International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1037

(10/2013)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Information and network security – Network security

IPv6 technical security guidelines

Recommendation ITU-T X.1037

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	**X.1030–X.1049**
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1037

IPv6 technical security guidelines

Summary

The Internet Protocol version 6 (IPv6) is intended to provide many built-in benefits such as large address space, and self-configuration capabilities. Because it is a new protocol that is likely to be massively adopted in the coming years and operates differently than the 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, multicast addressing for specific services, the ability to assign multiple IPv6 addresses to a given interface, and for the use of the ICMPv6 protocol as the cornerstone of the IPv6 protocol machinery (dynamic neighbour discovery, ICMPv6 Router Advertisement (RA) messages that convey configuration information so that IPv6 terminal devices can automatically access to the IPv6 network, etc.) can be identified. Although somewhat equivalent capabilities exist in IPv4 and have been exposed to security threats for quite some time, IPv6 implementation and operation differs from IPv4, at the risk of raising specific security issues.

From that perspective, Recommendation ITU-T X.1037 provides a set of technical security guidelines for telecommunication organizations to deploy and operate IPv6 networks and services. 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.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1037	2013-10-07	17	11.1002/1000/11946-en

Keywords

Countermeasure, DHCPv6, DNS, domain name system, dynamic host configuration protocol, end nodes, firewall, IDS, Internet Protocol version 6, intrusion detection system, IPv6, NAT, network address translation, network devices, risk assessment, router, security threats, switch.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1037

IPv6 technical security guidelines

1 Scope

Recommendation ITU-T X.1037 specifies security threats raised by the introduction of the IPv6. It also provides a risk assessment related to these threats and documents 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, DHCP server) and security devices (e.g., intrusion detection system (IDS), and firewall (FW)) that will be also deployed in an 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. This Recommendation provides a security guideline focusing on IPv6 in enterprise networks. The guidelines for other environments such as home network and carrier network are outside the scope of this Recommendation.

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 Standard 802.1x-2010, *IEEE Standard for Local and metropolitan area networks – 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 2993] IETF RFC 2993 (2000), *Architectural Implications of NAT*.

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

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

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

[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 5902] IETF RFC 5902 (2010), *IAB Thoughts on IPv6 Network Address Translation*.

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

[IETF RFC 6104] IETF RFC 6104 (2011), *Rogue IPv6 Router Advertisement Problem Statement*.

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

[IETF RFC 6146] IETF RFC 6146 (2011), *Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers*.

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

[IETF RFC 6296] IETF RFC 6296 (2011), *IPv6-to-IPv6 Network Prefix Translation.*

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	IPv6 address record
AS	Autonomous System
CPE	Customer Premises Equipment
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
FIB	Forwarding Information Base
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
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
L2	Layer 2
LSA	Link State Advertisement
LSDB	Link State Database
MAC	Media Access Control
MLD	Multicast Listener Discovery
MTU	Maximum Transfer Unit
NA	Neighbour Advertisement
NAT	Network Address Translation
NAT64	Network Address Translation 6 to 4
NAT66	Network Address Translation 6 to 6
NDPMon	Neighbour Discovery Protocol Monitor
NDP	Neighbour Discovery Protocol
NPTv6	Network Prefix 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 Neighbor Discovery
TCP	Transmission Control Protocol
TTL	Time To Live
uRPF	unicast Reverse Path Forwarding

5 Conventions

None.

6 Topology of IPv6 network for enterprise networks

This clause describes a topology of the IPv6 enterprise network (including transition environments to IPv6 where there exist three different types of hosts: IPv4 only, IPv6 only and IPv4/IPv6-enabled) that will be used as an enterprise network for illustrating the attack scenarios and security countermeasures. The topology of an IPv6 enterprise network is illustrated in Figure 6-1 as an example. Similar to an IPv4 network, it consists of five segments: an external segment, a demilitarized zone (DMZ), a backbone segment, a server segment and a client segment. The external segment is a connection point between Internet service providers (ISPs) and a customer

premises equipment (CPE) installed in the enterprise network. 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 segment is a large-capacity, high-speed network, and other network segments are connected to each other through it. In the server segment there exist many different kinds of network service platforms (e.g., DNS server, DHCPv6 server), which are necessary for internal users. Finally, client computers are located in the client segment.

