International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 23

(09/2014)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.1037 – Supplement on security management guidelines for the implementation of an IPv6 environment in telecommunications organizations

ITU-T X-series Recommendations – Supplement 23

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
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

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

Supplement 23 to ITU-T X-series Recommendations

ITU-T X.1037 – Supplement on security management guidelines for the implementation of an IPv6 environment in telecommunications organizations

Summary

Supplement 23 to ITU-T X-series Recommendations provides security management guidelines for the implementation of IPv6 environment in telecommunication organizations in order to ensure the protection of information in the networks and protection of the supporting network infrastructure when transitioning from IPv4 to IPv6 and implementing an IPv6 environment.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X Suppl. 23	2014-09-26	17	11.1002/1000/12332

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

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication 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 publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication 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 publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. 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

Supplement 23 to ITU-T X-series Recommendations

ITU-T X.1037 – Supplement on security management guidelines for the implementation of an IPv6 environment in telecommunications organizations

1 Scope

This Supplement provides security management guidelines for the implementation of IPv6 environment in telecommunications organizations in order to ensure the protection of information in the networks and protection of the supporting network infrastructure when transitioning from IPv4 to IPv6 and implementing IPv6 environment.

2 References

[ITU-T X.1037] Recommendation ITU-T X.1037 (2013), *IPv6 technical security guidelines*.

[ITU-T X.1051] Recommendation ITU-T X.1051 (2008), *Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002.*

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

[IETF RFC 4941] IETF RFC 2460 (2007), *Privacy Extensions for Stateless Address Autoconfiguration in IPv6.*

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

3 Definitions

The definitions given in [ITU-T X.1037] apply.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

DAD	Duplicate Address Detection
DB	Database
DHCPv6	Dynamic Host Configuration Protocol version 6
DNS	Domain Name System
DoS	Denial-of-Service
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IT	Information Technology
L2	Layer 2
L3	Layer 3
LAN	Local Area Network
MAC	Media Access Control
MITM	Man-In-The-Middle
MLD	Multicast Listener Discovery
NA	Neighbour Advertisement

NAT	Network Address Translation
NDPMon	Neighbour Discovery Protocol Monitor
NS	Neighbour Solicitation
OS	Operating System
RA	Router Advertisement
SEND	Secure Neighbour Discovery
SLAAC	Stateless Address Auto Configuration
VPN	Virtual Private Network

5 Conventions

None.

6 Overview

The Internet protocol version 6 (IPv6) is intended to succeed IPv4, which is the protocol currently used to direct almost all of the Internet traffic. The Internet operates by transferring data between hosts using an addressing scheme, such as IPv4 or IPv6, to specify their source and destination addresses. Each host, computer or other device on the Internet, requires an IP address in order to communicate. The growth of the Internet has created a need for more addresses than are possible with IPv4.

IPv4 has allocated a space of 32 bits for IP addresses, which means that overall 2^{32} (4 294 967 296) addresses exist in the IPv4 space. However, the IPv4 address space becomes exhausted with the overall growth of the Internet.

IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with this long-anticipated IPv4 address exhaustion and is described in [IETF RFC 2460]. IPv6 uses 128-bit addresses, for an address space of 2^{128} (approximately 3.4×10^{38}) addresses. This equates to 665 570 793 348 866 943 898 599 addresses per square meter of the earth surface, and is equivalent to every individual on this earth having more than 40 000 IPv6 subnets assigned – this will therefore be sufficient for many more devices and users to use the Internet. This expansion allows for many more devices and users on the Internet as well as extra flexibility in allocating addresses and efficiency for routing traffic.

Despite of the well-known problem of IP address exhaustion, organizations in large parts of the world have been hesitant in changing over from IPv4 to IPv6. Organizations need to develop a migration strategy from IPv4 to IPv6, especially for ensuring continued communication around the world. However, IPv6 deployment is not easy to manage. There are a number of considerations an organization should take into account, and this supplement describes some of important processes required for information security management.

