing. The topology of the core of the network is shown in the Figure 1.

The IPv6 campus connectivity is implemented according to the Internet Transition Plan [4]. Most of the parts of the university already provide native IPv6 connectivity and significant part of devices connected to the campus network can fully use IPv6.

From the user perspective the BUT university campus network connects more than 2,500 staff users and more than 23,000 students. The top utilization is at student dormitories where more than 6,000 students are connected via 100 Mb/s and 1Gb/s links. It is a really big challenge to provide functional and stable IPv6 connectivity to that amount of users.

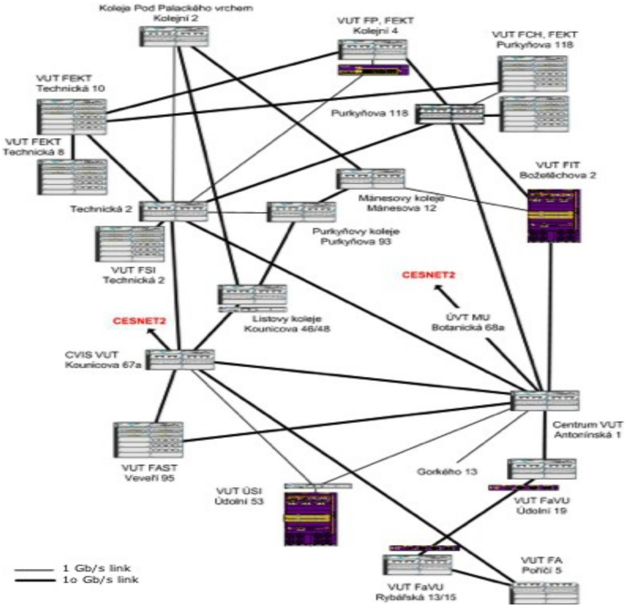

Figure 1: Topology of the BUT campus network

2 Current status of IPv6 deployment at Brno University of Technology

IPv6 related activities started at university several years ago. In that time a temporary IPv6 network was created especially for testing purposes. Routing was performed on the PC based routers with routing software XORP and outside connectivity to NREN was encapsulated inside tunnels. The IPv6 infrastructure was completely separated in order to minimize impact of IPv6 infrastructure to running IPv4 services. That means the IPv6 network was run on dedicated routers and cable/fiber infrastructure. There were not any critical services running on IPv6 in that phase.

The significant change became in 2010 when university started participating on HP ProCurve beta testing program. That was mainly focused on IPv6 features in the HP ProCurve devices that are widely used on the BUT network. Thanks to pretty good results from beta testing program the decision to move the core of the network to dualstack was made in the middle of 2010. IPv6 was enabled on all devices in the core network. At the end of 2010 the topology and the IPv6 network started completely following the topology of the IPv4 network. In the same time university decided to get own provider independent (PI) IPv6 address space to be able to use multihomed IPv6 connections. Today, the IPv6 and IPv4 network provide almost same services on wire speed.

During the process of moving to IPv6 we have encountered with several problematic issues. Some of them are very essential and nowadays there are still not proper solutions for them. In the following lines we will try to point out some of them.

3 IPv6 problems to solve and possible solutions

3.1 Addressing issues

One of the basic problems is address assignment for the client systems. The mixture of various OSs requires a solution of automatic address assignment that is supported by most systems. The stateful autoconfiguration using DHCPv6 is very difficult to use today because the lack of support in Windows XP, which is still very widespread OS, and older version of MAC OS. DHCPv6 does not support all configuration options (e.g. option for default route), so the stateless autoconfiguration (SLAAC) [3] has to be used as well. Unfortunately, the stateless autoconfiguration in some operating systems turns on privacy extensions which mean that the devices use a random end user identifier (EUI) named *Temporary IPv6 Addresses.* This is a brand new IPv6 feature that allows a node to automatically generate a random IPv6 address on its own.

However, this requirement contradicts the need to identify a malevolent user. Private, temporary addresses hinder the unique identification of users/hosts connecting to a service. This affects logging and prevents administrators from effectively tracking which users are accessing IPv6 services. Many internal resources require the ability to track the end user’s use of services.

If a local security policy requires better control, either fixed IPv6 addresses must be centrally assigned and logged, which is not a feasible option for a large network, or stateful configuration using DHCPv6 has to be deployed. However, in that case, same operating systems (Windows XP, older versions of MAC OS, some Linux and BSD systems) will not have access to IPv6 network.

