IEC 62676-1-2

Edition 1.0 2013-10

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Video surveillance systems for use in security applications – Part 1-2: System requirements – Performance requirements for video transmission

Systèmes de vidéosurveillance destinés à être utilisés dans les applications de sécurité – Partie 1-2: Exigences systèmes – Exigences de performances pour la transmission vidéo

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you to find IEC publications by a variety of criteria (reference number, text, technical committee,…).
It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Liens utiles:

Recherche de publications CEI - www.iec.ch/searchpub

La recherche avancée vous permet de trouver des publications CEI en utilisant différents critères (numéro de référence, texte, comité d'études,…).
Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

Just Published CEI - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications de la CEI. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (VEI) en ligne.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

IEC 62676-1-2

Edition 1.0 2013-10

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Video surveillance systems for use in security applications – Part 1-2: System requirements – Performance requirements for video transmission

Systèmes de vidéosurveillance destinés à être utilisés dans les applications de sécurité – Partie 1-2: Exigences systèmes – Exigences de performances pour la transmission vidéo

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX XA

ICS 13.320

ISBN 978-2-8322-1158-8

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

VIDEO SURVEILLANCE SYSTEMS FOR USE IN SECURITY APPLICATIONS –

Part 1-2: System requirements – Performance requirements for video transmission

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62676-1-2 has been prepared by IEC technical committee 79: Alarm and electronic security systems.

The text of this standard is based on the following documents:

FDIS	Report on voting
79/433/FDIS	79/446/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts in the IEC 62676, published under the general title *Video surveillance systems for use in security applications*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

The IEC Technical Committee 79 in charge of alarm and electronic security systems together with many governmental organisations, test houses and equipment manufacturers have defined a common framework for video surveillance transmission in order to achieve interoperability between products.

The IEC 62676 series of standards on video surveillance system is divided into 4 independent parts:

Part 1: System requirements

Part 2: Video transmission protocols

Part 3: Analog and digital video interfaces

Part 4: Application guidelines (to be published)

Each part has its own clauses on scope, references, definitions and requirements.

This IEC 62676-1 series consists of 2 subparts, numbered parts 1-1 and 1-2 respectively:

IEC 62676-1-1, *System requirements – General*

IEC 62676-1-2, *System requirements – Performance requirements for video transmission*

The second subpart of this IEC 62676-1 series applies to video transmission. The purpose of the transmission system in a Video Surveillance System (VSS) installation is to provide reliable transmission of video signals between the different types of VSS equipment in security, safety and monitoring applications.

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

VIDEO SURVEILLANCE SYSTEMS FOR USE IN SECURITY APPLICATIONS –

Part 1-2: System requirements – Performance requirements for video transmission

1 Scope

This part of IEC 62676 introduces general requirements on video transmission. This standard covers the general requirements for video transmissions on performance, security and conformance to basic IP connectivity, based on available, well-known, international standards.

Clauses 4 and 5 of this standard define the minimum performance requirements on video transmission for security applications in IP networks. In surveillance applications the requirements on timing, quality and availability are strict and defined in the last section of this standard. Guidelines for network architecture are given, how these requirements can be fulfilled.

Clause 6 and the next clauses of this standard define requirements on basic IP connectivity of video transmission devices to be used in security applications. If a video transmission device is used in security, certain basic requirements apply. First of all a basic understanding of IP connectivity needs to be introduced which requests the device to be compliant to fundamental network protocols. These could be requirements which may be applied to all IP security devices even beyond IP video. For this reason requirements are introduced in a second step for compliance to basic streaming protocols, used in this standard for video streaming and stream control. Since security applications need high availability and reliability, general means for the transmission of the video status and health check events have to be covered. These are defined in general requirements on eventing and network device management. In security proper maintenance and setup is essential for the functioning of the video transmission device. Locating streaming devices and their capabilities is a basic requirement and covered in ´device discovery and description´.

2 Normative references

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

IEC 61709, *Electric components – Reliability – Reference conditions for failure rates and stress models for conversion*

IEC/TR 62380, *Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment*

IEC 62676-1-1, *Video surveillance systems for use in security applications – Part 1-1: System requirements – General*

IEC 62676-2-1, *Video surveillance systems for use in security applications – Part 2-1: Video transmission protocols – General requirements*

ISO/IEC 10646, *Information technology – Universal multiple-octet coded character set (UCS)*

ISO/IEC 13818-9, *Information technology – Generic coding of moving pictures and associated audio information – Part 9: Extension for real time interface for systems decoders*

ISO/IEC 14496-2, *Information technology – Coding of audio-visual objects – Part 2: Visual*

ISO/IEC 14496-3, *Information technology – Coding of audio-visual objects – Part 3: Audio*

ISO/IEC 14496-10, *Information technology – Coding of audio-visual objects – Part 10: Advanced Video Coding*

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

ITU-T Rec. G.726, *40, 32, 24, 16 kbit/s adaptive differential pulse code modulation (ADPCM)*

IEEE Std 1413.1, *IEEE Guide for selecting and using reliability predictions based on IEEE 1413*

IETF RFC 1122, *Requirements for Internet Hosts – communication Layers*

IETF RFC 1157, *Simple Network Management Protocol*

IETF RFC 1441, *Introduction to version 2 of the Internet-standard Network Management Framework*

IETF RFC 2030, *Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI*

RFC 2069, *Digest Access Authentication*

IETF RFC 2131, *Dynamic Host Configuration Protocol*

IETF RFC 2246, *The TLS Protocol Version 1.0*

IETF RFC 2326:1998, *Real Time Streaming Protocol (RTSP)*

IETF RFC 2435, *RTP Payload Format for JPEG-compressed Video*

IETF RFC 2453, *RIP - Routing Information Protocol*

IETF RFC 2617, *HTTP Authentication Basic and Digest Access Authentication, June 1999*.

IETF RFC 3016, *RTP Payload Format for MPEG-4 Audio/Visual Streams*.

IETF RFC 3268, *Advanced Encryption Standard (AES) Cipher suites for Transport Layer Security (TLS)*

IETF RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*

IETF RFC 3410, *Introduction and Applicability Statements for Internet Standard Management Framework*

IETF RFC 3550, *RTP A Transport Protocol for Real-Time Applications*

IETF RFC 3551, *RTP Profile for Audio and Video Conferences with Minimal Control*

IETF RFC 3984, *RTP Payload Format for H.264 Video*.

IETF RFC 4346, *The Transport Layer Security (TLS) Protocol Version 1.1*

IETF RFC 4541, *IGMP and MLD Snooping Switches*

IETF RFC 4566, *SDP Session Description Protocol*

IETF RFC 4607, *Source Specific Multicast for IP*

IETF RFC 4862, *IPv6 Stateless Address Auto configuration*

3 Terms, definitions and abbreviations

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

3.1 Terms and definitions

3.1.1
adaptive jitter buffering
queuing of packets in switched networks exposed to unwanted variations in the communications signal to ensure the continuous video transmission over a network supported by the 'Adaptive' ability to adjust the size of the jitter buffer based on the measured jitter in the network

EXAMPLE: If the jitter increases, the buffer becomes larger and can store more packets; if the jitter decreases, the buffer becomes smaller and stores fewer packets.

3.1.2
advanced encryption standard
NIST encryption standard, also known as Rijndael, specified as unclassified, publicly-disclosed, symmetric encryption algorithm with a fixed block size of 128 bits and a key size of 128, 192 or 256 bits according to the Federal Information Processing Standards Publication 197

3.1.3
American Standard Code for Information Interchange
de-facto world-wide standard for the code numbers used by computers to represent all the upper and lower-case characters

3.1.4
asymmetric algorithm
algorithm used in the asymmetric cryptography, in which a pair of keys (a private key and a public key) is used to encrypt and decrypt a message to ensure the privacy of communications

3.1.5
authentication
process where an operators or systems identity is checked within a network

EXAMPLE: In networks, authentication is commonly done through the use of logon passwords.

3.1.6
authentication server
device used in network access control

Note 1 to entry: It stores the usernames and passwords that identify the clients logging on or it may hold the algorithms for access. For access to specific network resources, the server may itself store user permissions and

company policies or provide access to directories that contain the information. Protocols such as RADIUS, Kerberos and TACACS+, and 802.1x are implemented in an authentication server to perform user authentications.

3.1.7
authenticity
integrity and trustworthiness of data or an entity; validity and conformance of the information, or identity of a user

Note 1 to entry: The authenticity can be secured and verified using cryptographic methods.

3.1.8
authorization
approval, permission, or empowerment for a user or a component to do something

3.1.9
backbone
high-speed line or series of connections that forms a major pathway within a network

3.1.10
backbone layer
larger transmission line that carries data gathered from smaller communication lines that interconnect with it, e.g. a line or set of lines that local area networks connect to, in order to span distances efficiently e.g. between buildings

3.1.11
Bit/s
bit per second
unit of measurement of how fast data is transferred from one node to another

3.1.12
bridge
device that is used to connect two networks including passing data packets between them using the same protocols

3.1.13
client
component that contacts and obtains data from a server

3.1.14
client/server
communication system providing services e.g. video streams, storage, logon access, data communication management and clients (workstations) subscribing these services

3.1.15
codec
compression-decompression or enCOder/DECoder process

3.1.16
common gateway interface
CGI
standardized method of communication between a client, e.g. web browser, and a server, e.g. web server

Note 1 to entry: This note applies to the French language only.

3.1.17
compression delay
delay caused by the compression of data

3.1.18
congestion
situation in which the traffic presents on the network exceeds available network throughput/ capacity

3.1.19
core layer
part of the network providing optimal transport between sites or system functionality e.g. recording

3.1.20
data encryption standard
DES
cryptographic algorithm method developed by the US National Bureau Standards

Note 1 to entry: This note applies to the French language only.

3.1.21
dynamic host configuration protocol
DHCP
protocol by which a network component obtains an IP address (and other network configuration information) from a server on the local network

Note 1 to entry: This note applies to the French language only.

3.1.22
distribution layer
part of the network providing policy-based connectivity

3.1.23
domain name system
DNS
system that translates Internet domain names into IP addresses

Note 1 to entry: This note applies to the French language only.

