International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1044

(10/2019)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Information and network security – Network security

Security requirements of network virtualization

Recommendation ITU-T X.1044

International Telecommunication Union

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 (1)	
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 (1)	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 (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
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
QUANTUM COMMUNICATION	X.1700–X.1729

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

Recommendation ITU-T X.1044

Security requirements of network virtualization

Summary

Recommendation ITU-T X.1044 analyses security challenges and threats to network virtualization (NV) and specifies security requirements for the physical resources layer, the virtual resources layer and the logically isolated network partition (LINP) layer in network virtualization.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1044	2019-10-29	17	11.1002/1000/14042

Keywords

Network virtualization, NV.

* 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 UIT-T X.1044

Security requirements of network virtualization

1 Scope

This Recommendation analyses security challenges and threats to network virtualization (NV), and specifies security requirements for the physical resources layer, the virtual resources layer and the logically isolated network partition (LINP) layer in NV.

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.

[ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing.*

[ITU-T X.1631] Recommendation ITU-T X.1631 (2015) | ISO/IEC 27017:2015, *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services.*

[ITU-T X.1642] Recommendation ITU-T X.1642 (2016), *Guidelines for the operational security of cloud computing.*

[ITU-T Y.3011] Recommendation ITU-T Y.3011 (2012), *Framework of network virtualization for future networks.*

[ITU-T Y.3012] Recommendation ITU-T Y.3012 (2014), *Requirements of network virtualization for future networks.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 logically isolated network partition (LINP) [ITU-T Y.3011]: A network that is composed of multiple virtual resources which is isolated from other LINPs.

NOTE – "logically isolated", which is the counter concept of "physically isolated", means mutual exclusiveness of the subjects (i.e., network partition, in this case), while the original subjects may be physically united/shared within the common physical constraints.

3.1.2 network virtualization [ITU-T Y.3011]: A technology that enables the creation of logically isolated network partitions over shared physical networks so that heterogeneous collections of multiple virtual networks can simultaneously coexist over the shared networks. This includes the aggregation of multiple resources in a provider and appearing as a single resource.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAA Authentication, Authorization and Accounting

DDoS Distributed Denial of Service

DoS Denial of Service

FN Future Network

ID Identifier

LINP Logically Isolated Network Partition

NV Network Virtualization

NW Network

SNMP Simple Network Management Protocol

VRM Virtual Resources Manager

5 Conventions

In this Recommendation:

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "**is prohibited from**" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Overview

According to [ITU-T Y.3011] and [ITU-T Y.3012], network virtualization (NV) is a technology that realizes isolated and flexible networks in order to support a broad range of network architectures, services and users that do not interfere with others. It also enables the easy establishment of experimental networks and accelerates research and development on future network (FN) technologies. Therefore, NV is considered to be a key technology for realizing FNs.

As specified in [ITU-T Y.3011], NV has three layers: physical resources layer, virtual resources layer and LINP layer.

- **Physical resources layer**: Physical resource management enables effective and consistent use of physical resources that may include heterogeneous types of equipment, e.g., routers and servers developed by different vendors.
- **Virtual resources layer**: Virtual resource management enables LINPs to bind physical resources and virtual resources.
- **LINP layer**: LINP management enables LINP operators to apply management policies to an LINP.

Figure 1 illustrates the high-level concept of NV.