7 Considerations of IPv4 and IPv6

7.1 IPv6 features

The main objective for successful transition is to allow IPv6 and IPv4 hosts to interoperate. A second objective is to allow IPv6 hosts and routers to be deployed in the Internet in a highly diffuse and incremental fashion, with few interdependencies. The third objective is an easy transition for end-users, system administrators and network operators.

The IPv6 transition mechanisms are a set of protocol mechanisms implemented in hosts and routers, with some operational guidelines for addressing and deployment, designed to make the transition to work with as little disruption as possible. These will ensure that IPv6 hosts can interoperate with IPv4

hosts in the Internet up until the time when IPv4 addresses run out. The IPv6 transition mechanisms provide a number of features, including:

- Incremental upgrade and deployment: Individual IPv4 hosts and routers may be upgraded to IPv6 one at a time without requiring other hosts or routers to be upgraded at the same time. New IPv6 hosts and routers can be installed one-by-one.
- Minimal upgrade dependencies: The domain name system (DNS) server must first be upgraded to handle IPv6 address records before upgrading hosts.
- Easy addressing: For IPv4 hosts or routers being upgraded to IPv6, they may continue to use their existing address. So, no need for new address assignment.
- Minimal operational upgrade cost and training expenses: Little or no preparation work is needed in order to upgrade existing IPv4 systems to IPv6, or to deploy new IPv6 systems.

7.2 Transition from IPv4 to IPv6

There are several options an organization can chose from when transitioning over from IPv4 to IPv6. However, any decision should be well thought out, and the organization should ensure that the strategy chosen fulfils their requirements, is feasible to implement and provides the organization with appropriate information security during and after the transition. The three main options for transition are:

1) Providers do everything (see clause 7.3);
2) "Dual" strategy in parallel (see clause 7.4);
3) Total migration from IPv4 to IPv6 (see clause 7.5).

7.3 Providers do everything

The benefit of this approach is that the organization can keep its IPv4 addresses and uses everything as usual. The provider will use network address translation (NAT) to translate from IPv6 to IPv4 or vice versa.

Pros:

- This option does not need extra modification or reconfiguration in the organization;
- There is no need to change the internal IP version; internally, everything can just continue running as before.

Cons:

- A lot of reliability on the provider;
- The organization needs to coordinate ALL of its services with that provider.

Security considerations:

- Additional access control needs to be implemented to prevent improper usage by malicious users;
- Improper address translation implementation may be subject to buffer overflow attack – this can be an issue related to the provider (see [ITU-T X.1037]);
- There are restrictions on the use of this solution, some of which negatively impact the security features of IPv6;
- These translation techniques are complicated and are intended to be used as a last resort.

7.4 Dual stack approach

IPv6 was delivered with a lot of migration techniques but many were ultimately rejected and today a small set of practical approaches is left. One technique, called dual stack, involves running IPv4 and

IPv6 concurrently. End-hosts and network devices run both protocols, and if IPv6 communication is detected that is the favoured protocol.

Pros:

- The end user is in control of all changes in its infrastructure;
- No need to change internal IP version.

Cons:

- Double address administration is required on firewalls, DNS servers and edge routers.

Security considerations:

- Organizations that run dual-stack device will have to deal with the vulnerabilities of both protocols;
- Dual-stack operation can raise other security problems if consistent security policies are not created for both IPv6 and IPv4 traffic. For example, if a firewall is not configured to apply the same level of screening to the IPv6 packets as for the IPv4 packets, the firewall may let IPv6 pass through to dual-stack hosts within the enterprise network, potentially exposing them to attack.

7.5 Total migration to IPv6

Another possibility is, of course, to totally migrate from IPv4 to IPv6. If this option is chosen, it is recommended to use a phased approach for the transition from IPv4 to IPv6. The use of a phased implementation will enable an organization to implement IPv6 with as little disruption to the current environment as possible.

Pros:

- No further need for network address translation (NAT);
- It is possible to use all benefits of IPv6, such as host-to-host IPsec, Jumbograms and other.

