International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 11

(09/2011)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.1245 – Supplement on framework based on real-time blocking lists for countering VoIP spam

ITU-T X-series Recommendations – Supplement 11

ITU-T

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	
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.

Supplement 11 to ITU-T X-series Recommendations

ITU-T X.1245 – Supplement on framework based on real-time blocking lists for countering VoIP spam

Summary

Supplement 11 to ITU-T X-series Recommendations provides a technical framework based on a real-time blocking list (RBL) for countering voice over Internet protocol (VoIP) spam, which consists of four functional entities: a VoIP spam prevention system (VSPS), a VoIP spam prevention policy server (VSPPS), an RBL central system for VoIP spam prevention (VSP-RBL), and a user-reputation system (URS). This supplement also specifies the functionalities, procedures, and interfaces of each functional entity for countering VoIP spam.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X Suppl. 11	2011-09-02	17

Keywords

RBL, URS, VoIP, VoIP spam.

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 11 to ITU-T X-series Recommendations

ITU-T X.1245 – Supplement on framework based on real-time blocking lists for countering VoIP spam

1 Scope

This supplement to ITU-T X.1245 provides a framework based on RBL for countering VoIP spam. The scope of this supplement consists in:

– defining the functional architecture for countering VoIP spam,

– defining four functional entities: VoIP spam prevention system (VSPS), VoIP spam prevention policy server (VSPPS), RBL central system for VoIP spam prevention (VSP-RBL), and user-reputation system (URS) in the framework,

– describing the procedures and interfaces associated with the functional entities.

Compliance with all relevant laws and regulations should be considered before adopting the anti-spam methods described in this supplement.

2 References

None.

3 Terms and definitions

3.1 Terms defined elsewhere

This supplement uses the following terms defined elsewhere:

3.1.1 spam [b-ITU-T X.1240]: The meaning of the word "spam" depends on each national perception of privacy and what constitutes spam from the national technological, economic, social and practical perspectives. In particular, its meaning evolves and broadens as technologies develop, providing novel opportunities for misuse of electronic communications. Although there is no globally agreed definition for spam, this term is commonly used to describe unsolicited electronic bulk communications over e-mail or mobile messaging for the purpose of marketing commercial products or services.

3.1.2 spammer [b-ITU-T X.1240]: An entity or a person creating and sending spam.

3.1.3 spam over instant messaging (SPIM) [b-ITU-T X.1244]: A spam targeting users of instant messaging service.

3.2 Terms defined in this supplement

This supplement defines the following terms:

3.2.1 call spam: Unwanted, automatically-dialled and pre-recorded VoIP telephone calls.

3.2.2 global RBL: A set of RBLs which are integrated from local RBLs and managed by VSP-RBL.

3.2.3 inbound domain: Domain to which a call is going.

3.2.4 local RBL: A set of real-time blocking lists (RBLs) managed by a VoIP spam prevention policy server (VSPPS) in each domain.

3.2.5 outbound domain: Domain from which a call is coming out.

3.2.6 RBL central system for VoIP spam prevention (VSP-RBL): An entity that creates and manages the global real-time blocking list (RBL).

3.2.7 real-time blocking list (RBL): A list of IP addresses or domain names that can be a basis to block immediately during VoIP call set-up.

3.2.8 user-reputation system (URS): An entity that calculates the VoIP spam score.

3.2.9 VoIP spam: Spam emerging over VoIP services.

3.2.10 VoIP spam prevention policy server (VSPPS): An entity that creates and manages the local RBL.

3.2.11 VoIP spam prevention system (VSPS): An entity that detects and blocks VoIP spam during the call process.

4 Abbreviations and acronyms

This supplement uses the following abbreviations and acronyms:

ACS	Auto Calling System
ACTR	Average Call Traffic Rate
CBR	Call Barring Rate
CDR	Call Duration Rate
CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
CRR	Call Recipient Rate
ICT	Inter Call Time
IM	Instant Messaging
IP	Internet Protocol
IPSec	IP Security Protocol
IVR	Interactive Voice Response
P2P	Peer to Peer
RBL	Real-time Blocking List
SIP	Session Initiation Protocol
SPIM	SPam over Instant Messaging
TCT	Total Call Time
TLS	Transport Layer Security
TTP	Trusted Third Party
URS	User-Reputation System
VoIP	Voice over Internet Protocol
VSP-RBL	RBL central system for VoIP Spam Prevention
VSPPS	Voice Spam Prevention Policy Server
VSPS	Voice Spam Prevention System

5 Conventions

None.