IPv6 auto configuration options also increase complexity. There are two fundamentally different mechanisms and protocols where one cannot fully work without the other. Configuration of Recursive DNS servers is nowadays not possible using SLAAC and with DHCPv6 it is not possible to configure the default gateway address (default route). As a result, the only working method is to use both protocols simultaneously. Failure of either mechanism whether through faulty configuration, bugged software or targeted attack, leads to denial of IPv6 connection to the user. Moreover diagnostics are fairly complicated and it requires good knowledge of both mechanisms.

3.2 First hop security

IP address autoconfiguration process might be perceived as a honey pot for a hacker. If the hacker is able to interfere the configuration process, the whole user's traffic can be rerouted to the attacker PC. In many cases it does not need to be a targeted attack, but simply an accident, where a user connects a Wi-Fi router with a preconfigured DHCP server to the network and cause a network malfunction for other users.

This problem, as the other problems with first hop security, is known in IPv4 world for quite long time. For this reason some mechanisms were created in the IPv4 world which would prevent or at least complicate some of these attacks. The best place to implement protection for end users is on the end-user switch access port to which the user is connected. Different vendors use slightly different terminology for individual types of protection but generally we can meet the following ones:

- **DHCP Snooping:** Some ports are explicitly defined in the switch configuration so port is able to receive DHCP responses from DHCP (so called trusted port). It is assumed that somewhere behind the trusted port is a DHCP server. If a reply from a DHCP server arrives to a port not defined as trusted the response is discarded. Any DHCP server running on the client system (whether intentionally or by accident) does not threaten other clients on the network because the answers will not reach further than the access port for which this protection has been activated. DHCP snooping is usually prerequisite for other protection mechanisms such as IP lockdown or ARP protection as described below.
- **Dynamic ARP protection, ARP inspection:** DHCP snooping database contains MAC address – IP address – switch port combination. This database is then used on untrusted ports to inspect ARP packets. Other MAC addresses not recorded in the database are discarded. This eliminates attacks focused on creating fake records in the ARP table (poisoned ARP cache).
- **Dynamic IP Lockdown, IP source guard:** Another degree of protection is achieved by inspecting source MAC and IPv4 address on untrusted ports for all packets entering the port. This eliminates spoofing a source IPv4 or MAC address. Another often appreciated feature of this mechanism is the fact that the client cannot communicate over the network unless an IP address from the DHCP server is obtained.

The IPv6 autoconfiguration and neighbor discovery can be vulnerable to similar attacks as autoconfiguration in IPv4 networks [7]. Nowadays, network administrators of IPv6 networks are facing mainly to problem with rogue router advertisements, which is similar to the problem of fake DHCP server in IPv4 networks. Many rogue advertises are generated by Windows computers. This is a serious issue because computers propagate their own interface as a default gateway. Unfortunately this behavior can be in some conditions caused by properly used Internet connection sharing service. The Figure 2 shows the number of rogue advertises on the network with approximately 2000 active devices connected to.

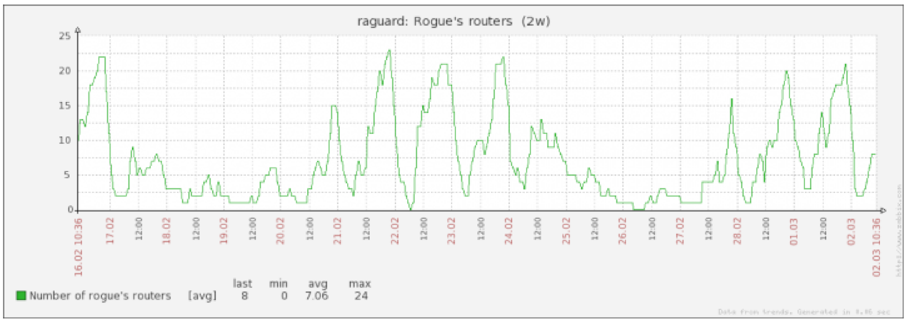

Figure 2: Number of rogue's routers

Described solutions for mitigating attacks in IPv4 networks are implemented in most of access switches on the market. IPv6 techniques for autoconfiguration are different so new solutions are necessary. Security mitigation techniques in IPv6 networks are described below.