3.1.24
dual homing
single device offering two or more network interfaces

3.1.25
dynamic jitter buffer
collecting and storing video data packets for processing them in evenly spaced intervals to reduce distortions in the display

3.1.26
encryption
type of network security used to encode data so that only the intended destination can access or decode the information

3.1.27
fail-over
the capability of an application to recover from a failure on an entity by automatically switching over to a surviving instance, providing no loss of data or continuity, also known as ‘run-time failover’ and often used in connection with

3.1.28
forensics
field of science of applying digital technologies to legal questions arising from criminal investigations

3.1.29
frame
data structure that collectively represents a transmission stream including headers, data, and the payload and provides information necessary for the correct delivery of the data

3.1.30
gateway
hardware or software set-up that translates between two dissimilar protocols

3.1.31
H.261
ITU video coding standard originally designed for ISDN lines and data rate with multiples of 64 Kbit/s using real time protocol (RTP)

3.1.32
H.263
ITU standard supporting video compression (coding) for streaming video via RTP based on and replacing the H.261 codec

3.1.33
H.264
ISO ITU-T MPEG-4 Part 10 standard, also named Advanced Video Coding (AVC) supporting video compression (coding) from low bit-rate network streaming applications to HD video applications with near-lossless coding for network-friendly video representation

3.1.34
host
computer on a network that is a repository for services available to other components on the network

3.1.35
hot-swap
property of controller which allows circuit boards or other devices to be removed and replaced while the system remains powered up and in operation

3.1.36
Hyper Text Mark-up Language
HTML
coding language used to create Hypertext documents for use on the World Wide Web

Note 1 to entry: This note applies to the French language only.

3.1.37
Hypertext Transfer Protocol
HTTP
connection oriented protocol for transmitting data over a network or protocol for moving hyper text files across the Internet

Note 1 to entry: This note applies to the French language only.

3.1.38
Hypertext Transfer Protocol Secure
HTTPS
encrypts and authenticates communication between server and clients

Note 1 to entry: This note applies to the French language only.

3.1.39
Internet Control Message Protocol
ICMP
error protocol indicating, for instance, that a requested service is not available or that a host or router could not be reached

Note 1 to entry: This note applies to the French language only.

3.1.40
identification
ID
a machine-readable character string

3.1.41
IEEE 802.1x
method for authentication and authorization in IEEE-802 networks using an authentication server e.g. RADIUS server

3.1.42
Institute of electrical and electronics engineers
IEEE
professional association of engineers for the advancement of technology

3.1.43
Internet group management protocol
IGMP
communications protocol used to manage the membership of IP multicast groups

Note 1 to entry: This note applies to the French language only.

3.1.44
Internet protocol
IP
network layer 3 protocol in the OSI model containing addressing and control information to enable data packets to be routed in a network and primary network layer protocol in the TCP/IP protocol suite according to IETF RFC 791

Note 1 to entry: This note applies to the French language only.

3.1.45
Internet protocol address
IP address
address of a host computer used in the Internet Protocol

Note 1 to entry: The IP address corresponds to a fully qualified domain name. At present, it consists of 32 bits and is generally represented by a sequence of four decimal numbers (each in the range from 0 to 255), separated by dots. The IP address of a computer usually comprises two parts: a part corresponding to the network number of the network on which this computer is located, and a part identifying the computer within its network. In the new version IPv6 of the Internet Protocol, the IP address consists of 128 bits.

Note 2 to entry: The Internet protocol is not limited to the Internet, and may be used on other networks.

3.1.46
IP
Internet protocol
main protocol used in conjunction with TCP (Transfer Control Protocol)

SEE: TCP/IP.

3.1.47
Images per second
IPS
measurement or unit for the rate of pictures transmitted or displayed to create a video stream

Note 1 to entry: A rate of 25 IPS (PAL) or 30 IPS (NTSC) is considered to be real-time or full motion video.

3.1.48
Internet Protocol, version 4
IPv4
most widely used version of the Internet Protocol (the "IP" part of TCP/IP)

3.1.49
Internet Protocol Version 6
IPv6
successor to IPv4

Note 1 to entry: Already deployed in some cases and gradually spreading, IPv6 provides a huge number of available IP Numbers – over a sextillion addresses. IPv6 allows every device on the planet to have its own IP Number.

3.1.50
jitter
delay variation or continuity the packets arrive at their destination

Note 1 to entry: ´The received flow variation or pumping of stream´.

3.1.51
kilobits per second
kbit/s
unit of data transmission rate

3.1.52
latency
time that elapses between the initiation of a network request for data and the start of the actual data transfer

3.1.53
layer 2 switch
OSI (Open Systems Architecture) data link layer device responsible for transmitting data across the physical links in a network

3.1.54
layer 3 device
OSI device that determines network addresses, routes for information transport

EXAMPLE: A router is a layer 3 device; switches can also have layer 3 capability.

3.1.55
local area network
LAN
communications network serving users and devices within a limited geographical area, such as a building or a protected area

Note 1 to entry: This note applies to the French language only.

3.1.56
local-access layer
part of the network bringing edge devices into the network and providing operator access

3.1.57
login
account name used to gain access to a component to be used in combination with a password or the act of connecting to a component or system by giving valid credentials (usually “username" and "password")

3.1.58
managed switch
switch that can be monitored and administered in the network via its own IP address

3.1.59
media access control address
MAC address
unique identifier attached to network adapters i.e a name for a particular adapter

Note 1 to entry: This note applies to the French language only.

3.1.60
management information base
MIB
a structured collection of information for remote servicing using the SNMP protocol

Note 1 to entry: This note applies to the French language only.

3.1.61
multipurpose Internet mail extensions
MIME
standard for defining the type of payload streamed from a server to a client

Note 1 to entry: This note applies to the French language only.

EXAMPLE: ´video/h264´ is used for streaming H.264 encoded video.

3.1.62
MJPEG
motion JPEG
ISO/IEC digital video encoding standard, where each video frame is separately compressed into a JPEG image

3.1.63
MPEG-4
digital video encoding and compression standard that uses interframe encoding to significantly reduce the size of the video stream being transmitted compared to intraframe only encoding

Note 1 to entry: In interframe coding, a video sequence is made up of so called I- or key-frames that contain the entire image. In between the key-frames are delta frames, which are encoded with only the incremental differences. This often provides substantial compression because in many surveillance video sequences, only a small part of the pixel is different from one frame to another.

3.1.64
multicast
throughput-conserving technology that reduces throughput usage by simultaneously delivering a single stream of information, here video content, to multiple network recipients

3.1.65
N+1 fail-over
fail-over capability of N identical applications in operation by automatically switching over to 1 unused application instance

3.1.66
N+n redundancy
capacity of a parallel redundant system with N representing the number of applications needed to meet the critical load and n is the number of extra applications for redundancy purposes

3.1.67
network connectivity
the physical (wired or wireless) and logical (protocol) connection of a computer network or an individual device to a network

3.1.68
network design
way of arrangement of the various clients and servers in a network for the purposes of connectivity, performance, and security

3.1.69
network layer
Layer 3 of the OSI reference model, controlling communication links and data routing across one or more links

3.1.70
network management
administrative services performed in managing a network, such as network topology and software configuration, monitoring network performance, maintaining network operations, and diagnosis and troubleshooting problems

3.1.71
network performance
to stream data in accordance with requests from the security application

Note 1 to entry: Since video streaming is mostly real-time, it is critical to be delivered within a specific time.

3.1.72
network topology
pattern of connection between nodes in a network, e.g. hierarchical topology

3.1.73
node
communication device attached to a network or end point of a network connection such as a device attached to a network such as a workstation, IP video device, printer, etc.

3.1.74
network time protocol
NTP
standard for synchronizing computer system clocks in packet-based communication networks

Note 1 to entry: This note applies to the French language only.

Note 2 to entry: NTP uses the connectionless network protocol UDP (see UDP) for enabling time to be reliably transmitted over networks with variable packet runtime.

3.1.75
packet loss
the loss of data packets during transmission over a network

Note 1 to entry: ´The leak in the stream´.

3.1.76
packet switching
method used to transmit data in a network from many different sources on the same connection, directed along different routes to many different sinks at the same time

3.1.77
packets
data structures that collectively represent the transmission stream including headers and data associated with the network layer when the communication protocol is connection-oriented

3.1.78
physical topology
the physical layout of the network; how the cables are arranged; and how the components are connected

3.1.79
port
number or identifier for a particular service on a server, mostly standardized for certain services e.g. RTSP, UPnP, HTTP, etc.

3.1.80
protocol
set of rules governing how two components or entities communicate

Note 1 to entry: Protocols are used in all levels of communication. There are hardware and software protocols.

3.1.81
protocol data unit
PDU
unit of data equivalent to the frame which is passed between protocol layers

Note 1 to entry: This note applies to the French language only.

3.1.82
remote authentication dial-in user service
RADIUS
protocol using an authentication server to control network access

Note 1 to entry: This note applies to the French language only.

3.1.83
rapid spanning tree protocol
RSTP
link layer network protocol that ensures a loop-free topology for any bridged LAN including the basic function to prevent network loops and ensuing multicast functionality

Note 1 to entry: This note applies to the French language only.

3.1.84
redundancy (network)
alternative routing or protection switching to enable a reliable video transmission e.g. by Resilient Packet Ring (RPR),Spanning Tree Protocol (STP), Rapid Spanning Tree (RSTP)

Note 1 to entry: ´Identifying and replacing a broken link or stream´

3.1.85
request for comments
RFC
proposed and published internet standards, reviewed by the Internet Engineering Task Force, as consensus-building body that facilitates discussion, and eventually a new standard (STD) is established

Note 1 to entry: This note applies to the French language only.

3.1.86
router
device that routes information between interconnected networks, able to select the best path to route a message by determining the next network point to where a packet should be forwarded on its way to its final destination

Note 1 to entry: A router creates and/or maintains a special routing table that stores information on how best to reach certain destinations. A router handles the connection between 2 or more Packet-Switched networks by passing packets designated by source and destination addresses through and deciding on the actual route to send them on.

3.1.87
resilient packet ring
RPR
Layer 2 MAC-based protocol technology defined by IEEE's 802.17 for fast recovery from connection link failures and cuts at Layer 2

Note 1 to entry: This note applies to the French language only.

3.1.88
real-time control protocol
RTCP
supporting protocol for real-time transmission of groups within a network

quality-of-service feedback from receivers to the multicast group and support for synchronization of different media streams e.g. video, audio, metadata

Note 1 to entry: This note applies to the French language only.

3.1.89
real-time transport protocol
RTP
Internet protocol for transmitting real-time data such as video

Note 1 to entry: RTP itself does not guarantee real-time delivery of data. It only provides mechanisms for the sending and receiving streaming data. Typically is based on the UDP protocol.

