

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.627.2

(03/2022)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Broadband, triple-play and advanced multimedia
services – Advanced multimedia services and applications

Requirements and protocols for home surveillance systems

Recommendation ITU-T H.627.2

ITU-T H-SERIES RECOMMENDATIONS
AUDIOVISUAL AND MULTIMEDIA SYSTEMS

CHARACTERISTICS OF VISUAL TELEPHONE SYSTEMS	H.100–H.199
INFRASTRUCTURE OF AUDIOVISUAL SERVICES	
General	H.200–H.219
Transmission multiplexing and synchronization	H.220–H.229
Systems aspects	H.230–H.239
Communication procedures	H.240–H.259
Coding of moving video	H.260–H.279
Related systems aspects	H.280–H.299
Systems and terminal equipment for audiovisual services	H.300–H.349
Directory services architecture for audiovisual and multimedia services	H.350–H.359
Quality of service architecture for audiovisual and multimedia services	H.360–H.369
Telepresence, immersive environments, virtual and extended reality	H.420–H.439
Supplementary services for multimedia	H.450–H.499
MOBILITY AND COLLABORATION PROCEDURES	
Overview of Mobility and Collaboration, definitions, protocols and procedures	H.500–H.509
Mobility for H-Series multimedia systems and services	H.510–H.519
Mobile multimedia collaboration applications and services	H.520–H.529
Security for mobile multimedia systems and services	H.530–H.539
Security for mobile multimedia collaboration applications and services	H.540–H.549
VEHICULAR GATEWAYS AND INTELLIGENT TRANSPORTATION SYSTEMS (ITS)	
Architecture for vehicular gateways	H.550–H.559
Vehicular gateway interfaces	H.560–H.569
BROADBAND, TRIPLE-PLAY AND ADVANCED MULTIMEDIA SERVICES	
Broadband multimedia services over VDSL	H.610–H.619
Advanced multimedia services and applications	H.620–H.629
Content delivery and ubiquitous sensor network applications	H.640–H.649
IPTV MULTIMEDIA SERVICES AND APPLICATIONS FOR IPTV	
General aspects	H.700–H.719
IPTV terminal devices	H.720–H.729
IPTV middleware	H.730–H.739
IPTV application event handling	H.740–H.749
IPTV metadata	H.750–H.759
IPTV multimedia application frameworks	H.760–H.769
IPTV service discovery up to consumption	H.770–H.779
Digital Signage	H.780–H.789
E-HEALTH MULTIMEDIA SYSTEMS, SERVICES AND APPLICATIONS	
Personal health systems	H.810–H.819
Interoperability compliance testing of personal health systems (HRN, PAN, LAN, TAN and WAN)	H.820–H.859
Multimedia e-health data exchange services	H.860–H.869
Safe listening	H.870–H.879

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

Recommendation ITU-T H.627.2

Requirements and protocols for home surveillance systems

Summary

Recommendation ITU-T H.627.2 defines the requirements and protocols for Internet protocol (IP) based network access of varied types of equipment under home security surveillance scenarios including the architecture, protocol for transmission, access and service functions as well as other relevant requirements under the home surveillance considerations.

This Recommendation specifies a way to eliminate the difference in network communication and access management of heterogeneous devices, simplify the construction complexity of home security platforms, improve the security and reliability of data transmission between home security equipment and the home surveillance platform, and finally guarantee high-qualified development of home surveillance service.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T H.627.2	2022-03-16	16	11.1002/1000/14971

Keywords

Home surveillance, interface, protocols, requirements.

* 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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2022

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope	1
2	References.....	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation.....	1
4	Abbreviations and acronyms	2
5	Conventions	3
6	Message syntax and semantics	3
7	Requirements for home surveillance systems (HSS).....	3
8	Reference architecture for HSS	3
	8.1 Architectural framework	4
	8.2 Functional entities	4
	8.3 Protocols and interfaces.....	5
9	Protocols for home surveillance system (HSS)	7
	9.1 Requirements of the network transmission function	7
	9.2 Requirements of access function	7
	9.3 Requirements of service function	7
	Appendix I – Interface message examples.....	16
	I.1 Messages of the scheduling service interface.....	16
	I.2 Messages of device management interface	16
	I.3 Messages of video service interface	31

Recommendation ITU-T H.627.2

Requirements and protocols for home surveillance systems

1 Scope

This Recommendation specifies the requirements and protocols for home surveillance systems (HSS) and covers the following aspects:

- Requirements for home surveillance systems;
- Reference architecture for home surveillance systems;
- Protocol interface framework for home surveillance systems;
- Relevant protocols of home surveillance systems.