6 Overview of VoIP spam

6.1 General aspects

VoIP, like e-mail and other Internet applications, is susceptible to abuse by malicious parties that initiate unsolicited and unwanted communications. Increasingly, telemarketers, prank callers, and other telephone-system abusers, are likely to target VoIP systems.

VoIP spam is a kind of real-time voice spam emerging over VoIP services, such as telemarketing that includes communications with a telemarketer and interaction with the IVR system or ACS. The problem with VoIP spam is the difficulty in detecting unwanted calls; after all, it can be assumed that recipients are unaware that they are victims of a VoIP spam until they answer it. As VoIP becomes more and more popular around the world, the threat of VoIP spam is also rapidly increasing.

The following list describes the main characteristics of VoIP spam that have the potential to emerge as threats to VoIP service providers and users:

– ability to send VoIP spam in bulk and cheaply to unspecified recipients through the Internet, using equipment or software that generates calls and sends messages automatically;

– ability to circumvent the spam-filtering policies of service providers because VoIP spam can be sent directly to a recipient (P2P method);

– inability to analyse content of voice calls. Unlike the contents of e-mails, which can be analysed before delivery to the recipient, the contents of voice calls are obviously not available for analysis beforehand. This eliminates the most effective measure that is currently in use to counter e-mail spam;

– the potential to be more disruptive than e-mail spam because the larger size of voice files can seriously slow down networks;

– ability for spammers to leave a bogus voice-mail message from a bank, thereby gaining financial/private information or asking the telephone owner to call a false number.

6.2 Spam flow

There are two types of VoIP spam; one is call spam and the other is instant messaging (IM) spam. In this supplement, the VoIP protocols focus only on [b-ITU-T H.323] and SIP. Clauses 6.2.1 and 6.2.2 describe the definition and call flow of each type of spam.

6.2.1 Call spam

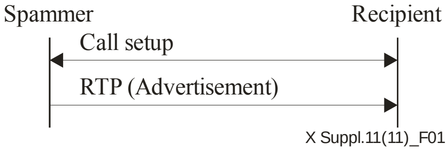

Figure 1 – Call spam flow

Call spam refers to any of the commercial messages sent via VoIP. Due to the wide array of tools already available to spammers on the Internet, it is a potential venue for large volumes of unsolicited calls. Figure 1 describes the call spam flow. After call establishment, the spammer will send call spam created by an automatic tool to unspecified recipients.

6.2.2 Instant messaging (IM) spam

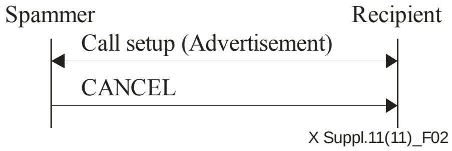

Figure 2 – IM spam flow

Instant messaging spam is defined as a bulk unsolicited set of instant messages containing the message that the spammer is seeking to convey. Figure 2 describes the IM spam flow. The spammer sends IM spam in a call setup message. In the case of e-mail spam, the advertisement is displayed when the e-mail is opened, and the recipient might immediately remove it by checking the title. Since the IM spam in VoIP automatically shows up on the screen in the VoIP terminal, the recipients will be forced to view the advertisement. In addition, the spammer sends IM spam at little or no cost by putting the telephone down even before a call is established.

7 Functional architecture for countering VoIP spam

7.1 Overall architecture

The functional architecture for countering VoIP spam consists of two kinds of domains: outbound domain and inbound domain. The outbound domain and the inbound domain contain senders and recipients, respectively. The functional architecture consists of four kinds of functional entities as shown in Figure 3: a VoIP spam prevention system, a VoIP spam prevention policy server, an RBL central system for VoIP spam prevention, and a user-reputation system. Both domains belong to the VoIP service provider, while VSP-RBL belongs to the trusted third party (TTP), for example CERT, CIRT, or a national authority.