This IPv6 security guideline focuses on describing IPv6 security threats and countermeasures from the viewpoint of network components: network devices (in all segments), client and server end nodes (in client and server segments), and security devices (in DMZ segment). For this purpose, the remainder of this Recommendation is organized as follows:

- IPv6 threats recognized in network device are described in clause 7.
- IPv6 threats recognized in clients, servers, and other end devices are described in clause 8.
- IPv6 threats recognized in security devices such as firewalls and IDS devices are described in clause 9.

For the countermeasures against each threat, they can be recommended to be implemented in several network components. For example, countermeasures against denial of service attacks targeting the DHCPv6 server can be implemented on a firewall as well as a DHCPv6 server itself (see Threat and Measure 16 in clause 8.2.1).

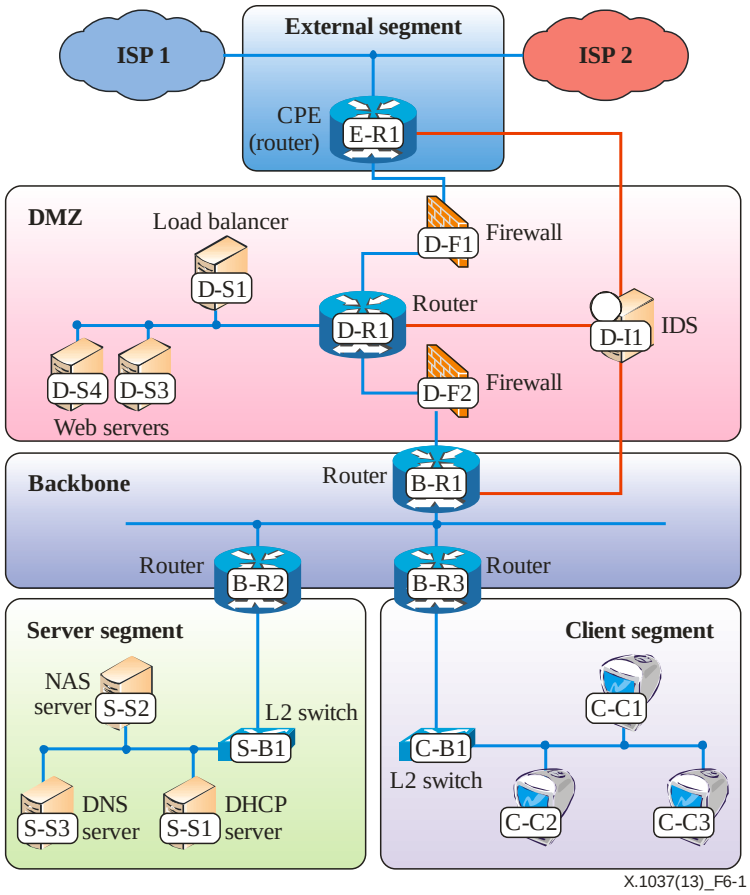

Figure 6-1 – Example topology of an IPv6 enterprise network

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 between routers. There are nine types of LSAs (e.g., network LSA, router LSA, AS-external LSA) and the LSA header includes information about the 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 the 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 the 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 unauthorized nodes. In addition, it is effective for a router to configure the maximum number of LSAs that the router can handle.

Threat 2:

Neighbour cache is used for maintaining entries that identify IPv6 neighbours to which traffic has been sent recently. Entries are keyed on the neighbour's on-link unicast IP address and contain information like the 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 IPv6 addresses to a host via a 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 to 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 allowed 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 two arbitrary 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 usefulness 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 as a countermeasure against the security risk of RH0, which specifies that routers must ignore packets with RH Type 0. Therefore, operators and developers are recommended to verify that their devices are configured correctly according to this specification.

Threat 4:

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 the Internet control message protocol version 6 (ICMPv6) 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 the MLD Querier 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 Querier. 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 that contain a link local address as the source address.