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 H.626] Recommendation ITU-T H.626 (V2) (2019), *Architectural requirements for video surveillance system*.
- [ITU-T H.626.4] Recommendation ITU-T H.626.4 (2018), *Architecture for a point-to-point visual surveillance system*.
- [IETF RFC 2818] IETF RFC 2818 (2000), *HTTP Over TLS*.
- [IETF RFC 7230] IETF RFC 7230 (2014), *Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 central management unit: A functional unit located in the main part of a home surveillance system. It is used for centralized system management, service operation management, etc. The main functions include management, authorization, accounting, charging, location and presence.

3.2.2 cloud storage: A functional unit located at the central part of a home surveillance system. It is used to retrieve and store media and as well as provide a streaming media service. The main functions include media storage, media serving, media indexing, and media downloading, etc.

3.2.3 customer unit: A functional unit located at the customer part of a home surveillance system. It is used to present multimedia information (such as audio, video, image, alarm signal, etc.) to the end user.

3.2.4 home surveillance system: A telecommunication service focusing on video (including audio and image) application technology, which is used to remotely capture multimedia information (such as audio, video, image, alarm signal, etc.) and present them to the end users in a user-friendly manner. Above service is expected to be realized via a managed broadband network with ensured quality, security and reliability for home surveillance applications.

3.2.5 media distribution unit: A functional unit located in the main part of a home surveillance system. It is used to transport media from the premises unit (PU) to the customer unit (CU). The main functions include media reception, media processing, media routing, media transmission, media forwarding, media replication, etc.

3.2.6 premises unit: A functional unit located at the remote part of a home surveillance system and is used to capture multimedia information (such as audio, video, image, alarm signal, etc.) from a surveilled object.

3.2.7 service platform: A series of functional units and subsystems located at the central part of a home surveillance system. It is used to integrate all capabilities and provides home surveillance services to customers. The main functions include service-control function, media switching, distribution, storage, and control and management.

3.2.8 service control unit: A functional unit located in the main part of a home surveillance system. It is used for access service control and signal call control between the premises unit (PU) and the customer unit (CU). The main functions include access registration, access identification, authentication, authorization, call control, location, presence, and target media serving function selection.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CCS	Central Control Server
CMU	Centre Management Unit
CS	Cloud Storage
CU	Customer Unit
HSS	Home Surveillance System
MDU	Media Distribution Unit
MS	Media Server
PTZ	Pan/Tilt/Zoom
PU	Premises Unit
REST	Representation State Transfer
RPC	Remote Procedure Call
SCU	Service Control Unit
SRT	Secure Reliable Transport
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol

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 document is to be claimed.
- The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement needs not be present to claim conformance.
- The keywords "can optionally" and "may" indicate an optional requirement which is permissible, without implying any sense of being recommended. These terms are 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 Message syntax and semantics

This Recommendation outlines the urgent requirements for home surveillance systems. When regarding the overall architectural framework of home surveillance systems, it references the architecture based on [ITU-T H.626] and [ITU-T H.626.4] with a few extensions. This Recommendation gives a more detailed description of protocol interfaces based on the reference architecture as well as the relevant protocols for such systems, including device management, media stream transmission, recording cloud storage (CS) and their related functions.

7 Requirements for home surveillance systems (HSS)

This Recommendation is targeted at providing a series of comprehensive requirements and protocols for a home surveillance system that is implemented in public IP based networks. The home surveillance system (HSS) is required to provide some advanced services such as remote real-time surveillance, video remote storage, and video playback. In addition, it is recommended to provide other value-added services when new AI technologies are used to realize object detection or identification. All devices accessing the HSS are recommended to follow the protocols and interface specifications defined in the following sections.

8 Reference architecture for HSS

In this clause, a reference architecture for HSS will be presented in detail.