Note 2 to entry: This note applies to the French language only.

3.1.90
real time streaming protocol
RTSP
control protocol standard (RFC 2326) for delivering, receiving and controlling real-time data streams such as video, audio and metadata and starting entry point for negotiating transports such as RTP, multicast and unicast, including the negotiating of Codec’s

Note 1 to entry: Can be considered as "remote control" for controlling video streams delivered by a server.

Note 2 to entry: This note applies to the French language only.

3.1.91
security certificate
SC
piece of exchanged information that is used by the SSL protocol to establish a secure connection

Note 2 to entry: This note applies to the French language only.

3.1.92
segment
section of a network

3.1.93
server
software program that provides services to other applications in the same or other computers

3.1.94
simple network management protocol
SNMP
set of standards for communication with devices connected to a TCP/IP network for the management of network nodes (servers, workstations, routers, switches and hubs, video transmission devices, etc), enabling network administrators to manage network performance, find, solve network problems and plan network extensions

EXAMPLE: Management systems get notified of network node problems by receiving traps or change messages from network devices implementing SNMP according to IETF RFC 1157, 1441, 3410.

Note 1 to entry: This note applies to the French language only.

3.1.95
simple network management protocol version 1
SNMPv1
simple request/response protocol for management system issuing requests to a managed network device that in return send a response according to IETF RFC 1157

3.1.96
simple network management protocol version 2
SNMPv2
identical protocol to SNMPv1 adding and enhancing some protocol operations and the SNMPv2 trap operation based on a different message format for replacement of the SNMPv1 trap according to IETF RFC 1441

3.1.97
simple network management protocol version 3
SNMPv3
SNMP protocol version adding security and remote configuration capabilities to the previous SNMP versions including the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control according to IETF RFC 3410

3.1.98
simple network time protocol
SNTP
adaptation of the Network Time Protocol (NTP) synchronizing computer clocks on a network, when the accuracy of the full NTP implementation is not needed according to IETF RFC 2030

Note 1 to entry: This note applies to the French language only.

3.1.99
single point of failure
SPOF
a component in a device, or a node in a network, which, if it were to fail would cause the entire device or network to fail, normally eliminated by adding redundancy

Note 1 to entry: This note applies to the French language only.

3.1.100
six nines availability
availability A of a system defined as A = MTBF/(MTBF + MTTR), describing the total time of availability for operation as a proportion of the total time no less than 0,999 999 or 99,999 9 %

3.1.101
simple network time protocol
SNTP
a simplified version of NTP

Note 1 to entry: This note applies to the French language only.

SEE: NTP.

3.1.102
simple object access protocol
SOAP
protocol for client-server communication used to exchange service requests and responses "on top of" HTTP exchanging data in a particular XML format specifically designed for use with SOAP

Note 1 to entry: This note applies to the French language only.

3.1.103
speed of data transfer
the rate at which information is transmitted through a network, usually measured in megabits per second

3.1.104
secure socket layer
SSL
application layer security protocol to enable encrypted, authenticated communications across networks

Note 1 to entry: This note applies to the French language only.

3.1.105
storage area network
SAN
high-speed network or sub network whose primary purpose is to transfer data between network devices and storage systems consisting of a communication infrastructure, providing physical connections, a management layer and storage elements

Note 1 to entry: This note applies to the French language only.

3.1.106
streaming performance
quality of the network stream determining how an operator perceives the information including the factors availability, errors, caused by noise, congestion or component failures, delay, jitter, throughput, loss

3.1.107
subnet mask
method that allows one large network to be broken down into several smaller ones

Note 1 to entry: Depending on the network class (A, B, or C), some number of IP address bits are reserved for the network address (subnet) and some for the host address. For example, Class A addresses use 8 bits for the subnet address and 24 bits for the host portion of the address.

3.1.108
switch
device that connects network devices to hosts, allowing a large number of devices to share a limited number of ports

3.1.109
transmission control protocol/Internet protocol
TCP/IP
suite of protocols that define networks and the Internet in general

Note 1 to entry: This note applies to the French language only.

3.1.110
throughput (network)
digital transmission capacity to support the required quality of the video stream

EXAMPLES: 1 Mbit/s up through 10 Mbit/s.

Note 1 to entry: The size of the possible video stream pipe.

3.1.111
time protocol
network protocol allowing time clients to obtain the current time-of-day from time servers

3.1.112
topology
(physical) network configuration including cables other equipment

(logical) flow of data between logical entities including the specification of protocols involved independent of the physical location

3.1.113
transceiver
transmitter/receiver
device that receives and sends signals over a medium

3.1.114
transport stream
TS
content binary stream usually in reference to an MPEG-2 AV stream format

Note 1 to entry: This note applies to the French language only.

3.1.115
user datagram protocol
UDP
stateless protocol for the transfer of data without provision for acknowledgement of packets received

Note 1 to entry: This note applies to the French language only.

3.1.116
universal plug and play
UPnP
architecture for pervasive peer-to-peer network connectivity of devices of all form factors

Note 1 to entry: It is designed to bring easy-to-use, flexible, standards-based connectivity to ad-hoc or unmanaged networks. It is a distributed, open networking architecture that leverages TCP/IP and Web technologies to enable seamless networking in addition to control and data transfer among networked devices.

Note 2 to entry: This note applies to the French language only.

3.1.117
unmanaged switch
basic switch that does not offer remote network administration capability

3.1.118
uniform resource identifier
URI
address for resources available on a network starting with a “scheme" such as HTTP or RTSP

Note 1 to entry: This note applies to the French language only.

3.1.119
uniform resource locator
URL
unique address for a file that is accessible on the Internet

Note 1 to entry: This note applies to the French language only.

Note 2 to entry: URL was previously Universal Resource Locator.

3.1.120
unicode transformation format
UTF
character code preserving the full US-ASCII range, providing compatibility with file systems, parsers and other software that rely on US-ASCII values but are transparent to other values

Note 1 to entry: This note applies to the French language only.

3.1.121
UTF-8
encoding schema with UCS-2 or UCS-4 characters as a varying number of octets, where the number of octets, and the value of each, depend on the integer value assigned to the character in ISO/IEC 10646

3.1.122
video transmission device
VTD
video device with at least one IP network interface handling video

Note 1 to entry: This note applies to the French language only.

3.1.123
wide area network
WAN
network connecting computers within large areas, e.g. beyond the limits of a single protected site

Note 1 to entry: This note applies to the French language only.

3.1.124
workstation
computer connected to a network at which operators interact with the video display

3.1.125
XML
eXtensible Markup Language
widely used protocol for defining data formats, providing a very rich system to define complex data structures

Note 1 to entry: This note applies to the French language only.

3.1.126
XML schema
definition including constrains of data in an XML document

3.2 Abbreviations

AAC	Advanced Audio Codec
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
ATM	Automatic Teller Machine
AVC	Advanced Video Codec
CIF	Common Intermediate Format
CPU	Central Processing Unit
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DVR	Digital Video Recorder
DVB	Digital Video Broadcast
GPS	Geo Positioning System
H.264-CBP	ISO/IEC 14496-10 and ITU H.261 Reduced complexity Baseline Profile
HD	High Definition
HTTP	Hypertext Transfer Protocol
I/O	Input / Output
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IESG	Internet Engineering Steering Group
IGMP	Internet Group Multicast Protocol
IP	Internet Protocol
ISO	International Standards Organization
IT	Information Technology
JPEG	Joint Picture Experts Group
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Message Authentication Code
MD 5	Message Digest Algorithm Version 5
MIB	Management Information Base
MIME	Multipurpose Internet Mail Extensions
MJPEG	Motion JPEG
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
NAS	Network Attached Storage
NTP	Network Time Protocol
NTSC	National Television System Committee
NVR	Network Video Recorder

OASIS	Organization for the Advancement of Structured Information Standards
OID	Object Identifier
OR	Operational Requirements
OSI	Open Systems Interconnection
PAL	Phase Alternation Line
PC	Personal Computer
PDU	Protocol Data Unit
PING	Packet Internet Groper
POS	Point of Sales
PPM	Packets Per Million
PTZ	Pan / Tilt / Zoom
RFC	(Request for comment) IETF Standards Draft
RPR	Resilient Package Ring
RSA	(Public Key Cryptosystem invented by) Rivest, Shamir and Adleman
RTCP	Real Time Control Protocol
RTP	Real-time Transport Protocol
RTSP	Real Time Streaming Protocol
SDP	Session Description Protocol
SMI	Structure of Management Information
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SOAP	Simple Object Access Protocol
SPOF	Single Point of Failure
SRTP	Secure Real-time Transport Protocol
SSL	Secure Sockets Layer
SSM	Source-Specific Multicast
STD	Standard
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TLS	Transport Layer Security
TS	Transport Stream
TTL	Time-to-live
UCS	Universal Character Set
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTC	Universal Time Coordinated
UTF	Unicode Transformation Format
UTF-8	8-bit Unicode Transformation Format
VACM	View-based Access Control Model
VCA	Video Content Analysis

VSS	Video Surveillance System
VT	Video Transmission
VTD	Video Transmission device
W3C	World Wide Web Consortium
WAN	Wide Area Network
WSDL	Web Services Description Language
XML	eXtensible Markup Language

4 Performance requirements

4.1 General

This video transmission standard addresses the requirements of devices in security applications with differing application characteristics, such as embedded, PC based, operator workstations, and others. Digital encoding and decoding video devices, VSS client workstations, video storage, NVRs and DVRs have a differing set of functions in video streaming and network connectivity. The following summarizes these functionalities:

– stream encoding
– stream receiving and decoding
– stream recording
– live streaming and displaying
– playback streaming and replaying
– camera controlling
– health and status monitoring
– video content analysis
– metadata creation and streaming
– auxiliaries

Due to the nature of non-analog video transmission, especially video IP networks, using shared connections, compression and streaming techniques, following requirements shall be applied:

For different applications, such as PTZ camera tracking, recording, video motion detection, remote monitoring, etc., there are different requirements on the performance of VTDs. Therefore this standard introduces different performance classes. For each application the requirements shall be specified and include classes for: time service accuracy (Table 1), interconnection timing (Table 2), throughput sharing (Table 3 and 4), streaming (Table 5), network jitter (Table 6) and monitoring (Table 7).

Different functions of the system can have different performance classes.

NOTE Performance classes are independent of security grades.

These requirements do not apply to mobile cell based interconnections, but shall be applied to fixed wireless network connections and transport applications, such as on-board systems.

