International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.626.4

(08/2018)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

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

Architecture for a point-to-point visual surveillance system

Recommendation ITU-T H.626.4

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**
Ubiquitous sensor network applications and Internet of Things	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.626.4

Architecture for a point-to-point visual surveillance system

Summary

Recommendation ITU-T H.626.4 defines the architecture of a P2P visual surveillance system, including its functional requirements, functional architecture, entities, service flows and interfaces. This is a type of visual surveillance system, which provides a way for users to access video streams directly from cameras through a network, without transferring video streams via a visual surveillance platform.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T H.626.4	2018-08-29	16	11.1002/1000/13670

Keywords

Architecture, point-to-point, 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

Recommendation ITU-T H.626.4

Architecture for a point-to-point visual surveillance system

1 Scope

The visual surveillance service is a telecommunication service focusing on video (including audio) application technology, which is used to capture multimedia (such as audio, video, image and various alarm signal) and present them to end users in a user-friendly manner, based on a managed broadband network with ensured quality, security and reliability.

P2P visual surveillance is a type of video surveillance (VS) system, which provides a way for users to access video streams directly from cameras through the Internet, without transferring any video streams via the VS platform.

This Recommendation focuses on the architecture of a P2P visual surveillance system, including its functional requirements, functional architecture, entities, service flows and interfaces.

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 G.711] Recommendation ITU-T G.711 (1988), *Pulse code modulation (PCM) of voice frequencies*.

[ITU-T G.722] Recommendation ITU-T G.722 (2012), *7 kHz audio-coding within 64 kbit/s.*

[ITU-T H.264] Recommendation ITU-T H.264 (2017), *Advanced video coding for generic audiovisual services*.

[IETF RFC 3550] IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.

[IETF RFC 7826] IETF RFC 7826 (2016), *Real-Time Streaming Protocol Version 2.0.*

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 unit [b-ITU-T H.626]: 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.

3.1.3 functional architecture [b-ITU-T Y.2012]: A set of functional entities, and the reference points between them, used to describe the structure of an NGN. These functional entities are separated by reference points, and thus, they define the distribution of functions.

NOTE 1 – The functional entities can be used to describe a set of reference configurations. These reference configurations identify which reference points are visible at the boundaries of equipment implementation and between administrative domains.

NOTE 2 – The definition is not only applicable to NGNs, but also to other IP packet switch based networks.

3.1.4 functional entity [b-ITU-T Y.2012]: An entity that comprises an indivisible set of specific functions. Functional entities are logical concepts, while groupings of functional entities are used to describe practical, physical implementations.

3.1.5 interface [b-ITU-T Y.101]: A shared boundary between two functional units.

NOTE – An interface is defined by various characteristics pertaining to the functions, physical interconnections, signal exchanges and other characteristics as appropriate.

3.1.6 mobile customer unit [b-ITU-T H.626.1]: Mobile client software installed in customers' mobile devices. It is used to initiate the service and provide customers with video viewing.

3.1.7 premises unit [b-ITU-T H.626]: 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.

3.1.8 reference point [b-ITU-T Y.2012]: A conceptual point at the conjunction of two non-overlapping functional entities that can be used to identify the type of information passing between these functional entities.

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

3.1.10 service platform [b-ITU-T H.626]: A series of devices and subsystems located at the centred part of a visual surveillance system. It is used to integrate all of the capabilities and provide visual surveillance services to customers. The main functions include service control function, media switching, distribution, storage, control and management functions.

3.1.11 surveilled object [b-ITU-T H.626]: The target (such as site, human, and related environment) on which surveillance is performed.

3.1.12 visual surveillance [b-ITU-T H.626]: A telecommunication service focusing on video (but including audio) application technology, which is used to remotely capture multimedia (such as audio, video, image, alarm signal, etc.) and present them to the end user in a user friendly manner, based on a managed broadband network with ensured quality, security and reliability.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 centre management unit: The centre management unit is located at the centre of the P2P visual surveillance system. Its main functions include a centralized system management, service operation management, etc.

3.2.2 media transmission unit: The media transmission unit is located at the centre of the P2P visual surveillance system. It is used to transport media from the premises unit (PU) to the customer unit \ mobile customer unit (CU\M_CU), when the P2P communication channel fails. It assists the media stream from the PU to traverse the private network to the CU; its main functions include media receiving, media processing, media routing, media transmission, media forwarding, etc.

3.2.3 mobile customer unit: A mobile device is 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.

3.2.4 P2P visual surveillance system: The P2P visual surveillance system is a new type of video surveillance system, which provides a way for users to access video streams directly from P2P cameras via networks, without transferring video streams by the visual surveillance platform.

3.2.5 service control unit: The service control unit is located at the centre of the P2P visual surveillance system. It is distributed network equipment, fulfilling access of the premises unit (PU), network video recorder (NVR), customer unit (CU) and mobile customer unit (M_CU). Its main functions include access registration, access authentication, identification, authorization, call control, location, presence and target media serving function selection.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAA Authentication, Authorization and Accounting
CIF Common Intermediate Format
CMU Centre Management Unit
CRM Customer Relationship Management
CU Customer Unit
IP Internet Protocol
IPC Internet Protocol Camera
LAN Local Area Network
M_CU Mobile Customer Unit
MTU Media Transmission Unit
NAT Network Address Translator
NVR Network Video Recorder
P2P Point-to-Point
PTZ Pan/Tilt/Zoom
PU Premises Unit
RTCP Real-time Transport Control Protocol
RTP Real-time Transport Protocol
RTSP Real-Time Streaming Protocol
SCU Service Control Unit
SD card Secure Digital memory card
SMS Short Message Service
STUN Simple Traversal of UDP over NATs
TCP Transmission Control Protocol
TURN Traversal Using Relay NAT
URL Uniform Resource Locator
VS Visual Surveillance

5 Conventions

In this Recommendation, the following conventions apply.

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

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

The keywords "can optionally" indicate an optional requirement that is permissible, without implying any sense of being recommended.

6 Functional requirements

6.1 Service requirements

6.1.1 Self-service of users

The user is required to register services using a mobile phone number, and a specified camera is assigned to the user's account, after the service has been approved by the telecommunication operator.

6.1.2 Plug and play

The system is required to connect the user to cameras through the internet directly, without any extra configurations for equipment, achieving the goal of zero configurations.

6.1.3 Diversified custom terminal devices

It is required to support a variety of terminal devices, including mobile phones, tablets and personal computers. A requirement for users is the ability to watch real-time video at anytime and anywhere, and with several choices of video formats, CIF, D1 and 720P for instance. The frame rate varies from 1 to 25 fps.

6.1.4 PTZ operation (optional)

It is recommended to support the ability to tilt the camera and zoom it in and out remotely over the CU/M_CU.

6.1.5 Night vision (optional)

The built-in infrared lamp is recommended to increase the light and then enhance the video resolution under low illumination environments, especially in the dark night scenario.

6.1.6 Video record and playback on SD card (optional)

It is recommended to support video storage, searching and playback on SD card. The record strategy is also configurable remotely.

6.1.7 Video record and playback on NVR

It is required to support video record on the NVR which is bound to a specified IPC. It is also required to support the record strategy setting and recorded video playback on the CU. The video files can be exported from the NVR, and they can be played quickly, slowly and reversely, even at the speed of one frame per second.

6.1.8 Audio intercommunication

The system is recommended to allow users to talk to each other, between the CU/M_CU and the IPC.

6.1.9 Alarm messaging

The system is recommended to send alarm messages to users' mobile phones, relating to events such as log in/out, full storage and IPC offline, etc. The content of messages can be set over the CU.

6.1.10 Video sharing

The system is recommended to allow users to share the surveillance video to its sub account.

6.1.11 Unified wireless LAN configuration

It is recommended to allow users to set the wireless LAN over the unified wireless LAN configuration interface in the CU/M_CU conveniently, or switch to another wireless LAN.

6.1.12 Fixed timing snapshot

The IPC is recommended to support image snapshots and send them to the specified phone according to given timings set by users.

6.1.13 Cloud storage

It is recommended to transfer and store, search and playback the video in the remote cloud storage. Users are recommended to pay for extra cloud storage, given that some fixed storage space is free.

6.1.14 Network management

It is required to support management of the IPCs, storage devices and network failures.

6.2 Platform requirements

– A portal is provided for users to access services such as self-service, video browsing, recorded video search and playback, alarm and IPC configuration. The portal also has functions of advertising and IPC subscribing.

– A portal is provided for administrators from telecommunication operators to access functions such as equipment management, user management, vendor management, system configuration, device remote upgrade, log management, statistics and report.

– The M_CU is required to access the platform.

– The system is required to interwork with cloud storage systems.