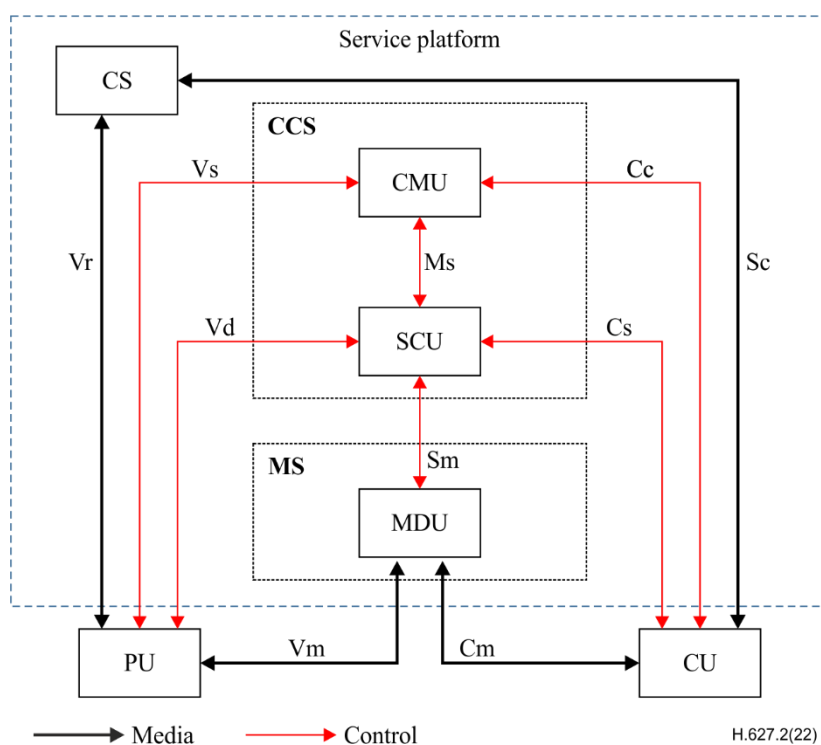


Figure 8-1 – Reference architecture of home surveillance system

8.1 Architectural framework

The architectural framework of home surveillance systems contains three major parts, including a premises unit (PU), customer unit (CU) and a service platform.

PU is a functional unit to capture multimedia information from a surveilled object. CU is a functional unit to present multimedia information towards the end user. There are four additional functional units in the service platform, namely, core storage (CS), service control unit (SCU), media distribution unit (MDU), and centre management unit (CMU). CS is used to retrieve and store media and as well as provides a streaming media service. SCU is used for access service control and signal call control between the PU and the CU. MDU is used to transport media from the PU to the CU. CMU is used for service and operational management functionality.

In order to provide the following functions via the service platform, all PUs are required to access the service platform with authentication and authorization according to the requirements and protocols for home surveillance systems in clause 9.

8.2 Functional entities

There are three main functional entities in the service platform, they are signalling control service, media broadcasting service and video service.

- a) Signalling control service is responsible for control signalling between PUs and the service platform. PUs are required to access the service platform through interface Vs and interface Vd shown in Figure 8-1.
- b) Media broadcasting service is responsible for push flow, transcoding, distribution and other functions of PUs. PUs are required to access the service platform through the interface Vm.
- c) Video service is responsible for record slice uploading, storage, playback and other functions of PUs. PUs are required to access service platform through the interface Vr.
- d) Scheduling service is responsible for sending instructions to PUs to connect to the designated signalling server and the peer-to-peer server.

8.3 Protocols and interfaces

8.3.1 Interface stack

This specification mainly defines the protocols of interfaces (Vs/Vd/Vm/Vr) between PUs and the service platform, including signalling and data transmission protocols. The entire protocol stack is presented in Figure 8-2 which consists of three functions, they are the transmission function, access function and service function.

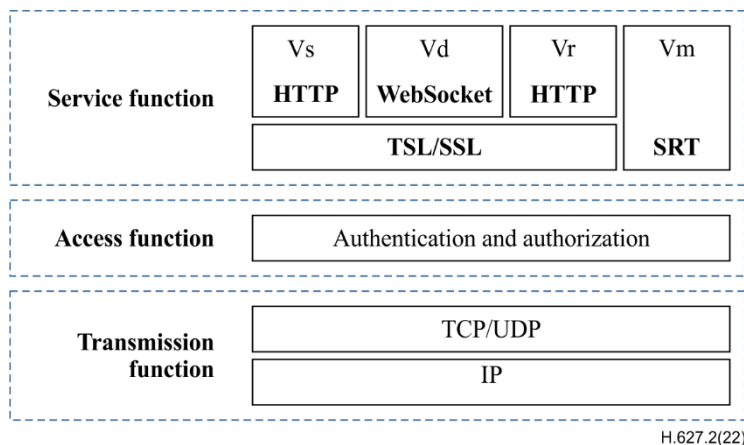


Figure 8-2 – Interface stack

The transmission function uses transmission control protocol (TCP) / user datagram protocol (UDP) protocol for data transmission. Signalling control service is achieved by interfaces Vs and Vd, respectively. Media broadcasting service is achieved by interface Vm, video service is achieved by interface Vr, and device management is achieved by interface Vd.