Threat 5:

Since the smallest subnet size in IPv6 is /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 IPv6 addresses are used for interfaces of the routers and the rest remains unused. Although it depends on the router implementation, 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:

Point-to-point link addressing within networks MUST use /127s Global Unicast Address prefixes. This is not only for the sake of optimizing the IPv6 addressing space (it's not even the primary motivation), but also for preventing typical Ping-Pong attacks. Indeed, the Ping-Pong attack can be summarized as follows:

- Routers A and B are connected with a P2P link. A is assigned `2001:db8:dead::1/64` address on its P2P I/F and B is assigned `2001:db8:dead::2/64` address on the corresponding P2P I/F that connects it to A.
- An IPv6 datagram arrives at A with `2001:db8:dead::3/128` as the destination address.
- The destination is for the subnet associated with the P2P link, but does not correspond to A's I/F address. So A forwards the IPv6 datagram on the P2P link, because there is usually NO Neighbor Discovery operation on a P2P link. That's the *Ping*.
- B receives the said datagram and checks the destination address mentioned above. This address belongs to the prefix associated with the P2P link and B therefore forwards the datagram back on the P2P link. That's the *Pong*.

- A then receives the packet and the cycle is repeated.

An attacker can therefore flood IPv6 traffic with unused destination addresses on a /64 subnet. The traffic bounces back and forth until the corresponding Hop Limit expires. This results in bandwidth consumption and unauthorized router resource usage. Hence the use of /127 prefixes.[1]

NOTE – This clause currently focuses on enterprise networking environments that only run OSPFv3 as the IPv6 Interior Gateway Protocol (IGP) . Additional security considerations related to the activation of other routing protocols, like MP-BGP and RIPng are considered.

7.2 Switch

7.2.1 Security threats and countermeasures

Threat 6:

An IPv6 address consists of a 64-bit prefix and a 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 information base (FIB) of an L2 switch by sending massive packets with different MAC addresses.

Measure 6:

IEEE 802.1x authentication [IEEE 802.1x] 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 the L2 switch. In addition, developers are recommended to maintain the total number of FIB entries by appropriately discarding older entries when the total number exceeds a threshold.

Threat 7:

RA Guard ([IETF RFC 6105]) has been proposed to mitigate attack vectors based on forged ICMPv6 Router Advertisement (RA) messages. Basically, an RA-Guard-capable L2 switch observes its ports and determines to forward or not RAs received from connected devices based on L2 and L3 header information and static configurations. However, by sending an RA message with forged fragment packets, an attacker can avoid the inspection of an RA Guard so that the attacker can deliver rogue RA messages to legitimate hosts in a network.

Measure 7:

In order to avoid the attack, RA-Guard-capable L2 switches should parse the IPv6 entire header chain in the packet, to identify whether the packet is a Router Advertisement message. Especially if the packet is a first fragment, the switch should check the validity of the fragment offset.

---

[1] A split-horizon mechanism would assume that a packet received on a subnet that corresponds to the subnet used for the P2P link addressing, but does not belong to the receiving interface does not have to be forwarded back out the same interface (if the destination on the subnet exists, this destination already received the packet).

7.3 NAT device

7.3.1 Security threats and countermeasures

Threat 8:

A 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, the so-called NAT and prefix translation version 6 (NPTv6), translates IP addresses of packets between two distinct IPv6 networks as well as NAT64, which translates IP addresses 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 (i.e., binding information base (BIB)) 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 device. This kind of attack exists in an IPv4 environment as well, but as IPv6 has an enormous number of available IP addresses, the effects of the attack can be more dramatic in an IPv6 environment than in an IPv4 environment.

Measure 8:

The IETF is discussing stateless NPTv6 (without a state table) function. In a case where developers implement a stateful NPTv6 device, they should appropriately control the number of entries in the state table so as not to exceed the upper limit of entries. Additionally, discussions in IETF about threats and measures of DoS attacks against NAT devices in [IETF RFC 2993] (sections 8 and 9), [IETF RFC 4864], [IETF RFC 5902], [IETF RFC 6146] (section 5), [IETF RFC 6092] and [IETF RFC 6296] (section 7) are useful for network operators.

