International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

F.743.2

(07/2016)

SERIES F: NON-TELEPHONE TELECOMMUNICATION SERVICES

Multimedia services

Requirements for cloud storage in visual surveillance

Recommendation ITU-T F.743.2

ITU-T F-SERIES RECOMMENDATIONS

NON-TELEPHONE TELECOMMUNICATION SERVICES

TELEGRAPH SERVICE	
Operating methods for the international public telegram service	F.1–F.19
The gentex network	F.20–F.29
Message switching	F.30–F.39
The international telemessage service	F.40–F.58
The international telex service	F.59–F.89
Statistics and publications on international telegraph services	F.90–F.99
Scheduled and leased communication services	F.100–F.104
Phototelegraph service	F.105–F.109
MOBILE SERVICE	
Mobile services and multidestination satellite services	F.110–F.159
TELEMATIC SERVICES	
Public facsimile service	F.160–F.199
Teletex service	F.200–F.299
Videotex service	F.300–F.349
General provisions for telematic services	F.350–F.399
MESSAGE HANDLING SERVICES	F.400–F.499
DIRECTORY SERVICES	F.500–F.549
DOCUMENT COMMUNICATION	
Document communication	F.550–F.579
Programming communication interfaces	F.580–F.599
DATA TRANSMISSION SERVICES	F.600–F.699
MULTIMEDIA SERVICES	**F.700–F.799**
ISDN SERVICES	F.800–F.849
UNIVERSAL PERSONAL TELECOMMUNICATION	F.850–F.899
HUMAN FACTORS	F.900–F.999

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

Recommendation ITU-T F.743.2

Requirements for cloud storage in visual surveillance

Summary

Recommendation ITU-T F.743.2 defines the cloud storage service requirements in visual surveillance. Cloud storage enables service users to have ubiquitous, convenient, on-demand network access to a shared pool of configurable storage resources, which can be rapidly provisioned and released with minimal management effort or service-provider interaction. Cloud storage can realize flexible and reliable data storage for large-scale visual surveillance, and its components are modularized and allocated dynamically based on real usage. This Recommendation provides the application scenarios and requirements for cloud storage in visual surveillance.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T F.743.2	2016-07-14	16	11.1002/1000/12895

Keywords

Cloud storage, picture storage, video file uploading, video metadata management, video stream storage, visual surveillance.

[*] 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

Page

Recommendation ITU-T F.743.2

Requirements for cloud storage in visual surveillance

1 Scope

This Recommendation describes the brief functional model, application scenarios and requirements for cloud storage in visual surveillance (VS) systems, based on the requirements and architectures defined by [ITU-T F.743], [ITU-T H.626] and [ITU-T H.626.1].

A visual surveillance service is a telecommunication service focusing on video (and audio) application technology, which is used to remotely capture multimedia (e.g., audio, video, image, various alarm signals), and present this to end users in a friendly manner (including accessibility aspects), based on a broadband network with ensured quality, security and reliability. Cloud storage is a data storage model for enabling service users to have ubiquitous, convenient and on-demand network access to a shared pool of configurable storage resources, which can be rapidly provisioned and released with minimal management effort or service-provider interaction. In cloud storage systems, the physical and virtual resources can be dynamically assigned and reassigned according to user demand. Cloud storage can realize scalable, flexible and reliable data storage for large-scale visual surveillance.

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 F.743] Recommendation ITU-T F.743 (2009), *Requirements and service description for visual surveillance*.

[ITU-T H.626] Recommendation ITU-T H.626 (2011), *Architectural requirements for visual surveillance*.

[ITU-T H.626.1] Recommendation ITU-T H.626.1 (2013), *Architecture for mobile visual surveillance*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 application [b-ITU-T Y.101]: A structured set of capabilities, which provide value-added functionality supported by one or more services.

3.1.2 customer [b-ITU-T M.60]: An entity which receives services offered by a service provider based on a contractual relationship. It may include the role of a network user.

3.1.3 customer unit [ITU-T F.743]: A device located at the customer part of a visual surveillance system and used to present multimedia information (such as audio, video, image, alarm signal, etc.) to the end user.

3.1.4 premises unit [ITU-T F.743]: A device located at the remote part of a visual surveillance system and used to capture multimedia information (such as audio, video, image, alarm signal, etc.) from a surveilled object.

3.1.5 service [b-ITU-T Y.101]: A structure set of capabilities intended to support applications.

