International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 14

(09/2012)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.1243 – Supplement on a practical reference model for countering e-mail spam using botnet information

ITU-T X-series Recommendations – Supplement 14

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 14 to ITU-T X-series Recommendations

ITU-T X.1243 – Supplement on a practical reference model for countering e-mail spam using botnet information

Summary

Botnets are a major source of e-mail spam. Botnet related devices, including master, command and control (C&C) servers and infected computers, are decentralized on the Internet, which greatly challenges any party to identify botnets and discover specific botnet-related information. Therefore, information sharing becomes a crucial factor to counter e-mail spam sent by a botnet. This Supplement provides a reference model which can be applied to the interactive gateway system for countering spam, in accordance with Recommendation ITU-T X.1243. In this reference model, spam-countering gateways can share botnet-related information with each other. This Supplement mainly focuses on countering e-mail spam sent by a botnet.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X Suppl. 14	2012-09-07	17

Keywords

Botnet, e-mail, 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 14 to ITU-T X-series Recommendations

ITU-T X.1243 – Supplement on a practical reference model for countering e-mail spam using botnet information

1 Scope

This Supplement to ITU-T X-series Recommendations provides a practical reference model for countering e-mail spam sent by a botnet, which can be applied to the interactive spam-countering gateway specified in [ITU-T X.1243]. This Supplement also specifies the working procedure, functional entities and system interfaces of this reference model. Furthermore, this Supplement describes the function for making signatures and filtering rules based on botnet information.

The objective of this Supplement is to design and implement an interactive gateway for countering e-mail spam. This Supplement mainly focuses on countering e-mail spam sent by a botnet.

2 References

[ITU-T X.1243] Recommendation ITU-T X.1243 (2010), *Interactive gateway system for countering spam.*

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following terms defined elsewhere:

3.1.1 bot [b-ITU-T X.1244]: Bot is a contraction of "robot", which is a program that operates as an agent for a user or another program to simulate a human activity.

3.1.2 email [b-ITU-T X.1241]: This term is mainly used to indicate the electronic mail transmitted over a telecommunication network.

3.1.3 email spam [b-ITU-T X.1241]: This term is used to describe unsolicited electronic communications over email, which is usually sent for specific purposes.

3.2 Terms defined in this Supplement

This Supplement defines the following terms:

3.2.1 botnet: A collection of Internet-connected computers whose security defences have been breached and are controlled by an unknown party. Each compromised device, known as a "bot", is created when a computer is penetrated by software from a malware distribution source. The controller of a botnet is able to direct the activities of these compromised computers through communication channels formed by standards-based network protocols.

3.2.2 botnet information: Botnet information refers to the topology-related information of a botnet, such as command and control (C&C) IP addresses, zombie IP lists, binary update server IP addresses, spam template server IP addresses, etc.

3.2.3 botnet master: An individual responsible for controlling and maintaining a botnet.

3.2.4 command and control server: Server used as a command and control point by a botnet operator.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

BDE	Botnet Detection Engine
BID	Botnet Information Database
C&C	Command and Control
DDoS	Distributed Denial of Service
ID	Identity
IP	Internet Protocol
LscDB	Local spam-countering Database
MMS	Multimedia Messaging Service
MX	Mail exchange
SCG	Spam-Countering Gateway
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SRM	Spam Receiver Monitor function
SSFRG	Spam Signature and Filtering Rule Generator
SSM	Spam Sender Monitor function
URL	Uniform Resource Locator

5 Conventions

None.

6 Background

A botnet is a collection of Internet-connected computers whose security defences have been breached and are controlled by an unknown party (see Figure 1). The botnet master can use the remotely controlled botnet to launch various kinds of attacks such as spam, distributed denial of service (DDoS), theft of personal information, etc. The most significant characteristics of a botnet are that the botnet master can control every attack property (such as type, method and time, etc.), and that command and control (C&C) servers and infected computers are distributed all over the world. These factors make it difficult to identify a botnet.

