INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2009-2012

STUDY GROUP 17

TD 2223

English only

Original: English

Question(s): 2/17 Geneva, 24 August-2 September 2011

TEMPORARY DOCUMENT

Source: Editors

Title: A revised draft text of X.ipv6-secguide

Attachment is a revised draft text of X.ipv6-secguide based on the Q2/17 discussion. This should be reviewed in Q2/17.

TSB Note: All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Attachment

CONTENTS

1 Scope 3

2 References 3

3 Definitions 3
- 3.1 Terms defined elsewhere 3
- 3.2 Terms defined in this Recommendation 3

4 Abbreviations and acronyms 3

5 Conventions 4

6 Topology of IPv6 Network 4

7 Network Devices 5
- 7.1 Router 5

8 Client/Server Devices 6
- 8.1 End nodes 6
- 8.2 DHCP Server 7

9 Security Devices 8
- 9.1 IDS 8
- 9.2 Firewall 9

Appendix I Use case: IPv6 Promotion Council in Japan 10
- I.1 Background and objectives of IPv6 Promotion Council in Japan 10
- I.2 Aims of the Council 10
- I.3 Security Considerations for Information 10

Appendix II Use case: IPv6 Technical Verification Consortium 11
- II.1 Objectives of IPv6 Technical Verification Consortium in Japan 11
- II.2 Activities of the Consortium 11

Bibliography 12

X.ipv6-secguide

Technical security guideline on deploying IPv6

1 Scope

This Recommendation specifies security threats in IPv6 and provides practical risk assessment of them and the technical solutions of a secure IPv6 deployment. This Recommendation focuses on three components, i.e., network devices (e.g., router, switch), server/client devices (e.g., end nodes, DHCP server) and security devices (e.g., IDS, FW) that will be essentially deployed on IPv6 network. The purpose of this Recommendation is to provide a technical security guideline to operators of enterprise networks that are planning to deploy IPv6, so that they are able to mitigate security threats on their IPv6 network.

2 References

None

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 **[TBD]**

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 [TBD]

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
DMZ	DeMilitarized Zone
IDS	Intrusion Detection System
FW	Firewall
ISP	Internet Service Provider
LSA	Link State Advertisement
RA	Router Advertisement
NS	Neighbor Solicitation
NA	Neighbor Advertisement
DAD	Duplicate Address Detection

DHCPv6	Dynamic Host Configuration Protocol version 6
ICMPv6	Internet Control Message Protocol version 6
DNS	Domain Name System
OSPFv3	Open Shortest Path First version 3
MAC	Media Access Control
CPU	Central Processing Unit

5 Conventions

None.

6 Topology of IPv6 network

This clause describes the general topology of IPv6 network (including transition environment to IPv6 where there exist three different types of hosts: IPv4 only, IPv6 only and IPv4/IPv6-enabled) which will be used in enterprise networks. Similar to the IPv4 network, it consists of five segments: external segment, DMZ, backbone, server segment and client segment. The external segment is a connection point between ISPs and a perimeter router of an organization. DMZ is a zone for providing external services (e.g., Web server, Load balancer) to users and it is general to deploy security devices such as IDS, Firewall into DMZ. The backbone is a large-capacity, a high-speed central section, and other network segments are connected to each other through it. In the server segment, there exist many different kinds of server systems (e.g., DNS server, DHCP server) which are necessary for internal users. Finally, client computers are located in the client segment.