3.1.6 visual surveillance [ITU-T F.743]: A telecommunication service focusing on video (but including audio) application technology, which is used to remotely capture multimedia (such as audio, video, image, alarm signals, etc.) and present them to the end user in a friendly manner, based on a managed broadband network with quality, security and reliability ensured.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 cloud storage: A data storage model for enabling service users to have ubiquitous, convenient and on-demand network access to a shared pool of configurable storage resources, which can be rapidly provisioned and released with minimal management effort or service-provider interaction. In cloud storage systems, the physical and virtual resources can be dynamically assigned and reassigned according to user demand.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AS	Application System
CU	Customer Unit
DVR	Digital Video Recorder
IPU	Intelligent Premises Unit
MCU	Mobile Customer Unit
MSU	Media Storage Unit
NVR	Network Video Recorder
PU	Premises Unit
VS	Visual Surveillance
VSCS	Visual Surveillance Cloud Storage

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.

6 Overview

Currently, large-scale visual surveillance system deployment has contributed to the explosive growth of surveillance video data. Moreover, the massive amount of surveillance video data contains a lot of valuable information which can be mined to provide more intelligent services. Attention is needed to the efficient storage of video data and fast access to information of interest to users.

When the surveillance industry changes to all IP network usage, the network video recorder (NVR), as a main component for surveillance video storage, will gradually replace the existing digital video recorder (DVR). However, an NVR which is installed on single physical server may reach the maximum storage or throughput limitation due to predefined resource limitations. In addition, the current NVR-based storage model does not efficiently support the analysis and mining of the massive amount of video data.

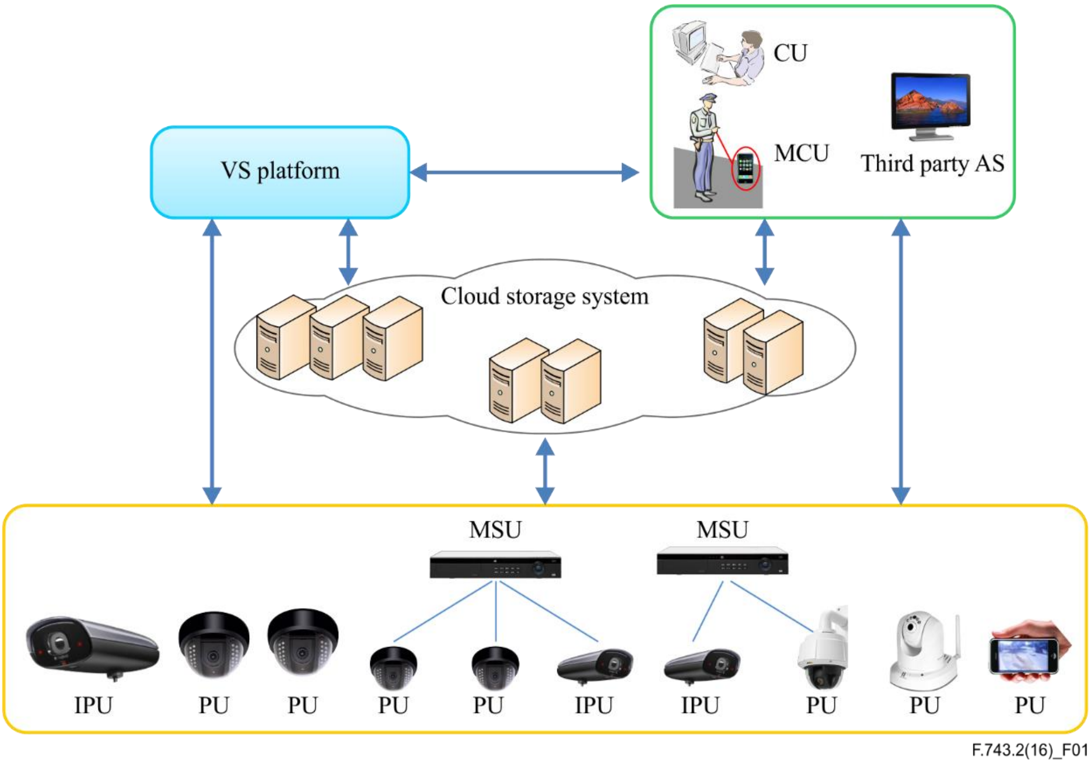

Figure 1 – Cloud storage model for visual surveillance

Cloud storage is a new model for enabling service users to have ubiquitous, convenient and on-demand network access to a shared pool of configurable storage resources, which can be rapidly provisioned and released with minimal management effort or service-provider interaction. From a telecommunication perspective, users do not buy resources but rather purchase cloud services provided by cloud environments. This can improve the system flexibility and reduce the expenditure of users' systems.