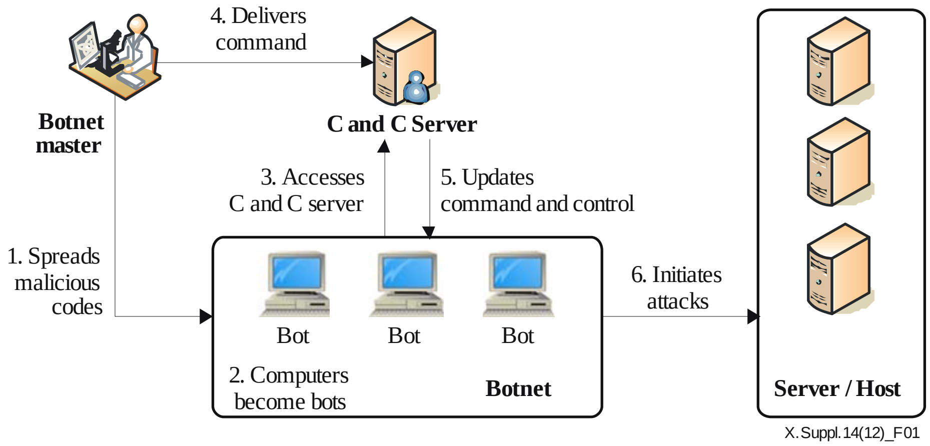


Figure 1 – Common working procedure of a botnet

Botnets have become the major source for e-mail spam, which generates massive unwanted e-mail traffic on networks and negatively influences e-mail receivers. First, a botnet master can send spamming attack commands to a C&C server. Second, after the C&C server receives the command, the C&C server will update the attack information in the infected computers to include target addresses, e-mail content and the sending rate. Finally, the infected computers will send e-mail spam according to the attack information. Generally, the botnet uses normal e-mail addresses as sender e-mail addresses. Meanwhile, the botnet generates e-mail content and subjects randomly. Therefore, it is difficult to detect e-mail spam from normal e-mails in network devices including e-mail servers. The e-mail spam is commonly filtered by e-mail receivers rather than e-mail servers, which causes serious waste of network resources and negatively influences e-mail receivers. Considering that most e-mail spam is sent by botnets, it will be more effective and efficient to use botnet information for identification of e-mail spam. In addition, spam-filtering rules stored in e-mail gateways can be also updated simultaneously based on botnet information.

It is very hard to identify botnet masters and C&C servers from botnets. It is also very difficult to recognize spam control and attack messages from Internet flows. Considering the above difficulties, it is more practical to identify infected computers and recognize e-mail spam in real time. Therefore, botnet information used for countering e-mail spam can generally be IP addresses of infected computers, behaviours of the botnet, etc.

7 Reference model for countering e-mail spam using botnet information

7.1 General architecture

Botnet information usually needs to be synchronized between different spam-countering gateways via a botnet detection system. The general architecture for countering e-mail spam sent by a botnet is shown in Figure 2, which is in accordance with the architecture of the spam-countering gateway (SCG) specified in [ITU-T X.1243].

