

BS EN 50132-5-2:2011
Incorporating corrigendum July 2012



BSI Standards Publication

Alarm systems — CCTV surveillance systems for use in security applications

Part 5-2: IP Video Transmission Protocols

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

raising standards worldwide™



National foreword

This British Standard is the UK implementation of EN 50132-5-2:2011, incorporating corrigendum July 2012. Together with BS EN 50132-5-1:2011 and BS EN 50132-5-3:2012, it supersedes BS EN 50132-5:2001 which is withdrawn.

The start and finish of text introduced or altered by corrigendum is indicated in the text by tags. Text altered by CENELEC corrigendum July 2012 is indicated in the text by **AC1** **AC1**.

The UK participation in its preparation was entrusted by Technical Committee GW/1, Electronic security systems, to Subcommittee GW/1/10, Closed circuit television (CCTV).

A list of organizations represented on this subcommittee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

ISBN 978 0 580 73700 8

ICS 13.310; 33.160.40

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2012.

© The British Standards Institution 2012. Published by BSI Standards Limited 2012

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

**Alarm systems -
CCTV surveillance systems for use in security applications -
Part 5-2: IP Video Transmission Protocols**

Systèmes d'alarme -
Systèmes de surveillance CCTV à usage
dans les applications de sécurité -
Partie 5-2: Protocoles de Transmission de
Vidéo d'IP

Alarmanlagen -
CCTV-Überwachungsanlagen für
Sicherungsanwendungen -
Teil 5-2: IP Video Übertragung Protokolle

This European Standard was approved by CENELEC on 2011-10-31. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Management Centre: Avenue Marnix 17, B - 1000 Brussels

Contents		Page
Foreword.....		9
Introduction		10
1	Scope	11
2	Normative references.....	11
3	Definitions and abbreviations.....	12
3.1	Terms and definitions	12
4	Video Transmission network architecture (informative)	28
4.1	General	28
4.2	Networking and connectivity	30
4.3	Device discovery and description	30
4.4	Video media types and payload formats	31
4.5	Video Transport.....	31
4.6	Eventing and Health Check	31
5	The Building Block of Existing Standards (informative)	31
6	CCTV system device model	32
6.1	Overview	32
6.2	Device model elements	33
7	General IP interoperability requirements	33
7.1	General Protocol Requirements Overview	33
7.2	General High Level IP Video Interface and Protocol Requirements	34
7.3	Non-Conformance Video Transmission Systems and Devices.....	34
7.4	Mandatory Documentation for the IP Video Interface of a VTD	35
8	Video and Data Transport: Mandatory Streaming Requirements	37
8.1	Detailed RTSP Protocol Requirements and Definitions	37
9	Device discovery and description	42
9.1	UPnP Device Discovery and Description (METHOD 1).....	42
9.2	Zeroconf service discovery and description (METHOD 2)	45
9.3	Web Service Discovery (METHOD 3).....	48
10	Eventing Requirements	48
11	Video Network Device Management Requirements.....	49
11.1	Requirements for standard MIB compliance	49
11.2	SNMP Trap Notification Requirements.....	53
11.3	MIB Enterprise Tree Definitions for Video Transmission Devices	54
11.4	Monitoring and Polling Applications	62
11.5	CCTV SNMP Trap Requirements for Event Management.....	62
11.6	Security Requirements SNMP	62

12	Requirements on other IP Video Interfaces	63
13	Bibliography	63
APPENDIX I - IP Interoperability Implementation Based on HTTP and REST Services		66
APPENDIX I.A – REST Service Model Version 1.1		67
1	Introduction	67
2	Design Considerations.....	67
2.1	REST Overview.....	67
2.2	Conformance	68
2.3	HTTP Methods and REST.....	69
2.4	HTTP Status Codes and REST	69
2.5	Unique Identifiers	72
2.6	ID Encoding	72
3	Architecture and Namespace.....	73
4	System Flow	76
4.1	Service Discovery	76
4.2	Persistent Connections.....	77
4.3	Authentication	77
4.4	Access Restrictions	78
4.5	Setting Configurations	78
4.6	Getting Configurations.....	79
4.7	Getting Capabilities.....	80
4.8	Uploading Data.....	80
4.9	Receiving Data.....	81
4.10	Operations	81
4.11	Diagnostics.....	82
4.12	Response Status	82
4.13	Processing Rules	83
5	XML Modeling.....	83
5.1	File Format.....	83
5.2	Data Structures.....	83
5.3	Lists	83
5.4	Capabilities	84
6	Custom Services & Resources	85
7	Interface Design	85
7.1	Protocol	85
7.2	Hostname.....	86
7.3	Port	86
7.4	URI	86

7.5 Query String 86

7.6 Resource Description 86

8 Standard Resource Descriptions 88

8.1 index 88

8.2 indexr 88

8.3 description..... 88

8.4 capabilities 88

Appendices 88

8.5 Schemas 88

APPENDIX I.B – IP Media Device API Specification Version 1.0..... 94

1 Overview 94

2 Scope 94

3 Problem Definition 94

4 Conformance 95

4.1 Service Requirements 95

4.2 Resource Requirements 95

5 Media Streaming 99

5.1 Streaming with RTP and RTSP 99

5.2 Streaming using HTTP Server Push..... 103

6 Common Data Types..... 103

6.1 Built-in Types 103

6.2 ReceiverAddress 104

6.3 TimeBlockList 104

7 Service Command Details..... 105

7.1 /System 105

7.2 /System/Storage 111

7.3 /System/Storage/volumes 112

7.4 /System/Network 114

7.5 /System/IO 129

7.6 /System/Audio 133

7.7 /System/Video 134

7.8 /System/Serial 142

7.9 /Diagnostics..... 144

7.10 /Security..... 145

7.11 /Security/AAA 145

7.12 /Streaming 147

7.13 /PTZ..... 156

7.14 /Custom/MotionDetection 167

7.15	/Custom/Event	172
APPENDIX II - IP Interoperability Implementation Based on Web Services		185
INTRODUCTION		185
1	Scope	186
2	Normative references	187
3	Terms and Definitions	189
3.1	Definitions	189
3.2	Abbreviations	190
4	Overview	192
4.1	Web Services	192
4.2	IP configuration	193
4.3	Device discovery	194
4.4	Device management	194
4.5	Imaging configuration	197
4.6	Media configuration	197
4.7	Real-time streaming	201
4.8	Event handling	202
4.9	PTZ control	202
4.10	Video analytics	203
4.11	Storage	205
4.12	Security	205
4.13	Client code examples	205
5	Web Services frame work	207
5.1	Services overview	207
5.2	WSDL overview	209
5.3	Namespaces	210
5.4	Types	212
5.5	Messages	213
5.6	Operations	213
5.7	Port Types	216
5.8	Binding	216
5.9	Ports	216
5.10	Services	216
5.11	Error handling	216
5.12	Security	220
6	IP configuration	222
7	Device discovery	223
7.1	General	223

7.2	Modes of operation	223
7.3	Discovery definitions	224
7.4	Remote discovery extensions	227
8	Device management.....	234
8.1	Capabilities.....	234
8.2	Network.....	237
8.3	System.....	250
8.4	Security.....	264
8.5	Input/Output (I/O)	274
8.6	Service specific fault codes.....	276
9	Imaging configuration.....	281
9.1	Imaging settings.....	281
9.2	Service specific fault codes.....	288
10	Media configuration	289
10.1	Audio and video codecs	289
10.2	Media Profile.....	290
10.3	Video source	307
10.4	Video source configuration	307
10.5	Video encoder configuration	311
10.6	Audio source	316
10.7	Audio source configuration	317
10.8	Audio encoder configuration.....	321
10.9	Video analytics configuration.....	326
10.10	Metadata configuration	330
10.11	Stream URI.....	334
10.12	Snapshot	336
10.13	Multicast	336
10.14	Synchronization Points.....	337
10.15	Service specific fault codes.....	338
11	Real time streaming	340
11.1	Media stream protocol	340
11.2	Media control protocol.....	351
11.3	Error Handling	355
12	Event handling	355
12.1	Basic Notification Interface	355
12.2	Real-time Pull-Point Notification Interface	358
12.3	Notification Streaming Interface.....	360
12.4	Properties	360

12.5	Notification Structure	362
12.6	Synchronization Point.....	370
12.7	Topic Structure.....	370
12.8	Get event properties.....	373
12.9	SOAP Fault Messages.....	374
12.10	Notification example	374
12.11	Service specific fault codes	380
13	PTZ control	380
13.1	PTZ Model	381
13.2	PTZ Node	383
13.3	PTZ Configuration	384
13.4	Move Operations	388
13.5	Preset operations	394
13.6	Home Position operations	398
13.7	Auxiliary operations	400
13.8	Predefined PTZ spaces	401
13.9	Service specific fault codes	404
14	Video analytics	407
14.1	Scene Description Interface.....	407
14.2	Rule interface	416
14.3	Analytics Modules Interface	424
14.4	Service-specific fault codes.....	429
15	Security.....	431
15.1	Transport level security	431
15.2	Message level security.....	432
	Annex II.A (informative) Notification topics.....	433
A.1	Media configuration topics	433
	Annex II.B (informative) Scene descriptions	437
	Annex II.C (normative) Video IP Network Interface XML Schemata.....	439
C.2	Device Management Service WSDL.....	448
C.3	Imaging Service WSDL.....	459
C.4	Media Service WSDL	466
C.5	PTZ Service WSDL	512
C.6	Remote Discovery Proxy Services WSDL	530
C.7	Common Network Video Schema	533
C.8	Topic Namespace XML.....	596
C.9	Event WSDL.....	606
	Bibliography.....	618

APPENDIX III - IP Interoperability Implementation Based on another Specification 619

Foreword

This document (EN 50132-5-2:2011) has been prepared by CLC/TC 79, Alarm systems.

The following dates are fixed:

- latest date by which this document has (dop) 2012-10-31
to be implemented at national level by
publication of an identical national
standard or by endorsement
- latest date by which the national (dow) 2014-10-31
standards conflicting with this
document have to be withdrawn

This document partially supersedes EN 50132-5:2001 and introduces the new video transmission methodology based on IP protocols into the standard series.

EN 50132 consists of the following parts, under the generic title *“Alarm systems – CCTV surveillance systems for use in security applications”*:

Part 1	System requirements
Part 5-1	Video transmission – General Video Transmission Performance Requirements
Part 5-2	IP Video Transmission Protocols
Part 5-3	Video transmission – Analog and Digital Video Transmission
Part 7	Application guidelines

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

Introduction

The European Electrotechnical Standardisation Organisation for Alarm Systems together with many governmental organisations, test houses and equipment manufacturers has defined a common framework for Surveillance Video Transmission in order to achieve interoperability between products.

This Video transmission standard is divided into 3 independent parts and sections:

Part 1: General video transmission performance requirements

Part 2: IP Video transmission protocols

Part 3: Analog and digital video transmission

Each part offers its own clauses on scope, references, definitions, requirements

The purpose of the transmission system in a closed circuit television (CCTV) installation is to provide reliable transmission of video signals between the different types of CCTV equipment in security, safety and monitoring applications.