Cons:

- Double address administration on firewalls, DNS servers and edge routers until the rest of the world has implemented one of the three strategies.

Security considerations:

- The organization can use all IPv6 benefits without restriction.

8 Information security management for IPv6 deployment

8.1 Overview

As the above considerations have demonstrated, an organization should apply some thoughts before migrating from IPv4 to IPv6. As IPv6 is the future and is inevitably coming, organizations should develop a strategy to identify their approach to this change. This strategy should take into account the business impacts and risks associated with this change and should make implementation decisions based on the impacts and risks and the possibilities that the organizations have to address the risks.

This should be followed by an implementation of the IPv4 to PIv6 strategy to initiate and complete the change in the best way for the organization. Once the change has been completed, the implemented solutions should be audited and reviewed to ensure that everything is working as intended.

8.2 Business impact analysis

A telecommunication business impact analysis for the IPv4 to IPv6 transition is an organization wide effort that aims to understand the organization's business and information technology (IT) environments in order to determine the business processes, services and applications that are dependent on the use of the Internet. This leads to the identification of all critical business processes, services and applications and the impact of any disruptions based on their importance to the overall business of the organization. Business impact analysis, in combination with risk assessment, can provide a detailed understanding of the business, risks, and focus on the priorities that would not otherwise be apparent to the top management.

When conducting a business impact analysis, the organization identifies the list of critical business functions dependent on Internet services required for continued successful business operation. The business impact analysis should include:

- Establishing the context of assessment, defining criteria for criticality and evaluating the potential impact related to a disruptions caused by the transition from IPv4 to IPv6;
- Considering systematically defined criteria for evaluating the potential impacts of disruptions caused by the transition from IPv4 to IPv6;
- Taking into account legal, regulatory and contractual requirements which the organization has to fulfil and which might be negatively impacted by the transition from IPv4 to IPv6;
- Defining the required output from the business impact analysis to develop the transition strategy.

The results of the business impact analysis should at least include the following most important details as input into the development of the IPv6 strategy:

- Categorization of each of the activities according to their priority for continuity throughout the transition;
- The maximum time period within which the activity needs to be resumed in case of disruptions throughout the transition;
- Prioritized timeframes for resuming these activities at a specified minimum acceptable level, taking into consideration the time within which the impacts of not resuming them would become unacceptable;
- Dependencies and supporting resources of these activities, including suppliers, outsource partners and other relevant stakeholders.

8.3 Risk assessment

Once the business impact analysis has been completed, a risk assessment should be used to identify the probability and impact of a variety of risks that may cause business interruptions to services when transitioning over from IPv4 to IPv6.

The identification of risks should consider any factor that might interrupt the business processes, services and applications during the transition process, and any factor that might make the transition impossible in the first place. This can include any of the technical topics considered in clauses 7.3 to 7.5, the pros and cons of the various options for transition. It should also include a consideration for choosing suitable personnel to carry out the actions necessary for the transition and evaluation of the technical soundness of the systems involved.

Part of this risk assessment should be an IPv6 readiness assessment for all equipment that will be involved if IPv6 was implemented. This should include assessment of the:

- Network hardware;
- Servers, PCs (e.g., operating systems);
- Network management and security;

- Applications;
- IT systems;
- Organizational capability (IPv6 skills).

The results of the business impact analysis and risk assessment process should give an overview of the critical business processes, services and applications and the impacts and risks associated with transition from IPv4 to IPv6. Especially, this process should help to identify which of the three strategies explained in clauses 7.3-7.5 is the most suitable one for the organization and which risks remain if that strategy is chosen.

8.4 IPv6 strategy development and implementation

Based on the results of the business impact analysis and risk assessment, the organization shall identify a strategy on how to migrate from IPv4 to IPv6. The first element of the strategy should be to identify which of the three options listed in clause 7 the organization should choose. This choice should be based on the following considerations:

1. If the preferred choice is to rely on the service provider, ensure that the provider has all necessary resources, capabilities, systems and processes in place, and update to contract to include provisions for the transition, as well as for the possibility that it might fail or negatively impact the organization's business. It is also important that all services using Internet are coordinated with the service provider, which might result in increased costs.