– An interface with an SMS gateway is required to be provided.

– The system is required to interwork with a CRM for user authentication and verification.

6.3 CU/M_CU requirements

6.3.1 M_CU

The M_CU supports:

– user login;

– displaying whether camera status is online or offline;

– real-time video browsing based on RTSP, RTP/RTCP over TCP;

– PTZ operation;

– instant image snapshot over M_CU;

– local record of video;

– audio and video simultaneously;

– remote setting of wireless LAN which an IPC connects to.

6.3.2 Web client

The web client supports:

– video based on standard codec including ITU-T H.264 and audio based on standard codec, including ITU-T G.711 and ITU-T G.722;

– user login;

– network control with digital signature, which upgrades to the latest versions automatically;

– PTZ operation;

– users to alter the key for login, set record strategy and storage paths;
– image snapshot over real-time video manually; the storage path is configurable;
– both local and front-end record of video;
– remote configuration of the IPC wireless LAN;
– cloud storage for video, and the searching and playback of video recordings remotely;
– record setting strategy:
  1) starting or stopping the local recording process manually with video files stored in the local PC; the storage paths are configurable;
  2) front-end and cloud storage include periodic and cyclic record;
– all major operation system;
– mainstream browsers.

7 Functional architecture

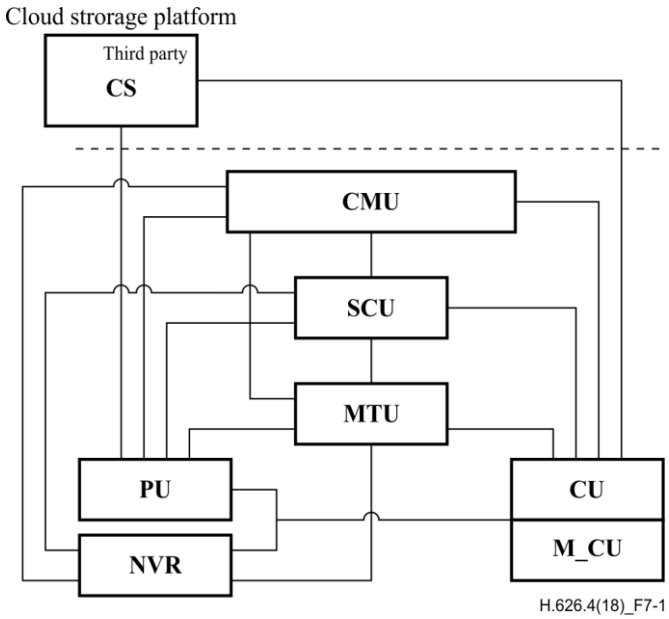

Figure 7-1 – System composition of P2P visual surveillance

The system architecture is presented in Figure 7-1, which includes the premises unit (PU), client unit (CU), mobile client unit (M_CU), cloud storage (CS), network video recorder (NVR), central management unit (CMU), service control unit (SCU) and media transmission unit (MTU). All components are connected via the IP bearer network.

The CU sends requests to the central service platform for connection with capabilities' information such as the maximum resolution, video type, bit rate that the CU supports, and to get the address of the requested PU. After authentication, the central service platform transfers the capability information to the requested PU, and transfers the address to the CU. Then the CU connects to the PU using the address.

The PU receives information of the capability of the CU through the central service platform. Then the PU adjusts the parameters of surveilled video and encodes them into real-time media streams according to the information, and then transmits the media streams to the CU.

7.1 CMU: centre management unit

The centre management unit (CMU) is used for centralized system management, service operation management, etc.

Accordingly, the main functions of the CMU are management, authorization, accounting and charging, location and presence, web server and cloud storage management. The detailed functional features are:

– management: managing content, service, network, terminal devices, etc.;
– authorization: authorizing access rights;
– accounting and charging: providing monitoring of service records and charging policy, etc.;
– location and presence: locating the PU, the NVR, and presenting the PU and the NVR online/offline status;
– web server: serving the web client;
– cloud storage management: managing the configuration of cloud storage, executing the cloud storage program, responding to the request of cloud record playback.

7.2 SCU: service control unit

The service control unit (SCU) is a distributed network equipment, fulfilling the need of the PU, the NVR, the CU and the M_CU access.

Accordingly, the main functions of the SCU are access registration, access authentication, identification, authorization, call control, presence, clock synchronization and target media serving function selection. The detailed functional features are:

– access registration: receiving the access registration request from the CU and the PU, and registering them with the registration management server;
– access authentication: receiving the access authentication request from the CU and the PU, and transmitting authentication signals between the AAA servers;
– identification: identifying the CU and the PU, and comparing identities with subscriber data and terminal data to find the matching results;
– authorization: authorizing the CU and the PU;
– call control: controlling call sessions with the PU and the CU, establishing and maintaining media transport path information (media routing table). The related session methods may include setup, tear down, update, modify and keep-live in order to access, route and relay;
– presence: presenting the status of the CU\M_CU and the PU\NVR, such as online, offline, active, inactive, etc.;
– clock synchronization: unified time criteria and clock synchronization control;
– media serving function selection: selecting one media serving function unit (i.e. media transmission unit and related media storage unit) when the SCU controls multiple media serving function units.

7.3 MTU: media transmission unit

The media transmission unit (MTU) is used to transmit media data from the PU to the CU\M_CU, when the P2P communication channel fails.

Accordingly, the MTU assists the media stream from the PU to traverse the private network to the CU; its main functions include media receiving, media processing, media routing, media transmission, media forwarding, etc. The detailed functional features are:

– serving as simple traversal of UDP over NATs (STUN), traversal using relay NAT (TURN) servers;

– media receiving: receiving media data (stream and files) from the PU;
– media processing: mixing/de-mixing, decoding/encoding and transcoding media that is received by the MTU, as required;
– media transmission: transmitting media to one CU or multiple CUs on request according to media routing information.

NOTE – Transmission from one PU to multiple CUs requires conversion from a unicast media channel to a multicast media channel.

7.4 PU: premises unit

The premises unit (PU) refers to the premises subsystem within the VS system. It includes functional entities such as media capturing, media adjustment and media transmission.

It supports:

– capturing multimedia information (such as audio, video, image, alarm signals, etc.) from the surveilled object;
– multimedia (audio, video, image) encoding and adjustment: The PU can adjust the parameters of captured multimedia and encode them into real-time stream according to the capabilities information from the CU;
– outputting alarm signals to external devices;
– parsing PTZ command codes and transmitting them to devices in order to control the camera;
– network transport, transforming the multimedia into IP data packets, transmitting bidirectional media stream and alarm signals to other entities;
– the media storage function is optional for the PU;
– audio decoding and play functions are optional for the PU.

7.5 NVR: network video recorder

The network video recorder (NVR) is used to record the surveillance video in the front end. The video is transferred to the NVR, exported from the NVR, searched and played back.

7.6 CU: customer unit

The customer unit (CU) is the customer unit within the VS system. It is used to present multimedia information (such as audio, video, image, and alarm signals) to the end user. It supports:

– multimedia decoding;
– audio play and video/image display function;
– interfaces for end users to operate the VS system;
– configuration of network access, including wireless LAN hotspot selection and account setting.

7.7 M_CU: Mobile customer unit

The functions of the mobile customer unit (M_CU) are similar to the CU. The difference is that the M_CU is based on a mobile terminal.

7.8 CS: cloud storage platform

The cloud storage platform (CS) is an external system which interworks with a P2P visual surveillance system, providing storage services. It receives the video from the IPC and responds to CU and M_CU requests.

8 Service flow

8.1 PU registration

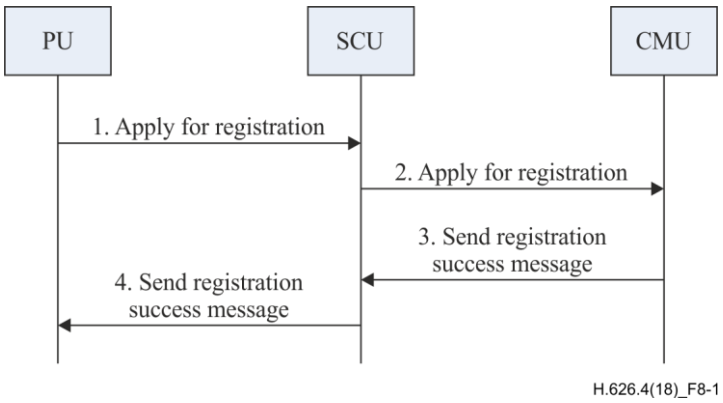

Figure 8-1 – Flow for PU registration

Step 1: The PU sends an applying for registration message to the SCU.

Step 2: The SCU sends an applying for registration message to the CMU.