If minimum requirements on the network performance for the proper operation of a VTD or VSS exist, these shall be defined and documented.

The requirements start at a lower class 1 and grow with the classes, the higher the number.

4.2 Network time services

4.2.1 General

The Video Transmission Device (VTD) will require network time services for a real-time clock, eventing, logging and for the video transport stream (TS).

The VTD shall never start streaming video for recording purposes, if the requirements below on the accuracy of the time stamping of the video frames cannot be granted. This shall especially be verified after start-up or re-initiation after power loss of the VTD. Otherwise the integrity of the stream recordings may be corrupted and may not allow the correct replay not only of the concerned frame sequences, but also of other recordings. This has even higher impact on images used for the evidential purposes.

4.2.2 Real-time clock

The real time clock in the Video Transmission device should be synchronized with a time normal using RFC 2030, Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI. The addresses of the SNTP servers should come from the Time Server DHCP option (4). The more accurate system time shall be used as default: the SNTP best accuracy is 0,25 µs, whereas the usage of the ´Time Server´ according to RFC 868 offers only a best accuracy of 1 s.

4.2.3 Accurate time services for the transport stream

As an option, Network Time Protocol (NTP) (Version 3) as detailed in RFC 1305 should be implemented when time services with an accuracy of 1 ms to 50 ms according to the requirements of Table 1 are needed. The IP addresses of the time servers should come from the Network Time Server DHCP option (42). The Network Time Protocol should be tried first and only on failure shall Simple Network Time Protocol be used. A null Network Time Server DHCP option (42) means no server is available and Simple Network Time Protocol should be used.

Table 1 – Time service accuracy for video transport stream

Class	T1	T2	T3	T4
Time service accuracy for transport stream	80 ms	40 ms	5 ms	1 ms

The NTP timestamps in the Real Time Protocol header shall increase steadily over consecutive packets in the RTP stream. They should correspond to local time and shall be adjusted, if necessary, to stay consecutive. After VTD restart, the system time re-synchronisation may be delayed up to 10 s for SNTP or up to 15 s for time server protocol (NTP).

4.3 Video transmission timing requirements

4.3.1 General

Video Transmission devices and their interconnections shall be designed in accordance with the system requirements IEC 62676-1-1 as part of the VSS.

4.3.2 Connection time

The connection time needed to initiate the transmission of a stream from a source to a receiver is of interest. This time has to be considered especially in systems where camera roundtrips, sequencing or guard tours of different cameras is needed. The initial connection time shall be much lower than the dwell time of the camera sequence, see Table 2.

Table 2 – Interconnections – Timing requirements

Video transmission devices shall have a maximum	Class			
	I1	I2	I3	I4
Initial connection time for every new video stream request of	2 000 ms	1 000 ms	500 ms	250 ms

NOTE In RTSP Multicast streams an I-Frame request optimizes this connection time.

4.3.3 Connection capabilities

If a VSS video transmission network is designed and configured in a way that single or multiple video transmission receiver devices request video images and the simultaneous request of image streams by all possible receivers may exceed the available capacity of the network at a time, the video transmission device shall offer means according to following Table 3.

Table 3 – Video transmission network requirements

Video transmission devices in a shared network shall offer means to configure:	Class			
	C1	C2	C3	C4
the maximum data rate of video streams for every video channel			X	X
the maximum data rate for all available video streams of a single device			X	X
the maximum data rate or number of video streams to all client devices in the network			X	X

Table 4 – Video transmission network requirements

Video transmission devices in a shared network shall offer means to:	Class			
	P1	P2	P3	P4
Prioritize certain streams over others, e.g. streams for recording or alarms over live image streams			X	X
Prioritize certain users over others, e.g. for PTZ control			X	X

At no time the video transmission receiver shall allow the opening and initializing of connections to new video stream sources on cost of the video streams already displayed or recorded in order to avoid frame loss

At no time the video transmission receiver shall allow the display of live streams on cost of the video streams recorded, in order to avoid frame loss.

If the qualities of video for live viewing by an operator and for recording needs to be different, the video transmission device shall offer a minimum of 2 streams of different quality settings.

If the quality of video for continuous recording and for event based alarm recording needs to be different, the video transmission device shall offer an additional stream, if the quality setting is different from the other 2.

4.4 Performance requirements on streaming video

4.4.1 Introduction latency, jitter, throughput

Recommendations given in this subclause are informative.

Video streams are sensitive to accumulated delay, which is known as latency. The network contributes to latency in several ways:

- Transmission delay – The length of time a video packet takes to cross the given media. Transmission delay is determined by the speed of the transmission media and the size of the video packet.
- Forwarding delay – The length of time an internetworking device (such as a switch, bridge, or router) takes to send a packet that it has received.
- Processing delay – The time required by a networking device for looking up the route, changing the header, and other switching tasks. In some cases, the packet header has also to be manipulated. For example, the encapsulation type has to be changed. Each of these steps can contribute to the processing delay.
- Coding/Decoding Delay – The time required to encode and/or decode an image to or from a video stream, which is influenced by the performance of the VTD and the type, profile and level of CoDec. For instance the H.264 profiles ´Main´ with 350 ms and ´Baseline´ Profile with 120 ms coding delay or MPEG4 may offer a delay of 110 ms and MPEG2 Low Delay with less than 180 ms.
- Display Delay – The time required by the presentation unit to change the appearance of a picture element, usually not to be considered

4.4.2 Requirements on network jitter

If a VSS network sends video data with variable latency, it introduces jitter. The most common technique to reduce jitter is to store incoming video data in a buffer from where it is displayed. The buffer reduces the effect of jitter like a shock absorber.

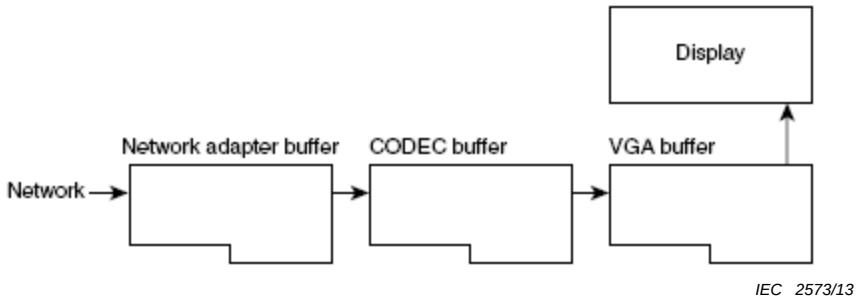


Figure 1 – Network buffer

The overall need is that even when video traffic has a jitter, the operator watching the video images shall not be destructed. For that reason, video security networks shall use techniques to minimize jitter for live and replay streams.

One way to provide minimized jitter and packet loss is to increase network speeds to assure that sufficient throughput is available during event- and peak-traffic times.

4.4.3 Packet loss

There are different reasons for network packet loss. Packet loss may be introduced by network congestion, where a network is over-utilized or –subscribed, other traffic may be blocking, and network infrastructure equipment may face problems and fail. The network may be configured in a wrong way e.g. with duplicate IP addresses.

In IP video streaming packet loss may have impact on the video quality, may cause frame blocking, local image distortions with unclear images areas, smear, artefacts, pixelization, blur, flicker, decreasing frame rates, frozen images. In addition packet loss can also cause excessive latency and delay possibly leading to VTD stream disconnections.

NOTE In broadcast industry a packet loss of 100 ppm or one lost packet per minute for 2CIF MPEG-4 real-time streams is generally considered as un-viewable and 2 ppm or one lost packet per hour as unacceptable for the user according to the DVB standard.

The impact of packet loss on video streaming depends upon a number of factors including the percentage of packet loss, the distribution of loss over time and the capabilities of the VTDs to handle loss. In differential encoded video streams the current frame is predicted from the previously transmitted video. Video packets are dependent on previous packets. If these packets have not been successfully received, then the current packet is not useful. This is known as loss propagation. This propagation stops with the arrival of intra coded frames (I-Frames).

The VTD shall be capable to detect packet loss and compensate the effects. The VTD shall be able to provide an acceptable operator and user experience and video perception during packet loss. The reduction of the visual effects associated with the stream delivery is critical to the end-user retention. At least the visual impression of the packet loss shall be masked or hidden according to the needs to fulfil the surveillance task and objective. A VTD shall offer state-of-the art error and loss concealment techniques. The VTD shall offer any packet loss or error concealment capability e.g. by using packet information of the encoded video from neighbouring macroblocks, prior or future frames, in order to estimate the video content of the current frame.

4.4.4 Level of performance

When addressing performance needs of Streaming-Video traffic, the following requirements apply, see Table 5.

Table 5 – Performance requirements video streaming and stream display

Class	S1	S2	S3	S4
Maximum Loss	240 ppm	120 ppm	60 ppm	30 ppm
Maximum one-way latency live stream (incl. encoding, networking, decoding, display)	600 ms	400 ms	200 ms	100 ms
Max Trick Play (Pause, Single Step,,..) Reaction Time	400 ms	200 ms	200 ms	100 ms
Round-trip latency incl. visualisation and control e.g. PTZ	700 ms	500 ms	300 ms	200 ms
Round-trip latency incl. visualisation and control e.g. PTZ, when moving objects need to be monitored and tracked	650 ms	450 ms	250 ms	150 ms

Streaming video archives and recordings have easier performance requirements because they are not sensitive to delay (the video can take some time to cue up) and are largely not jitter sensitive (because of application buffering). Streaming-Video might contain valuable content, such as security applications, in which case it requires performance guarantees.

Since the performance of video streaming is evaluated best by the visual impression, it is best to test and verify the display performance parameters. The general requirement for the display of streaming video shall offer a smooth visual impression to the end-user. The display jitter shall be no more than 1/10 of the frame rate interval.

4.4.5 Packet jitter

The maximum peak-to-peak packet jitter is defined as the variation in delay between the live or replay source of the stream and the end device. The peak-to-peak jitter, J, implies that the deviation in network delay, d, is bounded by $-J/2 \leq d \leq +J/2$. To give a technical comparison and an example, the Video Transmission device according to Class M4 shall comply with the Real Time Interface Specification of ISO/IEC 13818-9 with jitter of 20 ms.

Table 6 – Video stream network packet jitter

Class	M0 ms	M1 ms	M2 ms	M3 ms	M4 ms
Maximum peak-to-peak packet jitter	-	160	80	40	20

The VTD receiver has to offer a buffer for compensating the specified jitter. This actually means that a VTD has to offer bigger buffers to achieve a proper receiving and decoding of video frames with larger jitter. This delay adds up in the VTD receiver buffer, which shall be large enough to compensate for variation in the inter-arrival times (jitter).