- **Source Address Validation Improvements (SAVI):** The Source Address Validation Improvement method was developed to complement ingress filtering with finer-grained, standardized IP source address validation [13]. Framework has option for DHCP servers [8] and tries to solve a mechanism similar to the one we described with DHCP snooping for IPv4. It is limited to DHCPv4 and DHCPv6 and does not deal with the problems of rogue Router Advertisement messages. SAVI is mainly supported in devices produced by Hewlett Packard - A series.
- **SEND – Secure Network Discovery:** This method tries to deal with autoconfiguration problem in a totally different way. SEND is based on signing packets with cryptographic methods [12]. Apart from a router it does not require support on the active network devices level. The validity verification itself through message certificate takes place at the end-user system. IPv6 address of the end-user system is a result of a cryptographic function (see, we have another auto configuration method). Using SEND directly excludes using EUI 64 addresses and Privacy Extensions. SEND has one big advantage - it not only solves the auto configuration problem but also other safety problems of the Network Discovery protocol (RFC 2461). Another advantage is independent infrastructure; hence it can also be used in Wi-Fi networks for instance.

  The main shortcoming of SEND is the fact that it requires the support of public key infrastructure according to X 509. To make it work properly you need to install a certificate of the authority which issues router certificates. There are other than security risks associated with SEND. SEND is a patented Cisco technology (US patent number 20080307), therefore no-one would be surprised that it is implemented especially on devices of this company. Presence of patent raised several discussion especially with SEND and RA Guard integration. According to Cisco statement, Cisco will not assert any patents against any party that implements the standard [14].

  SEND protocol is not supported on any operation systems. There are some basic Linux implementation and kernel patches, however that cannot be used in production environment. Windows OS, as the most widespread OS, nor Mac OS do not support the SEND protocol even in the most recent versions. SEND protocol could potentially solve security problems of NDP protocol, however it cannot be deployed and there are no indications, that this should change in the future.
- **RA Guard:** Another alternative which however deals only with the issue of fake router advertisements is IPv6 Router Advertisement Guard [5]. It is similar technique as DHCP snooping, but for Router Advertisement packets. It tries to block fake router advertisements on the access user port. Apart from tools which should ease the initial switch configuration (learning mode), it opens the path to integration with SEND. In this mode the switch works as so called node-in-the-middle, where switch with activated RA Guard uses information from SEND to verify packet validity and for the connected end-user system it appears as normal Router Advertisement packet. As you could guess from the title RA Guard does not solve DHCP or DHCPv6 issues in any way. We can already find an implementation in some Cisco devices.

All of the above possibilities can be used rather theoretically today. Either they are not implemented on clients or the device support is missing. Another issue is that if the protective devices are to be truly purposeful they must be placed as close to the end-user system as possible. This could often mean a complete replacement of network infrastructure which is a job that few will want to undergo just to implement IPv6. More affordable solutions which would at least alleviate efforts to paralyze the IPv6 auto configuration mechanism are following.

- **Access Lists on the switch:** This solutions was published by Petr Lampa within the CESNET working group. It assumes that we can configure IPv6 access lists on the active device.

```
01: ipv6 access-list block-ra-dhcp
02: 10     deny icmp any any 134 0
03: 20     deny udp any eq 547 fe80::/64 eq 546
04: 30     permit ipv6 any any
05: exit
06: interface 1–44
07:        ipv6 access-group block-ra-dhcp in
08: exit
```

The aforementioned access list will block all ICMPv6 messages type 134 (RA messages line no. 2) and it will block traffic to the 546 target port (dhcpv6-client, line no. 3). The rules are subsequently applied to the inputs of ports to which the clients are connected (line no. 7). This can eliminate instances of rogue routers and DHCPv6 servers. The aforementioned example can be used for some HP switches and can be an inspiration for other platforms as well. A required condition to use this mechanism is IPv6 ACL support on the relevant switch. The problem of that solution is that very few access switches supports creation if IPv6 access-lists today. Also price of that switches is usually two or three times higher comparing to the switches where those IPv6 are not implemented.

Passive monitoring

Another option is detection of fake Router Advertisements. This will not protect us much from a well-crafted and targeted attack but it can at least detect incorrectly configured clients. We will need to use this solution if none of the options above can be used. For many networks it would be the only usable solutions for a long time. All tools for detection of rogue Router Advertisements work based on the same principle. They connect to the `ff02::1` multicast group where the aforementioned messages spread and thus will be able to monitor all messages appearing on the network. They can then tell the administrator about the undesirable status, call an automated action (Ndpmon, Ramond), or even send a message canceling the validity of fake Router Advertisements (rafixd) back to the network.

3.3 User tracking, monitoring and accounting

Long-term network monitoring, accounting and backtracking of security incidents is often achieved in IPv4 networks using NetFlow probes and collectors. This can be a problem if IPv6 is deployed and privacy extensions are allowed in the network. Same user can than communicate with different addresses. That means that address cannot be used as a unique identifier anymore. As the part of deploying IPv6 we tried to develop extension to existing monitoring systems to allow easier tracking users in an IPv6 network.