Step 3: If the PU has not been registered, the CMU sends a registration success message to the SCU.

Step 4: The SCU sends a registration success message to the PU.

8.2 Users bind device

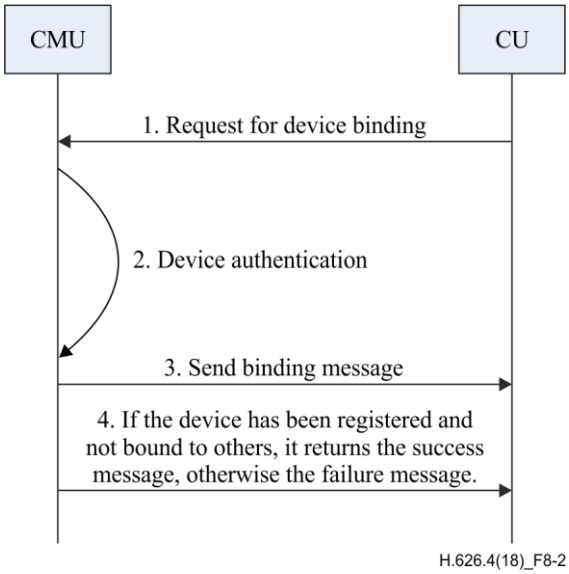

Figure 8-2 – Flow for user device binding

Step 1: The CU sends a request to the CMU for device binding.

Step 2: The CMU does device location authentication.

Step 3: The CMU sends a device binding message to the CU.

Step 4: If the device has been registered and not bound to others, it returns the success message, otherwise the failure message.

8.3 Private network traversal

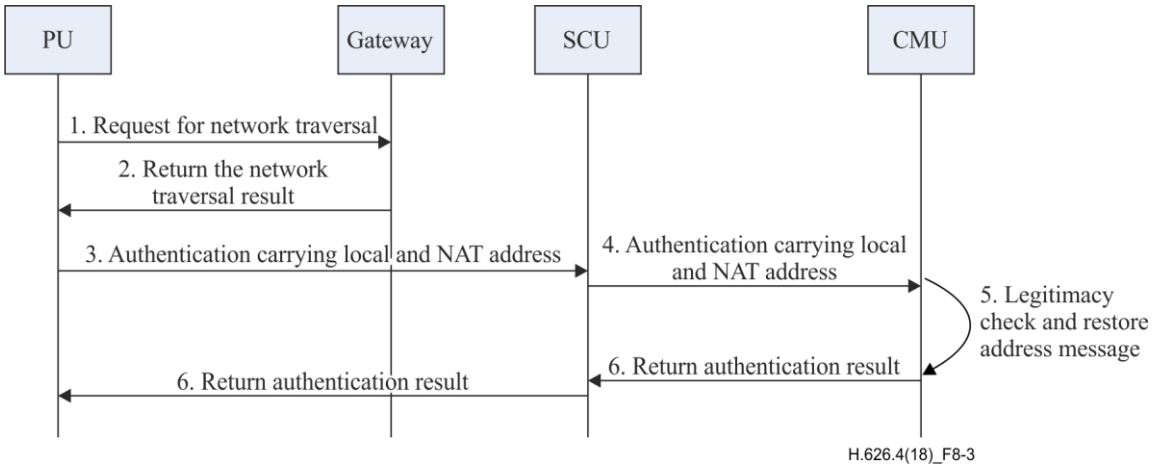

Figure 8-3 – Flow for private network traversal

Step 1: The PU sends a request to the gateway for network traversal.

Step 2: The gateway returns the network traversal result to the PU.

Step 3: The PU sends the authentication carrying local and NAT address to the SCU.

Step 4: The SCU sends authentication to the CMU carrying the local and NAT address.

Step 5: The CMU does a legitimacy check and restores the address message.

Step 6: The CMU returns the authentication result to the SCU.

Step 7: The SCU returns the authentication result to the PU.

8.4 Media play

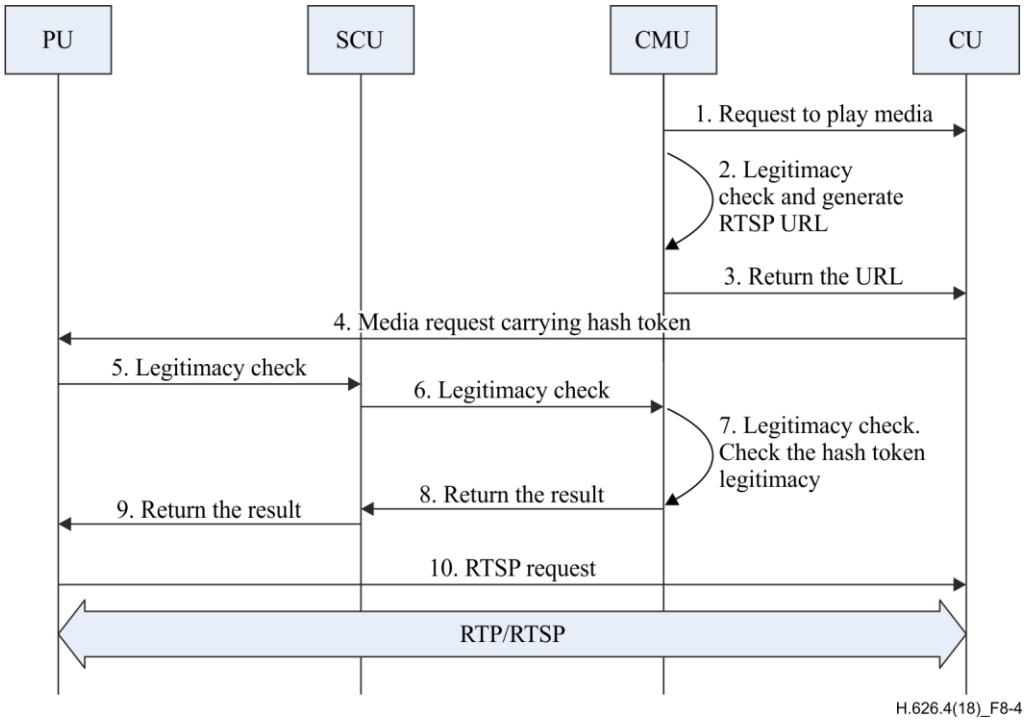

Figure 8-4 – Flow for media play

Step 1: The CU sends a request to the CMU for playing media.

Step 2: The CMU does a legitimacy check and generates the RTSP URL.

Step 3: The CMU sends the RTSP URL to the CU.

Step 4: The CU sends the media request to the PU carrying a hash token.

Step 5: The PU sends the SCU the legitimacy check message.

Step 6: The SCU sends the CMU the legitimacy check message.

Step 7: The CMU checks the hash token legitimacy.

Step 8: The CMU sends the result to the SCU.

Step 9: The SCU sends the result to the PU.

Step 10: The PU responds to the CU with the RTSP request.

8.5 PTZ control

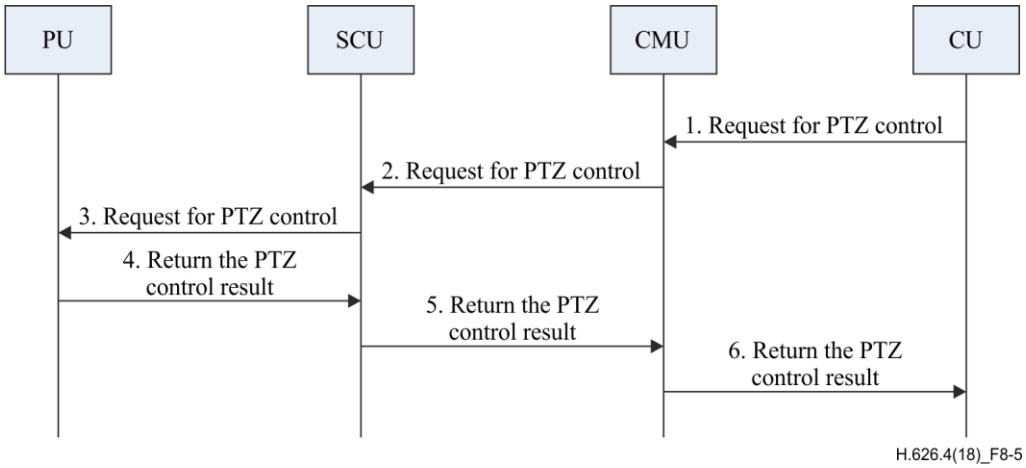

Figure 8-5 – Flow for PTZ control

Step 1: The CU sends the request to the CMU for PTZ control.

Step 2: The CMU sends the request to the SCU for PTZ control.

Step 3: The SCU sends the request to the PU for PTZ control.