8 End nodes (clients, load balancer) and servers

8.1 End nodes

8.1.1 Security threats and countermeasures

Threat 9:

IPv6 hosts can automatically configure their addresses (e.g., global addresses) based upon the prefix information conveyed in Internet control message protocol version 6 (ICMPv6) router advertisement (RA) messages. Since they can also choose a default router according to the information conveyed in 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 intercept or disturb the victim's communications.

Measure 9:

To minimize the security risk raised by forged RA messages, it is recommended to apply the RA Guard (see [IETF RFC 6105]).

Threat 10:

When IPv6 hosts configure their addresses using RA messages, they have to conduct the 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 10:

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 addresses of hosts and the physical port connected to the host. Consideration of a rogue RA in IETF ([IETF RFC 6104]) is also useful information for this issue.

Threat 11:

IPv6 provides a link layer address resolution mechanism with the neighbour discovery protocol (NDP). Once a node determines its link local IP address, 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 are used to not only perform address resolution, but also other functions: reachability checks between neighbours, and duplicate address detection. When a node receives a NA message in response to a NS message, 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) hosts 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 11:

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 can be used. 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.

Threat 12:

An IPv6 router notifies IPv6 nodes via "ICMP redirect messages" of appropriate first-hop nodes towards their destinations. An ICMPv6 message 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 12:

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 ICMPv6 redirecting, operators (or users) should carefully apply such configuration only to requisite minimum nodes such as end nodes that are never required to change their default routes. Another possible solution should be to implement a mechanism which observes and controls ICMPv6 redirect messages on L2 switches.

Threat 13:

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 unauthorized packet induces *N* error message packets as a reflection to the sender of the original packet. By intentionally sending a large number of unauthorized packets to a multicast address with spoofed source addresses as another (victim) node, an attacker can conduct a packet amplification attack against the victim node, which disrupts the victim's communications.

Measure 13:

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 the sake of optimized packet processing) and thus ICMPv6 Packet Too Big messages should not be rate limited. Another solution, uRPF (see [IETF RFC 3704] for discussion of RPF), can prevent the attack by inhibiting attackers from sending packets with a spoofed source address.

Threat 14:

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 path MTU of an arbitrary path before starting communication with a destination node. Since reassembly of fragmented packets is performed by a destination node, a malicious node can exhaust the destination node's computational resources by sending a large number of fragmented packets to the destination. IPv6 faces the same problems of fragmentation/defragmentation inherent to IPv4.

Measure 14:

A simple countermeasure against the DoS attack abusing fragmentation is to appropriately limit the rate of fragment packets (e.g., 1000 packets per second) at a receiver node.

Threat 15:

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 and the 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 the Pad1 options one by one.

Measure 15:

Regarding the security risk raised 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 header to disturb the DoS attack. According to this policy, [IETF RFC 2460] recommends security appliance vendors implement a function to check the validity of padding option.

8.2 DHCP server

8.2.1 Security threats and countermeasures

Threat 16:

IPv6 hosts may configure their addresses by using a stateful dynamic address allocation protocol such as the DHCPv6 if they receive any RA messages with M flag set from routers. During the stateful configuration, IPv6 hosts send DHCPv6 SOLICIT messages to all DHCPv6 servers using a link-scoped multicast address (for DHCPv6 relays) and a site-scoped multicast address (for DHCPv6 clients) 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 the addresses that DHCPv6 servers have, other IPv6 hosts are unable to obtain their addresses. Other threats such as man-in-the-middle attack by a malicious server, and DoS attack using replayed DHCPv6 messages are indicated in [IETF RFC 3315] section 23.

Measure 16:

The countermeasures for attacks against DHCPv6 servers have been discussed in section 21, 22 and 23 of [IETF RFC 3315]. As one of the countermeasures against the threat, the DHCP authentication mechanism is effective to mitigate the threat, which applies the authentication option to DHCPv6 messages.

However, even though DHCP authentication is applied, the attack can still be conducted in a case where a node with a legitimate authentication key is compromised by an attacker. Therefore, as another approach, it is also effective against the attack if the DHCPv6 server limits the rate of DHCPv6 SOLICIT messages. The same approach, the rate-limit of DHCPv6 SOLICIT messages, is also effective on firewalls. Another countermeasure on network devices is to limit the number of MAC addresses connected to a physical port on the L2 switch (i.e., to a certain value).