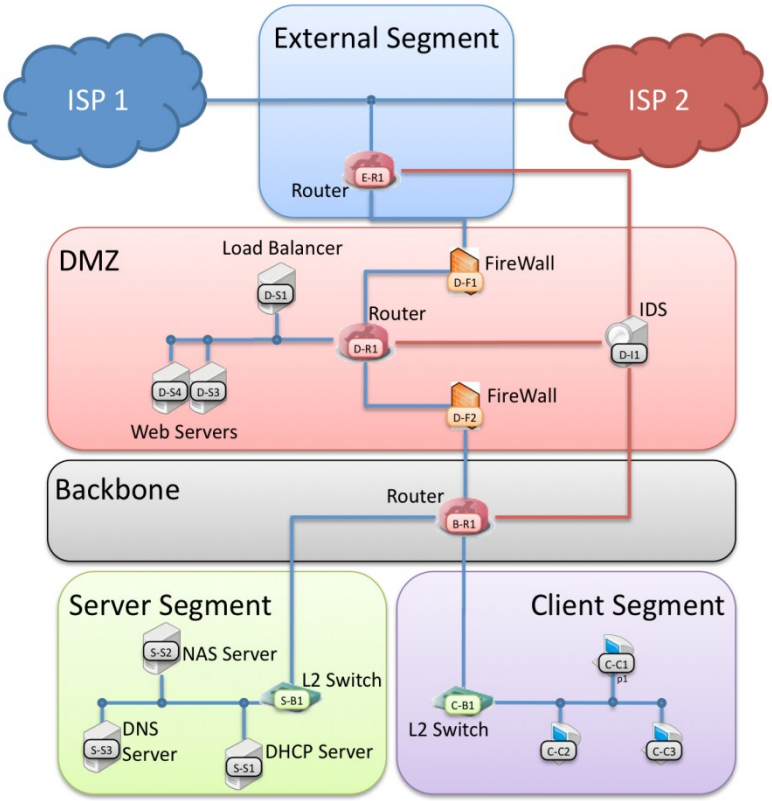

Figure 6-1 – Topology of IPv6 network

7 Network devices

7.1 Router

7.1.1 Security threats

Threat 1: OSPFv3 is specified in RFC 2740. OSPFv3 uses LSA to exchange information of link state between routers. There are nine types of LSA (e.g., network LSA, router LSA, AS-External LSA) and LSA header includes information about LSA function code and the flooding scope (e.g., Link-local, area) of the LSA embedded in the header. OSPFv3 is able to handle unknown LSAs using the "U" bit in the header. If the value of U bit is set to 1 in an LSA, this means the LSA is unknown. Thus, if a router receives such LSAs, the router must store all of them into its LSDB. Therefore, attackers can crash LSDB of a router by issuing a tremendous amount of unknown LSAs. Also, since OSPFv3 can decide the flooding scope of LSAs with "S1" and "S2" bits, attackers are able to launch DDoS attack to routers more easily by using the two bits.

Threat 2: Neighbor cache is used for maintaining entries of individual neighbors to which traffic has been sent recently. Entries are keyed on the neighbor's on-link unicast IP address and contain such information as its link-layer address, a flag indicating whether the neighbor is a router or a host, the reachability state, the number of unanswered probes, etc. If there is no existing neighbor cache entry for NS message, the router creates a new entry. Therefore, if attackers send a large number of NS messages with different source IP addresses to a host via the victim router and reply NA messages for all of the NS messages at the same time, the router must create lots of neighbor cache entries. As a result, attackers are able to overflow the router's neighbor cache.

7.1.2 Practical risk assessment

Attack scenario 1: Figure 7-1 shows an attack scenario of LSA flooding. In this attack scenario, the Web server (S-C1) and the client (C-C1) communicate with each other, and the attacker (C-C2) continuously sends a large amount of LSAs to the router (B-R1). The risk assessment of IPv6 technical verification council in Japan resulted in that the router could not store LSAs more than the maximum number of LSAs. Also, the router's operation became extremely heavy and consequently it could not work normally.