Step 4: The PU returns the PTZ control result to the SCU after the PTZ control is completed.

Step 5: The SCU returns the PTZ control result to the CMU.

Step 6: The CMU returns the PTZ control result to the CU.

8.6 Media share

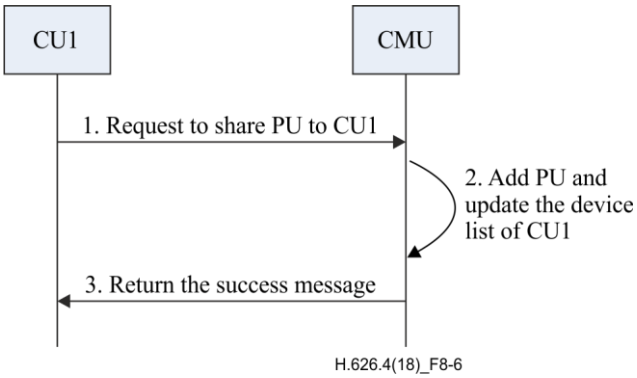

Figure 8-6 – Flow for media share

Step 1: CU1 sends the request to the CMU for sharing the PU to CU1.

Step 2: The CMU adds the PU device and updates the device list of CU1.

Step 3: The CMU returns the success message of device sharing.

8.7 Record and play back

8.7.1 Recording and playback on the CS

8.7.1.1 Recording

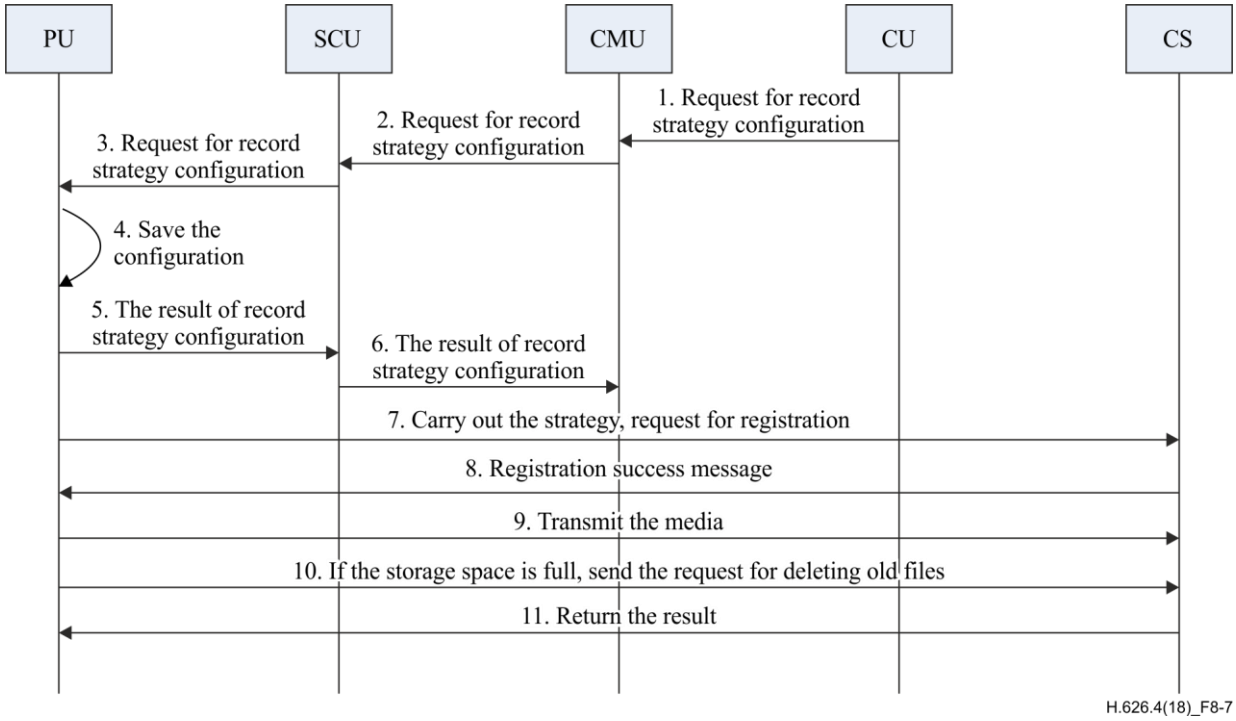

Figure 8-7 – Recording on CS

Step 1: The CU sends a request to the CMU for record strategy configuration.

Step 2: The CMU sends the request for record strategy configuration to the SCU.

Step 3: The SCU sends the request for record strategy configuration to the PU.

Step 4: The PU saves the strategy configuration.

Step 5: The PU sends the result of record strategy configuration to the SCU.

Step 6: The SCU sends the result of record strategy configuration to the CMU.

Step 7: The PU carries out the strategy and sends the request to the CS for registration.

Step 8: The CS returns a registration success message to the PU.

Step 9: The PU starts to transmit the media to the CS.

Step 10: If the storage space of the CS is full, the PU sends the request to the CS for deleting the old files.

Step 11: The CS returns the result to the PU.

8.7.1.2 Playback

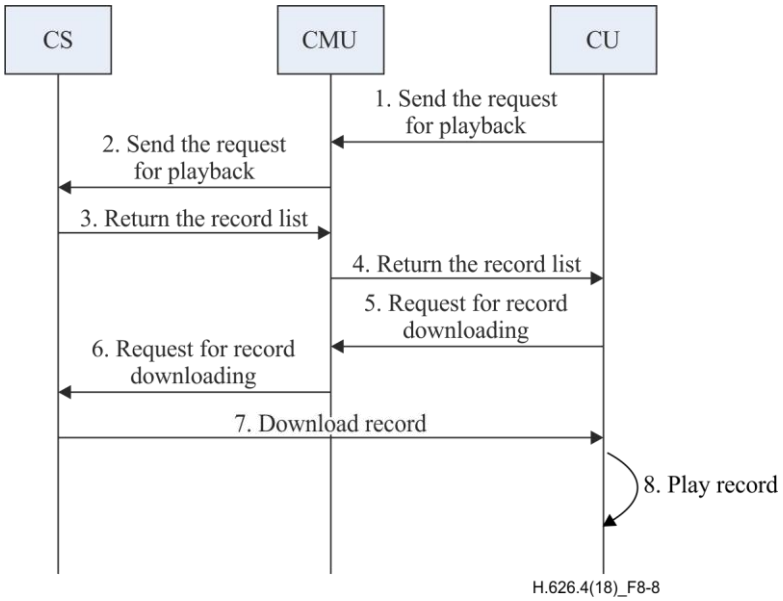

Figure 8-8 – Playback on CS

Step 1: The CU sends the request to the CMU for playback.

Step 2: The CMU sends the request to the CS for playback.

Step 3: The CS returns the record list to the CMU.

Step 4: The CMU returns the record list to the CU.

Step 5: The CU sends the request to the CMU for downloading the record.

Step 6: The CMU sends the request to the CS for downloading the record.

Step 7: The CS downloads the record to the CU.

Step 8: The CU plays the record.