8.3 DNS server

8.3.1 Security threats and countermeasures

Threat 17:

If a malicious node, which is serving rogue DHCPv6 and DNS services, sends a rogue RA message with a M flag bit set, the other nodes that received the RA messages are forced to use the DHCPv6 service which is operated by the attacker. After that the malicious node sends DHCPv6 Advertise messages so that the malicious node can disguise itself as a DNS server for victim nodes. 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 AAAA record with the malicious node's IPv6 address. As a result, the victim is unlikely to form a valid IPv6 address and the IPv6 service is therefore denied.

Measure 17:

DHCPv6 snooping on the L2 switch is effective to avoid this attack, which disturbs the activities of the illegal DHCP server. The DHCP message authentication mechanism ([IETF RFC 3315], section 21) is also effective for this attack. Additionally, the RA Guard disturbs the attack at the first step of the process by dropping the illegal RA message from the attacker, unless the RA message is not fragmented (see Threat/Measure in clause 7.2.1).

9 Security devices

9.1 Intrusion detection system

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 routers carry out the encapsulation of outgoing IPv6 packets and the decapsulation of incoming IPv6 packets. Therefore, if an IPv6 host attacks another IPv6 host via a 6to4 router, and if the intrusion detection system (IDS) does not support the encapsulation/decapsulation of 6to4 packets, 6to4 packets are unable to be detected as cyberattacks or suspicious packets. In addition, [IETF RFC 6169] describes similar threats caused by other auto-tunnelling mechanisms such as Teredo and ISATAP.

Measure 18:

IDSs are recommended to support the decapsulation function of the encapsulated IPv6 packets and IPv6-in-IPv4 packets over 6to4 tunnels, if these IDSs are deployed in network boundaries. Or if the IDSs do not have these functions, they should be deployed inside CPE or inside hosts so that they can inspect pre-tunnelled traffic.

NOTE – Other tunnelling techniques like TEREDO and ISATAP should be further considered.

9.2 Firewall

9.2.1 Security threats and countermeasures

Threat 19:

The IPv6 fragment header is used by the IPv6 source host in order to send a packet larger than the path MTU that has been discovered on an arbitrary path. A source host fragments a large packet into multiple smaller packets with the fragment header so that the destination host can reassemble fragmented packets into the original packet according to the fragment header. Each fragmented 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:

A simple solution is to avoid fragmentation. If IPv6 packet fragmentation cannot be avoided, one of the countermeasures on firewalls 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

Examples of threats

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

The following examples of threats provide practical ideas of 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 readers in order to provide additional explanation on several threats discussed in the Recommendation.

Example 1: Figure I.1 shows an example where the web server (S-C1) and the client (C-C1) are communicating with each other. On the backbone segment, routers (B-R1, B-R2 and B-R3) are running OSPFv3. If an attacker somehow compromises a host (C-C2) on the backbone segment and sends a large amount of LSAs to the router (B-R3), the number of received LSAs may exceed the router's capacity. Consequently, the router's OSPFv3 process may become extremely heavy, resulting in abnormal forwarding behaviour. This example is associated with Threat 1.

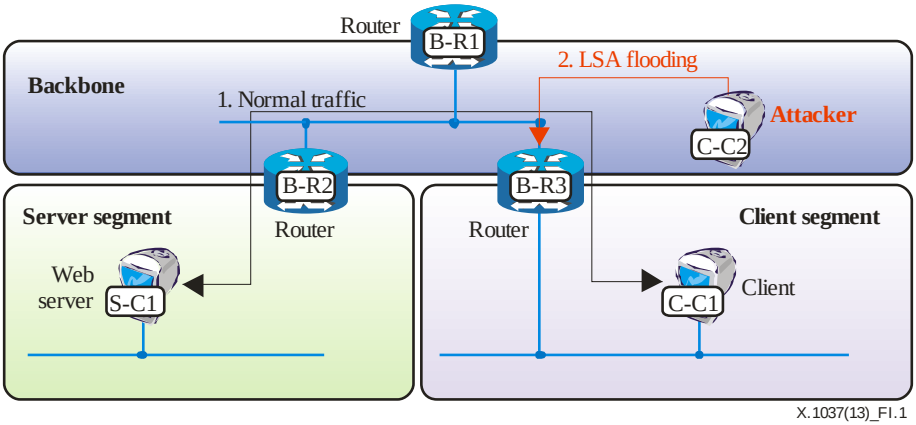

Figure I.1 – LSA flooding (Threat 1)