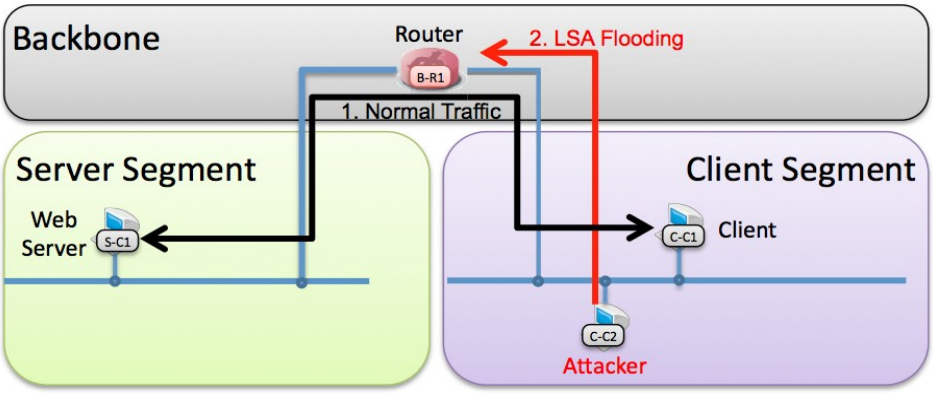

Figure 7-1 – Attack scenario of LSA flooding

7.1.3 Countermeasures

Measure 1: When using OSPFv3 on a router, it is recommended to implement the authentication function based on RFC 4552, so that the router is able to discard LSAs from illegal nodes. Also, it is available to configure the maximum number of LSAs that the router can manage.

Measure 2: The most practical solution for the neighbor cache problem is to limit the maximum number of NA messages that a host can return against NS messages within a fixed interval. Another

option is to design a router that is able to continue its working even if the router's neighbor cache is overflowed.

8 Client/Server devices

8.1 End nodes

8.1.1 Security threats

Threat 1: IPv6 hosts can automatically configure their addresses (e.g., global addresses) using Internet Control Message Protocol version 6 (ICMPv6) Router Advertisement (RA) messages. Since they also can choose a default router based on RA messages, RA messages can be used for man-in-the-middle attack. In other words, if a malicious node sends a forged RA message where the default router is set to itself to victim hosts, the malicious node is able to steal and watch all traffic of the victim hosts.

Threat 2: When IPv6 hosts configure their addresses using RA messages, they have to conduct Duplicate Address Detection (DAD) procedure to verify the uniqueness of the tentative addresses on a link. During the procedure for detecting duplicate addresses, IPv6 hosts that have tentative addresses send Neighbor Solicitation (NS) messages on the link and a node already using the tentative address replies with a Neighbor Advertisement (NA) message. If there is no response, the tentative address can be assigned to the interface of IPv6 hosts. However, a malicious host on the link can prevent IPv6 hosts from obtaining their addresses: if a malicious host always replies NA messages against NS messages of other IPv6 hosts, they are unable to obtain their addresses.

8.1.2 Practical risk assessment

Attack scenario 1: Figure 8-1 shows an attack scenario of forged RA messages. In this attack scenario, the router (B-R1) sends legitimate RA messages to the client (C-C1) that wants to communicate with the Web server (S-C1), but the attacker also makes forged RA messages that have default gateway address as its own address and sends them to the client. The risk assessment of IPv6 technical verification council in Japan verified that the attacker could steal all traffic between the client and the Web server.

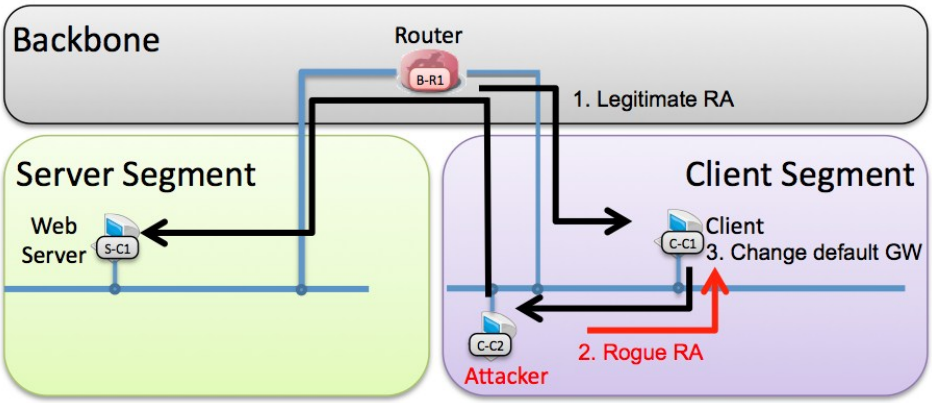

Figure 8-1 – Attack scenario of forged RA messages

Attack scenario 2: Figure 8-2 shows an attack scenario of DAD procedure. In this attack scenario, the router (B-R1) sends legitimate RA messages to the client (C-C1) that wants to obtain its own IP address and the client sends NS messages to check the uniqueness of the IP address. When the attacker (C-C2) received NS messages from the client, it replies NA messages against all NS

messages. The risk assessment of IPv6 technical verification council in Japan observed that the client could not obtain its own IP address during the attack. After the attacker stopped sending forged RA messages, the client could get its own IP address.