The main idea of the extension is collecting and putting together data obtained from differed parts of the network. A neighbor cache database [6] on routers and forwarding databases on switches can provide to us information about relation between IPv6 address port on switch and a MAC address used by user. In the next step a MAC address can be used for identifying user in the database provided by radius server.

All of these pieces of information, together, provide a complex view of the network and can help to identify a host. A tuple *(IPv6 address, MAC address, Login name)* is sufficient to identify a host/user. In practice, an extended tuple is built: (*Timestamp, IPv6 address, MAC address, Switch port, Login)* as described in the Figure 3*.*

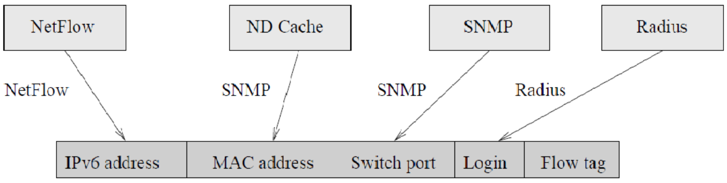

Figure 3: Extended NetFlow record

Timestamp is added to provide a history of communication. Switch port is necessary if the user is blocked or if an unregistered MAC address is used on some port. In addition to these values, the VLAN number and interface statistics are stored; however, these data are not necessary for host identification.

It is important to note that this data structure is not created at once, but it is filled in when data are available. For instance, NetFlow data are taken from the NetFlow probe when they are sent to the collector. However, there is no information about MAC addresses yet. The address is downloaded later from the switch's ND cache. Login data from RADIUS can also be added. However, RADIUS data are not available for every user - only for those who are connected using 802.1x authentication. For other users, only the IPv6 address and the switch port number and MAC address are used for identification.

Collecting Monitoring Data

Data are collected using the SNMP protocol and stored in the central database where the network administrator can search data using the IPv6, IPv4 or MAC addresses as keys. Useful tool for pooling and storing information from switches and routers is Network Administration Visualized (NAV) [9]. SNMP pools the data from switches every fifteen minutes. The mapping between the IPv6 address and its corresponding MAC address is downloaded from the router's neighbor cache. Port, VLAN number and other information comes from the switch's FDB (Forwarding Database) table. Traffic statistics are obtained from NetFlow. NetFflow records alone are not sufficient for user surveillance and activity tracking because of the temporary IPv6 addresses as described in previous sections.

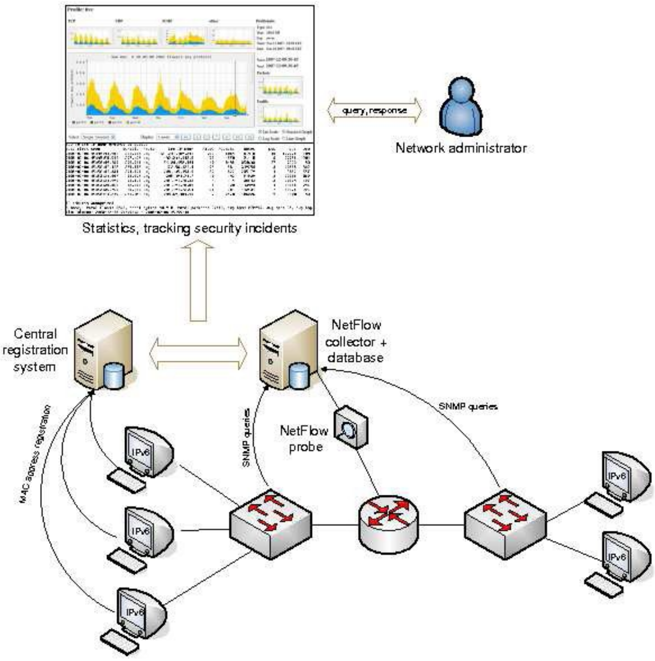

Figure 4: The Central Monitoring System for IPv4 and IPv6 at BUT

Therefore, NetFlow records are extended by additional information called *flow tags*. The flow tag is added to a flow record after its creation, usually when the information is received and stored at the main database. The tag is a unique identifier of the user, because NetFlow records are generated for every single connection of the user, even with different IPv6 addresses. Flow tags can be used as keys to identify the activities of any user stored in the system. This is necessary because not all data are available immediately in the central monitoring system, for example, due to a delay caused by SNMP pooling. When flow tags are added, more complex statistics based on the flow data are created, for example, top-N users.