Today CCTV surveillance systems reside in security networks using IT infrastructure, equipment and connections within the protected site itself.

This standard EN 50132-5-2 on network video ip protocol and interface definitions for video devices in surveillance applications is based on the general requirements for video transmission of EN 50132-5-1. Part 1 defines minimum IP connectivity requirements, basic video streaming, stream control, eventing, discovery and description functions, where this Part 2 is based on. Additionally Part 1 establishes minimum performance requirements, including interconnection, network video devices. EN 50132-7 Application Guidelines give guidance for Video Surveillance Installations in general, but takes special care of video ip networks. Any video transmission network should be designed in accordance with these standards. With prEN 50132-5-3 a detailed standard for non IP video transmission is defined. For signal and performance requirements on analog and uncompressed digital video transmission and interfaces this part 3 of the standard series shall be applied.

1 Scope

This European Standard introduces an IP network interface for devices in surveillance applications. In this part of the standard a network protocol is specified for the full interoperability of video devices. EN 50132-5-1 specifies the minimum network performance standards and general compliance to existing, well-known international network standards. On top of these basic layers protocols are defined to accomplish the full interoperability of video devices. In surveillance applications IP video devices have to use standardized protocols to accomplish following functionality: video streaming, stream control, event handling, discovery, capability description, device management, PTZ control, auxiliaries and other functions.

This European Standard consists of 3 sections. The first section defines protocol requirements to be fulfilled by any high-level IP video device interface.

The following two sections – Annex I and Annex II- define two alternative protocols, one is based on HTTP and REST services and the second is based on Web Services.

In the future a third high-level IP protocol may be defined in Annex III, which grants compatibility to the requirements of this standard series. Today no third IP video protocol implementation is available.

Some areas of this transmission standard are covered by more than one approach, e.g. UPnP, ZeroConf and WS-Discovery.

The network protocols recommended and defined by this Video Transmission Standard are selected with a sense for future relevance and further extensions.

Video transmission equipment may be combined with additional functions, e.g. for audio or metadata transmission.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 50132-1, *Alarm systems — CCTV surveillance systems for use in security applications — Part 1: System requirements*

EN 50132-5-1, *Alarm systems — CCTV surveillance systems for use in security applications — Part 5-1: Video transmission — General video transmission performance requirements*

EN 50132-7, *Alarm systems — CCTV surveillance systems for use in security applications — Part 7: Application guidelines*

3 Terms, definitions and abbreviations

3.1 Definitions

For the purposes of this document, the following terms and definitions apply.

3.1.1

adapter

component (hardware or software) offering two interfaces that enable something to be used in a different way from which it was intended, in order to make different components or applications compatible

3.1.2

agent

process e.g. software application on a network device or node that is responsible for all SNMP messages initiating traps and informs on detecting exceptional conditions in the network device and accepting requests from the SNMP manager with a replay of the requested data

3.1.3

analog

form of information that is represented by a continuous and smoothly varying amplitude or frequency changes over a certain range

3.1.4

analog video

video signal made of a continuous electrical signal

3.1.5

Application Program Interface (API)

set of interfaces for developers to interact with a component or application

3.1.6

Abstract Syntax Notation One (ASN.1)

description language used to describe SNMP data types in machine architecture-independent format

3.1.7

bandwidth

property of networks to describe the amount of data that can be carried from one point in the network to another in a given time period, usually a second, affected in video surveillance by frame rate, image resolution, compression ratio, image noise, complexity detail of a monitored scene

3.1.8

binding

associating an interface, a valid data format, and a concrete protocol to ensure smooth message transmission

3.1.9

camera presets

pre-defined camera angles, locations, and distances of PTZ cameras assigned with a number

3.1.10

capability

named piece of functionality (or feature) that is declared as supported or requested by an agent

3.1.11

capturing

process of transferring video from one source to another for use on a digital video device, network or storage, e.g. conversion of analog to digital

3.1.12

CCTV network

video surveillance system based on an ip video network used within a protected site

3.1.13

channel

one or more streams of video, audio and/or metadata that together constitute a unique entity for the purpose of surveillance

3.1.14

Common Intermediate Format (CIF)

video format used in video conferencing systems that supports both NTSC and PAL signals. CIF is part of the ITU H.261 video conferencing standard

3.1.15

codec

abbreviation of compression/decompression algorithm, used to encode and decode, or compress and decompress data, such as video

3.1.16

component

software or hardware object, meant to interact with other components, encapsulating certain functionality or a set of functionalities with clearly defined interfaces and conforming to a prescribed behavior common to all components within a standard

3.1.17

configuration policy

in SNMP one or more security groups including the assigned users or communities

NOTE SNMP agents that will be configured using the new policy should support the security models and security levels defined for the security groups selected. For example, a policy containing an SNMPv3 user configuration should not be configured on an agent that supports only SNMPv1 and/or SNMPv2c.

3.1.18

connectionless protocols

individual routing of packets between network correspondents without pre-establishing a "connection"

EXAMPLE IP protocol, UDP

3.1.19

connection-oriented protocols

transmission of packets between network correspondents along predetermined routes which are established at connection setup

EXAMPLE TCP

3.1.20

DES encryption

Data Encryption Standard as privacy protocol used to protect messages in transit across networks

3.1.21

Device Architecture 1.0 (DA)

UPnP device architecture version 1.0

3.1.22

device capability

set of video transmission device functions (at least 1) aggregated to support CCTV system or video transmission client usage

3.1.23

device description

formal definition of a network device, expressed in XML syntax, specified by a vendor

3.1.24

device function

non-decomposable operational property of a video transmission device for example video stream control

3.1.25

digital

Information coded in discrete, separate pulses or signal levels

3.1.26

discovery

act of locating a network device or machine-processable description of a service-related resource that may have been previously unknown and that meets certain functional criteria

3.1.27

discovery service

service that enables agents to retrieve services-related resource description

3.1.28

Domain Name System (DNS)

protocol that enables hierarchical naming system in a network for identification and resolving symbolic names such as domain or computer names for example translate <http://Videoserver1> or www.upnp.org into IP addresses

3.1.29

Document Type Definition (DTD)

document defining the format of the contents presented between the tags in an XML document, and the way they should be interpreted by the application reading the XML document

3.1.30

Dynamic Host Configuration Protocol (DHCP)

protocol to automatically provide IP addresses and other network configuration information to network nodes

3.1.31

Digital Video Recorder (DVR)

network video device recording multiple analog video channels onto a hard disk in digital format, which allows viewing, replay and management remotely via a VT client

3.1.32

elementary stream (ES)

single video stream of several MPEG-4 component carriers

3.1.33

eEmbedded device

device based on an embedded hardware platform mostly without the use of a general purpose operation system with a limitation to a core set of services only needed and implemented for a specific purpose, e.g. a DSP based video encoder device with an IP stack implementation for network connectivity

3.1.34

encryption

alteration of transmitting information to protect it from unauthorized tapping e.g. by AES encryption

3.1.35

event

notification of one or more changes in state variables sent by a network device

3.1.36

eventing

exchange of specially-formatted messages describing events of a event server e.g network device

3.1.37

frame

full frame of video as combination of two image fields interlaced together

3.1.38

full Transport Stream (TS)

piece-wise constant rate MPEG-4 video transport stream that is fully compliant with 2.4.2.2 of ISO/IEC 13818-1 characterized by its "even spaced" TS packets

3.1.39

High Definition(HD)

video image quality at HDTV level with a vertical resolution from 720p to 1080i and higher and an aspect ratio of 16:9

3.1.40

high level IP-interface

programmational application interface offering full interoperability for all services based on the same principle or technology

3.1.41

ideal network conditions

conditions of a network used for testing and validation of standard compliance

NOTE The effective network bandwidth, capacity, delay, jitter, loss should be substantially better than the aggregated bandwidth of the video streams under test, and there are no additional video transmission devices competing for the available network resources at the time of test.

3.1.42

identifier

associated with each object which uniquely identifies the object e.g. for SNMP in the global tree of objects

3.1.43

Internet Engineering Task Force (IETF)

standards body that forms Working Groups to develop technology for the Internet community

3.1.44

I-frame

intraframe of an image sequence of differential coded frames

3.1.45

Internet Protocol video (IP video)

representation of sequential image information in digital (discrete level) formats that are transferred using IP data packets (datagrams) including associated protocols for discovery, description, streaming, stream control, eventing, control and configuration of video network devices

3.1.46

interoperability

ability of communication of systems and units to provide services and to accept services from other systems and units, in order to use the services for efficient operation; ability for information or services to be exchanged directly and smoothly between providers and consumers

3.1.47

Internet Protocol (IP)

basic connectionless network-layer protocol

3.1.48

IP camera

device capturing and transmitting live video images over an IP network allowing remote viewing, recording, and management

3.1.49

IP video

transmission of video signals over an IP network

3.1.50

IP video interface

software point of communication for IP video between a device and the network

3.1.51

IP video network

collection of video transmission devices connected to each other allowing to communicate with each other, share resources and information over a variety of connection protocols

3.1.52

IP video packet transmission

process of addressing, transferring, and controlling IP video packets passing through switching points in a network

3.1.53

IP video surveillance

video surveillance system allowing analog and/or digital IP video to operate over a standard IP network by transmitting real-time video streams

3.1.54

IP video system

combinations of equipment, software, and processes that are used to gather video streams from various sources, organized into channels, creating or receiving digitized video signals, compressing digital video, packetizing video, distributed through various communication systems, managing the transfer of packets through a network, receiving and re-sequence the data packets, and rendering into a form that can be viewed by operators allowing them to select, monitor and control video on one or more types of presentation devices

3.1.55

jitter

variation in a network delay that is perceived by the receiver of each packet

3.1.56

keyframe

see I-frame

3.1.57

latency

delay in the response of far end participants, often a result of network congestion and geographic distance

3.1.58

link

relationship between two network nodes when one resource refers to the other resource e.g. by the means of a URI

3.1.59

manage

view, control, provision, update, monitor, health check, notify components of an ip system, e.g. by a centralized application, called management system

3.1.60

managed objects

parameters and values of network devices that can be read by the SNMP manager, like alarm status, control relay status, system uptime, etc defining in SNMP terms, every network device as a set of these managed objects

3.1.61

Management Information Base (MIB)

formal description of a set of objects that can be managed via SNMP as data structure describing SNMP network elements as a list of data objects, implemented by an agent, described in a MIB document, written in the ASN.1 data description language

NOTE To monitor SNMP devices, the SNMP manager will compile a MIB file for every different video transmission device in the network.

3.1.62

message authentication

assessment of an entity about the certainty that the purported sender of the message is in fact the sender of that message

3.1.63

Message Digest 5 (MD5)

standard encryption algorithm that generates out of data input such as a message of arbitrary length an output of a 128-bit fingerprint or message digest for the purpose to detect any modifications made to the input data when transmitted by recalculating the fingerprint or digest in a similar concept to CRC

NOTE The MD5 algorithm is used as part of the SNMPv3 security subsystem.