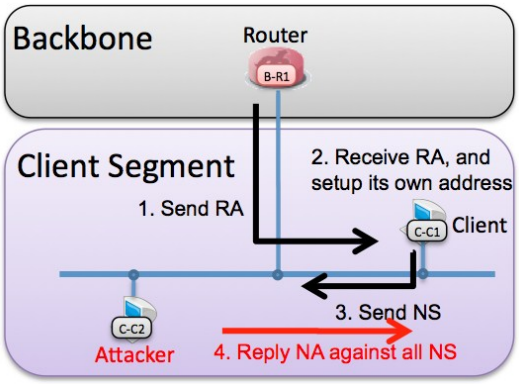

Figure 8-2 – Attack scenario of DAD procedure

8.1.3 Countermeasures

Measure 1: To minimize the security risk by forged RA messages, it is recommended that each host discards all of RA messages with an extremely short lifetime.

Measure 2: If administrators check the number of IP addresses that each node has and set its limitation for every host, the security risk by the malicious DAD can be mitigated. To this end, administrators can use open source tools such as NDPMon. In addition, a switch is able to detect malicious DADs by controlling the pair of the MAC address of hosts and the physical port connected to the host.

8.2 DHCP server

8.2.1 Security threats

Threat 1: IPv6 hosts may configure their addresses by using stateful configuration protocol such as the Dynamic Host Configuration Protocol version 6 (DHCPv6) if they didn't receive any RA messages from routers. During the stateful configuration, IPv6 hosts send DHCPv6 solicit messages to all DHCPv6 servers using DHCP multicast addresses so that they are able to obtain addresses as well as other configuration parameters (e.g., DNS servers). In that case, a malicious host is able to prevent other IPv6 hosts from obtaining addresses by exhausting address pool of DHCPv6 servers. In other words, if a malicious host issues a large amount of DHCPv6 solicit messages to obtain all addresses that DHCPv6 servers have, other IPv6 hosts are unable to obtain their addresses.

8.2.2 Practical risk assessment

Attack scenario 1: Figure 8-3 shows an attack scenario of DHCPv6 solicit messages. In this attack scenario, the attacker (S-C1) sends DHCPv6 solicit messages to the DHCPv6 server (S-S3) in order to exhaust its address pool. The client (D-C2) then sends HDCPv6 solicit messages to the DHCPv6 server to get DHCPv6 advertise messages. The risk assessment of IPv6 technical verification council in Japan observed that the DHCPv6 server's service was not stopped, but the client could not get DHCPv6 advertise messages from the DHCPv6 server during the attack. After the attacker stopped sending DHCPv6 solicit messages, the client could get DHCPv6 advertise messages from the DHCPv6 server.

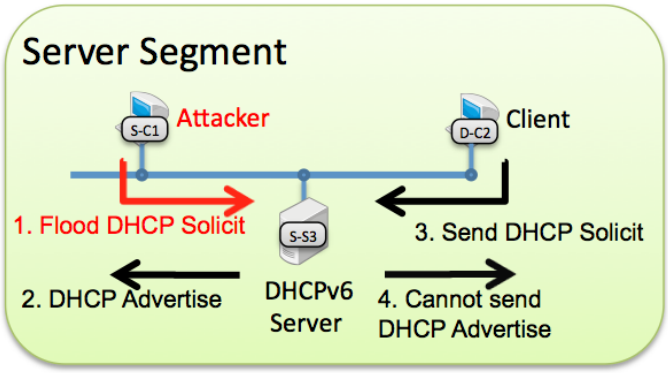

Figure 8-3 – Attack scenario of DHCPv6 solicit messages

8.2.3 Countermeasures

[TBD]

9 Security Devices

9.1 IDS

9.1.1 Security threats

Threat 1: 6to4 is a transition mechanism for migrating from IPv4 to IPv6. In the 6to4 framework, 6to4 hosts that want to communicate with IPv6 hosts (or 6to4 hosts) carry out encapsulation of outgoing IPv6 packets and decapsulation of incoming 6to4 packets. Therefore, if a 6to4 host attacks an IPv6 host via 6to4, IDS that does not support the decapsulation function of the encapsulated IPv6 packets and 6to4 packets is unable to detect cyber attacks or suspicious packets.

