Draft Recommendation ITU-T X.1037 (X.ipv6-secguide)

Technical security guideline on deploying IPv6

Summary

The Internet protocol version 6 (IPv6) is intended to provide many built-in benefits such as large address space, mobility, and quality of service (QoS), because it is a new protocol and operates in some different ways than Internet protocol version 4 (IPv4), both foreseeable and unforeseeable security issues will arise. Many new functions or requirements of IPv6, i.e., automatic configuration of interfaces, mandatory Internet protocol security (IPSec), mandatory multicast, multiple Internet protocol (IP) addresses and many new rules for routing, can be abused for compromising computer systems or networks.

Considering the above circumstances, Recommendation ITU-T X.1037 provides a set of technical security guides for telecommunication organizations to implement and deploy IPv6 environment. The content of this Recommendation focuses on how to securely deploy network facilities for telecommunication organizations and how to ensure security operations for the IPv6 environment.

Keywords

????

CONTENTS

Draft Recommendation ITU-T X.1037 (X.ipv6-secguide)

Technical security guideline on deploying IPv6

1 Scope

Recommendation ITU-T X.1037 specifies security threats in the Internet protocol version 6 (IPv6) and provides a practical risk assessment of these threats and the technical solutions for a secure IPv6 deployment. This Recommendation focuses on three components: network devices (e.g., router, switch), server/client devices (e.g., end nodes, dynamic host configuration protocol (DHCP) server) and security devices (e.g., intrusion detection system (IDS), and firewall (FW)) that will be essentially deployed on IPv6 network. Recommendation ITU-T X.1037 provides a technical security guideline to developers of network products, security operators and managers of enterprise networks that are planning to deploy IPv6, so that they are able to mitigate security threats on their IPv6 network.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[IEEE 802.1x] IEEE Starndard 802.1x (2010), *Port Based Network Access Control*.

[IETF RFC 1981] IETF RFC 1981 (1996), *Path MTU Discovery for IP version 6*.

[IETF RFC 2460] IETF RFC 2460 (1998), *Internet Protocol, Version 6 (IPv6) Specification*.

[IETF RFC 2675] IETF RFC 2675 (1999), *IPv6 Jumbograms*.

[IETF RFC 3315] IETF RFC 3315 (2003), *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*.

[IETF RFC 3627] IETF RFC 3627 (2003), *Use of / 127 Prefix Length Between Routers Considered Harmful.*

[IETF RFC 3704] IETF RFC 3704 (2004), *Ingress Filtering for Multihomed Networks*.

[IETF RFC 3810] IETF RFC 3810 (2004), *Multicast Listener Discovery Version 2 (MLDv2) for IPv6*.

[IETF RFC 3971] IETF RFC 3971 (2005), *SEcure Neighbor Discovery (SEND)*.

[IETF RFC 4443] IETF RFC 4443 (2006), *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification.*

[IETF RFC 4552] IETF RFC 4552 (2006), *Authentication/Confidentiality for OSPFv3*.

[IETF RFC 4604] IETF RFC 4604 (2006), *Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast*.

[IETF RFC 4884] IETF RFC 4884 (2007), *Extended ICMP to Support Multi-Part Messages*.

[IETF RFC 4890] IETF RFC 4890 (2007), *Recommendations for Filtering ICMPv6 Messages in Firewalls*.

[IETF RFC 5095] IETF RFC 5095 (2007), *Deprecation of Type 0 Routing Headers in IPv6*.

[IETF RFC 5340] IETF RFC 5340 (2008), *OSPF for IPv6*.

[IETF RFC 5722] IETF RFC 5722 (2009), *Handling of Overlapping IPv6 Fragments*.

[IETF RFC 6105] IETF RFC 6105 (2011), *IPv6 Router Advertisement Guard*.

[IETF RFC 6164] IETF RFC 6164 (2011), *Using 127-bit IPv6 Prefixes on Inter-Router Links*.

[IETF RFC 6494] IETF RFC 6494 (2012), *Certificate Profile and Certificate Management for SEcure Neighbor Discovery (SEND).*

[IETF RFC 6495] IETF RFC 6495 (2012), *Subject Key Identifier (SKI) SEcure Neighbor Discovery (SEND) Name Type Fields.*

[IETF RFC 6845] IETF RFC 6845 (2013), *OSPF Hybrid Broadcast and Point-to-Multipoint Interface Type.*

[IETF RFC 6860] IETF RFC 6860 (2013), *Hiding Transit-Only Networks in OSPF.*

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 abuse, abused, abusing: To use wrongly or improperly and to misuse. In the context of this Recommendation, "abusing" the IPv6 protocol or some feature of the protocol means to use it in ways that were unintended by the developers.