Cloud storage is used for aggregating and managing a particular data set. Figure 1 shows a cloud storage model for a visual surveillance system. A cloud storage system is a scalable, flexible and reliable video recording system that can optimize the storage resources for massive video sources. In a cloud storage system, each component is modularized and allocated dynamically based on actual usage, and data protection mechanisms are supported to improve system reliability. A cloud storage system enables convenient and fast access to a wealth of data across distributed and heterogeneous data sources in the cloud. Furthermore, this data storage system can be easily integrated with cloud computing frameworks which support efficient intelligent video analysis tasks. For the premises unit (PU) devices, video data can be uploaded to a cloud storage system by online/offline modes using streaming or other network data transfer protocols. The data sources can be IP cameras, mobile devices or other media storage units (MSUs), such as DVRs with networking capability, NVRs, and vehicle DVRs installed on cars. The visual surveillance (VS) platform can call the cloud storage service through standard interfaces provided by the cloud storage system. All types of authorized customer units (CUs) or authorized third-party application systems (ASs) can access the data stored in the cloud storage system.

7 Scenarios

This clause describes typical service scenario examples illustrating the cloud storage in visual surveillance and deriving its service requirements.

7.1 Video stream storage

Surveillance cameras capture video data continuously. User Bob has subscribed to the visual surveillance cloud storage (VSCS) service from the VS service provider, and wants to store streaming video data in the cloud directly.

Step 1: Bob logs into the VS system via his PC. He clicks a cloud storage menu function and goes to a video stream storage plan form. A camera list appears on the screen, which displays detailed information for each camera that Bob can access. Bob chooses the cameras whose captured video data needs to be stored in the cloud, and then sets the time interval during which the data should be recorded. The VS management system receives Bob's submitted video stream cloud storage plan, and forwards the plan to the cloud storage system.

Step 2: According to the video stream storage plan, the cloud storage system gets the video stream directly from the monitoring cameras, and then writes the video data to the cloud storage resource pool built on the storage device clusters.

Step 3: Bob can browse the camera's video data recorded in the cloud; he can also choose the camera name and the video starting time, and replay the video of interest stored in the cloud.

7.2 Video file uploading

Case 1: Video file uploading from NVR

An NVR is usually used as the local storage devices for continuously recording surveillance video from network cameras. NVR has a maximum storage capacity or throughput limitation due to predefined resource limitations. For example, an NVR can receive video streams from 16 cameras simultaneously, and can record the video data from those cameras for one month. In addition, the data reliability is difficult to guarantee when the NVR fails.

The public security department of a city has deployed a VS system in the city. Tom is the system administrator and is responsible for operating the visual surveillance system to carry out public security tasks. Currently, the surveillance video is recorded on the local NVRs. However, Tom's supervisor lets him retain the video data from some cameras for at least six months.

Step 1: Tom logs into the VS system. He chooses the surveillance cameras, sets the time interval to 12 months and sets the video file uploading period to 12 hours. Tom submits the video file uploading plan to the visual surveillance management system. This plan is then forwarded to the cloud storage system.

Step 2: According to the video file uploading plan, the cloud storage system retrieves the video files from the corresponding NVRs every 12 hours, and then writes this video data to the cloud storage resource pool built on the storage device clusters. The storage space assigned to this plan is large enough to store the video data for 12 months.

Step 3: Tom can download the video files from the cloud; he can also replay the videos stored in the cloud on demand.

Case 2: Video file uploading from mobile devices

Mobile visual surveillance devices are widely used today. The storage capacity of a mobile device is limited, and the user wants to access the video captured by a mobile device using any terminals, e.g., PC, anywhere. The user can then upload the captured video files from the mobile device to the cloud.

Step 1: Bob logs into the VS system through a mobile device. He often uses the camera of the mobile device to capture videos; these video files are stored in the mobile device.

Step 2: Since the storage space of the mobile device is limited, Bob applies for video cloud storage space in order to save more surveillance video data. He chooses the video files from his mobile device, and then uploads the files to the cloud through wireless channels.

Step 3: Bob logs into the visual surveillance system using a PC, and can download the video files (which were uploaded from his mobile device) from the cloud. He can also replay the videos, stored in the cloud, on demand.