4.4.6 Monitoring of interconnections

Table 7 specifies the maximum permitted period for an interconnection or signal to be unavailable. If an IP video connection for streaming, health check, or eventing is failing and the maximum permitted period is exceeded a tamper or fault signal or message shall be generated as specified in IEC 62676-1-1.

Table 7 – Monitoring of interconnections

The system shall offer	Security grade			
	1	2	3	4
Maximum permitted duration of device unavailability			180 s	30 s
Maximum detection time for live signal loss		8 s	4 s	2 s
The requirement above is intended to establish if communication is possible by monitoring the communication video to ascertain if it is available to convey a signal or message. Monitoring may take the form of listening for jamming when a video transmission device communicates via shares interconnections with other devices or other applications.				

NOTE These requirements correspond to IEC 62676-1-1:2013, Table 4 requirement 3 and Table 5 requirement ´video loss´

5 IP video transmission network design requirements

5.1 General

To give an understanding how the IP video network performance requirements of the previous clauses are covered in an installation, it's not only important to select and configure standardized IP video surveillance components, but also to provide an appropriate network structure. To ensure the performance of a video transmission network according to the requirements listed above following procedure to design a network is recommended:

Overall a VSS and its interconnections shall be designed in accordance with IEC 62676-1-1. There are three important elements to consider when designing an effective VSS:

– technical infrastructure
– operational requirements (OR)
– operational-processes and -procedures

This section details the design requirements for the VSS installation, focusing on IP connections and communications.

5.2 Overview

The two most important design elements are determining the number of video streaming servers and sources (i.e. IP video encoding devices) and the number of receivers or clients (user Interfaces, workstations, recording devices, decoders), because they define the load,

which can vary very much. These two factors are closely related, and influence each other. It is a combination of these two elements that have impact on a successful system design.

5.3 Digital network planning

5.3.1 General

For a proper network design follow these steps:

1) Map the necessary logical connections of the planned physical network infrastructure
2) Define a topology that matches the required connectivity
3) Plan network redundancy
4) Define baseline network traffic data based on continuous video stream at required visual resolution for recording and display of static and moving scenes
5) Simulate video stream traffic to verify this baseline data
6) Define capacity needs on average and peak video stream data based on user requested video to workstations, continuous video stream recordings and motion or alarm video recordings
7) Define a figure for the average and maximum simultaneity of streaming sources, the so-called selective factor
8) Identify each network link's throughput requirement in access-, distribution- and core layer
9) Identify potential bottlenecks. WAN links can be IP video traffic bottlenecks
10) Examine thoroughly the network hardware infrastructure to ensure support for immediate and future expansion in surveillance or Video Streaming capacity needs
11) Accurately document the network's topology, actually used capacity and maximum capacity.

5.3.2 Critical requirements for IP video streaming performance

5.3.2.1 General

To support video traffic equivalent quality standards and performance figures shall be met for acceptable video streaming services (see Figure 1). Four factors – throughput, latency, jitter, and packet loss – are critical from the network point of view. The management of each determines how effectively the network supports IP video traffic. In this standard an approach is specified, where a proper network design and overall system management guarantees the quality and performance of the video stream.

A fifth factor ´alternative routing´, the so-called ´protection switching´, is also an important consideration to help protect critical VSS- and operator-traffic.

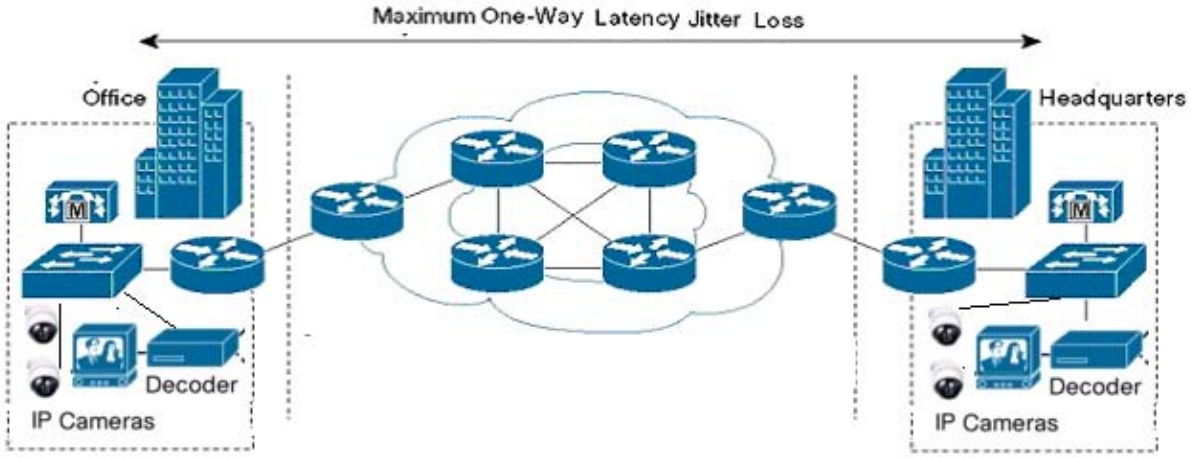


Figure 2 – Network latency, jitter, loss

5.3.2.2 Throughput: stream capacity planning

Before video related data is placed on a network, it has to be ensured that the network can support all existing applications (if any) together with the required data rate associated with the quality of video to be transported over the network. First, calculate the minimum data rate requirements for each major video node. The sum represents the minimum data rate requirement for any specific link. This amount shall consume no more than 75 % of the total data rate available on that link. This 75 % rule assumes that some data rate is necessary for overhead traffic. Examples of overhead traffic include routing protocol updates and keep-alives, as well as additional applications, such as VSS management and configuration traffic.

5.3.2.3 Streaming performance and stream management

One of the key requirements for the deployment of IP video is the ability to offer a streaming quality equivalent to the existing analogue VSS over Coax as a means for a much higher video throughput and quality. Perceived Video quality is very sensitive to three key performance criteria in a digital packet network, in particular: delay, packet loss, achievable bit rate (influencing compression level and artefact, resolution and framerate) IP, by its nature, provides a best-effort service and does not provide guarantees about the key criteria listed above.

5.3.3 Availability

The required availability can be achieved in an IP video network by using redundant and load-balancing and -sharing equipment and networks. The connection of a video encoder, the access gateway, trunk gateway and network video recorder need to be fault tolerant. The types of functionality often used to achieve fault tolerance include:

– redundant hardware
– redundant network connections
– N+n redundancy
– hot-swap capability
– fail-over capability for all components
– N+1 fail-over capability for one out of N identical components
– no single point of failure, except cameras and encoding
– dual network port video source devices e.g. IP cameras or encoders
– configuration, software and firmware that can be changed and upgraded without loss of service.

Alternative network traffic-protection schemes such as RSTP according to IEEE 802.1w shall provide a spanning tree convergence after a topology change or network failure within 1 second. STP shall respond within 30 s to 50 s.

5.4 Additional architecture principles

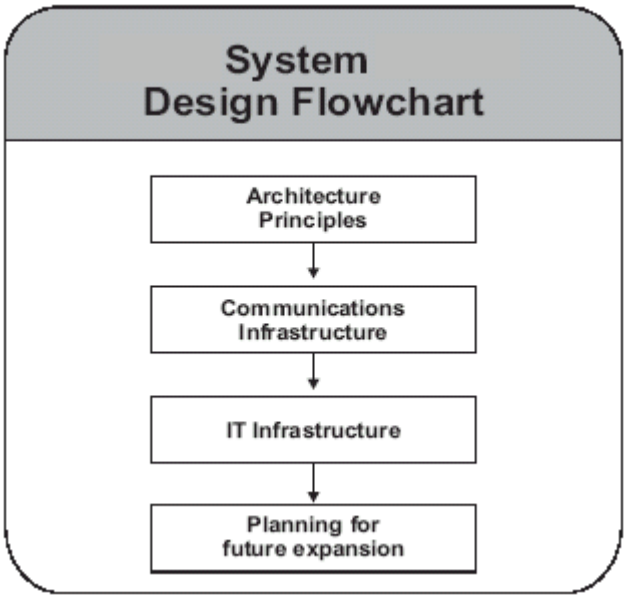


Figure 3 – System design

The architecture shall be based on the following principles:

1) separate functional components of the system to provide reliability and redundancy
2) ensure a controlled environment for reliability of devices and the comfort of operators
3) understand the design parameters in normal operation and in a second step in alarm-, or peak- situations, when event response times are higher than planned. When the VSS installation grows in size, the peak loads tend to average over time and sites
4) other principles (see Figure 3)

5.5 Network design

5.5.1 Small unicast network

The Figure 4 below depicts a LAN with three video surveillance workstations A, B and C, a video server D, a network video printer E, and a router F. This network is used to support a small surveillance system with up to 30 IP video channels.

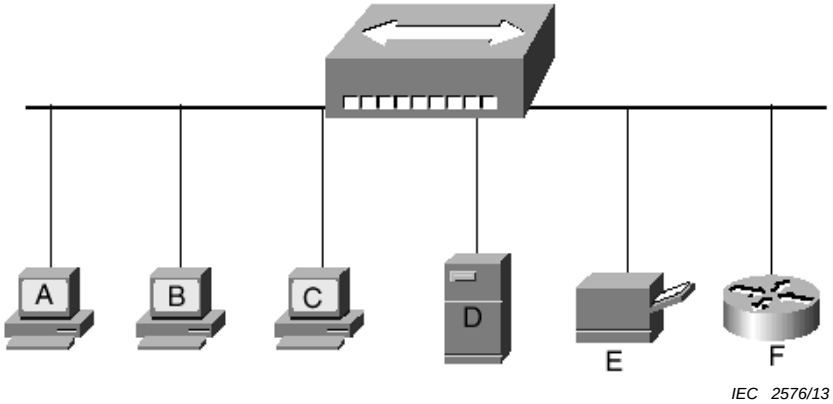


Figure 4 – Small network

5.5.2 Small multicast video network

The Figure 5 below depicts a LAN with three fixed workstations, a video server, a network multicast switch and more than 30 cameras. This network is used to support a small multicast surveillance system with over 30 IP video channels and multiple operators and clients monitoring most of the time the same video sources.