3.1.64

message

basic unit of communication containing the data to be transmitted between network nodes such as client and server

3.1.65

messaging

exchange of messages, which are specially formatted data packets, describing events, commands, status information, requests, replies, etc of a messaging source to a subscribing or listening client

3.1.66

MIB extensions

extension of a standard MIB for a single set of related management entities to include proprietary objects in SNMP

3.1.67

MIB family

family of SNMP variables consisting all of the leaf MIB variables with the same immediate parent node, or root (the object identifier without the instance information)

EXAMPLE In MIB-II the following variables form a single family since they are all children of ifEntry (1.3.6.1.2.1.2.2.1).

3.1.68

MIB view

set of MIB objects that are accessible in a given user/group configuration in SNMP

3.1.69

MIB-II

current standard for MIB definition in SNMP

3.1.70

MIB-CCTV

SNMP MIB Object under the Network Management Private Enterprise Code with the Prefix iso.org.dod.internet.private.enterprise.cctv 1.3.6.1.4.1.31373

3.1.71

Moving Picture Experts Group (MPEG)

working committee that defines and develops industry standards for digital video systems, specifying the data compression and decompression processes and how they are delivered on digital video systems

3.1.72

MPEG/H.264 level

amount of capability that a MPEG or H.264 profile can offer ranging from low level (low resolution) to high level (high resolution)

3.1.73

MPEG/H.264 profile

particular implementation or set of required features and tools that enable a particular application

3.1.74

Multipurpose Internet Mail Extension (MIME)

standard system for identifying the type of data streamed across network including graphics, photos, sound, video and formatted text documents

3.1.75

namespace document

information resource in UPnP identified by a namespace URI, e.g www.upnp.org, that contains useful information, machine- and/or human-usable and readable about definitions in a particular domain

3.1.76

network architecture

framework and technology foundation for the design, building and managing of a communication network, typically in a layered structure dividing the communication tasks into a number of smaller parts, each part accomplishing a particular sub-task and interacting with the other parts in a small number of well-defined ways

3.1.77

network connectivity

physical (wired or wireless) and logical (protocol) connection of multiple devices or a single device to a network, such as a ip video network

3.1.78

network hub

network device that can only send or receive at one time in the so-called half-duplex mode

3.1.79

network interfaces

point of communication between a device and the network

3.1.80

network node

grouping of one or more network components which provides network related functions, administered as a single entity

3.1.81

network protocol

defined rules and procedures for the network communications

3.1.82

network switch

network device with the ability to send and receive data at the same time using the so-called full-duplex mode

3.1.83

Next-Generation Network (NGN)

generic term used to describe packet-based networks converging traffic such as audio, video, and data with respect to the appropriate quality of service realized by special-purpose network technology

3.1.84

National Television Standards Committee (NTSC)

standardized video signal format used in the United States, delivering 29.97 frames per second

3.1.85

Network Video Recorder (NVR)

network video device recording multiple video streams onto a hard disk in digital format, which allows viewing, replay and management remotely via a VT client

3.1.86

Organization for the Advancement of Structured Information Standards (OASIS)

nonprofit, international consortium whose goal is to promote the adoption of product-independent standards for information formats such as Extensible Markup Languages (XML), Hypertext Markup Language (HTML) etc.

3.1.87

Object Identifier (OID)

unique identifier of a SNMP MIB object in the global tree of objects if form of sequence of elements, as specified by the standard RFC 1442, that uniquely identifies each object from a large hierarchy of identifiers

3.1.88

OID subtree

part of a MIB tree that is specific to a given entity or domain

EXAMPLE The subtree for the domain of CCTV applications has 1.3.6.1.4.1.323123 as root OID.

3.1.89

Open Network Video Interface Forum (ONVIF)

open industry forum for the development of a global standard for the interface of network video products

3.1.90

Open Systems Interconnection (OSI)

complete suite of network routing protocols developed by ISO including routing protocols between the different layers of the system

3.1.91

packet buffer

memory space for storing a packet awaiting transmission or for storing a received network packet

3.1.92

Packet Internet Gopher (PING)

ICMP (Internet Control Message Protocol) echo request to determine whether a device on an IP network is online

EXAMPLE Used as basic network program to diagnostically check the status of a network host or device to see if a particular network address (IP address or host name) is occupied or not, or if the host at that address is responding normally.

3.1.93

Phase Alternating Line (PAL)

analog color encoding system used in television systems in Europe and in many other parts of the world, defining the video signal, using 625 TV lines per frame, at a refresh rate equal to 25 frames per second standardized in prEN 50132-5-3

3.1.94

payload

true message data itself without protocol information

3.1.95

pixel (picture element)

one of the many elements that make up a digital image, representing the color and intensity

3.1.96

Polling

data communication for downloading most recent data in a regular interval

3.1.97

principle

fundamental rule applicable to a large number of situations and variations

3.1.98

Protocol Data Unit (PDU)

expression that describes the basic information element of a given protocol; for example, SNMP has various PDUs, such as get and get-next, describing protocol operations encoded in the form of messages before being sent to another protocol entity

3.1.99

protocol error

result and answer of an incorrectly formed protocol message, which may consist of illegal header values or payload, received unexpectedly or after a certain timeout

EXAMPLE HTTP and RTSP define a set certain of standard status codes to notify about protocol errors.

3.1.100

Physical Security Industry Alliance (PSIA)

physical security industry alliance for the development of a global standard for the interface of network video products.

3.1.101

Quality of Service (QoS)

software-based ability to guarantee the required level of network resources for real-time video traffic; a major performance indicator for networks especially for devices such as ip cameras, access control, and building management or security systems

3.1.102

recording

single container for a set of video, audio and metadata tracks with an endless timeline holding data at certain time frames or gaps without any information from any kind of real-time video source or input including associated non-video data stored on any kind of media

3.1.103

redundancy

ability to ensure connectivity in the case of a failed link or device

3.1.104

representation

data about the actual state of a resource or component

3.1.105

Request for Comment (RfC)

documents maintained by the IETF standards body containing standards in various stages of completion

3.1.106

routing redundancy

ability of a network when two routers have physical connections to the same subnet, where one is acting as the master router and the other as a backup router in case the master fails

3.1.107

RTCP packet

Real-Time Transport Control Protocol (RTCP) control packet that consists of a fixed header part similar to that of RTP data packets and structured elements that vary depending upon the RTCP packet type, as described in RFC3550

3.1.108

RTP payload

data transported in a packet by using Real-Time Transport Protocol (RTP), as described in RFC3550

3.1.109

RTP session

association among a set of participants who are communicating by using the Real-Time Transport Protocol (RTP), maintaining a full, separate space of Synchronization Source (SSRC) identifiers, transmitted to the same destination IP address and UDP port

NOTE Typically, there is a one-to-one mapping between RTP streams and RTP sessions, but it is possible for multiple RTP streams to use the same RTP session (port multiplexing). The associated RTCP traffic is also part of that RTP session although the packets are sent to the next higher UDP port number.

3.1.110

RTP stream

video stream that is encapsulated in RTP

NOTE All of the RTP packets have the same SSRC and are transmitted on the same RTP session.

3.1.111

RTSP session

session typically consisting of a VT client creating one or more RTP Sessions (SETUP) with a VT server, starting the stream with PLAY or RECORD, and closing the RTSP Session

3.1.112

Secure Hash Algorithm (SHA1)

algorithm which generates out of input data like a message of less than 264 bits in length a 160-bit hash code or fingerprint designed in a way that it hardly possible to find a matching text string

Service abstract resource that represents capabilities to perform tasks

3.1.113

service description

formal definition of a logical network service about its interface, expressed in in XML syntax

3.1.114

service interface

abstract boundary exposed defining types of messages that are involved in interacting with the service including a logical grouping of operations independent of transmission protocol and data format

3.1.115

Simple Network Management Protocol (SNMP)

protocol for managing IP network devices

3.1.116

Simple Service Discovery Protocol (SSDP)

multicast discovery and search mechanism that uses a multicast variant of HTTP over UDP

3.1.117

SNMP access restriction

restriction of access to a SNMP agent by configuring a community string based upon the source address of requests

NOTE If address restriction is enabled, only managers included in the list of IP addresses are able to query the agent using the community string.

3.1.118

SNMP agent

hardware device or software component that reports to a SNMP manager usually being a subsection of a larger device

3.1.119

SNMP community string

SNMP security password for reading, writing and issuing Trap messages

3.1.120

SNMP community

SNMPv1 or SNMPv2c configured request name used when making requests to agent. A54

3.1.121

SNMP event

change of status in a managed object e.g. generating traps for SNMP inform

3.1.122

SNMP inform

notification containing the same information as a trap, but including the sending of an additional verification response back to the agent

3.1.123

SNMP manager

monitoring applications issuing requests to agents, receiving responses, Trap- and Inform messages

3.1.124

SNMP notification targets

SNMP managers or agents that are selected to receive information from SNMP events, sent either as traps or Informs

3.1.125

SNMP security level

configured user level with or without authentication and/or with or without privacy

3.1.126

SNMP trap

message issued by a SNMP agent that reports an event as one-way communication to a SNMP manager

3.1.127

SNMPv3 simple network management protocol version 3

SNMP implementations according to the RFCs 3410 and 3418, providing a full administrative framework for authorization, access control, etc. including a remote configuration/ administration MIB

3.1.128

SNMPv3 USM User

user configured on an SNMP agent used when making a SNMPv3 request to this agent

3.1.129

streaming

process of sending video over a network to allow instant operation as the video is received, rather than requiring the entire file to be downloaded prior to operation

3.1.130

switch redundancy

ability of a network node to consider what action to be taken in the case of a link-down situation by determining which network ports are forwarding during failure, ensuring the best possible connection by using Spanning Tree Protocol (STP), Rapid STP (RSTP) or Fast-Uplink STP

3.1.131

system level device

device based on a general purpose operation system offering a broad range of services, e.g. a PC based DVR or NVR including general SNMP support

3.1.132

TCP ports

in computer networking an application- or process-specific software construct that acts as a communications endpoint used by Transport Layer protocols

EXAMPLE Transport Layer protocols, such as TCP, specify a source and destination port number in their packet headers next to the sender and receiver IP address.