The functional architecture is designed to use RBL. Two kinds of RBL are used for countering VoIP spam: local RBL and global RBL. The local RBL is created using a VoIP spam score defined in clause 7.5.1, or using a report on VoIP spam from recipients and managed by each VoIP service provider. However, the global RBL is created by integrating the local RBLs and is managed by the TTP.

During call set-up, each call is examined by the local RBL in the VSPPS of the outbound domain and is blocked when the IP address or domain name of the sender is already listed in the local RBL. Although not blocked by VSPS based on the local RBL, a call with a VoIP spam feature is immediately blocked when the VoIP spam score of the call calculated by URS exceeds the threshold. If the call is not blocked in the outbound domain, the VSPPS and URS of the inbound domain perform the same actions mentioned previously. Otherwise, the call is sent to one or more recipients. The procedures to counter IM spam are performed in the same manner.

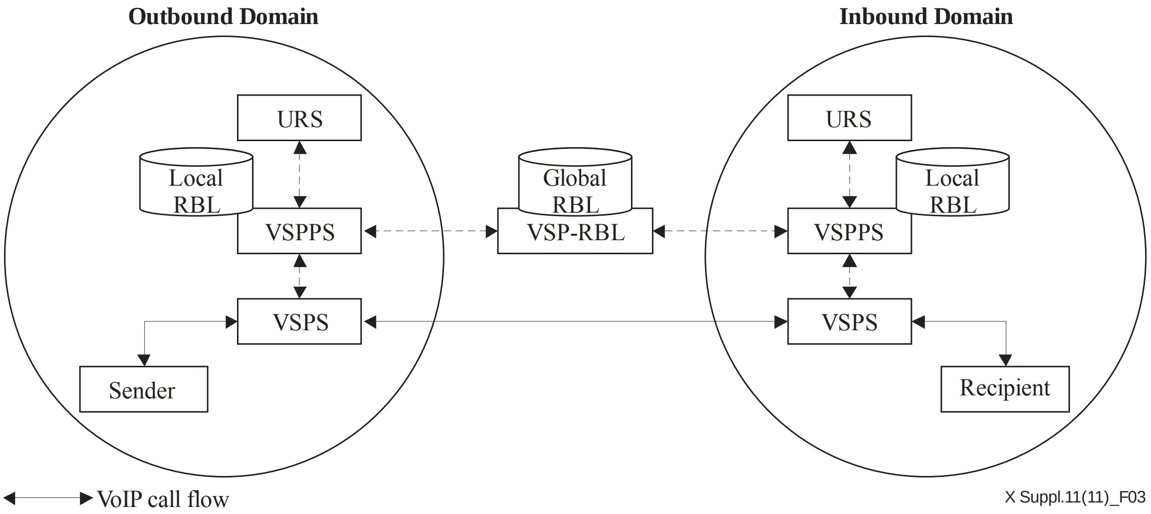

Figure 3 – Functional architecture for countering VoIP spam

7.2 VoIP spam prevention system (VSPS)

The VSPS is generally implemented as an independent server. It can also be implemented in the existing proxy server or call server. In this case, the administrator should carefully consider the performance of the proxy server or call server.

Before the sender/recipient communicates with VSPS, he/she is required to go through a mutual authentication procedure. Establishing a secure channel, such as TLS, IPSec, etc., between the sender/recipient and VSPS is also required.

The responsibilities of the VSPS of each domain are defined as follows:

The VSPS of the outbound domain basically has three responsibilities:

– To receive the local RBL from the VSPPS of the outbound domain.

– To detect and send information on suspicious senders to the VSPPS of the outbound domain.

– To block VoIP spam from suspicious senders according to the local RBL.

The VSPS of the inbound domain basically has four responsibilities:

– To receive the local RBL from the VSPPS of the inbound domain.

– To send information on VoIP spam from the recipient to the VSPPS of the inbound domain.

– To detect and send information on suspicious senders to the VSPPS of the inbound domain.

– To block VoIP spam from suspicious senders according to the local RBL.

7.3 VoIP spam prevention policy server (VSPPS)

VSPS and VSPPS are logically separated two functional entities, but they can also be implemented into one device.