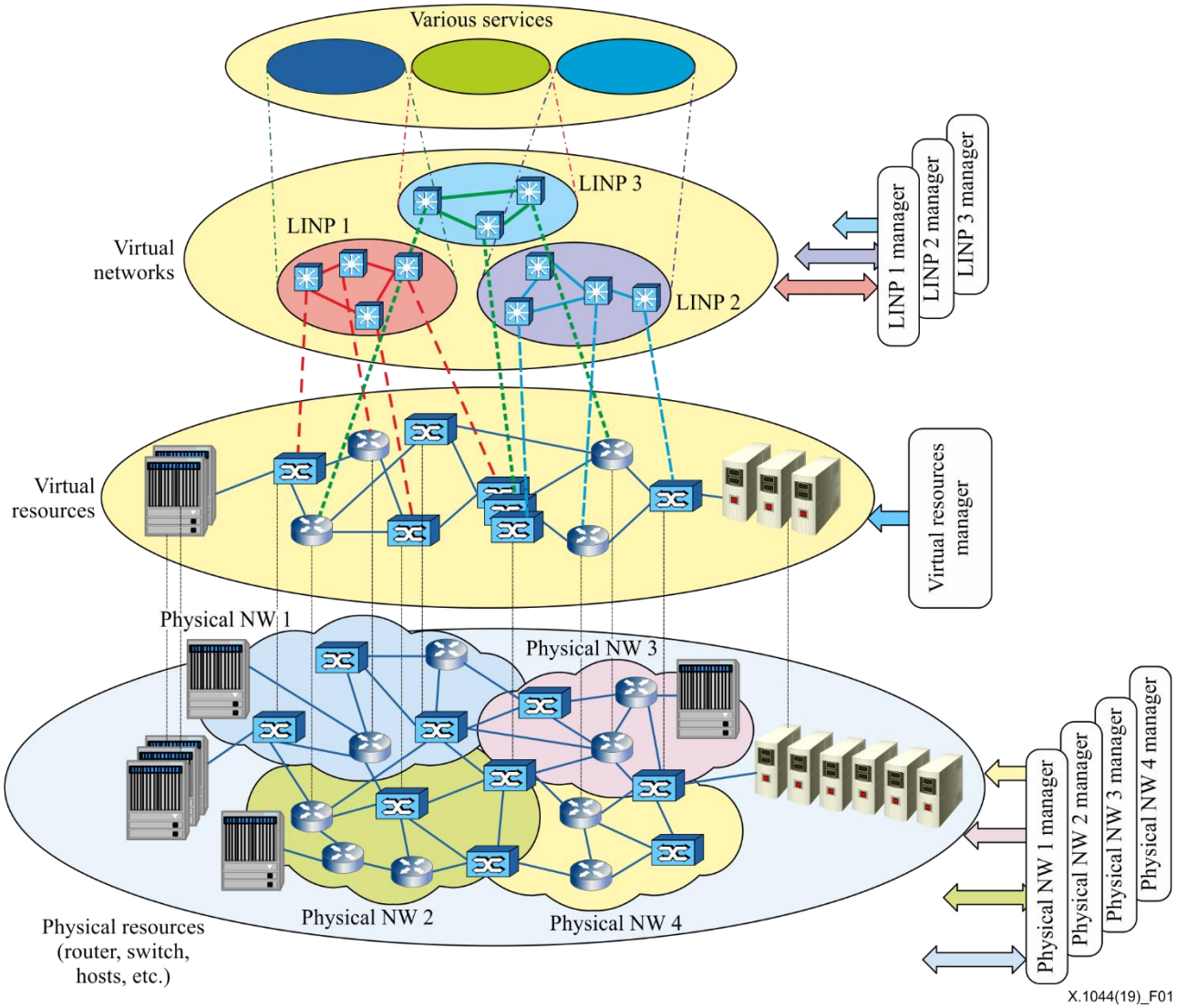

Figure 1 – Conceptual architecture of network virtualization

NV could realize diverse services and heterogeneous network architectures on a common physical network, and is considered to be a key technology for realizing FNs.

On the other hand, NV also face the following security threats and challenges.

- **To the physical resources layer**: Physical resource management enables effective and consistent use of physical resources that may include heterogeneous types of equipment, e.g., routers and servers developed by different vendors. Physical resources in NV face distributed denial of service (DDoS) attack, vulnerabilities due to shared use of physical network devices, etc.
- **To the virtual resources layer**: Virtual resource management enables LINPs to bind physical resources and virtual resources. The virtual resources layer is potentially subject to eavesdropping, man in the middle attack, etc.
- **To the LINP layer**: LINP management enables LINP operators to apply management policies to an LINP. The LINP layer is potentially subject to denial of service (DoS) attacks on LINP management platform, security vulnerabilities of operating system, broken access control, etc.

7 Security challenges and threats of network virtualization

7.1 Security challenges and threats to the physical resources layer

The physical resources layer in NV faces similar challenges and threats to the physical layer in cloud computing due to: a) physical and environmental threats, which include unsecure areas and equipment, such as earthquake, flood, fire; and b) technical attacks, which include DoS or DDoS attacks, malwares and system vulnerabilities.