3.1.133

Transmission Control Protocol (TCP)

connection-oriented transport-layer protocol establishing a connection between host and recipient, guaranteeing delivery and reliability through retransmission

3.1.134

TTL time-to-live

specified length of time that information e.g. DNS is stored in a cache and after that the information is deleted, e.g. entry from the DNS name server's cache

3.1.135

Universal Plug and Play (UPnP)

set of network protocols allowing devices to connect seamlessly and to simplify implementation of networks by defining and publishing UPnP device control protocols built upon open, Internet-based communication standards

3.1.136

UPnP Device Architecture (DA)

standard for the usage of devices and services in a generic manner, representing the core of UPnP upon which the device and service specifications are built

3.1.137

UPnP Device Control Protocol (DCP)

application level protocol designed for communication with and between network devices providing a framework for integration, controlling and monitoring, providing a framework for integrating based on a generic, object-oriented protocol which supports connection and connectionless communication between resources with an extensible set of methods

3.1.138

UPnP device description document

formal definition of a logical device, expressed in the UPnP Template Language

3.1.139

UPnP device description

formal definition of a logical device, expressed in the UPnP Template Language, written in XML syntax, specified by a vendor by filling in the placeholders in a UPnP Device Template, including, e.g. manufacturer name, model name, model number, serial number, and URLs

3.1.140

UPnP template language

written in XML syntax, specified by a vendor by filling in the placeholders in a UPnP Device Template, including, e.g. manufacturer name, model name, model number, serial number, and URLs

3.1.141

UPnP device schema

definition of elements and attributes used in UPnP Device Templates, written in XML syntax and derived from XML Schema Part 1: Structures and Part 2: Datatypes

3.1.142

UPnP device template

template listing the device type, e.g. SecurityCamera, the required embedded devices and services, written in a XML syntax, derived from the UPnP Device Schema

3.1.143

UPnP device type

standard type expressed by urn:schemas-upnp-org:device and followed by its unique name assigned by a UPnP Forum or additional vendor type denoted by urn:domain-name:device

3.1.144

UPnP service description document

formal definition of a logical device, expressed in the UPnP template language

3.1.145

UPnP service template

XML template listing action names, parameters for those actions, state variables, and the properties of those state variables, written in XML syntax AC1Text deleted AC1

3.1.146

User Datagram Protocol (UDP)

connectionless transport layer protocol used to send messages as part of the IP suite of protocols with low overhead, not using Acknowledging (ACK) or error-checking (CRC), e.g. SNMP messages, not guaranteeing the delivery of a data packet with the advantage of using fewer network resources than TCP, making it more suitable for transporting streams of data or large amount of status messages

3.1.147

Variable Binding (VarBind)

data field of a SNMP GetResponse or Trap PDU, listing a managed object and its current value

3.1.148

video encapsulation

mechanism for transporting video payload and metadata in Real-Time Transport Protocol (RTP) packets

3.1.149

video frame

single image shown as part of a sequence of images in a video stream

3.1.150

Video Device Profile

device configuration for video streaming mapping an imaging source to a codec, compression and quality setting

NOTE A VTD may offer different profiles depending on its capabilities in different streams for a single video source.

3.1.151

Video Management System (VMS)

system managing, accessing and controlling the video transmission devices in real time in the video surveillance environment

3.1.152

Video Transmission Device (VTD)

video device with at least one IP network interface handling video and typically coding or decoding video

EXAMPLE encoders, decoders, NVR systems, video management systems

3.1.153

Video Transmission Client (VT Client)

video network device acting as client or receiver requesting video streams, status messages, etc. from a connected VTD server for the purpose of video recording, display, etc.

EXAMPLE A VTD Client can be a Video Management System Workstation or a video decoder.

3.1.154

Video Transmission Server (VT Server)

video network device acting as server or sender, encoding and sending video to a connected VTD Client, providing video streams, video status information, etc.

EXAMPLE A VTD Server can be an IP network camera or a video encoder.

3.1.155

web server

specialized service, which allows Web browsers or other clients to retrieve data and files from servers connected to a network by listening via http connections

3.1.156

Web Service Definition Language (WSDL)

XML-based standard for specifying message-based distributed services containing either document- or procedure-oriented information

3.1.157

Web service

software entity that responds to SOAP messages capable of being defined, located via the Internet protocol, and interacting with other software applications, identified by a Uniform Resource Identity

3.1.158

XML schema

document that describes, in a formal way, the syntax elements and parameters of a web language, designed by W3C to replace DTD

3.1.159

XSD (XML Schema Definition)

same as XML Schema

3.1.160

Extensible Stylesheet Language (XSL)

suite of XML languages developed by W3C

3.1.161

Zeroconf (Zero Configuration Networking)

set of techniques that automatically create a usable IP network without configuration or special servers

NOTE In this standard only the service discovery is referred to.

3.2 Abbreviations

API	Application Program Interface
ASN.1	Abstract Syntax Notation One
CIF	Common Intermediate Format
CoDec	Compression and Decompression
COTS	Custom off the shelf
CRUD	Create, read, update, and delete
DCP	Device Control Protocol
DA	Device Architecture
DCP	Device Control Protocol
DNS	Domain Name System
DTD	Document Type Definition
DHCP	dynamic host configuration protocol
DVR	Digital Video Recorder
ES	elementary stream
GOP	group of pictures
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HTTPMU	HTTP (Multicast over UDP)
HTTPU	HTTP (Unicast over UDP)
HD	high definition
ICMP	Internet Control Message Protocol
^[AC1] IETF	Internet Engineering Task Force: standards body that forms Working Groups to develop specifications ^[AC1]
IP	Internet Protocol. basic connectionless network-layer protocol.
MD5	Message Digest 5
MIB	Management Information Base
MPEG	Moving picture experts group
MIME	multipurpose Internet mail extension
NGN	Next-Generation Network
NTSC	National Television Standards Committee
NVR	Network Video Recorder
OASIS	Organization for the Advancement of Structured Information Standards
OID	object identifier
ONVIF	Open Network Video Interface Forum
OSI	Open Systems Interconnect
PING	Packet Internet Gopher
PAL	Phase Alternating Line
Pixel	Picture Element
PDU	Protocol Data Unit
PSIA	Physical Security Industry Alliance
QoS	Quality of Service
RFC	Request for Comment
RTCP	Real-Time Transport Control Protocol
RTP	Real-Time Transport Protocol
SSRC	Synchronization Source
SHA1	Secure Hash Algorithm
SNMP	Simple Network Management Protocol

SSDP	Simple Service Discovery Protocol
SNMPv3	Simple Network Management Protocol version 3
SOAP	Simple Object Access Protocol
TCP	Transmission Control Protocol
TS	full transport stream
TTL	Time-to-live
UDA	UPnP Device Architecture
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
VarBind	SNMP variable binding
VMS	video management system
VTD	Video Transmsion Device
WSDL	Web Service Definition Language
WS	Web Service
W3C	World Wide Web Consortium
XML	Extensible Markup Language
XSD	XML Schema Definition
XSL	Extensible Stylesheet Language
Zeroconf	Zero Configuration Networking

4 Video Transmission network architecture (informative)

4.1 General

To achieve interoperability between connected digital video devices in the CCTV network, a common set of building blocks based on existing standards is needed as a basis to develop the video transmission standards. Table 1 shows the specific functional components and technology ingredients that are covered in the video transmission standards.

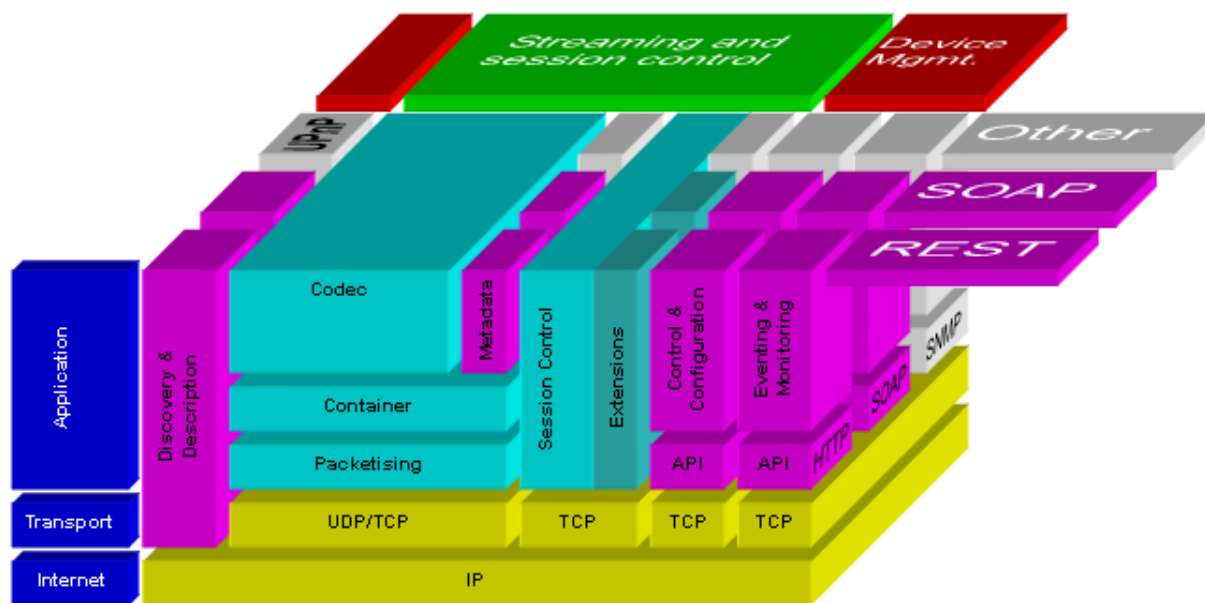


Figure 1 – Overview IP Video standard protocol

Figure 1 illustrates these functional components within the networking architecture of the video transmission standards. The video transmission standards define usage of these functional components to ensure interoperability among device classes defined in Clause 5. A brief overview of each functional component follows in the subsequent sub clauses.

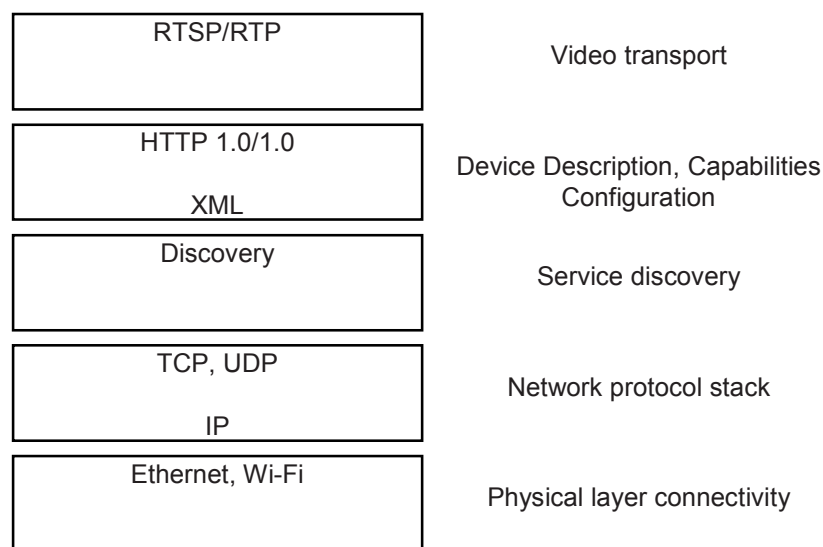


Figure 2 – Functional Protocol Layers

4.2 Networking and connectivity

4.2.1 General

The IP video protocol suite is the foundation for networking and connectivity for VT devices in the digital CCTV network. IP also provides the underlying network communications for applications in security. Based on industry-standard specifications from the IETF, IP is implemented and supported in a wide range of devices. IP has the following advantages for use by VT devices:

- IP has demonstrated that it allows applications to run over different network topologies transparently;
- IP allows connecting every device to a CCTV network or even to a security network;
- IP connectivity solutions are widely used and are cost-effective. The most common ones are Ethernet (802.3i and 802.3u) and wireless technologies (802.11n, 802.11b, and 802.11g) for devices in the CCTV security networking environment.