7.3 Video metadata management

The VS system can provide various intelligent services by using video/image analysis technologies. The intelligent traffic service is an example. For realizing these intelligent services, some video/image analysis algorithms are embedded in the traffic surveillance cameras, and these cameras can directly output video content metadata, such as: vehicle plate number, vehicle type, speed of vehicle, colour of vehicle. In addition, video analysis servers can be deployed in the data centre, and the surveillance video stream or the recorded video files can be processed to obtain the video content metadata on these servers.

Step 1: Model the surveillance video metadata, and design and implement the video metadata management system in cloud.

Step 2: The surveillance video metadata is obtained from the intelligent video/image analysis devices, and is sent to the cloud.

Step 3: An authorized user can browse and retrieve the surveillance video metadata stored in the cloud. Likewise, authorized application systems can access the video metadata in the cloud, and provide the various intelligent services based on the video metadata.

7.4 Picture storage

Case 1: Picture upload from surveillance camera

High-definition cameras are widely deployed on streets to capture high-resolution pictures. These pictures may contain useful information and can be processed further. For example, vehicle plate numbers can be extracted accurately from a picture by using a vehicle plate recognition algorithm.

Step 1: Network cameras continuously capture pictures, and send these pictures directly to the cloud.

Step 2: The cloud storage system receives the pictures, and writes the pictures to the cloud storage resource pool built on the storage device clusters.

Step 3: An authorized user or application system can access the pictures stored in the cloud.

Case 2: Picture uploading from mobile device

John is a traffic police officer, and one of his routine tasks is to find illegally parked vehicles and record the infraction.

Step 1: John logs into the surveillance system through a mobile device. He captures the picture of an illegally parked vehicle using the camera of the mobile device.

Step 2: The captured picture is then sent to the cloud through wireless channels.

Step 3: An authorized user or application system can access the pictures stored in the cloud.

8 Requirements for cloud storage in visual surveillance

8.1 User requirements

There are two types of cloud storage service users : the service consumer and the service provider.

8.1.1 Cloud storage service consumer requirements

- USR-001: A VSCS system is required to support registration and de-registration of the end user through the interface provided by the system, and the end user can view and modify personal information.
- USR-002: A VSCS system is required to support end-user login and logout from the system conveniently. The user name and password are required when an end user logs into the system.
- USR-003: A VSCS system is recommended to support end-user view of the user access logs or other system logs.
- USR-004: A VSCS system is required to support user's data uploading from a client device, including video files, pictures and video metadata.
- USR-005: A VSCS system is required to support the user's view and downloading of stored data via a client device, including video files, pictures and video metadata.
- USR-006: A VSCS system is recommended to support the video on demand and picture presentation for end users.
- USR-007: A VSCS system is recommended to support information retrieval for end users.
- USR-008: A VSCS system is recommended to support flexible storage space application for end users.
- USR-009: A VSCS system is required to support the view of a user’s storage space status, including the storage space occupancy rate, the remaining storage space.

8.1.2 Cloud storage service provider requirements

- USR-010: A VSCS system is required to support the provider's login and logout from the system conveniently. The provider’s name and password are required when logging into the system.
- USR-011: A VSCS system is required to support the provider's view of the cloud storage system operating status from the beginning to then-present time, including the system storage space occupancy rate, the system’s remaining storage space, the storage space occupancy rate of individual users, the remaining storage space of individual users, etc.
- USR-012: A VSCS system is required to support flexible storage space assignment for individual users.

8.2 Service requirements

8.2.1 Video storage service requirements

- SER-001: A VSCS system is required to support directly writing video streams, from multiple PUs, through the network.
- SER-002: A VSCS system is required to support video file uploading from multiple local video storage devices through the network, including NVRs, mobile video capturing devices, etc.
- SER-003: A VSCS system is required to support video file deletion.
- SER-004: A VSCS system is required to support video file browsing and searching; the searching conditions can be the source of video files, the capture time of video files, etc.

- SER-005: A VSCS system is required to support video file downloading through the network.
- SER-006: A VSCS system is required to support automatic video file overwriting when a user's storage space is full; the overwriting principle is that the oldest data is replaced first.
- SER-007: A VSCS system is recommended to support video playback for end users according to the source of the video file and the capture time of the video file. Video playback operations include fast forward, slow forward, pause, and stop.