The responsibilities of the VSPPS of each domain are defined as follows:

The VSPPS of the outbound domain basically has three responsibilities:

– To create and manage the local RBL.

– To provide the URS with information on suspicious senders from the VSPS and update the local RBL when the VoIP spam score of suspicious senders exceeds the threshold.

– To receive and update the local RBL according to the global RBL.

The VSPPS of the inbound domain basically has four responsibilities:

- To create and manage the local RBL.
- To receive information on VoIP spam calls from the recipient and update local the RBL by extracting the IP address from VoIP spam calls.
- To provide the URS with information on suspicious senders from VSPS and update the local RBL when the VoIP spam score of suspicious senders exceeds the threshold.
- To receive the global RBL, and update the local RBL reflecting it.

7.4 RBL central system for VoIP spam prevention (VSP-RBL)

VSP-RBL is implemented as an independent server and managed by TTP. In particular, if there is one VoIP service provider, VSP-RBL is not necessary.

VSP-RBL has four responsibilities:

- To create and manage the global RBL.
- To gather local RBLs from one or more VSPPSs.
- To combine local RBLs and update the global RBL.
- To distribute the global RBL to one or more VSPPS.

7.5 User-reputation system (URS)

URS and VSPPS are also logically separated two functional entities, but they can also be implemented into one device. A secure channel for exchanging information is required between URS and VSPPS when they are implemented into two devices.

The URS has two responsibilities:

- To receive information on suspicious senders and evaluate the VoIP spam score, based on six factors: call recipient rate (CRR), call duration rate (CDR), average call traffic rate (ACTR), call blocking rate (CBR), inter call time (ICT) and total call time (TCT).
- To notify VSPPS of the VoIP spam score of each suspicious sender.

7.5.1 VoIP spam score

The VoIP spam score is a quantitative value that reflects how malicious senders are. A sender with a higher score is most likely to be a spammer. To calculate the VoIP spam score, six factors described in clause 7.5 are used as quantitative values. They will be minimized or changed according to the anti-spam policy of service providers.

VoIP spam score = $\alpha \times \text{CRR} + \beta \times \text{CDR} + \gamma \times \text{ACTR} + \delta \times \text{CBR} + \varepsilon \times \text{ICT} + \zeta \times \text{TCT}$, where $\alpha + \beta + \gamma + \delta + \varepsilon + \zeta = 1$

The weight of each factor has a value ranging from 0 to 1; the sum of all weights is 1.

Table 1 presents the meaning of each factor; the equation shows how each factor is calculated.

Table 1 – Factors in calculating the VoIP spam score

Factor	Definition
CRR	The ratio of the number of recipients to the number of all attempted calls
CDR	The ratio of the number of suspicious calls to the number of all attempted calls, where a suspicious call is a call whose time duration is shorter than a certain value. For example, the call duration of a suspicious call would be below 30 seconds because spammers generally make a call within 30 seconds
ACTR	The ratio of the number of suspicious calls to the number of all attempted calls, where a suspicious call is a call whose required bandwidth is more than a certain value. For example, if a sender generates traffic over 10% of average call traffic, the call is considered a suspicious call
CBR	The ratio of the number of blocked calls to the number of all attempted calls
ICT	Average time interval between the call attempts of a sender per unit time
TCT	Average call time when a caller makes a certain number of calls. For example, the certain number should be bigger than 100

NOTE – Total number of telephone calls should not be too small in order to guarantee efficiency of the above factors.

7.6 Process for countering VoIP spam

The sender and recipient communicate through VSPS, which has the role of detecting and blocking the VoIP spam based on RBL. Therefore RBL should be kept up to date.

The process for countering VoIP spam starts whenever a sender tries to make a call. The process for countering VoIP spam is shown below.

– When a malicious sender sends a call setup message to the recipient, the VSPS of the outbound/inbound domain investigates a local RBL to check whether a malicious sender is listed or not.

– If the malicious sender is listed in the local RBL of each domain, a call is blocked immediately. If not, the call information is delivered to the URS for calculating the VoIP spam score.

– When a VoIP spam score exceeds the threshold of the service provider, the call is blocked and a local RBL is updated.