8.7.2 Recording and playback on NVR

8.7.2.1 Recording

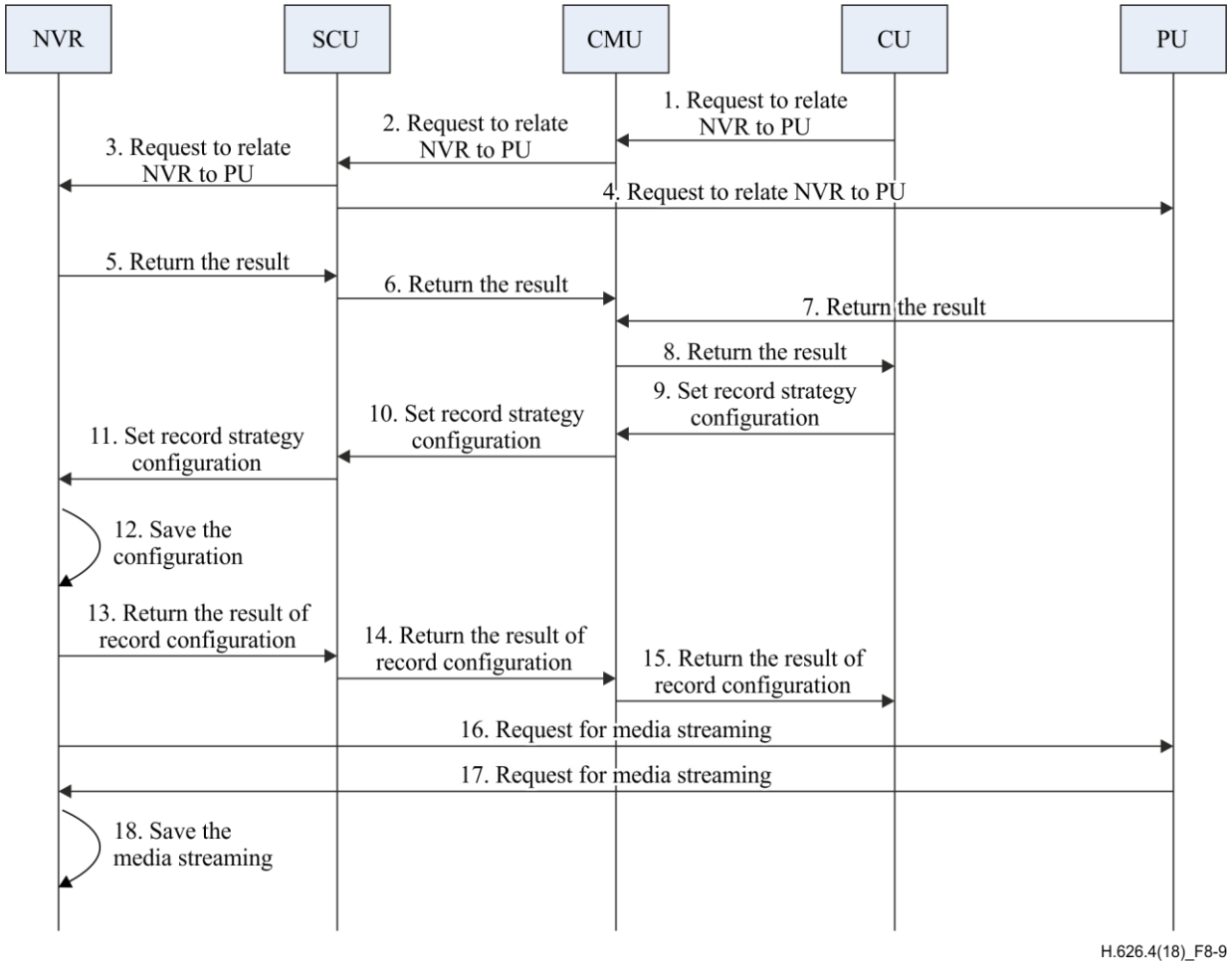

Figure 8-9 – Recording on NVR

Step 1: The CU sends the request to the CMU for setting the NVR to relate to the PU.

Step 2: The CMU sends the request to the SCU for setting the NVR to relate to the PU.

Step 3: The SCU sends the request to the NVR for setting the NVR to relate to the PU.

Step 4: The SCU sends the request to the PU for setting the NVR to relate to the PU.

Step 5: The NVR returns the result to the SCU.

Step 6: The SCU returns the result to the CMU.

Step 7: The PU returns the result to the SCU.

Step 8: The CMU returns the result to the CU.

Step 9: The CU sends the request to the CMU for setting the record strategy configuration.

Step 10: The CMU sends the request to the SCU for setting the record strategy configuration.

Step 11: The SCU sends the request to the NVR for setting the record strategy configuration.

Step 12: The NVR saves the record strategy configuration.

Step 13: The NVR returns the result of record configuration to the SCU.

Step 14: The SCU returns the result of record configuration to the CMU.

Step 15: The CMU returns the result of record configuration to the CU.

Step 16: When the strategy is executed, the NVR sends the request to the PU for media streaming.

Step 17: The PU returns media streaming to the NVR.

Step 18: The NVR saves the media streaming.

8.7.2.2 Playback

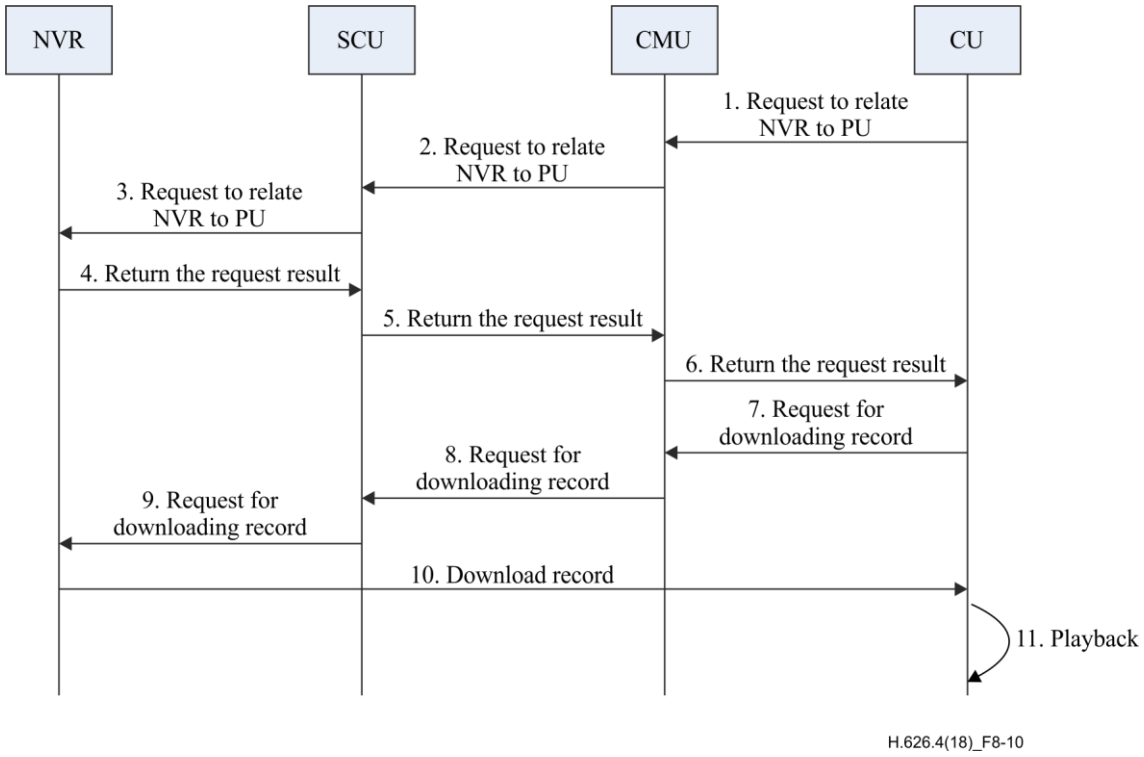

Figure 8-10 – Playback on NVR

Step 1: The CU sends the request to the CMU for the NVR related to the PU.

Step 2: The CMU sends the request to the SCU for the NVR related to the PU.

Step 3: The SCU sends the request to the NVR for the NVR related to the PU.

Step 4: The NVR returns the request results to the SCU.

Step 5: The SCU returns the request results to the CMU.

Step 6: The CMU returns the request results to the CU.

Step 7: The CU sends the request for downloading the record from the CMU.

Step 8: The CMU sends the request for downloading the record from the SCU.

Step 9: The SCU sends the request for downloading the record from the NVR.

Step 10: The NVR downloads the record to the CU.

Step 11: The CU plays back the video in local.

8.7.3 Recording and playback on PU

8.7.3.1 Recording

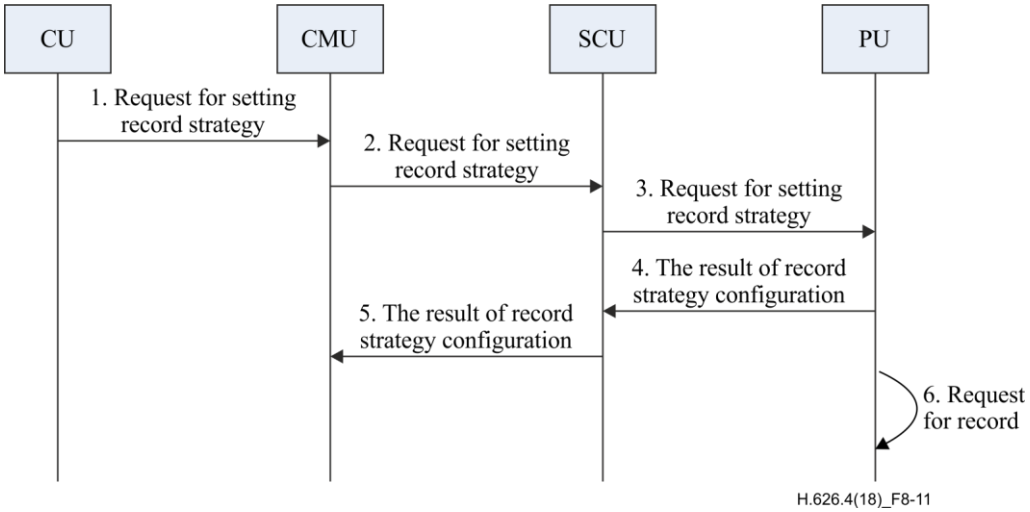

Figure 8-11 – Recording on PU

Step 1: The CU sends the request to the CMU for setting the record strategy.