In the access function, it is required to provide the PU with an authentication service during the access process. The service platform is required to set several security mechanisms, including the identity verification of PUs, the prevention of brute force attacks and replay attacks, etc. It is required that only the PU with successful authentication can access the service platform. It is required that the CU can only obtain the access right of its binding PU.

In the service function, the detailed protocols of interfaces (Vs/Vd/Vm/Vr) between PUs and the service platform are specified as below.

8.3.2 Interface definition

a) Interface Ms: CMU-SCU

It is used by the SCU to report the status, capability of the PU and the alarm information to the CMU. It is also used by the CMU to manage service resources, session status and transferring the session ID for authentication.

b) Interface Sm: SCU-MDU

It is used by the SCU to control the MDU for media distribution, media selection and media location.

c) Interface Cs: SCU-CU

It is used by the CU to send certain video requests to the SCU and to receive the responses.

d) Interface Cm: MDU-CU

It is used by the CU to send a request to the MDU and get the media to stream from the MDU.

e) Interface Cc: CMU-CU

It is used to send a request and return the authentication result, which includes configuration and status query, alarm information, video list and information of cloud storage and front-end storage from the CMU to the CU.

f) Interface Sc: CS-CU

It is used by the CU to send a query, certain video requests, on command and download command to the CS and get live media stream and to record files from the CS when using the on command and download function.

g) Scheduling service interface Vs

Interface Vs complies with HTTPS and JSON. Service platform uses Vs to realize PUs dispatching and signalling access among server rooms.

h) Device management interface Vd

Interface Vd complies with WebSockets and JSON. It defines the control signalling of security devices, including device management, status query, device control, status subscription, live broadcast, network configuration, cloud platform control, alarm reporting, talkback and other functions.

i) Media transmission interface Vm

Interface Vm complies with a secure reliable transport (SRT) protocol based on the user datagram protocol (UDP). It is used for pushing real-time audio and video media stream.

j) Video recording interface Vr

Interface Vr complies with HTTPS and JSON. It defines video recording services, including video segment storage allocation, video content upload, video meta-data upload, playback and other functions.

8.3.3 Interface message definition

The standard interface message using HTTPS and JSON is defined in Table 8-1. Here, the property of direction sets the direction for the message which is sent from the service platform to the PU or from the PU to the service platform. There are several properties contained in the "Request message body" which are request method, request URL, request message header and request content. For response message body, there are mainly three categories, namely, return status code, response message header and response message payload.

Table 8-1 – Interface message for HTTPS+JSON

Protocol type		HTTPS + JSON
Direction		
Request message body	Request method	
	Request URL	
	Request message header	
	Request content	
Response message body	Return status code	
	Response message header	
	Response content	

The standard message for WebSocket protocol and JSON format is defined in Table 8-2. Here, Request name refers to the main purpose of this message. The message type can be either remote procedure call (RPC) or Event type (seen in clause 9.3.2). The property of Direction defines the direction for the message which is sent from the service platform to the PU or from the PU to the service platform. There are several parameters that can be defined in the Request message body according to requirements. For response message body, there are mainly two types, namely, return status code and response content.

Table 8-2 – Interface message for WebSocket and JSON

Request name		
Message type		
Direction		
Request message body (Request content)		
Response message body	Return status code	
	Response content	

9 Protocols for home surveillance system (HSS)

9.1 Requirements of the network transmission function

The protocols defined in this Recommendation are required to support the secure reliable transport (SRT) / user datagram protocol (UDP), WebSocket / TCP and HTTP over TLS [IETF RFC 2818] transmission protocols requirements. The connection between interfaces is required to support HTTP short connection and long connection mechanisms which are in accord with the regulations specified as hypertext transfer protocol – HTTP/1.1 [IETF RFC 7230]. The data transmitted through networks is required to be encrypted using the secure sockets layer (SSL) / transport layer security (TLS) to ensure data security.

9.2 Requirements of access function

The interface information delivered via access function protocols is recommended to use the resource in representation state transfer (REST) architecture, using URI as a unique identification. The major purpose of the access function protocol is to provide authentication and access control for accessing devices. In general, HTTP protocols are recommended for access control. Specifically, a new parameter <Mac-Identity> is recommended to be used to extend the common HTTP header field for representing the requester. Here, the Mac address or similar unique information is required to identify the device when considering the public access networks environment.

9.3 Requirements of service function

This clause will provide a detailed description about the requirements of a service function.

9.3.1 Interface of scheduling service – Vs

A scheduling server sends instructions to PUs through Vs and instructs PUs to connect to the designated signalling server and the peer-to-peer server. The response information is required to contain a timestamp to synchronize the system time of the dispatching server to PUs. Vs uses HTTPS and JSON.