3.2.2 forged packet: A packet generated by an attacker, typically with illegitimate fields or entries that misuse the protocol format, in an attempt to violate network security by creating a denial-of-service (DoS) condition or attack situation.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAAA	Authentication, Authorization, Accounting, and Auditing
AS	Autonomous System
DAD	Duplicate Address Detection
DDoS	Distributed Denial-of-Service
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
DMZ	DeMilitarized Zone

DNS	Domain Name System
DoS	Denial-of-Service
FDB	Forwarding DataBase
FW	Firewall
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IDS	Intrusion Detection System
IGMP	Internet Group Management Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
ITS	Intelligent Transportation Systems
L2	Layer 2
LAN	Local Area Network
LSA	Link State Advertisement
LSDB	Link State DataBase
MAC	Media Access Control
MLD	Multicast Listener Discovery
MTU	Message Transfer Unit
NA	Neighbour Advertisement
NAS	Network Access Server
NAT	Network Address Translation
NAT64	Network Address Translation 6 to 4
NAT66	Network Address Translation 6 to 6
NDPMon	Neighbor Discovery Protocol Monitor
NDP	Neighbour Discovery Protocol
NPTv6	NAT and Port Translation version 6
NS	Neighbour Solicitation
OSPF	Open Shortest Path First
OSPFv3	Open Shortest Path First version 3
PMTUD	Path MTU Discovery
RA	Router Advertisement

SEND	SEcure Neighbour Discovery
TCP	Transmission Control Protocol
TTL	Time To Live
TV	TeleVision
uRPF	unicast Reverse Path Forwarding

5 Conventions

None.

6 Topology of IPv6 network

This clause describes the general topology of an IPv6 network (including transition environments to IPv6 where there exist three different types of hosts: Internet protocol version 4 (IPv4) only, IPv6 only and IPv4/IPv6-enabled) that will be used as an enterprise network model for illustrating the attack scenarios and security countermeasures. This IPv6 general network topology is illustrated in Figure 6-1. Similar to the IPv4 network, it consists of five segments: an external segment, a demilitarized zone (DMZ), a backbone, a server segment, and a client segment. The external segment is a connection point between Internet service providers (ISPs) and a perimeter router of an organization. The DMZ segment provides external services (e.g., web server, load balancer) to users, and it is also generally used to deploy security devices such as IDS and firewall. The backbone is a large-capacity, a high-speed central network, 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., domain name system (DNS) server, DHCP server) which are necessary for internal users. Finally, client computers are located in the client segment.

This IPv6 security guideline focuses on describing security threats and countermeasures on IPv6 from a viewpoint of network components: network devices, client and server end nodes, and security devices, which will be essentially deployed on the IPv6 networks. For this purpose, the remainder of this Recommendation is organized as follows. Clause 7 covers IPv6 threats and countermeasures for network devices. Clause 8 covers IPv6 threats and countermeasures for clients, servers, and other end devices. Clause 9 covers IPv6 threats and countermeasures of specific interest to security devices such as firewalls and IDS devices.

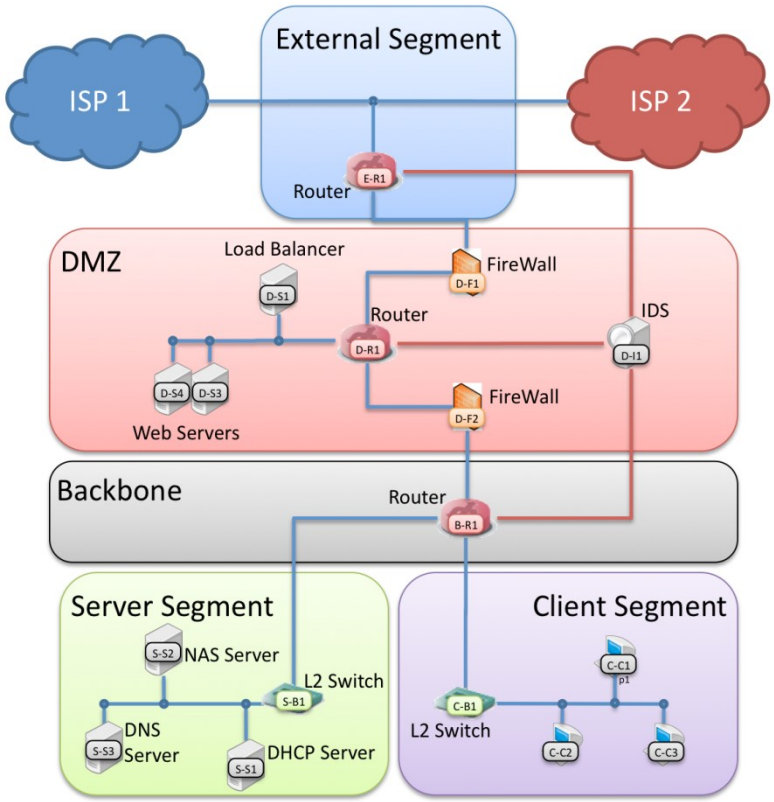

Figure 6-1 – Topology of IPv6 network

7 Network devices

7.1 Router

7.1.1 Security threats and countermeasures

Threat 1:

Open shortest path first version 3 (OSPFv3) is specified in [IETF RFC 5340]. OSPFv3 uses link state advertisement (LSA) to exchange information of link state between routers. There are nine types of LSAs (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 that LSA is unknown. Thus, if a router receives such LSAs, the router must store all of them into its link state database (LSDB). Therefore, attackers can crash LSDB of a router by issuing a tremendous amount of unknown LSAs. Furthermore, since OSPFv3 can decide the flooding scope of LSAs with "S1" and "S2" bits, attackers are able to launch more easily DDoS attacks to routers by using the two bits.