Step 2: The CMU sends the request to the SCU for setting the record strategy.

Step 3: The SCU sends the request to the PU for setting the record strategy.

Step 4: The PU returns the result of record strategy configuration to the SCU.

Step 5: The SCU returns the result of record strategy configuration to the CMU.

Step 6: The PU applies the strategy and sends the recording request.

8.7.3.2 Playback

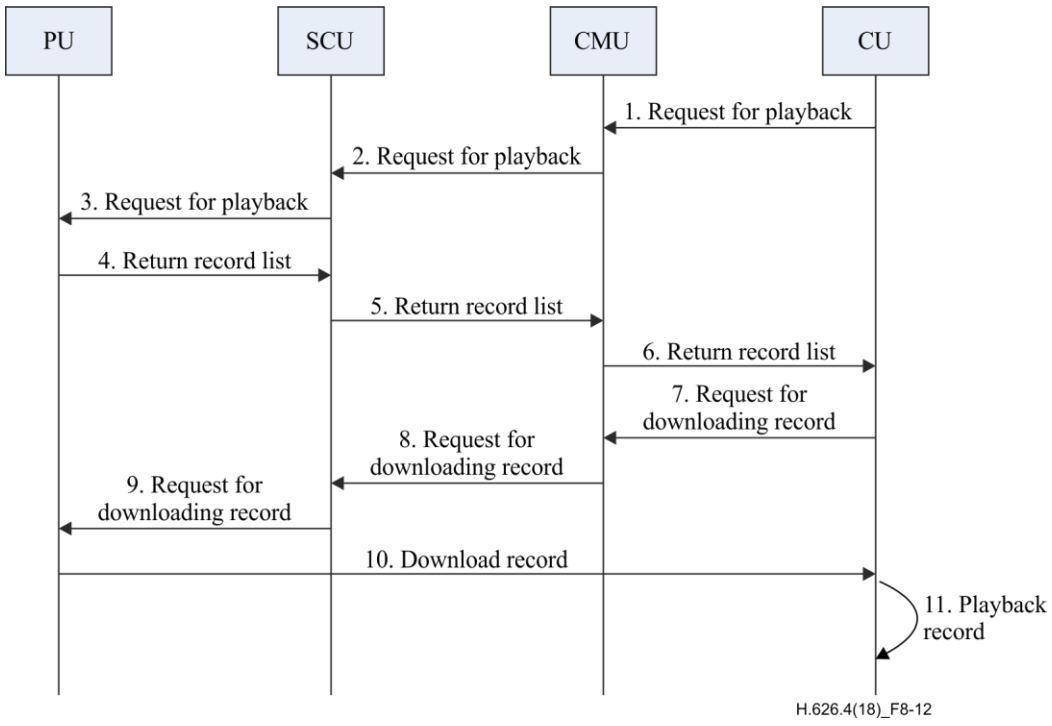

Figure 8-12 – Playback on PU

Step 1: The CU sends the request to the CMU for playback.

Step 2: The CMU sends the request to the SCU for playback.

Step 3: The SCU sends the request to the PU for playback.

Step 4: The PU returns the record list to the SCU.

Step 5: The SCU returns the record list to the CMU.

Step 6: The CMU returns the record list to the CU.

Step 7: The CU sends the request to the CMU for downloading the record.

Step 8: The CMU sends the request to the SCU for downloading the record.

Step 9: The SCU sends the request to the PU for downloading the record.

Step 10: The PU downloads the record from the CU.

Step 11: The CU plays back the record in local.

8.8 Alarm linkage

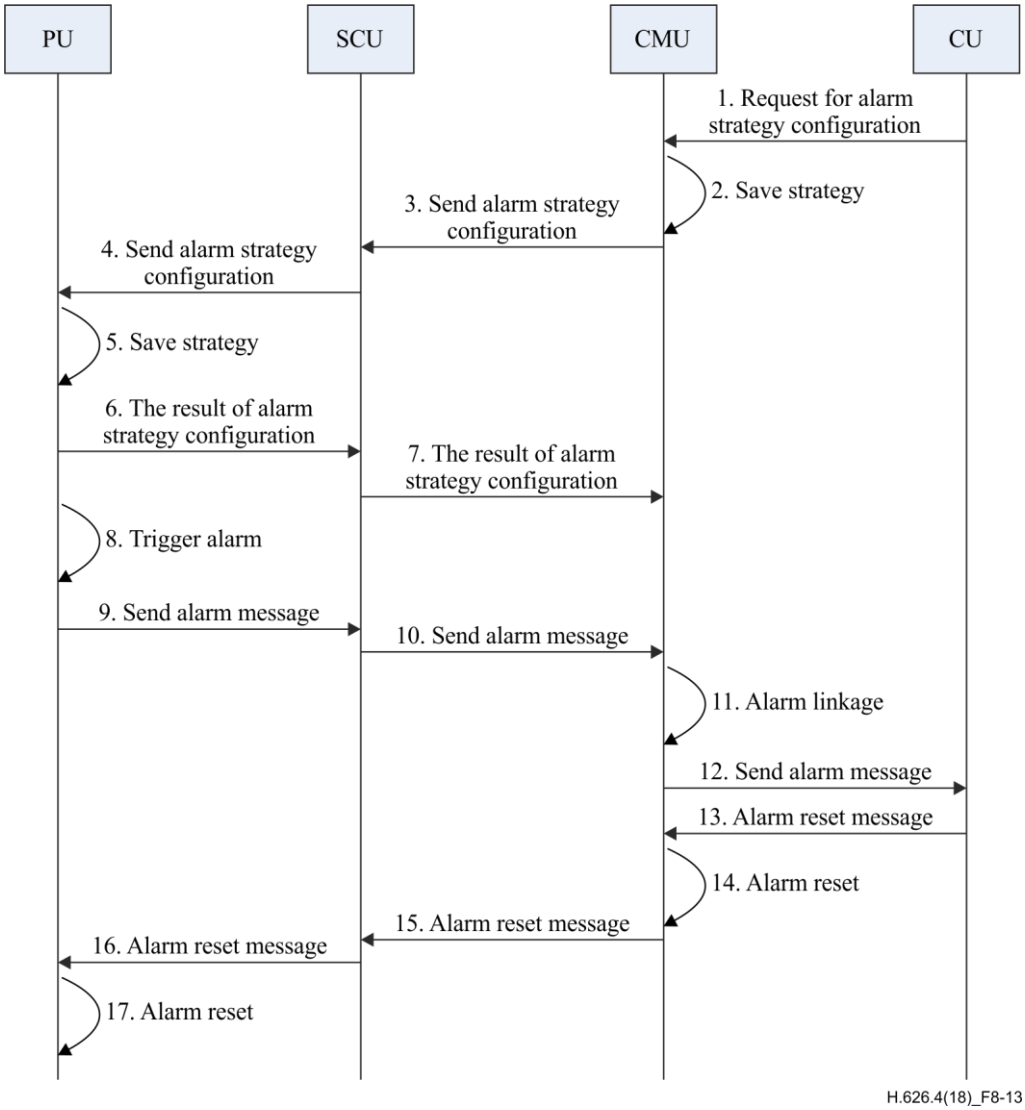

Figure 8-13 – Flow for alarm linkage

Step 1: The CU sends the request to the CMU for alarm strategy configuration.

Step 2: The CMU saves the alarm strategy.

Step 3: The CMU sends alarm strategy configuration to the SCU.

Step 4: The SCU sends alarm strategy configuration to the PU.

Step 5: The PU saves the alarm strategy.

Step 6: The PU sends the result of alarm strategy configuration to the SCU.

Step 7: The SCU sends the result of alarm strategy configuration to the CMU.

Step 8: The PU triggers the alarm.

Step 9: The PU sends the alarm message to the SCU.

Step 10: The SCU sends the alarm message to the CMU.

Step 11: The CMU carries out the alarm linkage.

Step 12: The CMU sends the alarm message to the CU.

Step 13: The CU sends the alarm reset message to the CMU.

Step 14: The CMU alarm resets.

Step 15: The CMU sends the alarm reset message to the SCU.

Step 16: The SCU sends the alarm reset message to the PU.

Step 17: The PU resets the alarm status.