   The organization needs to ensure that all of the security concerns listed in clause 7 are properly addressed, either through the service provider or by the organization and that there are no security problems as a result of changing from IPv4 to IPv6.

2. If the preferred choice is to use the dual stack approach, take provisions and ensure for the double address administration on firewalls, DNS servers and edge routers. In order to ensure security of the continued operation, the organization needs to ensure that it is appropriately addressing all vulnerabilities in the transition from IPv4 to IPv6. In addition, it should be ensured that consistent security policies are generated for both IPv6 and IPv4 traffic.

3. If the preferred choice is to completely migrate to IPv6, it should be ensured that there will be no adverse impact on the existing systems, including hardware, operating systems and the applications that are running. Double administration of all those systems that have to connect to IPv4 needs to be put in place due to what other organizations might have in place.

After the preferred option for the transition has been determined, the organization should develop a strategy that defines the exact actions, timeframes and responsibilities for the transition. Sufficient testing should be done before the actual transition starts to ensure that all systems remain fully functional as planned.

8.5 Auditing and review

Once the organization has implemented its IPv6 strategy, it needs to ensure that everything is working as intended. It is therefore helpful to conduct audits to identify whether the IPv6 strategy has been implemented completely and correctly and there are no negative impacts to the business, especially no security problems. The major objectives of an IPv6 networking audit are to:

- Provide management with an independent assessment of the effectiveness of the IPv6 network's architecture, security and alignment with the organization's networking and IT security policies and architecture.
- Provide management with an independent assessment of the effectiveness of the deployment of IPv6 technology in the organization and the conversion process.
- Provide management with an evaluation of the IT function's preparedness in the event of an intrusion.

- Identify issues that affect the security of the organization's network.

The results of the IPv6 networking audit need to be reacted to and if these results show that either the IPv6 strategy chosen or its implementation does not work as expected the organization should rethink the approach or improve its implementation. If the audit identifies any security problems, the organization needs to ensure that these are removed, the more serious they are, the sooner.

9 Examples of practical security controls for IPv6 deployment

9.1 Overview

This clause provides definitions for new objectives, new controls and new implementation guidance, as examples of practical security controls for IPv6 deployment in telecommunication organization. The following clauses are candidates of topics for security controls to be applied for IPv6 deployment.

9.2 Information security policies

The control objective and the contents from clause 5 of [ITU-T X.1051] apply.

9.3 Organization of information security

The control objective and the contents from clause 6 of [ITU-T X.1051] apply.

9.4 Asset management

The control objective and the contents from clause 7 of [ITU-T X.1051] apply.

9.5 Access control

It is recommended to establish an access control policy according to the requirements of business workflow and information security. Once established, it should be in written form and be subjected to review.

Assets management supervisor should control the access to the assets to avoid the security risk. The proper access rights should be provided to each user according to its job role.

In the process of establishment of access control policy, following aspects should be taken into consideration:

- Information and operation to which access should be controlled;
- Points where access controls should be implemented (IPv6 network, operating system (OS), application, folder/file);
- Separation of roles for access control (e.g., request of access, approval of access, access management);
- Roles for which the privileged access is permitted;
- Process for the decision and approval of access rights;
- Regulation and duties related with access control in the agreement.

9.5.1 Access IPv6 networks and IPv6 network services

It is recommended to limit users' access to only IPv6 networks/IPv6 network services they are specially allowed to utilize.

In the process of establishing the IPv6 networks/IPv6 network services utilization policy, the following aspects should be taken into consideration:

- IPv6 networks/IPv6 network services to be allowed to access;

- Approval process to decide who will be allowed to access which IPv6 networks/IPv6 network services;
- Management operating policy for access to IPv6 networks/IPv6 network services;
- The method to access IPv6 networks/IPv6 network services, such as virtual private network (VPN), wireless local area network (LAN);
- Requirement for user authentication;
- Monitoring of IPv6 network services;
- IPv6 network services utilization policy should be complied with access control policy in the organization.