Measure 1:

When using OSPFv3 on a router, it is recommended to implement the authentication function based on [IETF RFC 4552], so that the router is able to discard LSAs from illegal nodes. In addition, it is effective for a router to configure the maximum number of LSAs that the router can manage.

Threat 2:

Neighbour cache is used for maintaining entries of individual neighbours to which traffic has been sent recently. Entries are keyed on the neighbour's on-link unicast IP address and contain such information as its link-layer address, a flag indicating whether the neighbour is a router or a host,

the reachability state, the number of unanswered probes, etc. If there is no existing neighbour cache entry for neighbour solicitation (NS) messages, 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 respond with neighbour advertisement (NA) messages for all of the NS messages at the same time, the router must create many neighbour cache entries. As a result, attackers are able to overflow the router's neighbour cache.

Measure 2:

The most practical solution for the neighbour 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 work even if the router's neighbour cache is overflowed.

Threat 3:

Similar to the source route option in the IPv4 header, the original IPv6 specification permitted an IPv6 host to explicitly specify intermediate nodes by which packets are transmitted using the routing header extension, Type 0 (RH0) on each packet. Since RH0 can include multiple entries of the same IP address, attackers can construct packets that will oscillate between arbitrary two nodes specified in RH0, causing congestion between the nodes and consuming valuable router processing and forwarding resources, potentially leading to a DoS attack. Due to high potential for abuse, and relatively limited uselessness of RH0 (its primary use was for diagnostics and troubleshooting), the IETF deprecated support for RH0 in [IETF RFC 5095].

Measure 3:

Fortunately, [IETF RFC 5095] has already been standardized in 2007 in IETF as a countermeasure against the security risk of RH0, which specifies for routers to ignore RH0 packets. Therefore, operators and developers are recommended to confirm that their devices are configured correctly according to the specification.

Threat 4:

As IPv4 manages multicast clients by a specific protocol called Internet group management protocol (IGMP), IPv6 performs the same function but implements it differently, by using one of the functions of Internet control message protocol (ICMP) called multicast listener discovery (MLD), see [IETF RFC 3810]). An MLD capable router maintains multicast clients and addresses based on Multicast Listener Report and Multicast Listener Done messages sent by the clients. Since a router holds all multicast addresses according to the MLD messages sent by all clients, attackers can exhaust a router's memory resource by sending a large number of Multicast Listener Report messages to the router. In addition, multicast communications of legitimate multicast clients can be disrupted by sending a source spoofed (forged) Multicast Listener Done message to a router causing the removal of the IP addresses of legitimate multicast clients.

Measure 4:

The most fundamental solution for the MLD DoS attack against routers is to authenticate Multicast Listener Report /Done messages between a router and a client so that the router can discard forged MLD messages. In addition, as a practical solution for this security risk, routers are recommended to limit the rate of Multicast Listener Report messages. Another solution, see [IETF RFC 4890], recommends for firewalls to drop MLD messages sent from the link local address.

Threat 5:

Since the smallest subnet size in IPv6 is defined as /64, a /64 subnet is sometimes used for a point-to-point link between a pair of routers. In this case, only two in the huge number of IP addresses are used for interfaces of the routers and the rest remains as unused. Although it depends on the

implementation of routers, by specifying one of the remaining IP addresses for source and destination addresses of a packet, the packet may loop between the two routers until its time to live (TTL) reaches zero. Consequently, this vulnerability may lead to DoS attacks against routers.

Measure 5:

The packet loop attack on a point-to-point link has been basically solved by [IETF RFC 4443]. Developers and users are recommended to check whether their devices comply with [IETF RFC 4443]. Additionally, there may be some other practical measures as follows:

- assign a /127 prefix to a point-to-point link based on [IETF RFC 6164];
- filter packets destined to unused IP addresses of the point-to-point link;
- use only link local IP addresses on a point-to-point link.

Even though [IETF RFC 3627] declares that /127 prefix on a point-to-point link is illegal, [IETF RFC 6164] permits to use /127 prefix under certain conditions.

7.2 Switch

7.2.1 Security threats and countermeasures

Threat 6:

An IPv6 address consists of 64-bit prefix and 64-bit interface identifier (ID); hence, a 64-bit address space can be used for devices in a single local network. In a common Ethernet-based local network, since the 64-bit address space is larger than the media access control (MAC) address space (48 bits), all of the MAC addresses can be bound with at least one IPv6 address, while the IPv4 address space (32 bits) is not sufficient for binding with a MAC address. This means that a malicious node can conduct a DoS attack to exhaust a forwarding database (FDB) of an L2 switch by sending massive packets with different MAC addresses.