– Otherwise, the call is delivered to a recipient. When a recipient marks the call as VoIP spam, the recipient sends its information to the VSPPS of the inbound domain and a local RBL of the inbound domain is updated.

8 RBL update procedures for countering VoIP spam

8.1 Global RBL update procedures

Figure 4 shows the global RBL update procedures.

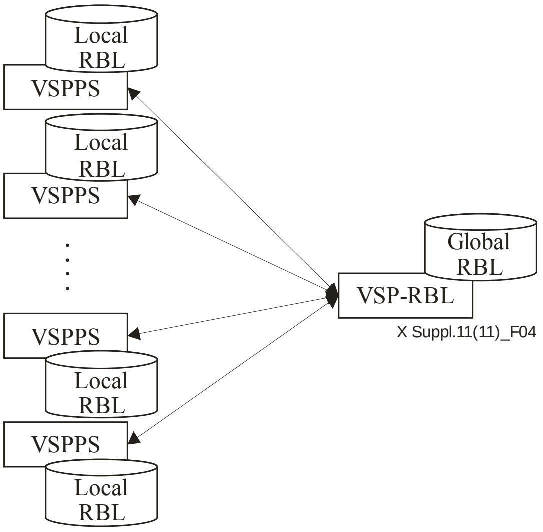

Figure 4 – RBL delivery procedure between VSPPSs and VSP-RBL

- At least one VSPPS transmits local RBLs to VSP-RBL.
- When the VSP-RBL receives local RBLs from one or more VSPPSs, it combines local RBLs and updates the global RBL.
- After updating the global RBL, the VSP-RBL sends the global RBL to one or more VSPPSs.

8.2 Local RBL update procedure

Figure 5 shows the local RBL update procedure. There are four ways to make the local RBL for countering VoIP spam.

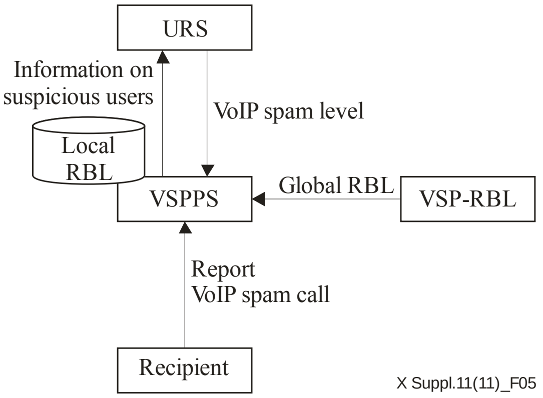

Figure 5 – Local RBL update procedure

1) From the recipient

– When the recipient receives a VoIP spam call, he/she transmits information on the VoIP spam call to the VSPPS of the inbound domain.

– VSPPS of the inbound domain extracts the IP address from a VoIP spam call and registers it in the local RBL.

2) From VSP-RBL

– The VSPPS receives the global RBL from VSP-RBL and updates the local RBL accordingly.

3) From URS

– If URS does not specify whether a call is VoIP spam or not, VSPPS sends information on the suspicious sender to URS.

– URS evaluates the VoIP spam score based on six factors, and notifies VSPPS of the VoIP spam score of each suspicious sender.

– VSPPS updates the local RBL when the VoIP spam score of suspicious senders exceeds the threshold.

Bibliography

[b-ITU-T H.323] Recommendation ITU-T H.323 (2006), *Packet-based multimedia communications systems.*

[b-ITU-T X.1240] Recommendation ITU-T X.1240 (2008), *Technologies involved in countering e-mail spam*.

[b-ITU-T X.1244] Recommendation ITU-T X.1244 (2008), *Overall aspects of countering spam in IP-based multimedia applications*.

[b-ITU-T X.1245] Recommendation ITU-T X.1245 (2010), *Framework for countering spam in IP-based multimedia applications*.

[b-IETF RFC 2327] IETF RFC 2327 (1998), *Session Description Protocol*.

[b-IETF RFC 3261] IETF RFC 3261 (2002), *Session Initiation Protocol*.

[b-IETF RFC 3550] IETF RFC 3550 (2003), *Real-time Transport Protocol*.

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, 2012