9.1.2 Practical risk assessment

Attack scenario 1: Figure 9-1 shows an attack scenario of 6to4 encapsulation. In this attack scenario, an attacker (S-C1) sends an exploit code to the client (C-C1) via 6to4 tunnel and the router (B-R1) forwards it to the IDS (D-I1). The risk assessment of IPv6 technical verification council in Japan observed that the IDS could not detect the exploit code due to its encapsulation.

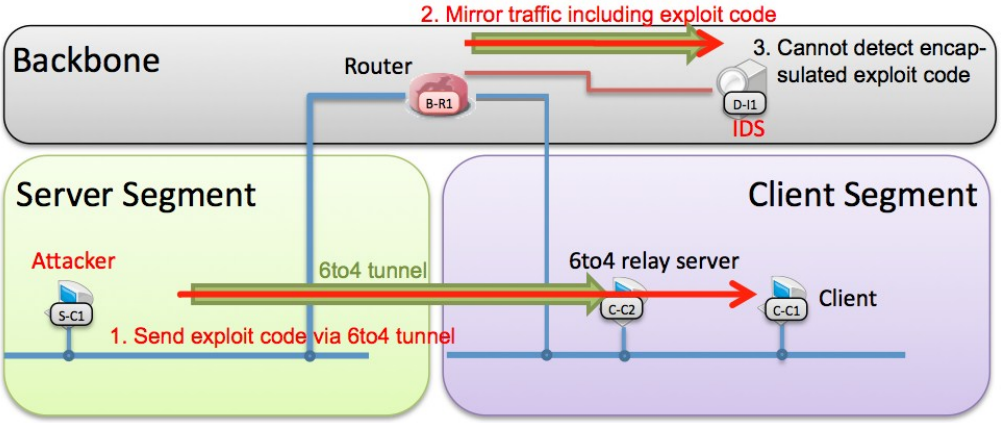

Figure 9-1 – Attack scenario of 6to4 encapsulation

9.1.3 Countermeasures

Measure 1: IDSs have to support the decapsulation function of the encapsulated IPv6 packets and 6to4 packets over 6to4.

9.2 Firewall

9.2.1 Security threats

[TBD]

9.2.2 Practical risk assessment

[TBD]

9.2.3 Countermeasures

[TBD]

Appendix I

Use case: IPv6 Promotion Council in Japan

(http://www.v6pc.jp/en/council/index.phtml)

(This appendix does not form an integral part of this Recommendation)

I.1 Background and objectives of IPv6 Promotion Council in Japan

The number of Internet users exceeded ninety four million in 2009 brings the percentage of the population using the Internet to 78 percent according to an MIC (Ministry of Internal Affair and Communications in Japan) report. TV's, information appliances and equipment and devices in buildings are all controllable via the Internet. Moreover, many new services will be provided in the next generation Internet, including in various areas such as ITS, mobile networks, learning and shopping. IPv6 was developed for this next generation Internet.

Next generation Internet using IPv6 provides a new infrastructure in a high information society supporting more attractive and convenient shopping, services in daily life and business activity. To develop this new social infrastructure in a timely manner, many bodies, like private companies, government agencies, organizations and personal users need to collaborate with one another and utilize their intellect to enhance the promotion of utilization of IPv6 strongly.

Based on the above background, the IPv6 Promotion Council established a membership agreement aimed at increasing membership and improving its executive capacity.

Under the e-Japan Priority Policy Program introduced in March 2001, the Japanese government set the goal of realizing an IPv6 enabled network environment making it possible for anyone to collect, process and transmit information anywhere. The IPv6 Promotion Council will contribute to the realization of this goal by promoting cooperation among government, industry and academia.