8.9 Parameter query and configuration

8.9.1 Parameter query and configuration on PU

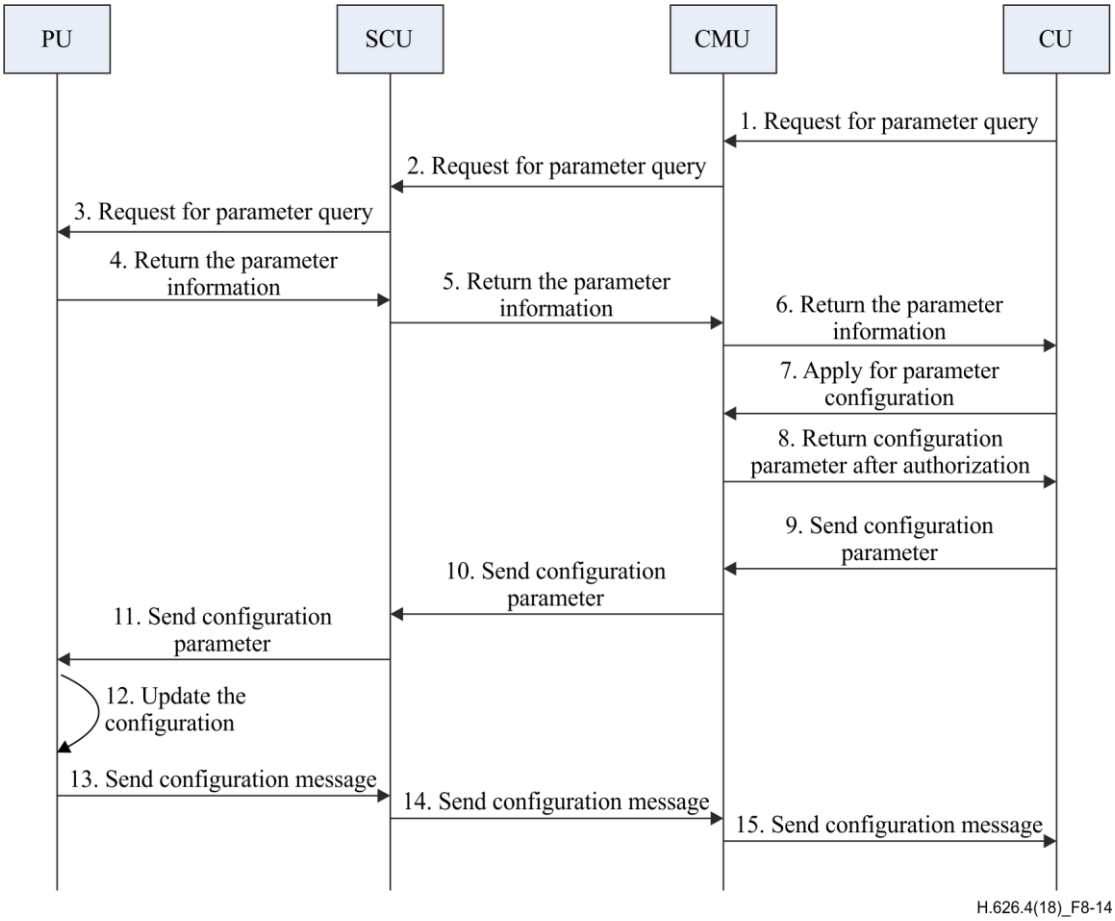

Figure 8-14 – Flow for parameter query and configuration on PU

Step 1: The CU sends the request to the CMU for parameter query.

Step 2: The CMU sends the request to the SCU for parameter query.

Step 3: The SCU sends the request to the PU for parameter query.

Step 4: The PU returns the parameter information to the SCU.

Step 5: The SCU returns the parameter information to the CMU.

Step 6: The CMU returns the parameter information to the CU.

Step 7: The CU sends applying for parameter configuration to the CMU.

Step 8: The CMU returns the configuration parameter after the user authorization.

Step 9: The CU sends the configuration parameter to the CMU.

Step 10: The CMU sends the configuration parameter to the SCU.

Step 11: The SCU sends the configuration parameter to the PU.

Step 12: The PU updates the configuration parameter.

Step 13: The PU sends the configuration state message to the SCU.

Step 14: The SCU sends the configuration state message to the CMU.

Step 15: The CMU sends the configuration state message to the CU.

8.9.2 Parameter query and configuration on CMU

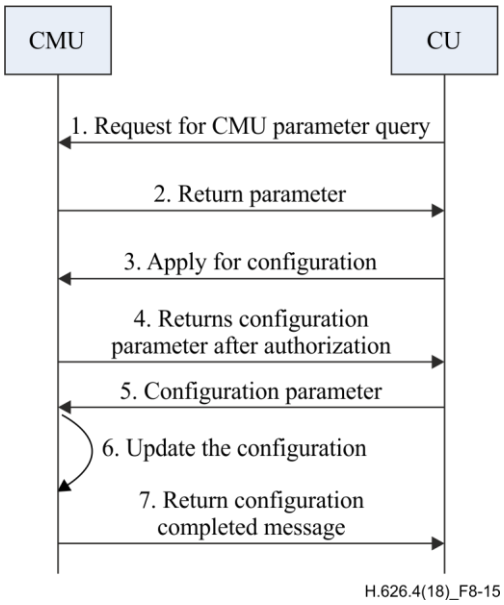

Figure 8-15 – Flow for parameter query and configuration on CMU

Step 1: The CU sends a request to the CMU for the CMU parameter query.

Step 2: The CMU returns the parameter information to the CU.

Step 3: The CU sends an application for the CMU configuration.

Step 4: The CMU returns the configuration parameter to the CU after user authorization.

Step 5: The CU sends the configuration parameter to the CMU.

Step 6: The CMU updates the configuration parameter.

Step 7: The CMU returns the configuration completed message to the CU.

8.10 Device reset

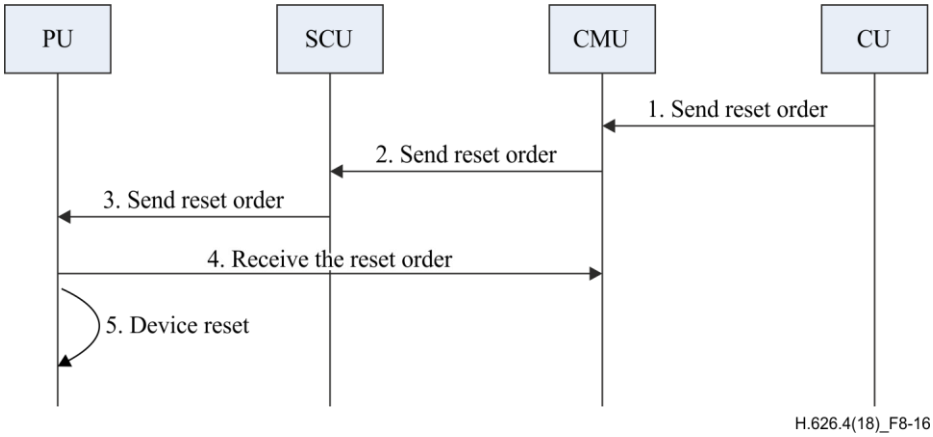

Figure 8-16 – Flow for device reset

Step 1: The CU sends the device reset order to the CMU.

Step 2: The CMU sends the device reset order to the SCU.

Step 3: The SCU sends the device reset order to the PU.

Step 4: The PU sends the received message after receiving reset order.

Step 5: The PU resets.

8.11 Upgrade

8.11.1 Device upgrade

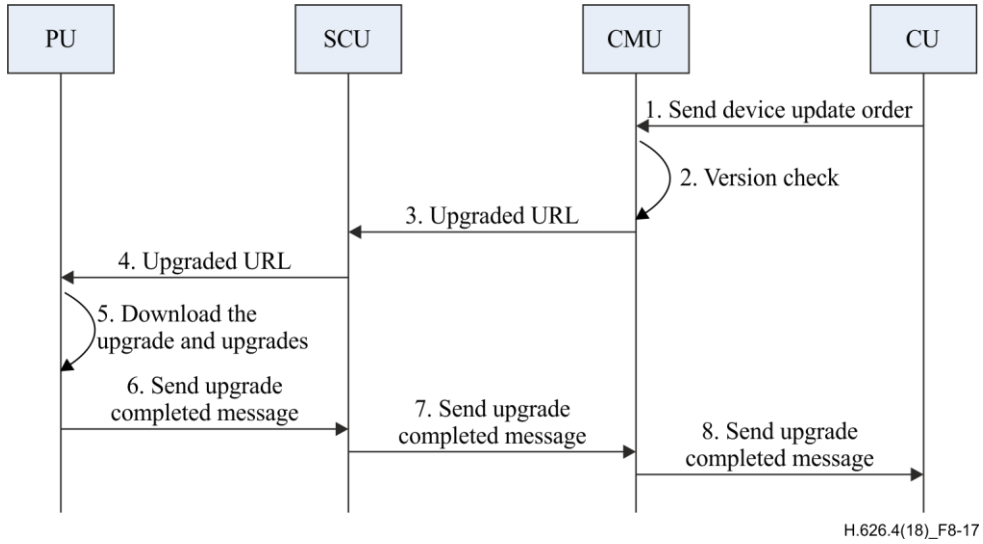

Figure 8-17 – Flow for device upgrade

Step 1: The CU sends the device upgrading order to the CMU.