7.2 Security challenges and threats to the virtual resources layer

The virtual resources layer faces the following challenges and threats:

a) Unavailability of physical resources: if the physical resources are attacked or broken, the virtual resources, which are the abstraction of those physical resources, will all lose their availability and data.

b) Unauthorized administration access: unauthorized administration access to the virtual resource management system can result in data loss. For example, attackers may use a system vulnerability to gain unauthorized administration access to the virtual resource management system and modify configuration information, such as the abstraction information from physical resources to virtual resources.

c) System vulnerability: virtual resources data or configuration information can be lost or maliciously modified due to system vulnerabilities.

d) Man in the middle attack: attackers can use man-in-the-middle attack if there is a malicious resource in the virtual resource layer that is not discovered.

e) Interface vulnerability: attackers may use an interface vulnerability to access the network resource, including interfaces between physical resources layer and virtual resources layer, and interfaces between virtual resources layer and LINP layer.

f) Blurred or non-existent network boundaries: NV is not traditionally considered secure because network boundaries are blurred or non-existent in NV.

g) Service unavailability: a virtual resources manager (VRM) that is used to administer all virtual resources and coordinate the allocation of LINPs can be subject to a DoS or DDoS attack, for example, which can result in service unavailability.

h) Insecure service access: insecure access to a VRM or a virtual resource make it possible for a malicious user to monitor or control the virtual resources, even if these resources are not allocated to the malicious user.

i) Account abuse: virtual resources are managed by multiple VRMs and users to provide both internal and external services. Users sharing administrator passwords or otherwise leaving credentials unsecure (e.g., written on notes stuck to a screen), careless or inadequately trained users or malicious actions by disgruntled employees will always pose a significant threat to any business.

7.3 Security challenges and threats to the logically isolated network partition layer

The LINP layer faces the following challenges and threats:

a) LINP performance degradation: since some LINPs are in a shared physical resource, performance degradation issue of LINPs may be very obvious when those LINPs are quite busy.

b) Service unavailability: many issues may cause service unavailability, e.g., the LINP management system is subject to DoS or DDoS, or unavailability of the physical resource, which is a key part of an LINP.

c) System vulnerability: attackers may use a system vulnerability to access an LINP management system, they may then monitor or control virtual resources, or steal important data, causing whole LINPs to crash.

d) Data loss and leakage: loss or leakage of data is a serious threat to the LINP layer when user services run on LINPs, especially for LINPs whose virtual resources are administered by an outside party that provides those LINPs to users.

e) Interface vulnerability: attackers may use interface vulnerabilities to access the network resource, including interfaces between LINPs and the LINP management system, as well as between the virtual resources layer and LINP layer.

f) Insecure service access: it is possible for a malicious user to monitor or control virtual resources, even if these resources are not allocated to the malicious user through insecure service access.

g) Internal threats: there is always a risk of individuals acting in a malicious or careless manner that puts the security of the service at risk, because some employees of these companies who own LINPs have administrator passwords or they have more opportunities to access LINP management system or something else.

h) Scalability issues: scalability issues for the number of possible LINPs in a shared physical network should be considered, because LINP performance degradation or service unavailability will occur if the number of LINPs in a shared physical network is too large.

i) Loss of trust: sometimes, it is difficult for a user whose virtual resources are administered by an outside party that provides those LINPs to the users to recognize their provider's trust level due to the black-box feature of the LINPs service. Such a lack of sharing at the security level with regard to LINP providers can become a serious security threat for some users in their use of LINP services.

8 Security requirements for physical resources layer in network virtualization

There are two security requirements for a physical resources layer in NV: a) physical and environmental security; and b) technical measures.

8.1 Physical and environmental security

Security requirements for physical and environmental security include secure areas and equipment described in Table 8-1. The objective, the associated implementation guidance and other information specified in clause 11 of [ITU-T X.1631] apply.

8.2 Technical measures

Security requirements against DoS or DDoS attacks, malware and system vulnerabilities to devices are described in Table 8-1. The objective, the associated implementation guidance and other information specified in clause 7.2.2.4 of [ITU-T X.1642] apply.

Table 8-1 summarizes the mapping of security threats and challenges to security requirements in a physical resources layer. The objective, the associated implementation guidance and other information specified in clause 11 of [ITU-T X.1631] and clause 7.2.2.4 of [ITU-T X.1642] apply.