The following sub clause specifies the detailed protocols to enable interoperability between VT devices in the digital CCTV network. In addition, the CCTV network environment requires supporting network infrastructure, such as access points, bridges, gateways, routers, and switches.

These non-normative devices are referred to in this standard as network infrastructure devices. EN 50132-5-1 provides performance criteria for video network streaming and infrastructure devices to facilitate a good user experience and interoperability for video transmission devices.

4.2.2 Network streaming performance: quality of service

Video surveillance applications on IP networks benefit from high network performance and a good quality of service (QoS) to optimize the way shared network resources are allocated among different surveillance applications, functions and devices.

All applications running on different video transmission devices have according to the nature of IP networks an equal opportunity to transmit data frames. Video surveillance is according to EN 50132-5-1 sensitive to delay, latency variations and bandwidth reductions. By stream limitations or prioritized streaming ip video devices define how the video packets access network resources. In contrast to broadcasting applications with an unknown number of clients, ip video in security does not define any QoS protocol today, The QoS in a surveillance network is guaranteed by the proper setup and configuration at design time for a certain number of operators or receivers and by using the capabilities of a video management system (VMS) taking care of all video streaming and requests of the single video transmission devices. Requirements on the quality and performance on streaming are listed in EN 50132-5-1

4.3 Device discovery and description

Device discovery and description enables a device on the CCTV network to discover the presence and capabilities of the device itself and other devices on the network and collaborate with these devices in a uniform and consistent manner. Next to ZeroConf and WS-Discovery, the UPnP device architecture, version 1.0, addresses all of these needs and simplifies device networking in the CCTV network. For this reason device discovery and description is part of the IP solution for VT devices. Clause 9 specifies the detailed protocols to enable interoperability between VT devices in the digital CCTV network.

4.4 Video media types and payload formats

Video formats describe how content is encoded and formatted for transport and final rendering on the CCTV network. The video formats listed in EN 50132-5-1 are intended to achieve a baseline for network interoperability while encouraging continued innovation in video codec technology.

The EN 50132-5-1 clause 'Video Media Formats' specifies the detailed protocols to enable interoperability between different VT devices in the digital CCTV network.

4.5 Video transport

Video transport defines how content travels across the CCTV network. VT devices that offer or receive video streams across the CCTV network shall support the streaming protocols. Clause 8 specifies the detailed protocols to enable interoperability between VT devices in the digital CCTV network.

4.6 Eventing and health check

In security providing video streams only is not sufficient: In Clause 10 and 11 the need to monitor the health status of video transmission devices and notify events is specified.

5 The Building block of existing standards (informative)

To achieve interoperability between connected digital video devices in the CCTV network, a common set of building blocks based on existing standards is needed as a basis to develop the video transmission standards as shown in the picture below.

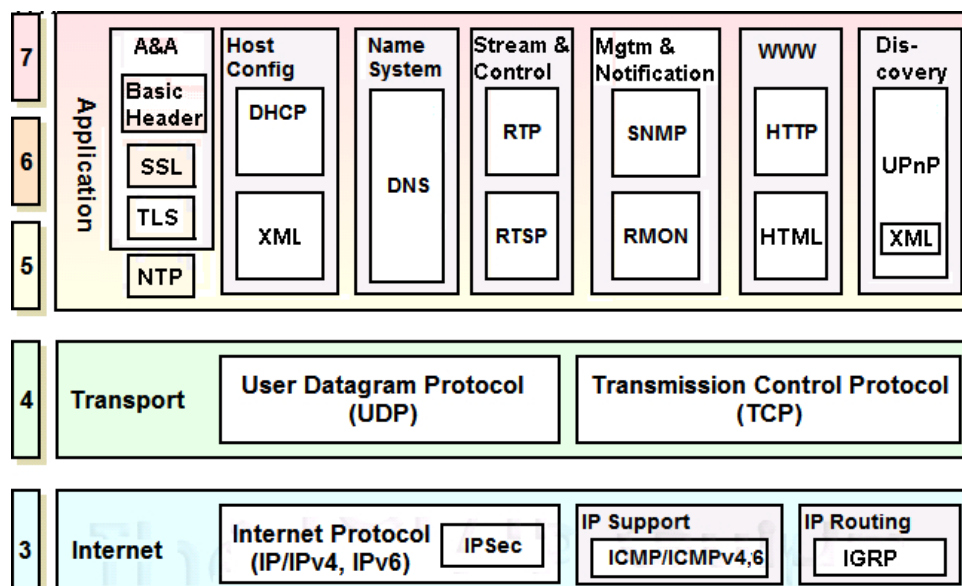


Figure 3 – Building Block of existing Standards

6 CCTV system device model

6.1 Overview

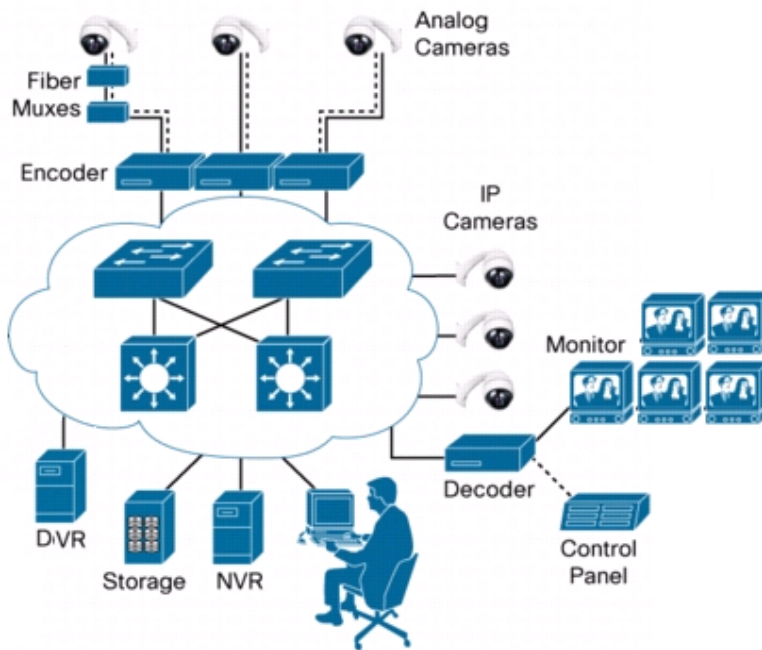


Figure 4 – VTD Example Network

The video transmission standards address the requirements of devices with differing application characteristics, such as embedded VTDs, system-level VTDs, operator workstations, video storage devices and others. Digital encoding and decoding VTDs, CCTV Client Workstations, NVRs and DVRs have a differing set of functionality in video stream formats and network connectivity. This clause provides a device model with consistent terms and usages for these device functionalities. To support interoperability between CCTV network devices, it is necessary for a decoding CCTV Client to meet all the requirements of the corresponding CCTV network encoding device. It is also necessary for a recording DVR, NVR or network storage to meet all the requirements of the corresponding CCTV network device. The following summarizes these devices functionalities:

- Stream encoding;
- Stream receiving and Decoding;
- Stream recording;
- Stream display;
- Stream replay;
- Camera controlling;
- Health and status monitoring;
- Video content analysis;
- Metadata creation and streaming;

- Auxiliaries.

In summary, the key point about the different device functionalities is that each may be uniquely optimized for the requirements of a particular application. The video transmission device standard focuses on interoperability of devices with the same codec's and of the same corresponding functionalities.

6.2 Device model elements

As described in the previous clause, devices adhering to the video transmission standards have different architectural layers. In summary, they are describing how devices and video content is found and controlled to achieve different system usages, device discovery and description for device control, video stream transport for the transfer of content, network stack for IPv4 protocol requirements, and network connectivity for supporting different network physical layers. Their interdependence is illustrated in Figure 4.

7 General IP interoperability requirements

7.1 General

Any IP video protocol shall be hardware and software independent, in order to be implemented in principle on any video transmission device platform.

The video transmission device compliant to this standard shall offer an IP protocol interface to

- support TCP / IP networking, real-time streaming, stream control,
- retrieve a unique IP address, manually or dynamically,
- be discovered in an IP network and provide the device URL,
- offer device description and capabilities via network,
- be configured via network,
- send notifications about device status and events to a configured receiving address,
- comply to the quality and performance requirements of this standard series EN 50132-5,
- offer maintenance API functions (initial setup, firmware upload, diagnostic functions, health monitoring, etc.),
- support a standardized Video Codec according to EN 50132-5-1,
- support a standardized Streaming and stream control protocol including Start-/Stop video transmission,
- control PTZ cameras including iris, focus and setting and calling of presets.

7.2 General protocol requirements overview

A VTD shall be compliant to the general requirements of EN 50132-5-1. Additionally following interoperability requirements have to be covered. A VTD has to offer means for

- IP connectivity according to Clause 7,

- Video streaming according to Clause 8,
- Video stream control according to Clause 8,
- device discovery and description according to Clause 9,
- event notification according to Clauses 10 and 11.

7.3 General high level IP video interface and protocol requirements

7.3.1 General

In the second section, the annexes, of this standard an architecture for a high-level IP video Interface is introduced, specified and defined. This High-level interface is a suite of software services, each one based on one technical principle to embed the different protocols of this standard into a common framework. For these two frameworks – the high-level ip video interfaces all mandatory requirements apply.

7.3.2 Versioning, capability exchange, and extensibility requirements

The IP Video protocol shall support schema versioning such that major version changes are defined as any change that breaks backward compatibility and minor version changes are defined as any change that does not break backward compatibility.

The IP Video protocol shall allow, but not require, a VTD server to expose multiple concurrent major versions and/or minor versions of the protocol concurrently.

The IP Video protocol shall make the major version and the minor version identification of a request message detectable by the application.

The IP Video protocol shall be extensible such that new operations and objects can be added to the protocol in a systematic manner.

7.3.3 implementations

Based on these general and basic interoperability requirements, this document defines and standardises high-level IP video interface implementations in the annexes. These implementations shall be platform and O/S independent. If a VTD shall support an additional high-level IP interface compatible to the requirements of this standard, following protocol implementations shall be supported:

- video ip interoperability based on web services according to Annex II; and / or
- video ip interoperability based on HTTP and REST service according to Annex I; and/or
- video ip interoperability based on another implementation according to Annex III.

Next to the EN 50132-5-2 compliance statement of the manufacturer or integrator, he shall clearly state in the product documentation, which High-Level IP Protocols supported: 'EN 50132-5-2 Video IP Interoperability based on Web Services' and/or 'EN 50132-5-2 Video IP Interoperability based on HTTP and REST Service'.