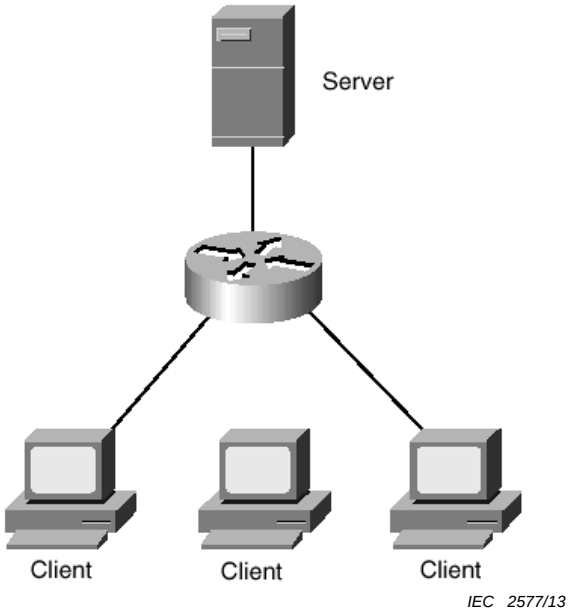


Figure 5 – Multicast network

5.5.3 Hierarchical VSS network

A hierarchical network design includes the following three layers of Figure 6:

- the backbone layer or core layer that provides optimal transport between sites or system functionality e.g. recording
- the distribution layer that provides connectivity
- the local-access layer that brings video transmission devices into the network and provides operator access

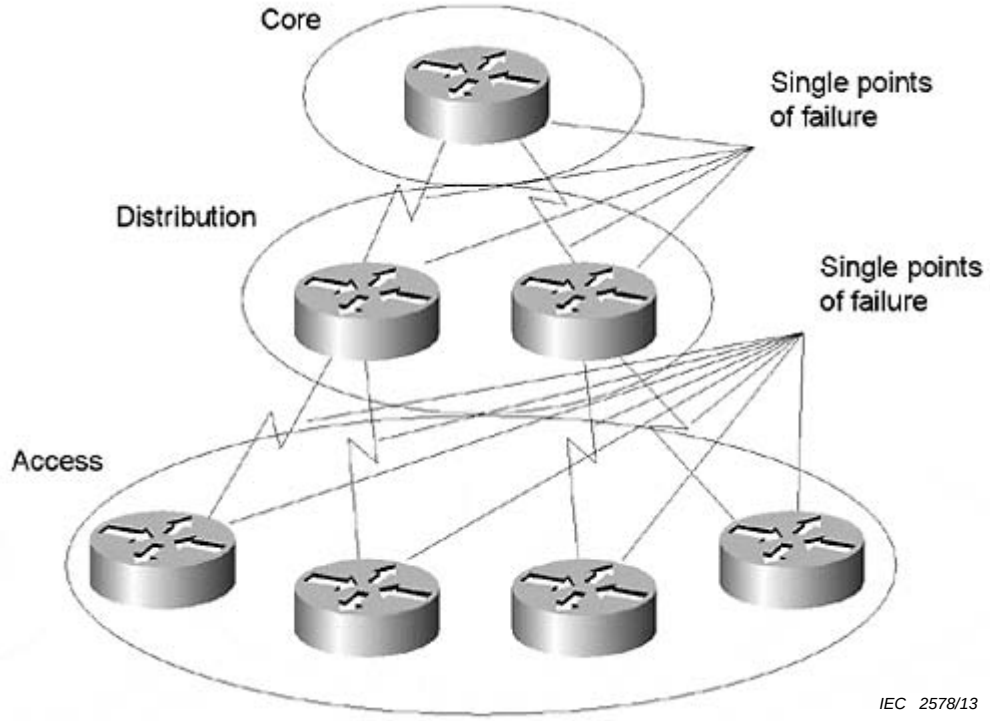


Figure 6 – Hierarchical network

Larger IP Video networks shall be based on the hierarchical network model. This model divides a network into three layers: core, distribution, and access layer.

The access layer is responsible for connecting devices to the network. Its defining characteristics generally are a high port density and/or the ability to overcome physical edge device or "last mile" challenges.

The distribution layer is where policies are applied. It is where access-lists and CPU intensive routing decisions shall occur (as opposed to just a default route or default gateway). Distribution layer designs focuses on aggregating access devices into components with high processing resources so that policies can be applied.

The core layer is the "backbone" of the network. Its job is simply to move high amounts of video stream packets from multiple video sources A to video receiver B as fast as possible and with the least possible manipulation.

Core and distribution are only separated into different switches in large networks. Very often in smaller IP video environments, one switch takes over both the tasks of the core and the distribution layer.

5.5.4 Effective video IP network capacity planning

IP video and network engineers, consultants and administrators characterize network capacity as the amount of traffic the network is designed to handle. Discussing network capacity in IP video systems becomes more a measure of how many simultaneous video streams the network can process. This concept of **"peak load"**, the maximum assumed video stream volume that the network shall be able to handle, will be the basis of the capacity planning process. During **capacity planning** the following shall be considered:

- number of encoders/cameras on the network
- video codec's and their performance in the VSS solution

- existing data traffic on the network
- decentralized or centralized recording and video content analysis
- connectivity to network storage, video recorders, video motion detectors
- number of streams of the encoders provided and the number of clients each one supports
- number of users and video operator clients in the network
- existing local area network (LAN) and/or wide area network (WAN) designs
- existing and selected network's hardware infrastructure
- network redundancy
- spare throughput available in the network

5.5.5 Wireless interconnections

When wireless interconnections are employed the factors below shall be considered:

1) siting of antennas to ensure reliable communication with other system components;
2) possibility of other RF equipment interfering with VSS interconnection equipment;
3) proximity of large metal objects to the equipment antenna;
4) possibility of intruders to interfere or block the interconnection.

5.6 Replacement and redundancy

5.6.1 Redundant network design

Redundancy provides alternate routes around single points of failure (SPOF).

Redundant network designs try to meet requirements for network availability by duplicating network links and interconnectivity devices. Redundancy eliminates the possibility of having a single point of failure on the network. The goal is to duplicate any required component whose failure could disable critical applications. The component could be an analog video matrix switch, a core router, a camera, a video encoder or decoder, a power supply, a network trunk line, a digital video recorder and so on.

Since redundancy is expensive to deploy and maintain, redundant topologies should be implement only where needed. A level of redundancy shall only be selected according to the requirements of the operational requirements for availability and affordability. Redundancy adds complexity to the network topology. Redundancy for cameras may be covered by a PTZ camera able to navigate to the scene of several static cameras or by a positioning of cameras, where the field of view of one camera is part of the following camera at a lower quality level.

A single point of failure is any device, interface on a device, or link that can inhibit the VSS from a certain surveillance task if it fails. Networks that follow a strong, hierarchical model tend to have many single points of failure because of the emphasis on summarization points and points of entry between the network layers. For example, in a strict hierarchical network, such as the one depicted in Figure 6, every device and every link is a single point of failure.

There are different designs to provide redundancy in the **core layer**. If the entire core network is in one building or one small protected site, each router is connected to two high speed LANs, Router A and B of Figure 7.

If the core routers are not all in one building or within one protected site the options become more limited.

The two most common methods for providing redundancy at the **distribution layer** are dual homing and backup links to other distribution layer routers

Dual homing **access layer** devices are the most common way of providing redundancy to remote locations within one protected site, but it is also possible to interconnect access layer devices to provide redundancy.

In Figure 7 Router G and Router H are access layer routers that are dual-homed with the backup circuit connected to different branches of the distribution layer.

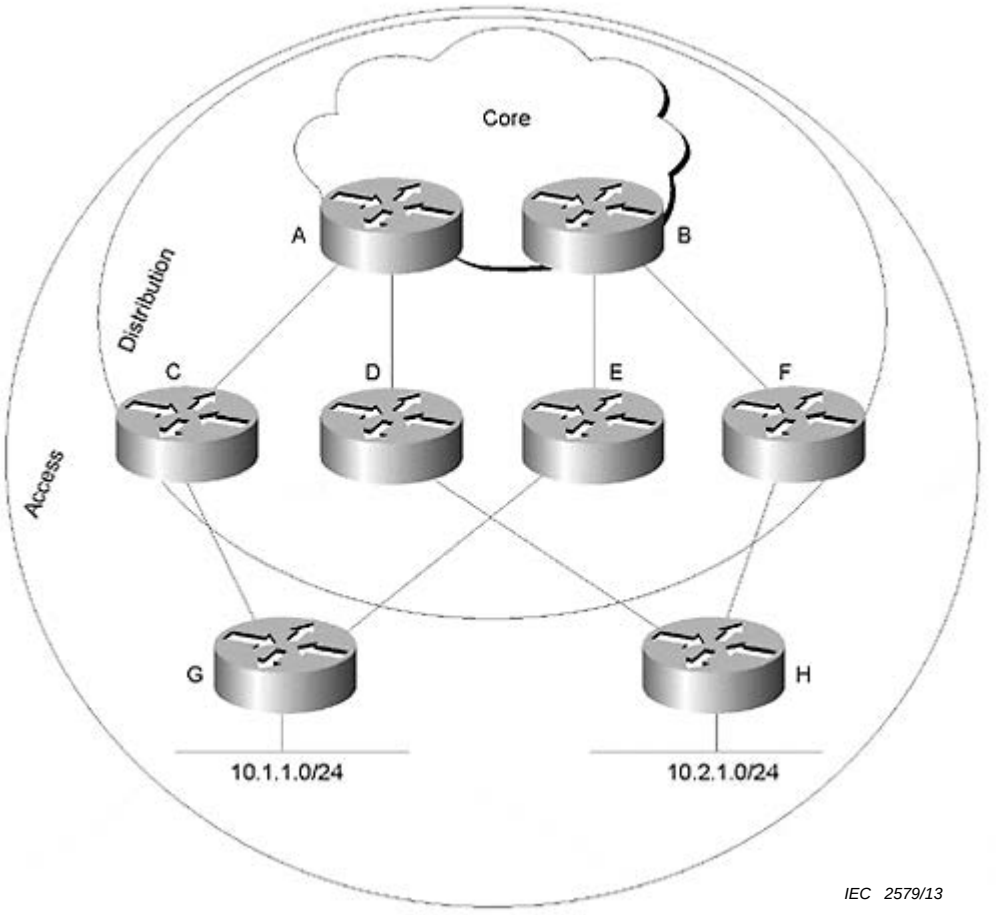


Figure 7 – Redundant network

5.6.2 Availability

Operational requirements (OR) assuredly demand a level of availability of the video network.