Example 2: Figure I.2 shows an attack scenario of forged RA messages. In this attack scenario, the router (B-R3) sends legitimate RA messages to the client (C-C1) that wants to communicate with the web server (S-C1). In this situation, the attacker (C-C2) also sends the client forged RA messages which specify the attacker as the default gateway. Using this attack, the attacker can intercept or disturb all traffic between the client and the web server. This is an example associated with Threat 8.

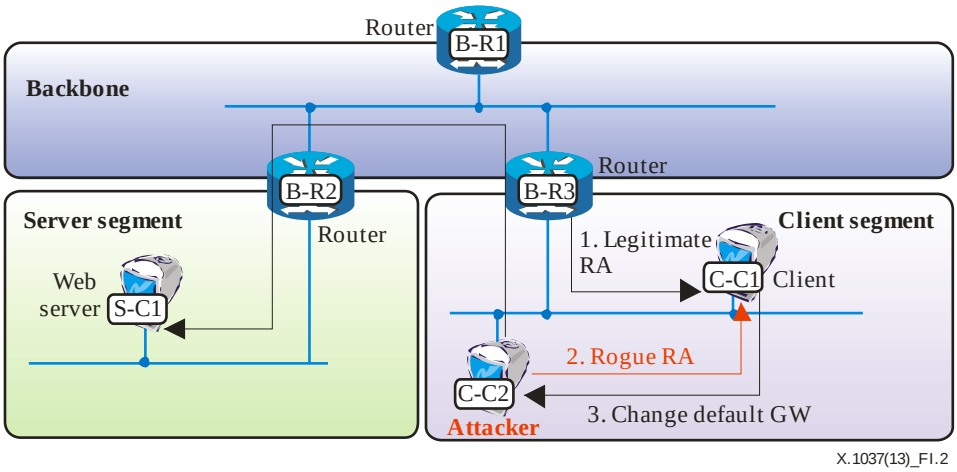

Figure I.2 – Forged RA messages (Threat 8)

Example 3: Figure I.3 shows an attack scenario of the 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 is a practical example associated with Threat 9.

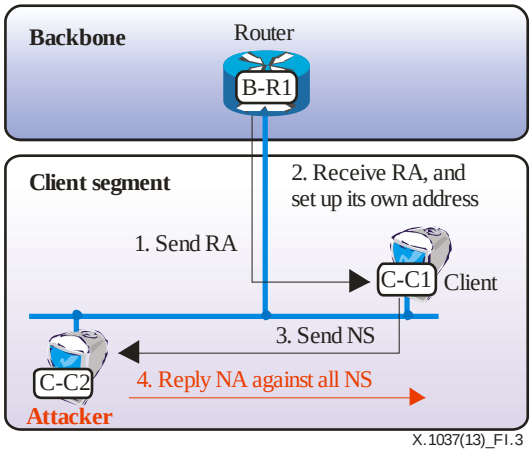

Figure I.3 – Abused DAD procedure (Threat 9)

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 the IPv6 Technical Verification Consortium 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 is a practical example associated with Threat 16.

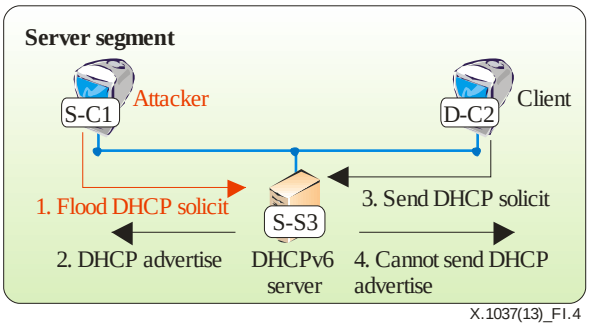

Figure I.4 – DHCPv6 SOLICIT messages (Threat 16)

Example 5: Figure I.5 shows an attack scenario of 6to4 encapsulation. In this attack scenario, an attacker (S-C1) sends the client (C-C1) via 6to4 tunnel a remote exploit code that induces a target host's unintended or unanticipated behaviour while the router (B-R1) forwards captured traffic to the IDS (D-I1). In this circumstance, the IDS could not detect the exploit code due to its encapsulation. This is an example associated with Threat 18.

