

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

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



International
Telecommunication
Union

Documents
Document Sharing Hub

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/>.

© ITU 2014

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

Table of Contents

		Page
1	Scope	1
2	References.....	1
3	Definitions	2
	3.1 Terms defined elsewhere	2
	3.2 Terms defined in this Recommendation.....	2
4	Abbreviations and acronyms	2
5	Conventions	3
6	Topology of IPv6 network for enterprise networks.....	3
7	Network devices	5
	7.1 Router	5
	7.2 Switch	7
	7.3 NAT device	8
8	End nodes (clients, load balancer) and servers.....	8
	8.1 End nodes	8
	8.2 DHCP server.....	11
	8.3 DNS server	11
9	Security devices	12
	9.1 Intrusion detection system.....	12
	9.2 Firewall.....	12
	Appendix I – Examples of threats.....	13
	Bibliography.....	17

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