Step 2: The CMU checks the version.

Step 3: The CMU sends the upgraded URL to the SCU.

Step 4: The SCU sends the upgraded URL to the PU.

Step 5: The PU downloads the upgrade and upgrades.

Step 6: The PU sends an upgrade completed message to the SCU.

Step 7: The SCU sends an upgrade completed message to the CMU.

Step 8: The CMU sends an upgrade completed message to the CU.

8.11.2 M_CU upgrade

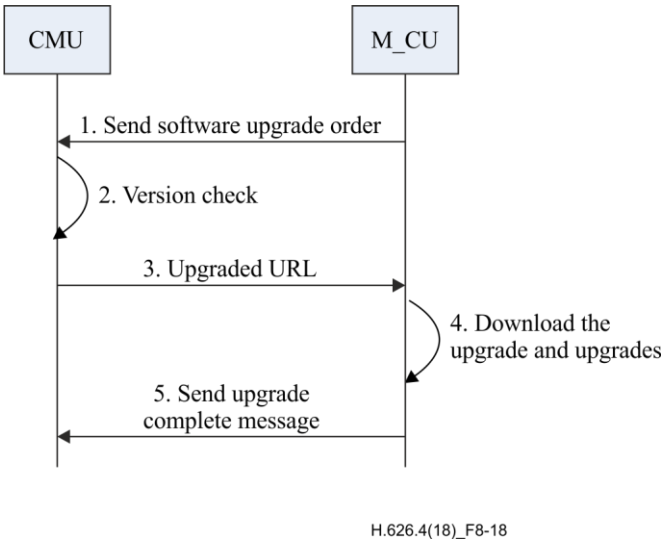

Figure 8-18 – Flow for M_CU upgrade

Step 1: The M_CU sends the software upgrade order to the CMU.

Step 2: The CMU checks the version.

Step 3: The CMU sends the upgrade URL to the M_CU.

Step 4: The M_CU downloads the upgrade and upgrades.

Step 5: The M_CU sends the upgrade completed message to the CMU.

9 Interfaces

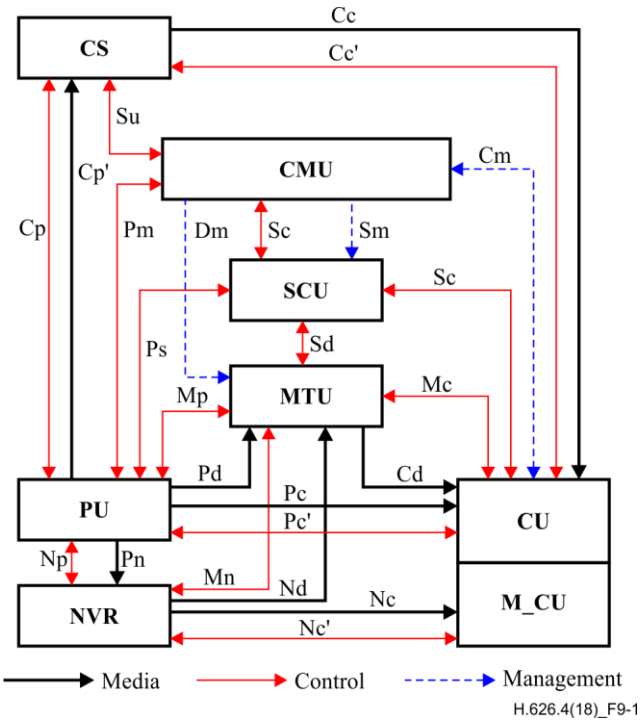

Figure 9-1 – Interfaces of P2P visual surveillance

The interfaces are presented in Figure 9-1.

9.1 Interface Pc: PU-CU

Interface Pc is between the PU and the CU.

It is used to directly deliver media streaming from the PU to the CU.

9.2 Interface Pc': CU-PU

Interface Pc' is between the CU and the PU.

It is used to deliver interaction signals directly between the PU and the CU (such as an RTSP request for real-time video or its response).

9.3 Interface Mp: MTU-PU

Interface Mp is between the MTU and the PU.

It is used to deliver interaction requests from the MTU to the PU and receive response while communicating via the STUN or TURN protocol.

9.4 Interface Pd: PU-MTU

Interface Pd is between the PU and the MTU.

It is used to deliver media streaming from the PU to the MTU while communicating via the STUN or TURN protocol.

9.5 Interface Cd: MTU-CU

Interface Cd is between the MTU and CU.

It is used to send media streaming from the MTU to the CU via the RTSP/RTP protocol.

9.6 Interface Mc: CU-MTU

Interface Mc is between the CU and the MTU.

It is used to send an RTSP request and receive response from the CU to the MTU.

9.7 Interface Dm: CMU-MTU

Interface Dm is between the CMU and the MTU.

It is used to return the authentication result from the CMU to the MTU.

9.8 Interface Sm: CMU-SCU

Interface Sm is between the CMU and the SCU.

It is used by the CMU to manage service resource, session status, and transferring the session ID for authentication.

9.9 Interface Sc: SCU-CMU

Interface Sc is between the SCU and the CMU.

It is used to report the status and capability of the PU, and the alarm information to the CMU, and it is used to return the result to the SCU.

9.10 Interface Cm: CMU-CU

Interface Cm is between the CMU and the 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.

9.11 Interface Ps: SCU-PU

Interface Ps is between the SCU and the PU.

It is used to manage the PU device, to query the running status of devices, to configure parameters and to upgrade software versions, and to control PTZ by forwarding PTZ control operation commands and to return results.

9.12 Interface Cp: CS-PU

Interface Cp is between the CS and the PU.

It is used to send login requests from the CS to the PU and to receive the login acknowledgement from the PU to the CS.

9.13 Interface Cp': PU-CS

Interface Cp' is between the PU and the CS.

It is used to send record files from the PU to the CS.

9.14 Interface Cc: CS-CU

Interface Cs is between the CS and the CU.

It is used to return real-time media stream and to record files from the CS to the CU when using the on command and download function.

9.15 Interface Cc': CU-CS

Interface Cc' is between the CU and the CS.

It is used to send a query, certain video requests, on command and download command from the CU to the CS and return results.

9.16 Interface Np: NVR-PU

Interface Np is between the NVR and the PU.

It is used to send a binding request and video request from the NVR to the PU, and to send the searching request of all PUs in a local area network, and to return the result from the PU to the NVR.

9.17 Interface Pn: PU-NVR

Interface Pn is between the PU and the NVR.

It is used to establish video channels to transmit video streams from the PU to the NVR.

9.18 Interface Nc: NVR-M_CU

Interface Nc is between the NVR and the M_CU.

It is used to directly deliver media streaming of a video record from the NVR to the M_CU.

9.19 Interface Nc': M_CU-NVR

Interface Nc' is between the M_CU and the NVR.

It is used to deliver interaction signals directly between the NVR and the M_CU (such as an RTSP request for video record or response).

9.20 Interface Mn: MTU-NVR

Interface Mn is between the MTU and the NVR.

It is used to send interaction requests from the MTU to the NVR and to receive responses while communicating via the STUN or TURN protocol.

9.21 Interface Nd: NVR-MTU

Interface Nd is between the NVR and the MTU.

It is used to send the media streaming of a video record from the NVR to the MTU while communicating via the STUN or TURN protocol.

9.22 Interface Sc: SCU-CU

Interface Sc is between the SCU and the CU.

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

9.23 Interface Su: CS-CMU

Interface Su is between the CS and the CMU.

It is used to send configuration information of the storage room of the surveilled point from the CMU to the CS, and to get the authorization to access subspace from the CS.

9.24 Interface Sd: SCU-MTU

Interface Sd is between the SCU and the MTU.

It is used by the SCU to control the MTU for media distribution, media selection and media location when the P2P communication channel fails.

9.25 Interface Pm: CMU-PU

Interface Pm is between the CMU and the PU.

It is used to manage the PU device, to query the running status of devices, to configure parameters and to upgrade the software version.

Bibliography

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

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

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

[b-ITU-T H.627] Recommendation ITU-T H.627 (2012), *Signalling and protocols for visual surveillance*.

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

[b-ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	**Audiovisual and multimedia systems**
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2018