8.2.2 Picture storage service requirements

- SER-008: A VSCS system is required to support direct writing of pictures, from multiple PUs, through the network.
- SER-009: A VSCS system is required to support picture uploading from multiple local video storage devices through the network, including PCs, mobile picture capturing devices, etc.
- SER-010: A VSCS system is required to support picture deletion.
- SER-011: A VSCS system is required to support picture browsing and searching; the searching conditions can be the source of the pictures, the capture time of the pictures, etc.
- SER-012: A VSCS system is required to support picture downloading through the network.

8.2.3 Video metadata storage service requirements

- SER-013: A VSCS system is required to support video metadata writing through the network.
- SER-014: A VSCS system is required to support video metadata deletion.
- SER-015: A VSCS system is required to support video metadata browsing and searching; the searching condition can be the source of video metadata, the creation time of video metadata, video metadata content, etc.

8.3 Security requirements

8.3.1 Authentication security requirements

- SEC-001: A VSCS system is required to provide the mechanisms for authentication and authorization, and it is required to only permit authorized users to access the system and use system services. A VSCS system is required to forbid an unauthorized user to handle any resources of the system.

8.3.2 Access security requirements

- SEC-002: A VSCS system is required to operate in environments where network address translation (NAT) and/or firewall devices are present. It is recommended to utilize specified firewalls, gatekeepers and other network devices to ensure security for access to some special cloud storage services.

8.3.3 Content security requirements

- SEC-003: A VSCS system is required to ensure the security of stored data such as video, picture, video metadata, etc. It is recommended to provide the mechanisms to protect the copyrights of the stored data, and to protect the stored data from being corrupted.
- SEC-004: A VSCS system is required to provide data protection mechanisms such as data backup, coding, etc. It is required to be able to recover the destroyed data.
- SEC-005: A VSCS system is required to protect user privacy.

8.3.4 System security requirements

- SEC-006: A VSCS system is required to have the capability of resisting various attacks.

- SEC-007: A VSCS system is required to provide the mechanisms for troubleshooting. It is required that a structural single-node problem be avoided (i.e., a problem at a single node should not cause failure of the entire system).

8.4 Management requirements

8.4.1 Storage management requirements

- MAN-001: A VSCS system is required to support storage space management. The storage space can be increased and decreased flexibly.

8.4.2 Equipment management requirements

- MAN-002: A VSCS system is required to provide the unified management of the storage equipment.

8.4.3 Service management requirements

- MAN-003: A VSCS system is required to provide the various storage service subscription means for users, and to provide the capabilities of querying, viewing and modifying their subscription information.
- MAN-004: A VSCS system is recommended to provide the capability of accounting, charging and billing for the service operation.
- MAN-005: A VSCS system is recommended to provide various alternative accounting modes, and to support flexible combinations of payment modes, billing modes, billing cycles, preferential pricing, etc.

8.4.4 Data management requirements

- MAN-006: A VSCS system is required to support data management in the cloud, including adding, deleting, browsing, indexing, searching.

8.4.5 System management requirements

- MAN-007: A VSCS system is required to provide a unified system management interface which can be called conveniently.
- MAN-008: A VSCS system is required to provide a visual interface for users.

8.4.6 Operation management requirements

- MAN-009: A VSCS system is required to monitor, record and display the running status of the system.

8.5 Scalability requirements

- SCA-001: A VSCS system is required to provide storage resource scalability. When the storage equipment is increased or decreased in the system, the storage capacity is increased or decreased accordingly, and the system service is uninterrupted.
- SCA-002: A VSCS system is required to provide storage space scalability for users. The storage space of individual users can be increased or decreased according to each user's demands.
- SCA-003: A VSCS system is required to provide user scalability. The number of supported users can be increased or decreased dynamically.

8.6 Reliability requirements

– REL-001: A VSCS system is required to ensure service reliability. When storage equipment fails or the storage system network operation is abnormal, the system service can be used normally.

– REL-002: A VSCS system is required to ensure data reliability. When data is destroyed, the system can recover it based on the data protection mechanism, e.g., data backup, data coding.

8.7 Performance requirements

– PER-001: A VSCS system is required to support concurrent user operations. The system can serve a large number of users simultaneously, while ensuring the service quality.

Bibliography

[b-ITU-T M.60] Recommendation ITU-T M.60 (1993), *Maintenance terminology and definitions*.

[b-ITU-T Y.101] Recommendation ITU-T Y.101 (2000), *Global Information Infrastructure terminology: Terms and definitions*.

[ITU-T FG TR] ITU-T FG Technical Report: Part 1 (2012), *Introduction to the cloud ecosystem: definitions, taxonomies, use cases and high-level requirements*.

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	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	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, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2016