9.5.2 Management of user access

It is recommended to ensure the approved users' access to IPv6 networks/IPv6 network services, while denying non-approved user access.

9.5.2.1 Registration and deletion of users

It is recommended to establish the process of registration and deletion of users for the proper assignment of access rights.

In the process, the following aspects should be taken into consideration:

- The identifier (ID) must be unique in order to link user and user activity, and to make users take responsibility for their activity. Common ID should be allowed only the emergency cases for the maintenance and operation purpose and must be recorded properly.
- Prompt deletion and invalidation of the ID provided to an employee who leaves the organization.
- Regular check of ID list to avoid the existence of improper IDs.
- Duplication of IDs.
- The following two steps should be considered in the process of registration and invalidation of access to information/information process facilities:
  - Assignment of the user ID;
  - Access right of the user ID.

9.5.2.2 Assignment of user access

It is recommended to establish the process of assignment and invalidation of access rights to all types of users of all IPv6 networks/IPv6 network services.

In the process, the following aspects should be taken into consideration:

- Approval must be obtained from the supervisor for IPv6 networks/IPv6 network services;
- The approved access level should comply with the access control policy and fulfil the requirements of regulation such as that related to job separation;
- Assurance access remains invalid until the completion of the approval process;
- Centralized recording management of access rights provided to user IDs;
- Prompt deletion or invalidation of the ID provided to an employee who leaves the organization, or changes of access rights to an employee who is promoted;
- Regular review of access rights of the supervisors of IPv6 networks/IPv6 network services.

9.5.2.3 Management of privileged access rights

It is recommended to limit the assignment and usage of privileged access rights.

Assignment of privileged access rights should be controlled according to the access control policy.

For the management of privileged access, the following aspects should be taken into consideration:

- Define the privileged rights related to the IPv6 system and its process such as OS, database (DB) management system, application, and specify the user that will use those privileged rights;
- Assign minimum privileged access rights according to the requirement of the users' role, in compliance with to the access control policy;
- Record all the process for the approval of privileged access rights and maintain its record. Privileged access rights remain invalid until the completion of the approval process;
- Determine the conditions for the expiration of privileged access rights;
- Assign privileged access IDs separately from common user IDs utilized in daily work. Privileged access IDs should not be utilized in daily work;
- In order to avoid the utilization of supervisor IDs for unapproved usage, a specific process for maintaining the system should be established and maintained;
- Private credentials should be kept confidential in case of utilizing a common supervisor ID (e.g., Utilization of one-time passwords or change of password after each assignment).

9.5.3 Management of user credentials

It is recommended to maintain the assignment of credentials according to the proper maintenance process.

The maintenance process for assignment of user credentials should include the following aspects:

- The temporary credential information should be changed at the time of initial usage;
- A process of identity verification should be established before the issuance of an initial temporary credential or its renewal;
- The temporary credential should be transferred to the user via a secure method;
- Temporary credentials should be unique and non-presumable;
- Credentials defined by a vendor or system integrator should be changed after installation of the system/software;
- Temporary credentials issued for specific tasks should be invalidated or deleted after the completion of the task.

The most common credential is passwords, but credentials could include the encrypted key stored in hardware tokens such as smart cards.

9.5.4 Management of user access terminals

9.5.4.1 Management of terminal and address under local environment

Several methods are proposed when assigning IPv6 addresses to terminals. It is recommended that the following management method be implemented to manage IPv6 addresses assigned to user terminals:

- Use of a unified method to assign IPv6 address to terminals inside the network;
- Assignment of an IPv6 address only to terminals approved to be connected to IPv6 networks;
- Recording of the combination of media access control (MAC) address and IPv6 address;
- Recording of the combination of user ID and terminal ID.