Measure 6:

IEEE 802.1x authentication which permits only certified addresses is one of the effective solutions against this attack as well as for limiting the number of MAC addresses on a single physical port of L2 switch. In addition, developers are recommended to maintain the total number of FDB entries by appropriately discarding older entries when the total number exceeded a threshold.

7.3 Network address translation (NAT) router

7.3.1 Security threats and countermeasures

Threat 7:

A Network Address Translation (NAT) device is commonly deployed on a border of a network and translates either source or destination IP addresses of a packet in order to bridge two different types of networks such as private-global networks and IPv4-IPv6 networks. Particularly, NAT66, so-called NAT and port translation version 6 (NPTv6), translates IP addresses of packets between two distinct IPv6 networks as well as NAT64 which translates IP address of packets between IPv6 and IPv4 so that both IPv6 and IPv4 nodes can communicate with each other. However, if an implementation of a NAT device has a state table to manage the status of each translated address, it might be vulnerable to the NAT state table exhaustion DoS attack. Namely, if a malicious IPv6 node sends a huge number of packets towards hosts behind a NAT device while changing its source IPv6 address for each packet, the node can eventually conduct a DoS attack against the NAT devices. This kind of attack exists in an IPv4 environment as well, but as IPv6 has an enormous

number of available IP addresses, the attack can be performed more easily in an IPv6 environment than in an IPv4 environment.

Measure 7:

IETF is discussing stateless NAT66 (without a state table) function. Basically there is no concern for the DoS attack unless a NAT66 device has a state table. Additionally, in a case where developers implement a stateful NAT device, they should appropriately control the number of entries in the state table so as not to exceed the upper limit of entries.

8 End nodes (clients, load balancer) and servers

8.1 End nodes

8.1.1 Security threats and countermeasures

Threat 8:

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 can also choose a default router based on RA messages, RA messages can be used for man-in-the-middle attacks. In other words, if a malicious node sends a forged RA message indicating itself as the default router to victim hosts, the victim hosts will forward all traffic to the malicious node that is then able to steal and watch all traffic of the victim hosts.

Measure 8:

To minimize the security risk by forged RA messages, it is recommended that each host discard all RA messages with an extremely short lifetime.

Threat 9:

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 neighbour solicitation (NS) messages on the link and a node already using the tentative address replies with a neighbour 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 by always replying with NA messages against NS messages of other IPv6 hosts, leaving the victim hosts in a state where they are unable to obtain their addresses.

Measure 9:

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 a neighbour discovery protocol (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.

Threat 10:

IPv6 provides a link layer address resolution mechanism by neighbour discovery protocol (NDP). Once a node determines its IP address by RA, the node exchanges neighbour solicitation (NS) and neighbour advertisement (NA) messages on a multicast address so that the node resolves IP addresses to corresponding MAC addresses. NS/NA messages have not only address resolution, but also other useful functions: verification of reachability between neighbours, and duplication address

detection. When a node receives NA in response to NS the node has sent, the node updates its neighbour cache that stores a set of entries about individual neighbours to which traffic has been sent recently. Therefore, a malicious node can easily impersonate other (victim) host on the same link by sending forged NA messages that declare the MAC address of the malicious node as the victim's address. Eventually, the malicious node can intercept or disturb the victim's communications.

Measure 10:

As a countermeasure against attacks abusing NS and NA, secure neighbour discovery (SEND), see [IETF RFC 3971]), which secures the neighbour discovery protocol (NDP) by applying public key based authentication to it. Although SEND is a fundamental solution against these attacks because it burdens operators by maintaining a number of public/private keys, it is difficult to operate SEND in large networks. Another way to protect legitimate nodes from these attacks should be to implement a mechanism which observes and controls NS/NA messages on L2 switches in a manner similar to RA Guard (see [IETF RFC 6105]).

Threat 11:

An IPv6 router notifies IPv6 nodes via "ICMP redirect messages" of appropriate first-hop nodes towards their destinations. An ICMP has two address fields: a destination address field and a target address field which is a link-local address to which subsequent packets for the destination address should be sent. Consequently, attackers can deceive other (victim) nodes to redirect their traffic to certain nodes on the same link by sending forged redirect messages to the victim nodes. Eventually, the malicious node can intercept or disturb the victim's communications.

Measure 11:

It is possible to prevent attacks of rogue ICMPv6 redirect messages by configuring every node not to receive ICMPv6 redirect messages. However, since this approach directly conflicts with the objective of ICMP redirecting, operators (or users) should carefully apply such configuration only to requisite minimum nodes. Another possible solution should be to implement a mechanism which observes and controls ICMPv6 redirect messages on L2 switches in a manner similar to RA Guard ([IETF RFC 6105]).