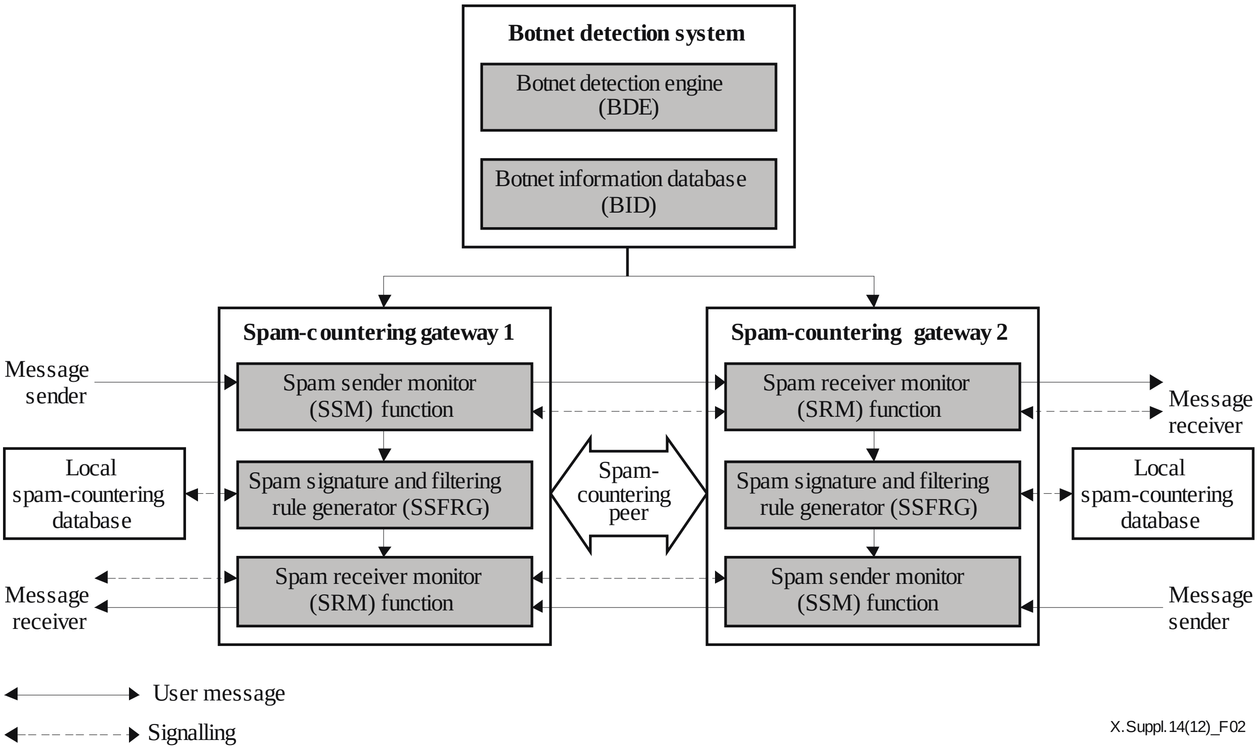

Botnet detection system
Botnet detection engine (BDE)
Botnet information database (BID)
Spam-countering gateway 1
Spam-countering gateway 2
Message sender
Spam sender monitor (SSM) function
Spam receiver monitor (SRM) function
Message receiver
Local spam-countering database
Spam signature and filtering rule generator (SSFRG)
Spam-countering peer
Spam signature and filtering rule generator (SSFRG)
Local spam-countering database
Message receiver
Spam receiver monitor (SRM) function
Spam sender monitor (SSM) function
Message sender
User message
Signalling
X.Suppl.14(12)_F02

Figure 2 – Reference model for countering e-mail spam sent by a botnet

In Figure 2, the detected botnet information is stored in the botnet information database (BID) after data pre-processing. The two functional entities, including the spam sender monitor (SSM) function and spam receiver monitor (SRM) function in the spam-countering gateway (SCG), can get botnet information from the BID. Then, the above two functional entities can monitor spamming activities from the botnet. If they find spamming activities, they will record the spam information, such as e-mail spam body, mail exchange (MX) queries, relay server and attached files. Afterwards, they will transmit it to the spam signature and filtering rule generator (SSFRG). The SSFRG will generate spam signature and filtering rules, which will be synchronized to the local spam-countering database (LscDB).

7.2 Functional entities in botnet detection systems

A botnet detection system is used to detect, collect and store botnet information, which consists of two functional entities: the botnet detection engine (BDE) and the botnet information database (BID).

– BDE: This functional entity is used to collect the botnet information which will be transmitted to the BID either directly or after pre-processing. Many countries or organizations operate such botnet detection systems to obtain botnet information by means of honeypot detection, security incident analysis, network traffic analysis, malware analysis, etc. Best practices are described in [b-ITU-T X-Sup.8]

– BID: This functional entity is used to store botnet information. Botnet information can include C&C servers' IP addresses/URLs, infected computers' IP addresses, attack behaviours and information of related servers. The botnet information can be used to detect e-mail spam sent by a botnet. This functional entity also provides botnet information to other systems requiring it.

7.3 Functional entities in spam-countering gateways

Countering e-mail spam is mainly realized through SCGs. The SCG has three functional entities: the SSM, the SRM and the SSFRG. Generally, each SCG has a sender gateway function and receiver gateway function. The SSM can check which e-mails are sent by a botnet based on the botnet information on the sender side. Similarly, the SRM can check which e-mail was sent by a botnet on the receiver side.