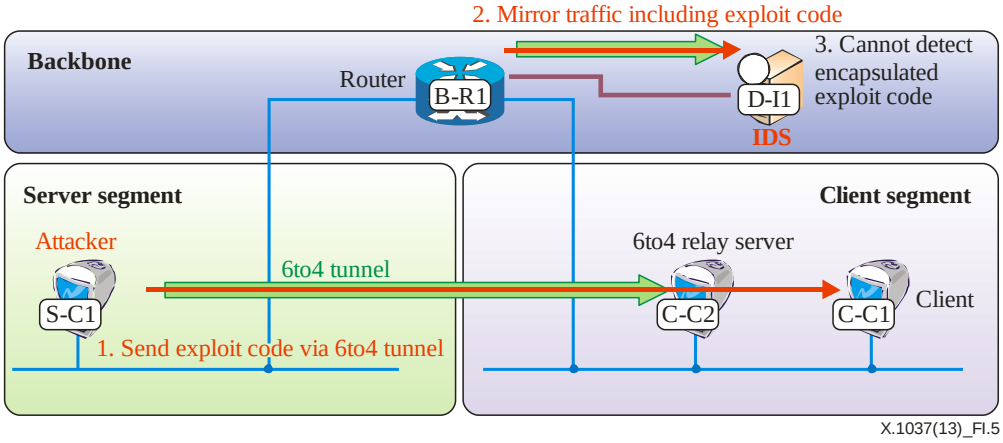

Figure I.5 – 6to4 encapsulation (Threat 18)

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 is a practical example associated with Threat 19.

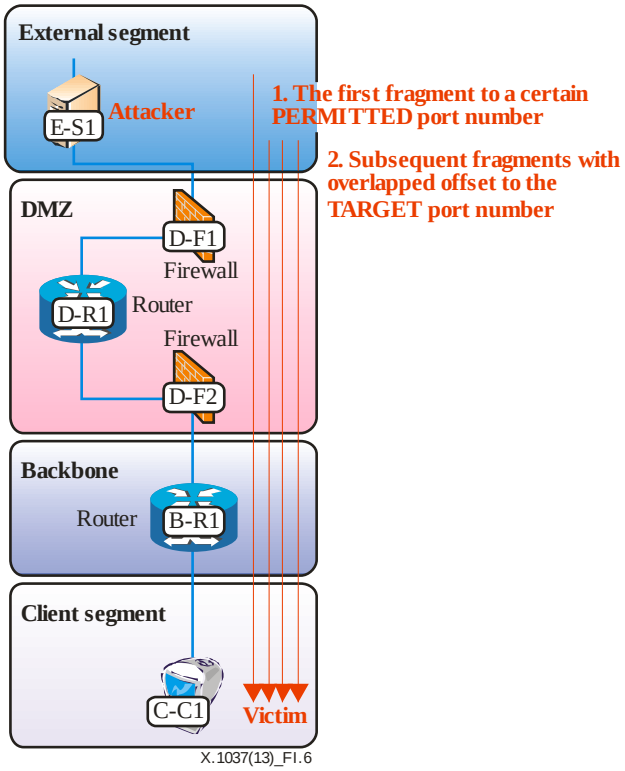

Figure I.6 – Overlapped fragments (Threat 19)

Bibliography

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

[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.*

[b-IPv6TVC] *IPv6 Technical Verification Consortium.*
<http://ipv6tvc.jp/english/default.html>

[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* (2009), *IPv6 Home Router Guideline*.
<http://www.v6pc.jp/pdf/v6hgw_Guideline_1_0-English.pdf>

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2014