Threat 12:

Unlike ICMP in IPv4, IPv6 multicast listeners can send ICMPv6 error messages to the sender of an illegal (e.g., forged) packet sent to a multicast address. If there are *N* multicast listener nodes on a certain multicast address, a single illegal packet induces *N* error message packets as a reflection to the sender of the original packet. By intentionally sending a large number of illegal packets to a multicast address with spoofing sources of the packets as another (victim) node, an attacker can conduct a packet amplification attack against the victim node, which disrupts the victim's communications.

Measure 12:

A simple solution for the packet amplification attack by forged multicast packets is to limit the rate of ICMPv6 error messages by firewalls. In fact, many firewall appliances have rate-limit mechanisms of ICMPv6 messages; hence, operators should configure their firewalls with rate-limit policies set to permit baseline (non-attack) ICMPv6 error message levels. It should be noted that path MTU discovery (PMTUD) is highly critical to the proper operation of IPv6 (for fragmentation support) and thus ICMPv6 Packet Too Big messages should not be rate limited. Another solution, uRPF (see [IETF RFC 3704]), can prevent the attack by inhibiting attackers from sending source address spoofed packets.

Threat 13:

While fragmentation of an IPv4 packet can be performed by routers between source and destination, fragmentation in IPv6 is only permitted to be performed on a source node. Typically, path MTU discovery (PMTUD), (see [IETF RFC 1981]), is used to automatically discover the IPv6 minimum link size along the path between source and destination before starting communication with a destination node. Since defragmentation of fragments is performed on a destination node, a malicious node can exhaust the destination node's computational resource by sending a large number of fragmented packets to the destination. Although there have been many problems regarding fragmentation/defragmentation since IPv4, IPv6 still faces the same problems.

Measure 13:

A simple countermeasure against the DoS attack abusing fragmentation is to appropriately limit the rate of fragment packets (e.g., 1'000 packets per second) at a receiver node.

Threat 14:

Several types of IPv6 extension headers contain variable length options. When these options do not fill out the required number of bytes to complete the extension header, a proper alignment is achieved by introducing padding options, either Pad1 or PadN options, to fill option fields with variable data length. Normally, the Pad1 option is used to fill one octet padding into an option field, PadN option is used to fill more than one-octet padding. However, an attacker can send forged packets with a large number of Pad1 options included in each packet. If the attacker sends a large number of such forged packets, they can exhaust computational resources of another (victim) node to process all of Pad1 options one by one.

Measure 14:

Regarding the security risk by the DoS attack abusing the padding option header, [IETF RFC 2460] describes that the PadN option should be used rather than the multiple Pad1 options if more than one-octet padding is required. Therefore, it will effectively work that routers drop packets that have more than one PAD1 option headers to disturb the DoS attack. According to this policy, [IETF RFC 2460] recommends security appliance vendors to implement a function to check the validity of padding option.

Threat 15:

IPv6 supports to transport up to approximately 4.3 GB packet by applying jumbo payload option ([IETF RFC 2675]) as long as path MTU allows for that transportation. However, if PMTUs in a local area network (LAN) environment are set too big without discretion, 4.3 GB packet may be transmitted inside the network, which may lead to performance degradation of the network. In addition, massive packets with illegal values different from the actual packet sizes may lead to inappropriate behaviour of the IPv6 stack on the receiver.

Measure 15:

In a network which does not allow jumbogram, a firewall should drop packets with jumbogram option. In a network which allows jumbogram, a firewall should check the validity of the header. For example, if a node received a packet with jumbogram option from an interface whose MTU is less than 65575 octets, the node should drop the packet.

8.2 DHCP server

8.2.1 Security threats and countermeasures

Threat 16:

IPv6 hosts may configure their addresses by using stateful configuration protocol such as the dynamic host configuration protocol version 6 (DHCPv6) if they had not received 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 the address pool of DHCPv6 servers. In other words, if a malicious host issues large amounts of DHCPv6 solicit messages to obtain all addresses that DHCPv6 servers have, other IPv6 hosts are unable to obtain their addresses.

Measure 16:

There are briefly two approaches that are effective to mitigate the security risks against DHCPv6 server mentioned in clause 8.1: solutions on DHCPv6 server and network devices. As the simplest countermeasure on DHCPv6 server, operators should allocate enough numbers of IPv6 addresses in order to endure the exhaustion attack. In addition, it is also effective against the attack that DHCPv6 server limits the rate of DHCPv6 solicit messages. The same approach, the rate-limit of DHCPv6 solicitation message, is also effective on firewalls as one of the solution on network devices. Another countermeasure on network devices is to limit the number of MAC addresses connected to a physical port on L2 switch to a certain value. This method is more effective than the previous ones because the measure is applied at a point closer to the attackers.