- SSM: This functional entity monitors e-mail sending activities, and identifies spam based on previously collected botnet information, such as spam relay server addresses, zombie IP addresses, malicious contents of the bodies of e-mails, blacklist URL links, e-mail sending rates, e-mail sentence structures, etc. If any e-mail is matched with the botnet information and is judged as e-mail spam, this entity will collect relevant information and transmit it to the SSFRG.
- SRM: This functional entity monitors e-mail receiving activities using botnet information, such as the spam relay server addresses, e-mail sender identities, zombie IP addresses, e-mail sentence structures and C&C names, etc. If any e-mail is matched with the botnet information and judged as e-mail spam, this entity will collect relevant information and transmit it to the SSFRG.
- SSFRG: This functional entity is used to process the spam information from the SSM and the RSM. Based on the processing results, this entity generates spam signatures and filtering rules. Then, the generated filtering rules will be sent to the LscDB, which will be used to further counter e-mail spam sent by botnets.

7.4 System interfaces

The system for countering e-mail spam sent by a botnet comprises a botnet detection system, an SCG and an LscDB. The system requires several interfaces for internal communication and information sharing, which are shown in Figure 3.

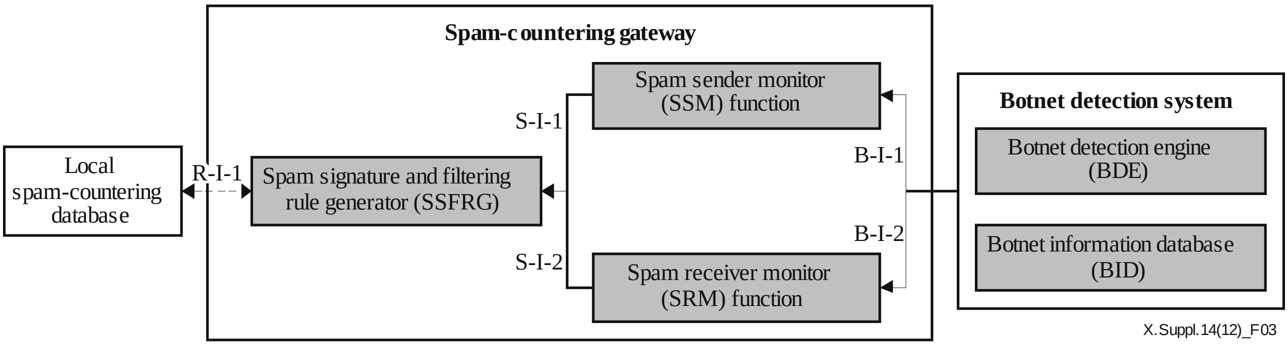

Spam-countering gateway
Spam sender monitor (SSM) function
S-I-1
B-I-1
Local spam-countering database
R-I-1
Spam signature and filtering rule generator (SSFRG)
B-I-2
S-I-2
Spam receiver monitor (SRM) function
Botnet detection system
Botnet detection engine (BDE)
Botnet information database (BID)
X.Suppl.14(12)_F03