There are multiple scopes of IPv6 addresses depending on the purpose of usage. The main ones are:

- Link local address;
- Global unicast address;
- Unique local address.

It is recommended that the method of propriety and assignment of IPv6 addresses be unified per type of scope.

In case of hiring stateless address auto configuration (SLAAC), it is also recommended to have a unified policy for the implementation of privacy extension according to [IETF RFC 4941].

9.5.4.2 Management of terminal and address under remote environment

It is recommended to apply the following management process if the users access information data remotely via an IPv6 network:

- Assign a unique ID to each user who accesses information data from remote areas;
- Use both user ID and authentication with credential for remote access;
- Use user ID and IPv6 address of remote area in authentication and record its result;
- Limit the information data to be accessed from remote areas to avoid access to unnecessary information data;
- IPv6 provides end-to-end communication, but a gateway exclusive for remote access should be installed. The remote access should be limited to access by the way of this special gateway;
- Proper encryption should be used for remote access to avoid tapping.

9.5.5 Filter control of firewall/router

It is recommended to configure packet filtering for routers and firewalls.

The following are filtering examples:

- Block unused or Internet control message protocol version 6 (ICMPv6) types used for experimentation
  - For example, 5-99, 100-126, 154-199, 200-254
- Minimum ICMPv6 type required for operation should be open for Internet access
  - For example, Type 1 (Destination Unreachable), type 2 (PTB), 3 (code 0, Time exceeded, 4 (code 1 and 2, parameter issue), 128 (Echo request), 129 (Echo response)
- Place restrictions on the following ICMPv6 message from the Internet
  - For example,Type 2, 4, 130-132, 143 (MLD) 133-134 (RS/RA), 141-142 (NS/MA)
- Anti-spoofing for firewall
  - Packets including source address not in use in the organization should not be transmitted to the Internet
- Filtering of Bogon pass
  - Configure filtering Bogon pass. Link local address, Site local address, space.6bone reserved by IETF are the example of Bogon pass. Bogon pass is varied by the operation status of IPv6 Internet. It is recommend to obtain the latest information.
- Filtering to tunnel protocol
  - Restrict the communication using the tunnel protocol to avoid the connection of terminals inside the organization to IPv6 outside the management of organization.

As for the filtering, it is recommended to confirm the filtering status and save filtered packet information/file, and IPv6 system administrator should review monthly the contents of saved information/file and record its result.

9.6 Physical and environmental security

The control objective and the contents from clause 9 of [ITU-T X.1051] apply.

9.7 Operations security for IPv6 migration

See clause 7.2 (Transition from IPv4 to IPv6) in this supplement.

9.8 Communications and operations security

The control objective and the contents from clause 10 of [ITU-T X.1051] apply.

9.9 Systems acquisition, development and maintenance

9.9.1 Design of IPv6 network

9.9.1.1 Design policy of IPv6 network

In the IPv6 environment, it is possible to allocate 2^{64} address spaces in a single segment. This means that all servers and clients can be located in a single segment. However, in order to correctly manage security controls for managed entities (servers and clients), the system should be appropriately segmented into several manageable parts and provide clear boundaries among segmented parts.

The following guideline should be applied for segmenting manageable parts in the IPv6 information system environment.

- Equipment roles

  Equipment which provide IPv6 services should be grouped and managed in the perspective of targeted consumers for the service provision. For example:

  – IPv6 services delivered to outside users (consumers)

    Equipment which is accessible from the Internet and provide www services, mail services, DNS services, etc. should be segmented into different manageable parts separate from others.

  – IPv6 services delivered to internal users (internal organization)

    Equipment accessible by any user within the organization should be segmented into parts accessible from any department in the organization but not accessible from the outside.

  – IPv6 services delivered to internal users in a department

    Equipment which is only accessible by a department of the organization should be segmented as not accessible by the other departments.

- User roles

  Equipment which is accessible by the IPv6 information systems should be appropriately grouped in terms of equipment users, and segmented into manageable parts. For example:

  – Segmentation in terms of departments

    Since usable IPv6 services and access level of IPv6 systems may differ among departments in the organization, IPv6 segmentation should be provided for each department unit.