8.3 DNS server

8.3.1 Security threats and countermeasures

Threat 17:

A malicious node can specify itself as a DHCPv6 server by sending a RA message with a flag of stateful address autoconfiguration mode (i.e., RA with m-flag = 1). Once the malicious node could disguise itself as a DHCPv6 server, it can also specify itself as a DNS server by using a DHCPv6 advertise. While the malicious node is pretending to be a DNS server, when a client (victim) tries to resolve an arbitrary node's name, the malicious node may return an authentication, authorization, accounting, and auditing (AAAA) record with the malicious node's IPv6 address. As a result, the malicious node can steal and watch all traffic from the victim client.

Measure 17:

DHCP snooping on L2 switch is effective to avoid this attack, which disturbs the activities of illegal DHCP server. DHCP message authentication mechanism ([IETF RFC 3315] section 21) is also effective for this attack. Additionally, RA guard disturbs the attack at the first step of the process by dropping the illegal RA message from the attacker.

9 Security devices

9.1 IDS

9.1.1 Security threats and countermeasures

Threat 18:

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 the encapsulation of outgoing

IPv6 packets and the decapsulation of incoming 6to4 packets. Therefore, if a 6to4 host attacks an IPv6 host via 6to4, IDS does not support the decapsulation function of the encapsulated IPv6 packets and 6to4 packets are unable to detect cyber attacks or suspicious packets.

Measure 18:

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 and countermeasures

Threat 19:

IPv6 fragment header is used by IPv6 source host in order to send a packet larger than the path MTU along the source and destination of the packet. A source host fragments a large packet into multiple smaller packets with the fragment header so that the destination host can integrate (defragment) them as the original packet according to the fragment header. Each fragment packet has offset information that indicates the location of the fragment in the original. However, since some firewalls inspect only the first fragment and pass subsequent fragments if the first one was permitted, a malicious sender can bypass firewalls by sending subsequent fragments whose offset is intentionally overlapped with the first fragment.

Measure 19:

One of the countermeasures on firewalls against the attack abusing overlapping IPv6 fragments is to apply the virtual defragmentation mechanism on firewalls, which reassembles fragments and inspects the original datagram before transmitting the fragments. As a countermeasure on end nodes, receiver nodes should discard datagrams that include overlapping fragments. In addition, [IETF RFC 5722] recommends disallowing overlapping fragments in order to prevent this attack.

Appendix I

Practical examples of threats

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

The following examples of threats provide practical ideas how to describe "threats" associated with those in the main body of this Recommendation. Examples do not cover all threats in this Recommendation; however, the following examples can be helpful for the readers in order to obtain a clear understanding of the several threats in this appendix.

Example 1: Figure I.1 shows an example when the web server (S-C1) and the client (C-C1) communicate with each other and the attacker (C-C2) can continuously send a large amount of LSAs to the router (B-R1). Under this circumstance, the router cannot store more than the maximum number of LSAs. Furthermore, the router's OSPF processing operations may become extremely heavy, resulting in abnormal forwarding behaviour. The above will be a practical example associated with Threat 1.

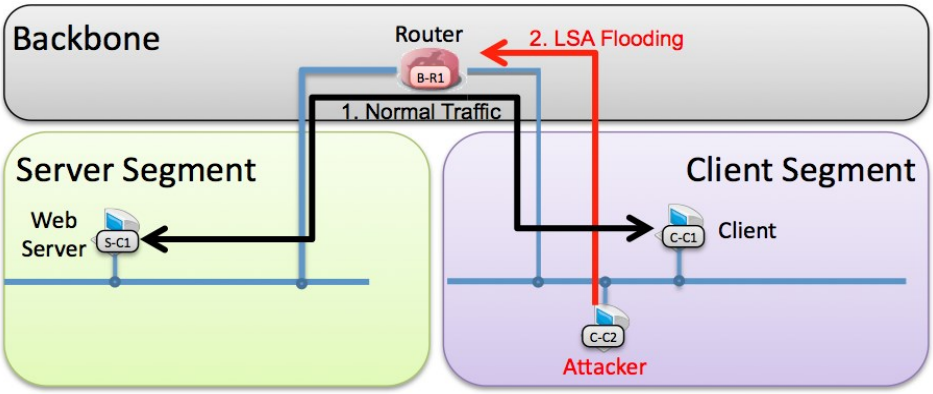

Figure I.1 – LSA flooding (Threat 1)

Example 2: Figure I.2 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 a default gateway address as its own address and sends them to the client. Using this attack, the attacker could steal all traffic between the client and the web server. The above will be a practical example associated with Threat 8.