The time dependency of the gathering of different data is crucial when accessing the ND Cache. This temporary memory at the router stores information needed to build the link between the IPv6 address and the MAC address. Because IPv6 addresses change in time and have limited validity, if the ND entry is lost, there is no way to link the IPv6 address and the user/host. To ensure that all information is stored properly in the monitoring system, the SNMP polling interval has to be shorter than the expiration timeout of the

ND Cache. Otherwise, some entries in the ND Cache could expire without being downloaded into the central system. Typical timeouts for collecting SNMP and RADIUS data are fifteen minutes. The ND Cache expiration timeout is usually set to more than one hour.

4 Conclusion

This paper presents security and addressing issues in IPv4 and IPv6 protocol and solutions how to solve them. Nowadays, the IPv6 traffic volume is low, but this is caused by the lack of IPv6 sources (web pages, servers) on the Internet. Also widespread operation systems such as Windows XP supports IPv6 but IPv6 is not enabled by default.

Next generation Windows systems together with Linux, Mac OS and Unix systems have however IPv6 protocol enabled by default and penetration of these systems is growing. Security and addressing issues discussed in this paper present overview problems we encountered when deploying IPv6 protocol on BUT campus network. Addressing issues and problems with user tracking in IPv6 protocol introduce the necessity for the new monitoring system which is able to overcome the specific problems in IPv6 address assignment. Solutions, how to solve these issues, are proposed. We discussed possibilities, how we are able to limit the impact of security problems in IPv6 network together with monitoring and tracking system which is able to identify and track a host in IPv4 and IPv6 network.

5 Bibliography

[1] T. Narten, R. Draves, and S. Krishnan. Privacy Extensions for Stateless Address Autoconfiguration in IPv6. RFC 4941, September 2007, url: http://tools.ietf.org/html/rfc4941

[2] T. Podermanski: Security concerns and solutions with IPv6, GN3 IPv6 Workshop - Networking without IPv4?, [online], url: http://ow.feide.no/geantcampus:ipv6_mar_2011

[3] S.Thomson, T.Narten, and T.Jinmei. IPv6 Stateless Address Autoconfiguration. RFC 4862, September 2007, url: http://tools.ietf.org/html/rfc4862

[4] J. Curran: An Internet Transition Plan, RFC 5211, July 2008, url: http://tools.ietf.org/html/rfc5211

[5] E. Levy-Abegnoli, G. Van de Velde, C. Popoviciu, J. Mohacsi: IPv6 Router Advertisement Guard, RFC 6105, February 2011, url: http://tools.ietf.org/html/rfc6105

[6] T.Narten, E.Nordmark, W.Simpson, and H.Soliman. Neighbor Discovery for IP version 6 (IPv6). RFC 4861, September 2007, url: http://tools.ietf.org/html/rfc4941

[7] S. Frankel, R. Graveman, and J. Pearce. Guidelines for the Secure Deployment of IPv6. Technical Report 800-119, National Institute of Standards and Technology, 2010. url:http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf

[8] J. Bi, J. Wu, G. Yao, F. Baker: SAVI Solution for DHCP (work in progress) July 2011, url: http://tools.ietf.org/html/draft-ietf-savi-dhcp-10

[9] UNINETT and Norwegian University of Science and Technology: NAV, [online], 2011-03-15, url: http://metanav.uninett.no/

[10] J. Bi, G. Yao, J. Wu, F. Baker.: Savi solution for Stateless Address – work in progress, April 2010, url: http://tools.ietf.org/html/draft-bi-savi-stateless-00

[11] E. Levy-Abegnoli, G. Van de Velde, C. Popoviciu, J. Mohacsi.: IPv6 Router Advertisement Guard. RFC 6105, February 2011. url:http://tools.ietf.org/html/rfc6105

[12] J. Arkko, Ed., J. Kempf, B. Zill, P. Nikander: SEcure Neighbor Discovery (SEND). RFC 3971, Febuary 2011, url:http://tools.ietf.org/html/rfc3971

[13] Wu, J., Bi, J., Bagnulo, M., Baker, F., and C. Vogt: Source Address Validation Improvement Framework", draft-ietf-savi-framework-04 (work in progress), March 2011.

[14] R. Albright, Cisco System's Statement of IPR related to draft-ietf-v6ops-ra-guard-02, April 2009, url : http://www.ietf.org/ietf-ftp/IPR/cisco-ipr-draft-ietf-v6ops-ra-guard-02.txt