7.4 Non-conformance video transmission systems and devices

Proprietary or undisclosed Vendor Specific API, either IP based or not, are not compliant to the requirements of this standard. Video Transmission Device Integration or Interoperability SDKs, which are not IP based, are not

compliant to this standard. IP based-Vendor APIs, which are undisclosed to the interested public are non-compliant.

7.5 Mandatory documentation for the IP video interface of a VTD

If a VTD is offering any IP interface, additionally or beyond of the scope of this standard series, this API shall be fully documented and available to the interested public. The Video Interface shall be specified and documented for an integrator in a complete manner and document details including the statement of performance including typical and minimum hardware and/or O/S requirements. Any programmatical Video API offered by the vendor of a video transmission device shall specify the necessary services and methods in terms of control and interface return values and public member functions. The video API shall list all services including its methods, complex and simple types, elements and attributes in following manner:

Example API Method:

METHOD: VARIANT_BOOL CaptureSingleFrame ([in] BSTR FilePath)

DESCRIPTION: This method captures the current image to a file.

Properties e.g. return values:

VARIANT_BOOL Active

Indicates if this cameo is active or not.

Member Function Documentation incl. Parameters and properties

VARIANT_BOOL CaptureSingleFrame ([in] BSTR FilePath)

This method captures the current image to a file.

Property Documentation:

FilePath specifies the location, where the image file will be placed

Example Service:

Service: IP Video Web Service

Description: IP Video API Version 2.0

Type: SOAP

Style: Document

Methods:

Method Name	Description
FindIPVideoItems	Finds ip video devices items
FindIPVideoItems2	Finds ip video devices items of type 2

Method: FindIPVideoItems

Description: Finds IP video devices

Action:

Style: Document

Input (Literal): The input of this method is the document element ns:FindIPVideoItems of type having the structure defined by the following table.

Element	Type	Occurs	Description
ns:MessageID	xs:string	0..1	pass a value in a request, return value response.
ns:MesgID2	xs:string	0..1	pass a value in a request, return value response.

Output (Literal): The output of this method is the document element ns:FindIpVideoItems2 of type having the structure defined by the following table:

Element	Type	Occurs	Description
ns:Timestamp	xs:dateTime	0..1	This value represents the date and time

Simple Types: FindIPVideoItems

Name	Description
ns:AckCodeType	Type declaration to be used by other schema

Complex Types

..

Elements Name	Description
ns:AboutVideoURL [type SimpleUserType]	A link to the user's AboutMe page

Attribute: ns:type [type ProductIDType]

Description: The nature of identifier being used.

Full-operational software application samples including the source code shall be included for the display of live images and, if available in the VTD, as well samples for the replay of recordings, if available. The general requirements of this chapter shall also be fulfilled by video transmission devices not supporting the standardized protocol implementations of this standard (see annexes).

8 Video and data transport: mandatory streaming requirements

8.1 General

Today a lot of incompatible video streaming and stream control implementations exist, although standards are used. In order to accomplish a minimal interoperability of video transmission devices additional requirements have to be applied for IP video devices in security applications.

A VTD shall comply to the general video streaming and stream control requirements of EN 50132-5-1. Additionally following protocol requirements apply:

8.2 Detailed RTSP protocol requirements and definitions

8.2.1 RTSP request URI definition

Any compliant VTD shall support following RTSP URI schema. This standardized URI has to be supported by a VTD, even when other high level IP interfaces and protocols offer a different way to refer a video source.

In RTSP the video streaming channels and sources shall be made available via an associated structured RTSP URI. The URI should be structured in following manner:

rtsp://<IP-Adr>:<RTSP Port No>/VideoChannel/<Channel No>/<VideoCoDec>/<Stream No>/<RecordingID>/<unicast>

An RTSP URI consists of a basis path and a set of parameters. For live streaming the RTSP Uri's have the following form:

Examples:

Channel 1 MPEG4 Stream 2:	rtsp://140.10.1.22:554/VideoChannel/1/mpeg4/2
Channel 2 H.264 Stream 1:	rtsp://140.10.1.22:554/VideoChannel/2/h264/1

<IP-Adr> is the IP Address of the video transmission device

<RTSP Port No> is the port numbers of the RTSP service on the VTD

<Channel No> specifies the video channel requested for streaming, if more than one is available

<VideoCoDec> specifies the requested type of video stream, if more than one is available

<Stream No> specifies the video stream in a given quality, if more than one is available

<RecordingID> specifies the name of the video recoding,

<Unicast> or <Multicast> for direct unicast streaming or multicast.

8.2.2 Available video streams

8.2.2.1 General

A VTD server shall offer already on an initial start-up a default configuration for a video stream. An initial setup for a video profile including type of codec, quality setting, etc. shall be provided according to the product documentation.

The VTD shall use the RTSP DESCRIBE method to get information on the available streams of a VTD server. The body of the response contains SDP as defined in RFC 4566.

Example Request :

```
C->S:  DESCRIBE rtsp://140.10.10.22:5554/VideoChannel/1/h264/2 RTSP/1.0
      CSeq: 19
      Authorization: Basic cm9vdDp0YXJnZ=
```

Example Response :

```
S->C: RTSP/1.0 200 OK
      CSeq: 0
      Content-Base: rtsp://140.10.10.22:554/VideoChannel/1/h264/2
      Content-Type: application/sdp
      Date: Wed, 26 Jul 2009 13:47:45 GMT
      Content-Length: 846
      v=0
      o=- 1216212527554872 1216212527554872 IN IP4 140.10.10.22
      s=Media Presentation
      e=NONE
      c=IN IP4 0.0.0.0
      b=AS:8064
      t=0 0
      a=control:*
      a=range:npt=0.000000-
      a=h264-iod:"data:application/h264-iod;base64,
      DFJlksdaldfhDHGluisefhblGDElergfHJGLEfiuewrfgilufaerhGLETUREGPFNMBX
      IUoEAAE8BAF71AQOAwABQHRkYXRhOmFwcGxpY2F0aW9uL2lwZWc0LW9LWF1O2Jhc2U
      2NCxBVGdCR3dvZkF4Y0F5U1FBWlAAACAAFFFAwAAQAYJAFFFFFFFFFFFFF"
      m=video 0 RTP/AVP 96
      a=framerate:30.0
      a=control:trackID=2
      ?videocodec=h264&resolution=640x480
      a=rtpmap:96 H264/90000
      a=fmtp:96 packetization-mode=1; profile-level-id=420029;
      b=AS:64
```

RTSP requires a presentation description. SDP shall be used as the format of the presentation description for both Video Transmission clients and servers. Video Transmission servers shall provide and clients interpret the SDP syntax according to the SDP specification RFC 4566 and appendix C of RFC 2326. The SDP delivered to the Video Transmission client shall declare the video types to be used in the session using a codec specific MIME media type for each media. MIME media types to be used in the SDP file are described in 5.4 of this document.

The SDP specification requires certain fields to always be included in SDP. Additionally to this a Video Transmission server shall always include the following fields in the SDP:

"a=control:"	according to clauses C.1.1, C.2 and C.3 in RFC 2326;
"a=range:"	according to clause C.1.5 in RFC 2326;
"a=rtpmap:"	according to clause 6 in RFC 4566;
"a=fmtp:"	according to clause 6 in RFC 4566.

As SDP Source filters for multicasting the Source-Specific Multicast (SSM) according to RFC4570 should be used.

8.2.2.2 SDP

SDP is a protocol that describes a media session. Because of the format of a session description, certain information is always needed. SDP is used to convey the transport addresses on which media flows, the format of the video, the corresponding RTP payload format, profile and level and the times when the session as well as the

video durations. There is some overlap between RTSP and the SDP: some of the information available in the session description is also available via RTSP commands.

To ensure correct codec interpretation, following stream description has to be followed:

The codec MIME subtype name shall be used followed by specified parameters such as clock rate and encoding parameters. Here is the general format for one video stream using RTP:

```
video <port> RTP/AVP <payload type> or
rtmpmap:<payload type> <encoding name>/<clock rate>[/<encoding parameters>]
```

The payload type value is defined by RFC 3551 and is referenced in the Session Description (SDP) [RFC 4566].

8.2.3 RTSP Session keep-alive message

Since the RTSP standard offers no built-in mechanism for keep-alive messages between video transmission client and server, the RTSP method SETPARAMETER shall be sent periodically. This has the advantage not to use another protocol and open additional TCP ports.

A client can use OPTIONS (allowed) as alternative for keep alive.

When using SETPARAMETER for keep alive, no body should be included. This method is the recommended RTSP method to use in request only intended to perform keep-alive. The method OPTIONS does also work. However it causes the server to perform more unnecessary processing and result in bigger responses than necessary for the task. The reason for this is that the server needs to determine what capabilities that are associated with the video resource to correctly populate the header{Public} and header{Allow} headers.

The VTD server device should handle any valid RTSP command from the VTD client as a “keep-alive” request and maintain an active session.

If RTP is used for video transport in combination with RTCP it shall also work as keep alive. The server can determine the client by used network address and port together with the fact that the client is reporting on the servers SSRC(s). A disadvantage of RTCP is that it only gives statistical guarantees to reach the server and that it is object to network packet loss. In sessions with short timeout intervals, or high packet loss any of the keep-alive mechanisms described above shall be used.

8.2.4 RTSP UDP stream timeouts

A VTD server shall verify that a VTD client is still listening to the UDP stream its sending. If the VTD server has not received any “keep-alive” message after 30 s, it shall stop streaming.

8.2.5 I-Frame request for differential encoded multicast streams

Video transmission clients joining multicast streams shall wait for the first I-frame of a video stream before displaying or recording the new video images. For surveillance applications this delay has to be short and the VTD Client shall issue an I-frame request using the RSTP method PLAY to the VTD server for this stream. The VTD server shall react in less than 1 s.

If many VTD clients initialize a connection at the same time to the same VTD server, causing many I-frame requests, the unit shall stay responsive, e.g. by ignoring some of the requested I-frames. This shall be done in a way that no VTD client has to wait more than 1 s before video display.

8.2.6 RTSP status codes

The RFC 2326 lists a complete set of error codes. VTD devices shall support and understand a minimum set of status codes:

200 Ok
401 Unauthorized
454 Session Not Found
503 Service Unavailable

8.2.7 RTSP method extension restrictions

RTSP can be extended in three ways, listed here in order of the magnitude of changes supported:

Existing methods for the use in VTDs can be extended by vendors with new parameters, e.g. headers, as long as these parameters can be safely ignored by video transmission devices as recipients. If the client needs negative acknowledgement when a method extension is not supported, a tag corresponding to the extension may be added in the field of the Require or Proxy-Require headers.