The mean time between failures (MTBF) of the components shall be considered when designing the network, the same for the mean time to repair (MTTR). Designing logical redundancy in the network is as important as physical redundancy. The VSS assembly shall have a minimum MTBF of 16 000 h based on IEC/TR 62380, IEC 61709, and IEEE 1413.1-2002.

5.7 Centralized and decentralized network recording and video content analytics

A VSS network can include all possible variants of centralized recording and video content analytics (VCA) or decentralized recording and VCA at the camera location.

There are many factors that influence the decision for centralized or decentralized recording and VCA. For example if the network covers several buildings, recording shall be located in each building. But central viewing and evaluating the recorded video data is easier in a centrally recording environment. Centralized recording is realized when the storage devices

are connected to the core switch, the same for centralized VCA. The entire network shall be able to transport the recorded video data or the streams to be analysed.

Decentralized recording or VCA is realized when the storage or VCA devices are connected to the Access layer switch. The network is segmented into “traffic zones”. The recorded or analyzed video data stays within the subnets and does not flood the network. If decentralized recording or VCA is realized, the access switches shall be designed for the expected traffic.

From the IT point of view the centralized solution will always be preferred. A centralized solution is easier to manage, backed up and easier to scale. Additionally all management software and hardware is concentrated e.g. in the control centre or in a part of the building. “At the edge” there is only cameras and encoders. The disadvantage of centralized recording or VCA is that one needs very powerful (and expensive) core switches. Another disadvantage is that fall-back solutions are complex. If the core switch fails, the entire system stops working when there is no failover. The decentralized solution offers more stability. When a switch or network segment fails, recording and VCA in the other segments are not affected. The scalability of decentralized recording is restricted. When new cameras are added to all network segments, the storages in the segment are possibly too small and shall be exchanged. In a centralized solution it is sufficient to exchange or expand the central storage device. Direct recording to NVR or network attached storage (NAS) is completely independent from switches. As long as the encoder and the storage device are up and running, recording continues. But therefore a number of small storage devices are needed which might be much more expensive than one large storage device.

A disadvantage of centralized VCA is that analysis is performed on the transmitted video stream, which is compressed in the given resolution and frame rate including artefacts.

6 General IP requirements

6.1 General

The intent of this clause is to specify basic network requirements and protocols, with a preference for existing, well-known and well accepted standards. This interface specification is written to provide the minimal set of requirements for video streaming and supporting protocols between VTD servers and clients. Overall the IP network shall support DNS, IPv4, DHCP, TTL, optionally IPv6.

6.2 IP – ISO Layer 3

All entities of a video transmission device shall be capable of implementing IP (Internet Protocol) as Layer 3 protocol. In order to ensure interoperability with existing TCP/IP networks, the entities shall implement IPv4 as defined in RFC 791. Support for IPv6 as defined in RFC 2460 is optional.

NOTE In the remainder of this text all references to IP (only ´IP´) is interpreted as IPv4.

6.3 Addressing

The foundation for networking is IP addressing. Each VTD shall have a Dynamic Host Configuration Protocol (DHCP) client and search for a DHCP server when the device is first connected to the network. If no DHCP server is available, in a so-called unmanaged network, the device shall assign itself an address. If during the DHCP transaction, the device receives a domain name, for example, through a DNS server or via DNS forwarding, the device should use that name in subsequent network operations; otherwise, the device should use its IP address.

This clause defines the IEC 62676-1-2 IP configuration compliance requirements on VTDs. The main requirements are listed below.

IP Configuration

The video transmission device shall have at least one network interface that gives it IP network connectivity and allows video and data exchange between video transmission devices e.g. between video transmission server and client.

It shall be possible to make static IP configuration on the video transmission device using a network or local configuration interface.

IPv4 addressing

The video transmission device should support dynamic IP configuration of local-link address according to RFC 3927.

The video transmission device may support any additional IP configuration mechanism.

IPv6 addressing

A video transmission device that supports IPv6 shall support stateless IP configuration according to RFC 4862 or shall support stateful IP configuration according to RFC 3315 or both.

DHCP

The video transmission device shall support dynamic IP configuration according to RFC 2131.

The preferred method of assigning an IP address to an entity is via DHCP according to RFC 2131. Each node supporting this layer shall have a function to obtain address setting information using a DHCP server. For operation, it is highly recommended that a DHCP server is deployed into an IP video network.

This standard does not specify any dynamic IP address setting method other than DHCP.

6.4 Internet control message protocol (ICMP)

6.4.1 General

ICMP messages are sent in several situations: for example, when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route.

6.4.2 Diagnostic requirements

To facilitate troubleshooting, the system entities shall implement the ´PING command according ICMP (RFC 792). According to RFC 1122 any host shall accept an echo-request and issue an echo-reply in return.

Any network host shall be able to send ICMP “echo request” packets to the video transmission target and listen for ICMP “echo response” replies. This provides a valuable diagnostic capability.

All video transmission clients shall be compliant to RFC 1122, that any host shall accept an echo-request and issue an echo-reply in return.

According to the Echo Request/Reply of RFC 792, every host shall implement an ICMP Echo server function that receives Echo Requests and sends corresponding Echo Replies. An ICMP Echo Request destined to an IP broadcast or IP multicast address shall be silently discarded.

The IP source address in an ICMP Echo Reply shall be the same as the specific-destination address of the corresponding ICMP Echo Request message. Data received in an ICMP Echo Request shall be entirely included in the resulting Echo Reply.

6.5 Diagnostics

For an easier diagnosis and maintenance of the video transmission network and its devices, the VTD should signal the basic network connection status via indicators e.g. LEDs next to the network connector, which should show the operating status and indications of possible failures and malfunctions:

If no other specification is given for a VTD, following indicator colours should represent the listed network connection status: A steady lighted green indicator should signal the status for a 10 Mb network connection, a green and orange for 100 Mb, orange for 1 Gb. A blinking of the indicator(s) every second should represent an ongoing data transmission. If no connection can be established, the indicator(s) should not be lighted. A lighted red indicator should signal the start-up process of a VTD. During a firmware upgrade the indicator should fast blink red. A blinking red every second should signal a VTD failure or defect such as broken power supply, fans, a corrupt configuration or firmware.

6.6 IP multicast

6.6.1 General

If a VTD is supporting multicast, then it shall operate according to RFC 1112. If a VTD is not supporting multicast according to this standard, it shall be clearly specified that the ´VTD is not supporting multicast´. All multicasting devices shall support Source Specific Multicast (SSM) extensions according to RFC 4607. The use of Any-source multicast (where the source IP address is not specified) is not recommended. For Source Specific Multicasting, the addressing scheme shall comply with RFC 4607 (range 232/8).

6.6.2 Internet group multicast protocol (IGMP) requirements

6.6.2.1 General

VDTs should be capable of generating IGMP messages to join/leave a multicast group. The minimum version of IGMP implemented should be version 3 according to RFC 3376.

6.6.2.2 IGMP snooping

Layer 2 devices (i.e. network switches) shall be capable of supporting “IGMP snooping” according to RFC 4541 and shall not flood multicast traffic indiscriminately out of all their interfaces in case of the availability of an IGMP querier.

7 Video streaming requirements

7.1 General

Today a lot of incompatible video streaming and stream control implementations exist, although standards are used. In this clause general requirements for the application of existing standards on video streaming are introduced.

The following clause contains requirements for the use of video stream transport in VTDs. The requirements are organized into a subclause that covers requirements common among all video transports and subclauses that cover requirements for specific video transport protocols such as RTP and others.

Video Transmission clients and servers shall support an IP-based network interface for the transport of session control and video data.

Control and video data shall be sent using TCP/IP according to STD 7 RFC 793 and/or UDP/IP according to STD 6 RFC 768. An overview of the protocol stack can be found in Figure 2 of this standard.

7.2 Transport protocol

7.2.1 General

The video transmission devices shall support UDP and/or TCP.

NOTE IEC 62676-2 series defines a protocol, how a VTD requests streams in the selected mode UDP or TCP.

Video transport requires real-time behaviour, provided in IP networks by the Real Time Protocols (RTP). RTP provides support for re-ordering, dejittering and media synchronization. All media streams transferred by the RTP protocol shall conform to RFC 3550, RFC 3551, RFC 3984, RFC 3016 and JPEG over RTP according to IEC 62676-2 series.

The RTP/UDP profile is the simplest and most widely supported option in current network streaming video systems. A VT device shall support the RTP/UDP protocol and should support RTP/UDP multicasting. RTP via TCP is an alternative means of media transport and a VTD may support this option according to RFC 4571. The RTSP/RTP over TCP provides the option of reliable transport. Furthermore, RTSP/RTP over TCP permits traversal of Network Address Translators and Firewalls.

The RTP Control Protocol (RTCP) provides feedback on streaming performance being provided by RTP and synchronization of different media streams. The RTCP protocol shall conform to RFC 3550.

All devices and clients shall support RTSP according to RFC 2326 for session initiation and playback control. RTSP shall use TCP as its transport protocol, the default TCP port for RTSP traffic is 554. The Session Description Protocol (SDP) shall be used to provide media stream information and SDP shall conform to RFC 4566.

7.2.2 JPEG over RTP

JPEG over RTP shall be basically in accordance with RFC 2435. This implementation only supports default Huffman tables, the aspect ratio is limited to 1:1 and 1:2 and the image size is limited to 2 040 x 2 040 pixels due to limited bit field of the RTP/JPEG header

For JPEG images of other aspect ratios, such as PAL or NTSC and for 4 mega pixel image sensors and more, an RTP extension header shall be included after the original standard header according to RFC 3550. The header extension shall be ignored by VTDs, not supporting these features. This may have the effect on incompatible VTD receivers that the stream is decoded, but offers e.g. the wrong aspect ratio.

7.2.3 JPEG over HTTP

If a VTP supports JPEG over HTTP it shall be in accordance with RFC 2453.

HTTP streaming separates each image into individual HTTP replies. RTP streaming creates packets of a sequence of JPEG images that can be received by VTD clients. A special mime-type ´multipart/x-mixed-replace;boundary=´ shall signal the VTD to receive several parts as reply separated by a special boundary, which is defined within the MIME-type. The TCP connection is active as long as the VTD receiver requests new frames and the VTD server provides frames.

7.3 Documentation and specification

7.3.1 General

The specification of the VTD and its video streaming interface shall document the number of VTD clients and/or servers being able to be connected for live and/or replay video streaming. If necessary the frame rate and quality of the video stream shall be specified as well.