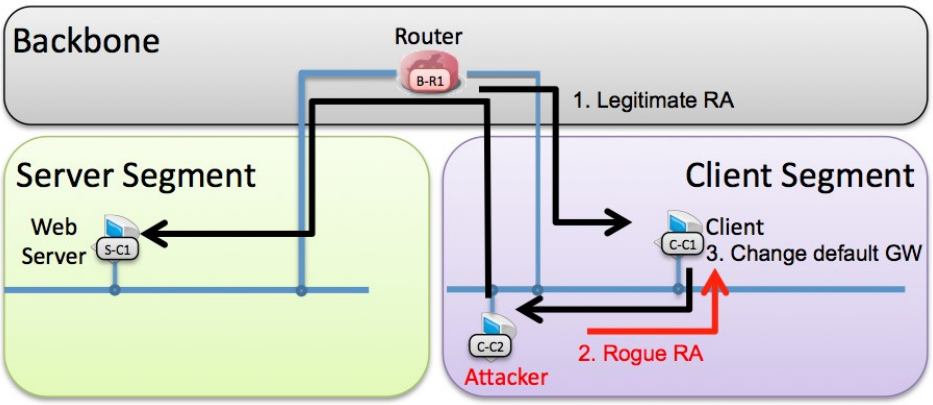

Figure I.2 – Forged RA messages (Threat 8)

Example 3: Figure I.3 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) receives the NS messages from the client, it replies with NA messages to all NS messages. Using this attack, the client could not obtain its own IP address during the attack. After the attacker stops sending forged RA messages, the client could get its own IP address. The above will be a practical example associated with Threat 9.

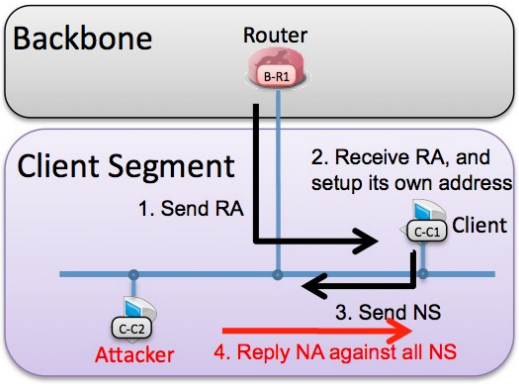

Figure I.3 – Abused DAD procedure (Threat 9)

Example 4: Figure I.4 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 ([b-IPV6TVC]) 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 stops sending DHCPv6 solicit messages, the client could get DHCPv6 advertise messages from the DHCPv6 server. The above will be a practical example associated with Threat 16.

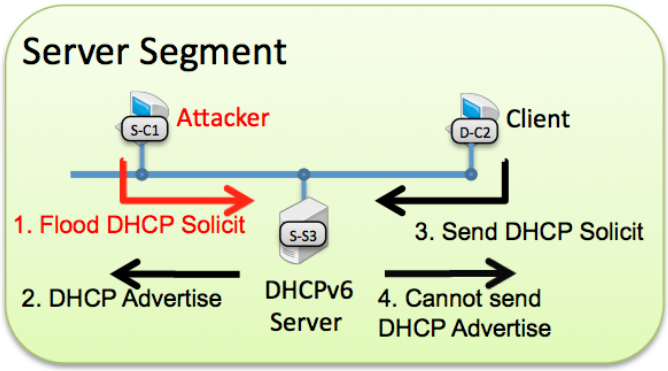

Figure I.4 – DHCPv6 solicit messages (Threat 16)

Example 5: Figure I.5 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 IDS (D-I1). Using this attack, IDS could not detect the exploit code due to its encapsulation. The above will be a practical example associated with Threat 18.

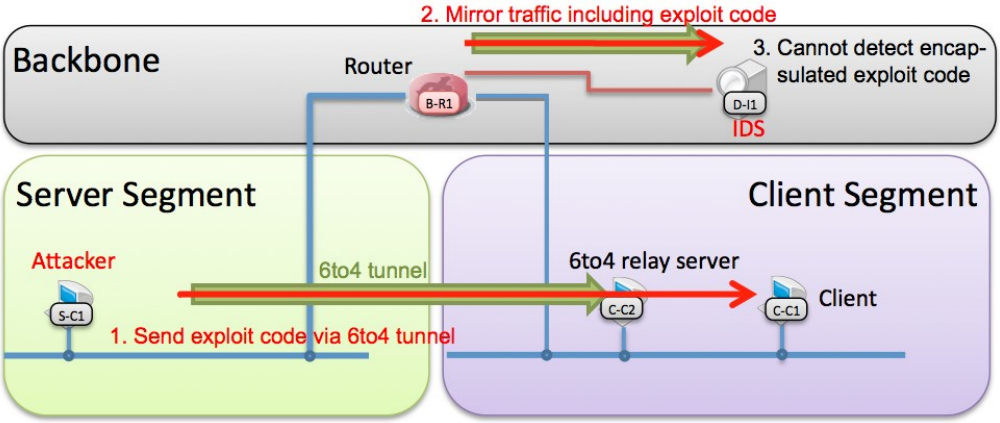

Figure I.5 – 6to4 encapsulation (Threat 18)

Example 6: Figure I.6 shows an attack scenario of overlapped fragments. At the beginning, an attacker (E-S1) sends the first fragment to a certain port number (e.g., 22/transmission control protocol (TCP)) permitted by firewalls (D-F1) and (D-F2). Since the port number is permitted, the first fragment is transmitted to a victim node (C-C1). Then the attacker sends the second fragment whose offset is set to zero (i.e., it overwrites the first fragment) to a target port number (e.g., 445/TCP). If the firewalls are configured not to inspect subsequent fragments, the second fragment successfully reaches to the victim node and overwrites the first fragment. Thus, the original port number (22/TCP) is overwritten by the arbitrary port number (445/TCP); hence, a defragmented datagram is able to attack a service on the port. The above will be a practical example associated with Threat 19.