New CCTV methods can be added by any vendor, e.g. to control a PTZ, select an area of interest, define the video resolution, protect alarm video recordings from being deleted, etc. via RTSP. If the recipient of the message does not understand the request, it shall respond with error code 501 (Not Implemented) so that the sender can avoid using this method again. A VTD sender device shall not request any non implemented RTSP method again during its runtime. A VTD client may also use the OPTIONS method to inquire about methods supported by the VTD server. The server shall list the methods it supports using the Public response header.

A new version of the protocol can be defined, allowing almost all aspects (except the position of the protocol version number) to change.

The basic capability discovery mechanism can be used to both discover support for a certain feature and to ensure that a feature is available when performing a request. For detailed explanation of this see RFC 2326.

8.2.8 RTSP method definitions

The RTSP methods indicate what is to be performed on the resource identified by the Request-URI. The method name shall be according to RFC2326.

If a VTD server , does not support a particular RTSP method, it shall return 501 (Not Implemented) and the requesting RTSP agent, in return, should NOT try this method again for the given agent / resource combination

8.2.9 RTSP method SETUP

The VTD Client shall establish a RTSP session within the first SETUP message with a unique session identifier. The VTD server shall choose a large, random and non-sequential session identifier which shall be at least eight octets long to grant a minimum security according to RFC 2326 section 3.4.

Table 1 – Security of RTSP sessions

	Grade 1	Grade 2	Grade 3	Grade 4
Session identifier length	op	8 octets	16 octets	32 octets
Key: Op = Optional M = Mandatory.				

Subsequent request messages in this session shall include the same session identifier. It also establishes the transport mode chosen to stream video from the device identified by the URI. The VTD shall configure via SETUP method the following streaming parameters:

- multicast address;

- multicast or unicast ports;
- multicast TTL.

Multicast Request Example:

```
C->S: SETUP rtsp://140.10.10.22:554/VideoChannel/1/h264/1/trackID=1 RTSP/1.0
      CSeq: 58
      Transport: RTP/AVP;multicast;destination=224.16.56.42;port=47700-47701;ttl=64
      Authorization: Basic cm9vdDp0YXJnZXQ=
```

Multicast Response Example:

```
S->C: RTSP/1.0 200 OK
      CSeq: 58
      Session: 0845636542;timeout=60
      Transport: RTP/AVP;multicast;destination=224.16.56.41;tll=64;port=47700-47701
```

for unicast:

```
C->S: Transport: RTP/AVP;unicast;client_port=15010-15011
```

```
S->C: Transport:RTP/AVP;unicast;client_port=15010-15011;server_port=50184-50185; ssrc=399D9E05;
      mode="PLAY"
```

8.2.10 RTSP method PLAY

The PLAY method tells the server to start sending data via the mechanism specified in SETUP.

For VTDs it is required that an absolute time value (clock) for the corresponding time is used, i.e. "clock=20030213T143205Z-". The UTC clock format shall be used. The other time formats defined by RFC 2326 shall not be used.

For a requested video stream from a recording, the VT server shall reply with the actual range that will be replayed, i.e. from which point of time and for how long any video stream content is delivered. This may differ from the requested range if alignment of the requested range to existing frame limits and boundaries is necessary for the streaming source.

NOTE Some video streams may need to be delivered from even earlier points. Also, some video stream formats have a very long duration per individual group of pictures (GOP), therefore it might be necessary for the client to parse the complete GOP, and select where to start.

For playback a VTD recording, the UTC clock according to ISO 8601 shall be used:

```
C->S: PLAY rtsp://video.cctvserver.com/videochannel/1 RTSP/2.0
      Cseq : 835
      Session : 12345678
      Range : clock=20061108T142300Z-20061108T143520Z

S->C: RTSP/2.0 200 OK
      Cseq: 835
      Date: 23 Jan 2006 15:35:06 GMT
      Server:CCTVServer 1.0
      Range: clock=20061108T142300Z-20061108T143520Z
      RTP-Info:url="rtsp://cctvserver.com/ videochannel/1"
              ssrc=0D12F123;seq=53745;rtptime=484589019
```

8.2.11 RTSP over HTTP

If a VTD needs to tunnel RTSP over HTTP, e.g. to provide means for passing firewalls etc., two HTTP sessions shall be provided for response and request on the HTTP port (default port: 80) and the RTSP port (default port: 554). The supported HTTP methods are GET and POST.

Example RTSP/HTTP URL:
`http://<ip-address>:80/VideoChannel/2/h264/1`

RTSP commands shall be base64 encoded and responses shall be text-only. The 2 sessions, RTSP and Http, shall exchange a unique x-sessioncookie in the RTSP header.

9 Device discovery and description

9.1 General

Any VTD device shall offer means to be detected in the network and offer a description about its video features and capabilities.

A VT client looking for available VTDs in the security network shall use the discovery protocol specified in this standard. The VT server compliant to this standard shall implement the device discovery and description service to provide information about its capabilities; the VT client shall receive and interpret those discovery and description messages. A VTD shall send messages initially, when connected to a network and when in operation it shall always listen for discovery messages, in order to answer accordingly.

This clause specifies 3 standard protocols for the discovery and description of a VTD in a network. The VTD has to offer at least one of the three discovery & description mechanisms: UPnP Device Description and Discovery according to 9.2 and/or ZeroConf according to 9.3 and/or WS-Discovery according to 9.4.

9.2 UPnP device discovery and description (METHOD 1)

9.2.1 General

If the VTD offers device discovery and description according to this standard EN 50132-5-2 based on UPnP following requirements apply:

The Implementation shall be in line with the series of ISO/IEC 29341 publications defining the UPnP architecture. For VTD devices supporting UPnP following parts shall be applied:

- Part 1: UPnP device architecture version 1.0
- Part 2: Basic device control protocol - basic device
- Part 5-1: Digital security camera device control protocol - Device
- Part 5-10 Digital security camera device control protocol - Motion image service

9.2.2 Introduction (informative)

The UPnP architecture supports zero-configuration networking. UPnP uses HTTP over UDP. A UPnP compatible VTD from any manufacturer can dynamically join a network, announce its name, convey its capabilities upon request, and learn about the presence and capabilities of other VT devices. DHCP and DNS servers are optional and are only used if they are available on the video network.

Discovery

The very first step in IP video networking is Discovery. The UPnP discovery protocol, defined in Part 1 of the UPnP Device Architecture, is known as the Simple Service Discovery Protocol (SSDP). When a device is added to the network, SSDP allows a device to advertise its services to VTD clients on the network. Similarly, when a VTD client is added to the network, SSDP allows him to search for transmission devices of interest on the network. The fundamental exchange in both cases is a discovery message containing a few, essential specifics about the device or one of its video services, for example, its type, identifier, and a pointer to more detailed information.

Description

After a VTD client has discovered another VT device, he still knows very little about the device. For the client to learn more about the device and its capabilities, or to interact with the device, he needs to retrieve the device's description from the URL provided by the device in the discovery message. The UPnP description for a device is expressed in XML and includes vendor-specific, manufacturer information like the model name and number, serial number, manufacturer name, URLs to vendor-specific web sites, etc. The description also includes a list of any embedded devices or services such as VCA, PTZ, multiple video channels, live streams, etc., as well as URLs for control, eventing, and display. For each service, the description includes a list of the commands, or actions, to which the service responds, and parameters, or arguments, for each action; the description for a service also includes a list of variables consisting of data type, value range, and eventing characteristics.

9.2.3 UPnP architecture overview

Figure 5 shows an overview of the various layers that make up the CCTV Network Architecture. The video transmission device network architecture maps to the UPnP Device Architecture in order to provide device discovery and description. The UPnP Architecture itself is built on the standard TCP/UDP over IPv4 suite of protocols.

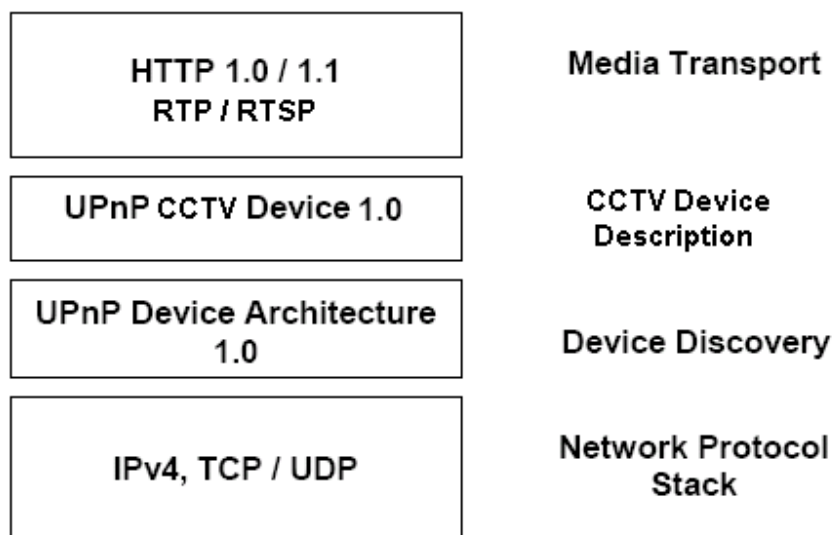


Figure 5 – UpnP Protocol Layers

9.2.4 Device capabilities

The video transmission device capabilities shall fully support the applicable mandatory portions of the UPnP device architecture v1.0 (UPnP DA) for discovery and description. This standard specifies UPnP device architecture 1.0 (UPnP DA) as the basic protocol framework for the device classes.

Part 1 of the UPnP device architecture 1.0 indicates that advances in minor version of the UPnP device architecture are a superset of earlier (minor) versions with the same major version. This means that future UPnP devices with a newer minor revision will implement all of the behaviour required of the previous device architectures.

Although not explicitly stated by the UPnP device architecture, the intent of such backwards compatibility rules is to enable forward compatibility of VTD Clients with newer, minor revisions of the UPnP device architecture. Forward compatibility of VTD Clients is required, which is necessary for future interoperability.

NOTE A version of the UPnP device architecture appears in the <specVersion> element of the device descriptions.

One way to implement this requirements is for the UPnP VTD Client to treat the minor version of an UpnP device architecture as 0 (i.e. ignore the minor version).

9.2.5 UPnP default port

UPnP devices and VTD Clients shall receive and process multicast discovery messages on port 1900. These requirements ensure that VTDs in the role of UPnP endpoints will be more likely to discover each other on the CCTV network.

9.2.6 UpnP discovery robustness

A VTD in the function of a UPnP endpoint should wait a random amount of time, between 0 ms and 100 ms after acquiring a new IP address, before sending advertisements or initiating searches on a new IP interface.

9.2.7 UPnP HTTP support and general rules

UPnP devices shall support HTTP/1.1. for performing UPnP communications. This requirement collection specifies that UPnP transactions that use HTTP shall minimally support HTTP/1.0.

The HTTP servers and clients of UPnP endpoints shall include the content-type header tag in every UPnP-related TCP-based HTTP transaction (device/service description) that contains an XML body. This content type shall always be marked as 'text/xml; charset="utf-8"' It should be noted that charset parameter value is case-insensitive and double quotations may be omitted. Furthermore, the XML shall be encoded in UTF-8.