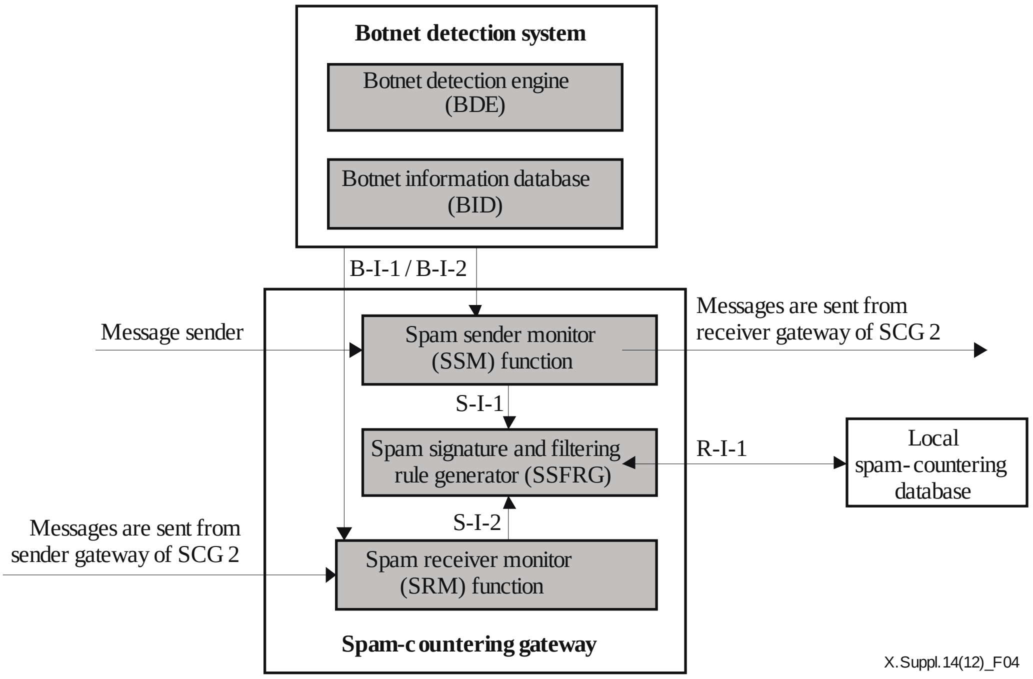
Figure 3 – Interfaces of the reference model

- B-I-1: B-I-1 is the interface between the BID and the SSM. The botnet information is used to identify the botnet and to recognize the spam sent by a botnet.
- B-I-2: B-I-2 is the interface between the BID and the SRM. The botnet information is used for the same purpose as the data through B-I-1.
- S-I-1: S-I-1 is the interface between the SSM and the SSFRG. Through the interface of S-I-1, detected spam traffic sent from the botnet is delivered to the SSFRG. Spam traffic can include MX queries, simple mail transfer protocol (SMTP) commands, etc.
- S-I-2: S-I-2 is the interface between the SRM and the SSFRG. The detected spam traffic sent from the botnet is delivered to the SSFRG, and is the same as through S-I-1.

- R-I-1: R-I-1 is the interface between the SSFRG and the LscDB. Through the interface R-I-1, the signatures and rules from SSFRG are transmitted to the LscDB to counter future e-mail spam by botnets.

8 Working procedure of the reference model

The procedures of the reference model for countering e-mail spam sent by a botnet are described in Figure 4.



Botnet detection system
Botnet detection engine (BDE)
Botnet information database (BID)
B-I-1 / B-I-2
Message sender
Spam sender monitor (SSM) function
Messages are sent from receiver gateway of SCG 2
S-I-1
Spam signature and filtering rule generator (SSFRG)
R-I-1
Local spam-countering database
S-I-2
Messages are sent from sender gateway of SCG 2
Spam receiver monitor (SRM) function
Spam-countering gateway
X.Suppl.14(12)_F04

Figure 4 – Working procedure of the reference model

- Step 1: Transmit botnet information (B-I-1/B-I-2).

  Botnet information stored in the botnet database is sent to the SSM/SRM through interface B-I-1/B-I-2.

- Step 2: Input e-mail.

  Every input e-mail will pass through the SSM/SRM.

- Step 3: Detected input e-mail spam is monitored by the SSM/SRM.

  Information in the input e-mail is compared against that in the botnet information database (BID). If it matches, then information concerning the e-mail spam is generated.

- Step 4: Spam information reporting (S-I-1/S-I-2).

  Information on spam detected by the SSM/SRM is sent to the SSFRG through interface S-I-1/S-I-2.

- Step 5: Generation of spam signature and filtering rule.

  Based on the information sent by the SSM/SRM, the SSFRG generates the spam signature and filtering rules.

- Step 6: Transmit spam-filtering rules (R-I-1).

  The generated signatures and filtering rules will be sent to the LscDB. These rules are stored in the LscDB and will be used to counter future spam sent by botnets.

Bibliography

[b-ITU-T X.1205]	Recommendation ITU-T X.1205 (2008), *Overview of cybersecurity*.
[b-ITU-T X.1241]	Recommendation ITU-T X.1241 (2008), *Technical framework for 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-Sup.8]	ITU-T X-series Recommendations – Supplement 8 (2010), *ITU-T X.1205 – Supplement on best practices against botnet threats*.

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, 2013