Table 8-1 – Physical resources layer: Security threat mapping to security requirements

Security threats	Security requirements	Reference
Secure areas threats	Physical security perimeter Physical entry controls Securing offices, rooms and facilities Protecting against external and environmental threats Working in secure areas Delivery and loading areas	Clause 11 of [ITU-T X.1631]
Equipment threats	Equipment siting and protection Supporting utilities Cabling security Equipment maintenance Removal of assets Security of equipment and assets off-premises Secure disposal or reuse of equipment Unattended user equipment Clear desk and clear screen policy	
DoS or DDoS attacks	Measures to secure network traffic	Clause 7.2.2.4 of [ITU-T X.1642]
Malwares	Measures against malware	
System vulnerabilities	Patch upgrade	

9 Security requirements for a virtual resources layer in network virtualization

The security requirements for a virtual resources layer include:

a) it is required that LINP identification means, such as an LINP identifier (ID), to differentiate LINPs, be provided;

b) it is required that security threats and challenges be considered throughout the design, development, deployment and runtime lifecycle of NV;

c) it is required that the VRM support logging and auditing;

d) it is required that the integrity and accuracy of virtual resource data be maintained;

e) it is recommended that standard data transmission techniques, e.g., the simple network management protocol (SNMP), be used;

f) it is recommended that access control methods to the interfaces, including interfaces between physical resources layer and virtual resources layer, as well as interfaces between virtual resources layer and LINP layer, e.g., white list and black list, be provided;

g) it is required that unified identity management for internal VRMs and external tenants, which contributes to the confidentiality, integrity, as well as availability of services and virtual resources, be provided. See the relevant content in the clause 9.2 of [ITU-T X.1601].

Table 9-1 summarizes the mapping of security threats and challenges to security requirements in a virtual resources layer.

Table 9-1 – Virtual resources layer: Security threat mapping to security requirements

Security threats	Security requirements
shared use of physical resources	b), d), e)
unauthorized administration access	a), b), c), d), f)
system vulnerability	b), c), d), f)
man in the middle attack	b), c), d), e), f)
interface vulnerability	b), c), d), f)
elastic network boundaries	b), c), d)
service unavailability	a), b), c), d), f)
insecure service access	a), b), c), d), e), f)
account abuse	b), c), d), f), g)

10 Security requirements for a logically isolated network partition layer in network virtualization

The security requirements for LINP layer include:

a) it is required that the LINP management system support logging and auditing;

b) it is required that the LINP providers ensure secure transmission during various virtual resources of a LINP;

c) it is required that interface security, through unilateral or mutual authentication, integrity checksum, end-to-end encryption, digital signature, etc., be ensured;

d) it is recommended that access control methods for the LINP management system, e.g., quarantine mechanisms, malicious access identification and authentication, authorization and accounting (AAA) functions, to be provided;

e) it is recommended that the number of possible LINPs in a shared physical network be carefully considered;

f) it is recommended that the LINP providers supply appropriate encryption methods for user data running on those LINPs.

g) it is recommended that key resources of an LINP be backed up, in case some disaster happens;

h) it is recommended that monitoring of the security and privacy of data and applications that are implemented and deployed in LINPs be maintained.

Table 10-1 summarizes the mapping of security threats and challenges to security requirements in an LINP layer.

Table 10-1 – Logically isolated network partition layer: Security threat mapping to security requirements

Security threats	Security requirements
LINP performance degradation	b), e)
service unavailability	b), c), e), f)
system vulnerability	a), c), d), f),g)
data loss and leakage	a), b), c), d), e), f), h)
interface vulnerability	b), c), f)
insecure service access	a), b), c), d), f), h)
insider threats	a), b), c), d), e), f), g), h)
scalability issues	b), e)
Loss of trust	a), b), c), d), f), g), h)

Bibliography

[b-ITU-T X.1603] Recommendation ITU-T X.1603 (2018), *Data security requirements for the monitoring service of cloud computing*.

[b-ISO/IEC 27033] ISO/IEC 27033 (2010), *Information technology – Security techniques – Network security – Part 3: Reference networking scenarios – Threats, design techniques and control issues*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Environment and ICTs, climate change, e-waste, energy efficiency; 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	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
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, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2020