UPnP endpoints (video transmission devices) that receive a content type of text/xml shall infer UTF-8 character set encoding.

9.2.8 UPnP device description rules

The total byte size of a device description file shall not exceed 20 480 bytes (20 KB). This byte limit includes the HTTP headers. This provides a known maximum size for device description documents.

9.2.9 UPnP XML namespace

Default namespace defined by the UPnP DA shall be used in device and service descriptions. All standard elements in device and service descriptions do not use a namespace prefix.

9.2.10 UPnP unknown header/tag/field robustness rule

UPnP endpoints shall be tolerant of unknown headers, tags, fields, attributes, and values for HTTP, XML and SOAP. Specifically, this tolerance requirement applies to

- HTTP headers, tokens, values,
- unknown XML elements and attributes in device description files or service description files.

This requirement addresses forward compatibility and also ensures broader interoperability between implementations that employ vendor extensions in the manner described by the

requirement collection.

If a URI is a device description then the URI may be a relative URI with its base as the base path of the LOCATION URL value.

EXAMPLE:
LOCATION `http://140.10.1.20/cctvdevicedesc.xml`

9.2.11 UPnP device description requirements

If a VTD UPnP device wants to change a device description, then the UPnP device shall

- first leave the UPnP network by sending an ssdp:byebye message,
- then change the desired device description or service description files, and
- finally join the UPnP network with the new XML files using an ssdp:alive message.

9.2.12 UPnP video transmission device template

This UPnP device template is for UPnP™ device architecture V 1.0. It defines a UPnP Device Control Protocol (DCP) standard to be used with standardized video transmission devices according to this standard.

A video transmission device supporting UPnP shall identify itself with the device type compliant with the following standardized DCT template:

[urn:schemas-upnp-org:device:DigitalSecurityCamera:1](#)

This device template is compliant with the Universal Plug and Play Architecture, Version 1.0.

The Video Transmission device compliant to the device type DigitalSecurityCamera Vers.1.0 shall provide a subset or all of the following functionality:

- Configuration of image capturing profiles;
- Streaming of JPEG still images;
- Streaming of real-time video.

VTDs shall implement the minimum version number supported by all embedded device items and services.

9.2.13 Vendor-defined Extensions

Whenever vendors create additional vendor-defined state variables, actions or properties, their assigned names and XML representation shall follow the naming conventions and XML rules as specified in UPnP Device Architecture, version 1.0, ISO/IEC 29341-1, Section 2.5, "Description: Non-standard vendor extensions".

9.3 Zeroconf service discovery and description (METHOD 2)

9.3.1 General

If the VTD offers device discovery and description according to this standard EN 50132-5-2 based on ZeroConf following requirements apply.

9.3.2 ZeroConf networking architecture overview

The following figure shows an overview of the various layers that make up the CCTV networking architecture. In this architecture ZeroConf provides the means to discover an HTTP URL for each VTD device on the network that shall be used to retrieve its description and to set its configuration. ZeroConf makes use of the standard TCP/UDP over IP suite of protocols.

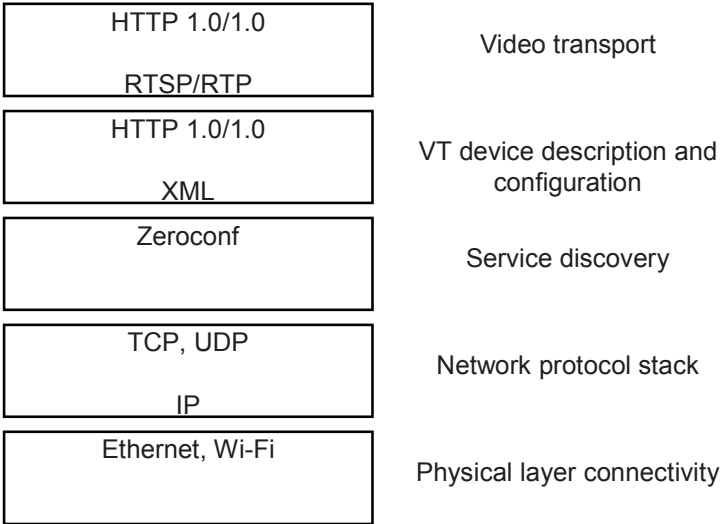


Figure 6 – ZeroConf protocol layers

9.3.3 Introduction

The location of network services, such as video sources and VTDs in Zeroconf is done over DNS service discovery: Multicast DNS/DNS-SD. Multicast DNS (mDNS) is a protocol that uses an interface protocol similar to the unicast Domain Name System, but is implemented over a multicast protocol. Each component on the network, such as a VTD, offers a list of DNS resource records and has to join the mDNS multicast group. Build on top of this DNS is the Service Discovery (DNS-SD). In contrast to UPnP using HTTP messages, this solution uses DNS messages such as DNS SRV, TXT, and PTR records to advertise its Service Names. The VTD has to offer services publishing the details of available services with instance, service type, domain name and optional configuration parameters:

```
C:\>dns-sd.exe -B _http._tcp
Browsing for _http._tcp
Timestamp    A/R  Flags if Domain      Service Type      Instance Name
10:34:16.305 Add   3 5 local.      _http._tcp.      HP Color LaserJet 3800 [8EC288]
10:34:16.305 Add   3 5 local.      _http._tcp.      AXIS 241Q - 00408C7E2AE1
```

A service type registry is maintained and published by DNS-SD.org. Service type names are given informally on a first-come basis. The services required for surveillance systems are listed below.

9.3.4 ZeroConf services definitions

9.3.4.1 General

ZeroConf is normally expected to operate in a local area network.

HTTP requests are made by the VTD's web interface. The HTTP response may contain XML content (for GET actions), XML response information (for PUT or POST actions), or various text/binary content (for retrieval of configuration data, etc.). VTDs shall be able to handle overlapping/simultaneous HTTP requests, as well as persistent connections to handle multiple HTTP transactions in parallel.

The XML content shall be described by .xsd documents.

One of the protocols offered by ZeroConf is the DNS Service Discovery (DNS-SD). VTDs shall implement ZeroConf Device discovery and description according to the IETF Draft DNS-Based Service Discovery . With this protocol each VTD device can declare on the network the service it provides. The VTD shall list the offered services according to RFC2782 including the extensions found at <http://www.dns-sd.org/ServiceTypes.html>:

9.3.4.2 HTTP-service

A VTD shall list an existing http-service by following description:

```
http           World Wide Web HTML-over-HTTP
Tim Berners-Lee <timbl at W3.org>
Protocol description: RFC 2616
Defined TXT keys: u=<username> p=<password> path=<path to document>
```

NOTE The meaning of this service type, though called just "http", actually denotes something more precise than just "any data transported using HTTP".

The DNS-SD service type "http" shall be used by a VTD to advertise content that:

- is served over HTTP,
- can be displayed by "typical" web browser client software, and
- is intended primarily to be viewed by a human user.

See the service list description for more details.

```
https          HTTP over SSL/TLS
Tim Berners-Lee <timbl at W3.org>
Protocol description: RFC 2616
Defined TXT keys: None
```

9.3.4.3 RTSP-Service

```
rtsp           Real Time Streaming Protocol
Rob Lanphier <robla at protonet.com>
Protocol description: RFC 2326
Defined TXT keys: None
```

9.3.4.4 ZeroConf services definitions for a VT device

A new type of DNS-SD service is needed for VT device description. The in this standard introduced service 'cctv' can also be used for configuration (alternatively two different DNS-SD services can be defined, one for description and one for configuration). This service is added in this standard for VTDs to the official service list:

```
cctv HTML-over-HTTP, entry point for CCTV configuration
Tim Berners-Lee <timbl at W3.org>
Protocol description: RFC 2616
Defined TXT keys: u=<username> p=<password> path=<path to XML file>
```

9.3.5 ZeroConf discovery examples

Example of HTTP user interface services provided in a network by some sample devices.

```
C:\>dns-sd.exe -B _http._tcp
Browsing for _http._tcp
Timestamp    A/R Flags if Domain      Service Type      Instance Name
10:34:16.305 Add   3 5 local.      _http._tcp.      HP Color LaserJet 3800 [8EC288]
10:34:16.305 Add   3 5 local.      _http._tcp.      AXIS 241Q - 00408C7E2AE1
10:34:16.305 Add   3 5 local.      _http._tcp.      HP LaserJet 5100 Series [C1EFDB]
10:34:16.305 Add   3 5 local.      _http._tcp.      AXIS 206M - 00408C6ED7A9
10:34:16.305 Add   2 5 local.      _http._tcp.      HP LaserJet M5035 MFP [A5D612]
```

Example of RTSP streaming services provided by a network encoder. This single encoder provides 5 different streams.

```
C:\>dns-sd.exe -B _rtsp._tcp
Browsing for _rtsp._tcp
Timestamp    A/R Flags if Domain      Service Type      Instance Name
10:35:03.182 Add   3 5 local.      _rtsp._tcp.      AXIS 241Q - 00408C7E2AE1 1
10:35:03.182 Add   3 5 local.      _rtsp._tcp.      AXIS 241Q - 00408C7E2AE1 2
10:35:03.182 Add   3 5 local.      _rtsp._tcp.      AXIS 241Q - 00408C7E2AE1 3
10:35:03.182 Add   3 5 local.      _rtsp._tcp.      AXIS 241Q - 00408C7E2AE1 4
10:35:03.182 Add   2 5 local.      _rtsp._tcp.      AXIS 241Q - 00408C7E2AE1 quad
```

NOTE 1 If the VTD needs to be compliant to EN 50132-5-2 'Interoperability based on HTTP and REST Services' the additional requirements on ZeroConf of Clause 4 of Appendix I.A need to be applied.

NOTE 2 If the VTD needs to be compliant to EN 50132-5-2 'Interoperability based on Web Services' the additional requirements on DNS service record lookup of 7.4 of Appendix II need to be applied.

9.4 Web service discovery (METHOD 3)

If the VTD offers device discovery and description according to this standard EN 50132-5-2 based on Web Services Dynamic Discovery (WS-Discovery), it shall be implemented according to the OASIS WS-Discovery standard. If the VTD shall be compliant to 'EN 50132-5-2 Interoperability based on Web Services' the additional requirements of Clause 7 of Appendix II 'Device Discovery' and 8.1 'Capabilities' shall be applied.

10 Eventing requirements

A VTD shall offer protocols to signal the health status and events associated to the video source. According to EN 50132-1 a VTD shall signal in the different security grades video loss, signal noise, signal too bright, too dark and camera depositioning. The notification of motion in the video image shall be done by the same means. These states and the change of these need to be signalled by the IP protocol in a defined manner by standardizes values, elements or attributes in order to let any VTD client, independent of the type of device or manufacturer, exactly know the detailed status of any video source. The VTD shall support

- WS-Base Notification according to the OASIS Standard 'Web Services Base Notification Vers. 1.3', and / or
- SNMP according to Clause 12. 'CCTV network device management', and/or