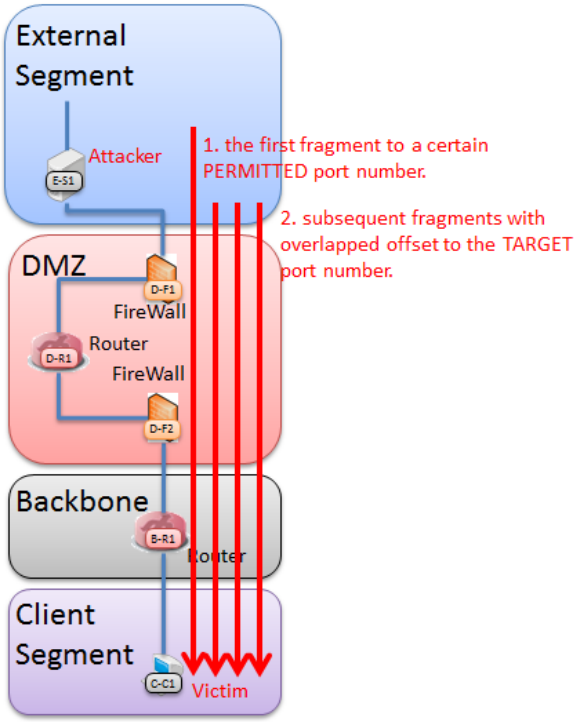

Figure I.6 – Overlapped fragments (Threat 19)

Appendix II

IPv6 Promotion Council in Japan

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

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

Recently, Televisions (TVs), 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 the intelligent transportation system (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 such as private companies, government agencies, organizations and personal users need to collaborate with one another and utilize their intellect to enhance the promotion of the utilization of IPv6 strongly.

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

II.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 businesses in hardware, software and service of networks and devices.

II.3 Security considerations for information

Deliverable of "IPv6 Home Router Guideline (ver1.0, June 22, 2009)" developed by IPv6 Promotion Council in Japan provides useful security considerations specifically for detailed setting of access restriction in [b-V6PC V.1.0].

Appendix III

Use case: IPv6 Technical Verification Consortium

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

III.1 Objectives of the IPv6 Technical Verification Consortium in Japan

On 28 July 2010, the National Research Institute and IPv6 product/service vendors in Japan 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 research activities. The outcome will be shared widely with communities to improve security and interoperability of IPv6.

III.2 Activities of the Consortium

The Consortium members will inspect the 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. The Consortium members will share their findings of the vulnerabilities with each other and devise countermeasures against them, so that the Consortium can contribute to the development of more secure and stable IPv6-based networks. The direction of the activity will be decided by consensus of all the Consortium members, and its main goal will be to ensure that future IPv6-based Internet networks are more secure and stable.

Bibliography

[b-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>

[b-V6PC] *IPv6 Promotion Council in Japan* <http://www.v6pc.jp/en/council/index.phtml>

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

[b-IPV6TVC] *IPv6 Technical Verification Consortium* <http://ipv6tvc.jp/english/default.html>

[b-IETF RFC 3964] IETF RFC 3964 (2004), *Security Considerations for 6to4*.

[b-IETF RFC 4593] IETF RFC 4593 (2006), *Generic Threats to Routing Protocols*.

[b-IETF RFC 4795] IETF RFC 4795 (2007), *Link-Local Multicast Name Resolution (LLMNR)*.

[b-IETF RFC 4861] IETF RFC 4861 (2007), *Neighbor Discovery for IP version 6 (IPv6).*

[b-IETF RFC 4864] IETF RFC 4864 (2007), *Local Network Protection for IPv6*.

[b-IETF RFC 4942] IETF RFC 4942 (2007), *IPv6 Transition/Coexistence Security Considerations*.

[b-IETF RFC 5942] IETF RFC 5942 (2010), *IPv6 Subnet Model: The Relationship between Links and Subnet Prefixes*.

[b-IETF RFC 5969] IETF RFC 5969 (2010), *IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) – Protocol Specification*.

[b-IETF RFC 6092] IETF RFC 6092 (2011), *Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service*.

[b-IETF RFC 6106] IETF RFC 6106 (2011), *IPv6 Router Advertisement Options for DNS Configuration*.

[b-IETF RFC 6169] IETF RFC 6169 (2011), *Security Concerns with IP Tunneling*.

[b-IETF RFC 6333] IETF RFC 6333 (2011), *Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion*.

[b-IETF RFC 6434] IETF RFC 6434 (2011), *IPv6 Node Requirements*.