  – Segmentation in terms of location

    Equipment should be segmented in terms of location of the users of the system. If several departments exist in a single location, then IPv6 address spaces for the departments should be assigned from the IPv6 address spaces specific for the location.

9.9.1.2 Security controls inside a segment

Communications among terminals in a single IPv6 segment should be appropriately managed to prevent security threats against IPv6 information system environment such as man-in-the-middle (MITM), tampering and IPv6 DoS attacks.

The following guidelines should be taken into considerations against vulnerabilities in the IPv6 environment described in clauses 8.1.1 (Threats 10 and 12) and 8.2.1 (Threat 16) of [ITU-T X.1037]:

- Guidelines for countering interruption of IPv6 address assignment

  To counter interruptions of IPv6 address assignment by abused duplicate address detection (DAD), it is recommended to verify corresponding relationships of the IPv6 address and the terminal by audit tools (e.g., neighbour discovery protocol monitor (NDPMon)). If there are any inconsistencies of the relationships, the corresponding terminal should be disconnected from the IPv6 segment.

  In regard to DoS attacks against dynamic host configuration protocol version 6 (DHCPv6) servers, the authentication mechanism of DHCPv6 should be implemented to deny illegitimate requests from malicious terminals. In the process, a management operating policy which includes deployment, announcement and management of access credentials for DHCPv6 service should be established. In addition, the number of DHCPv6 query (SOLICIT) messages should be appropriately limited at the DHCPv6 server.

- Guidelines for countermeasures against DoS attacks by abusing neighbour advertisement (NA) messages

  Secure neighbour discovery (SEND) is one of the countermeasures against a DoS attack by abused NA. Since public keys have to be delivered to each terminal for applying SEND, a management operating policy which includes publication and distribution of public keys should be established in advance. Another countermeasure can be used to check validity of each pair of L2 (MAC) and L3 (IPv6) addresses observed on the layer 2 (L2) switch to detect and avoid illegitimate NA.

- Guidelines for avoidance of interruption of IPv6 communication by abusing ICMPv6 redirect message

  To avoid interruption of IPv6 communication by abused ICMPv6 Redirect message, terminals should be configured to discard all incoming ICMPv6 Redirect messages. As another countermeasure, it is recommended to accept ICMPv6 Redirect messages only from permitted ports where routers are connected.

9.9.1.3 Security of communications among segments

Communications among terminals in multiple IPv6 segments should be appropriately managed to prevent security threats against the IPv6 information system environment. These include man-in-the-middle (MITM), tampering and IPv6 DoS attacks.

The following guidelines should be considered when dealing with the vulnerabilities in the IPv6 environment described in clauses 7.1.1 (Threat 2), 8.1.1 (Threat 9) and 9.2.1 (Threat 19) of [ITU-T X.1037]:

- Guidelines for measures against interruption regarding IPv6 default route

  Authentication of router advertisement (RA) messages based on SEND should be applied to a terminal to avoid attacks by illegitimate RA messages from a malicious terminal.

  As another countermeasure, it is recommended to apply L2 security solution such as RA Guard. In this solution, an L2 switch should be appropriately configured to filter out RA messages from unauthorized physical ports.

- Guidelines for measures against overflow attack of neighbour cache

  It is recommended to apply an appropriate upper limit of neighbour cache for each terminal in order to mitigate overflow attack of the neighbour cache.

- Guidelines for measures against firewall evasion with overlapping fragments

  [IETF RFC 5722] explicitly prohibits sending an overlapped fragment packet to IPv6 devices, which enables to evade packet inspection of a firewall. Therefore, terminals and firewalls should be implemented to discard fragments whose ranges overlap.

9.9.2 Development environment for IPv6 information system and programs

The control objective and the contents from clause 12 of [ITU-T X.1051] apply.

9.10 Information security incident management

The control objective and the contents from clause 13 of [ITU-T X.1051] apply.

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