I.2 Aims of the Council

1) Pursue an international leadership role for Japan in the Internet field

2) Develop rich human resources for continuous development of a new infrastructure for a high information society

3) Promote new business and vitalize existing business in hardware, software and service of networks and devices

I.3 Security considerations for information

Deliverable of "IPv6 Home Router Guideline (ver1.0)" was developed in June 22, 2009 can be shown at the following page [V6PC].

http://www.v6pc.jp/pdf/v6hgw_Guideline_1_0-English.pdf

Especially, detailed setting of access restriction is related to security considerations in 4.1.1.2 (p23).

Appendix II

Use case: IPv6 Technical Verification Consortium

(http://ipv6tvc.jp/default.aspx) (Only Japanese)

(This appendix does not form an integral part of this Recommendation)

II.1 Objectives of IPv6 Technical Verification Consortium in Japan

July 28th, 2010 - National Institute of Information and Communications Technology (NICT), Microsoft Japan and other 8 companies have established an "IPv6 Technical Verification Consortium" for verifying the security and interoperability of IPv6 technology. This consortium is organized to test and come up with solutions against over 60 security (threats and vulnerabilities) and interoperability issues identified through the NICT research activities. Microsoft Innovation Center Japan will take key position to host all testing and organize activities, and outcome will be shared to communities broadly to improve security and interoperability of IPv6.

II.2 Activities of the Consortium

Consortium members inspect vulnerabilities of their IPv6-enabled products and solutions such as network devices (e.g., router, switch, NAT, load balancer), security appliances (e.g., IDS, IPS, Firewall) and network service equipment (e.g., proxy server, DHCP server, Web server, DNS server) with respect to the IPv6 security issues that have been studied in NICT (National Institute of Information and Communications Technology). Consortium members also share all of the discovered vulnerabilities from the inspection with each other and devise countermeasures against them, so that the consortium can contribute to make more secure and stable IPv6-based networks. The direction of the activity will be decided under consensus of all consortium members and its main goal is to make the future IPv6-based Internet more secure and stable.

Bibliography

[IETF RFC 4864] IETF RFC 4864 (2007), Local Network Protection for IPv6. <http://www.ietf.org/rfc/rfc4864.txt>

[IETF RFC 4942] IETF RFC 4942 (2007), IPv6 Transition/Coexistence Security Considerations. <http://www.ietf.org/rfc/rfc4942.txt>

[IETF RFC 3964] IETF RFC 3964 (2004), Security Considerations for 6to4. <http://www.ietf.org/rfc/rfc3964.txt>

[IETF RFC 4593] IETF RFC 4593 (2006), Generic Threats to Routing Protocols. <http://www.ietf.org/rfc/rfc4593.txt>

[IETF RFC 3971] IETF RFC 3971 (2005), SEcure Neighbor Discovery (SEND). <http://www.ietf.org/rfc/rfc3971.txt>

[IETF RFC 5969] IETF RFC 5969 (2010), IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification. < http://www.ietf.org/rfc/rfc5969.txt>

[IETF RFC 6092] IETF RFC 6092 (2011), Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service. <http://www.ietf.org/rfc/rfc6092.txt>

[IETF RFC 6105] IETF RFC 6105 (2011), IPv6 Router Advertisement Guard. <http://www.ietf.org/rfc/rfc6105.txt>

[IETF RFC 6106] IETF RFC 6106 (2011), IPv6 Router Advertisement Options for DNS Configuration. <http://www.ietf.org/rfc/rfc6106.txt>

[IETF RFC 6169] IETF RFC 6169 (2011), Security Concerns with IP Tunneling. <http://www.ietf.org/rfc/rfc6169.txt>

[IETF Internet Draft] IETF Internet Draft (2011), Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion. <http://www.ietf.org/id/draft-ietf-softwire-dual-stack-lite-11.txt>

[IETF Internet Draft] IETF Internet Draft (2011), IPv6 Node Requirements. <http://www.ietf.org/id/draft-ietf-6man-node-req-bis-11.txt>

[NIST SP 800-119] NIST SP 800-119 (2010), Guidelines for the Secure Deployment of IPv6. <http://www.csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf >

[V6PC Ver.1.0] V6PC (2009), IPv6 Home Router Guideline (ver.1.0). <http://www.v6pc.jp/pdf/v6hgw_Guideline_1_0-English.pdf>

_____