RTP Payload Formats For interoperability purposes, the allowed set of media streaming options and formats for video, audio and meta data based on RTP is defined by this standard.

At least one of the following video streaming specifications shall be supported for compatibility reasons:

- JPEG over RTP
- MPEG-4 according to ISO/IEC 14496-2
- H.264 according to ISO/IEC 14496-10

and the following audio codecs:

- G.711 according to ITU-T G.711
- G.726 according to ITU-T G.726
- AAC according to ISO/IEC 14496-3

7.3.2 Non-compliant, proprietary and vendor specific payload formats

VTDs may support next to the listed compliant payloads additionally non-compliant or proprietary RTP payload formats. These are used when the real-time video format is proprietary and not intended to be part of any standardized system. However these proprietary formats shall be correctly documented and registered, because

– usage in standardized environments such as SDP. RTP needs to be configured regarding used RTP profiles, payload formats and their payload types. To accomplish this there is a need for registered names to ensure that the names do not collide with other formats.
– integration of 3rd party video devices: RTP payload formats are used for supporting proprietary formats. A written specification of the format will save time and money for both parties interoperating with each other: interoperability will much easier to accomplish.
– to ensure interoperability between different implementations on different platforms.

To avoid name collisions there is a central register keeping tracks of the registered Media Type names used by different RTP payload formats. When it comes to proprietary formats, they shall be registered in the vendors own tree. All vendor specific registrations uses sub-type names that start with “vnd.<vendor- name>”. All names that use names in the vendors own trees are not required to be registered with IANA. However registration is recommended if used at all in public environments.

New RTP payload Media Types may be registered in the standards tree by other standard bodies. The requirements on the organization are outlined in the media types registration document (RFC 4855 and RFC 4288). This registration requires a request to the IESG, which ensures that the registration template is acceptable.

Registration of the RTP payload name is something that is required to avoid name collision in the future. The list of already registered media types can be found at IANA (http://www.iana.org/assignments/media-types/video).

Vendor specific extensions shall use the payload type range 77-95, which is marked "unassigned"

7.3.3 Receiving unsupported RTP payload formats

A RTP payload format for a codec is a set of rules that define how the codec's video frames are packed within RTP packets. This is usually defined by an IETF RFC (or, for newer payload formats, an IETF Internet-Draft).

By default, the VTD video client will ignore any sub session whose RTP payload format it does not understand (because, if it doesn't know the RTP payload format, it doesn't know how to extract data from the incoming RTP stream).

The VTD client shall not be negatively influenced by incompatible video streams with unknown or corrupt codecs or video formats.

Vendor specific extensions shall use the payload type range 77-95, which is marked "unassigned"

7.4 Streaming of metadata

7.4.1 General

In video surveillance networks it is necessary to transport additional data next to the video stream, the so called Metadata. ATM/POS-, VCA-, GPS-, Geolocation, Number Plates, Access Control Cardholder IDs are some of the most common types of metadata. In general there are three alternatives to transport metadata assets with the actual video content:

– multiplexing: combined streaming containing video and metadata (not recommended);

– separate metadata and video data streams;

– multiple metadata streams (one for each type of metadata) and one video data stream.

Combined/multiplexed streaming has several disadvantages since the combined stream approach depends on a specific payload format, which provides the auxiliary header section where the metadata can be transported. Some RTP payload formats, such as for MPEG-4 Elementary Streams (RFC 3640), but other payload formats used in video surveillance do not provide the section ´auxiliary´. This conflicts with the requirements for interoperability. Furtheron saving on processing overhead by handling only one stream, brings some overhead due to the (de)multiplexing of the video and metadata.

End users expect that the metadata will be delivered with no, or a low level, of information loss. Therefore, a mechanism based on RTP shall be used and is specified here, which enables metadata arrival in correct order, and with detection and indication of loss. Metadata shall be transmitted on a separate RTP session in its own payload format.

7.4.2 XML documents as payload

7.4.3 General

If complex data formats need to be streamed as metadata, requiring a very rich system of complex data structures, XML documents shall be transmitted as RTP payload.

In a RTSP session the SDP description for metadata of Content Type and Subtype "application" shall be used as a dynamic payload type

```
SDP Example:

Client->Server: DESCRIBE rtsp://140.10.2.3/VideoChannel/1/h264 RTSP/1.0
CSeq: 1

Server->Client: RTSP/1.0 200 OK
CSeq: 1
Content-Type: application
```

```
Content-Length: XXX
```

The Metadata stream itself is then transported by RTP.

XML shall be streamed directly with one XML document after each other, via RTP. For synchronisation to the video stream a RTP timestamp shall be used with the time of occurrence. Only UTC timestamps shall be used within the metadata stream. This pure XML Metadata payload shall signal through the XML root node ´<?xml version="1.0" encoding="UTF-8"?> and the XML namespace xmlns used such as "http://www.xxx.org/ver10/schema" or "urn:yyy-org" that an XML document stream is following.

NOTE A XML Metadata schema and namespace for video surveillance applications is defined in IEC 62676-2-3.

8 Video stream control requirements

8.1 General

Today a lot of incompatible video streaming and stream control implementations exist, although standards are used. In this clause general requirements for the application of existing standards on video stream control are introduced,

In this clause the use of the Real Time Streaming Protocol (RTSP) according to RFC 2326 for live streaming and/or playback capable Video Transmission devices is specified.

RTSP is an application-level protocol for control over the delivery of data with real-time properties. Here the use of RTSP for VSSs is specified.

Session establishment refers to the method by which a Video Transmission client obtains the initial session description. The initial session description can e.g. be an URL to the content.

An example for a valid request from a Video Transmission client is:

```
rtsp://140.10.10.22:554/VideoChannel/1/h264/1/trackID=1
```

8.2 Usage of RTSP in video transmission devices

8.2.1 General

Live video streaming

The Live Stream is characterized as the equivalent of the traditional analog VSS. The actual video streams are typically delivered in multicast mode. This means that the presentation is linear and that there is no support for trick mode operation e.g. pause, fast forward and similar. The display is a continuous flow of data and events and not on demand.

Replay including trick modes

The Replay Streaming with Trick Modes is characterized as the equivalent of the Live Streaming with the addition to support for trick mode operation e.g. pause, reverse, fast forward and similar. Therefore the actual video streams are delivered in unicast mode only. The presentation is a continuous flow of events as well.

8.2.2 The use of RTSP with multicast

Optionally, it is possible to use RTSP for joining multicasts of Live Streaming.

NOTE In principle a multicast does not support trick mode operation, therefore it cannot be used.

Specifically, firewalls will be able to ascertain the incoming port being used i.e. this will allow them to open the ports and do any necessary port forwarding. Furthermore, it can be useful if the RTSP video server wishes to count the number of video clients subscribed.

When no indication is given by RTSP whether the mode of delivery is unicast or multicast, according to RFC 2326 the default video stream shall be delivered in multicast mode.

For any VTD shall the maximum number of unicast streams supported be specified.

8.3 RTSP standards track requirements

8.3.1 General

Following RTSP Requirements apply for Video Transmission Devices:

The video transmission device shall support the Real Time Streaming Protocol (RTSP) according to IETF RFC 2326: RTSP video transmission clients and servers shall implement all required features of the minimal RTSP implementation described in Appendix D of RFC 2326:1998.

8.3.2 High level IP video streaming and control interfaces

If any other interfaces, e.g. based on web services or HTTP requests, offer the initiation of streaming and retrieval of a video stream URI, this shall be in addition to the methods defined in this clause. It shall always be possible to refer to an URI according to the requirements of this clause.

VTDs offering a high-level interface for streaming and stream control shall support as well the minimal video stream control Interface introduced in the following including their minimum requirements:

8.3.3 Minimal RTSP method and header implementation

RTSP video transmission receiver shall implement the mandatory methods PLAY, OPTIONS, DESCRIBE, SETUP, TEARDOWN in the direction of the video transmitter (R->T). The default port number for a VTD RTSP server is 554. All clients and server shall implement all required features of the minimal RTSP implementation described in Appendix D of RFC 2326:1998.

8.3.4 RTSP authentication

The documentation of VTDs shall specify the methods supported for authentication. A VTD shall support one of the two methods ´Basic-´ or ´Digest-Authentication´ for the RTSP interface and the HTTP interface. In any case the Authentication has to be implemented according to RFC 2617 – HTTP Authentication: Basic and Digest Access Authentication. RTSP servers supporting HTTP digest authentication shall implement it according to RFC 2069. Digest Access Authentication is recommended in security grade 3 and 4 systems, because of the higher security provided. The range of valid user names, accounts and passwords to access a RTSP session is configured in the VTD.

9 Device discovery and description requirements

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

A VTD has to offer protocols for device discovery and description in an IP video network. The VTD shall support at least one of the 2 methods: WS-Discovery and/or Zeroconf.

In this standard, only the basic support of this functionality is required. In IEC 62676-2 series additionally a detailed protocol implementation is defined and required for these 2 device discovery and description methods.

10 Eventing requirements

A VTD has to offer protocols to signal the health status and events associated to the video source. According to IEC 62676-1-1 a VTD shall signal video loss, signal noise, signal too bright, too dark and camera deposition. The notification of motion and other video content analysis events in the video image shall be done by the same means. These states need generally to be signalled via the video IP interface in a defined manner by standardizes values, attributes or events, in order to let a VTD client exactly know the detailed status of any VTD server independent of device type, manufacturer or integrator software.

In this standard only the basic support of this eventing functionality is required. In IEC 62676-2 series eventing methods and detailed protocol implementations are defined and required.

Additionally following requirements for device management apply, if a VTD is operated in an IT network or office network environment:

11 Network device management requirements

11.1 General

This subclause concerns recommendations.

The two disciplines of IT networks and security networks are converging more and more. The end-users such as administrators are more and more responsible for both: IT equipment, security devices and their interconnecting networks.

If an IP based video surveillance system is operated in an IT environment, it is best to offer management services for video transmission devices using typical protocols for these kind of networks. Networks in industry, offices or within any IT environment already use the Simple Network Management Protocol (SNMP) to monitor and manage their information infrastructure. This enables the end-user, e.g. an administrator of a network including office and security network devices, to monitor e.g. the proper setup and operation of all the equipment by a single means at one end-point based on a single protocol:

Therefore VTDs should include the ability to communicate with enterprise-wide management systems based on the Simple Network Management Protocol (SNMP). VTDs should offer the capability to integrate into an SNMP-compliant management system that gives e.g. an administrator a single view of the various software and hardware transmission resources of this complex, distributed video network system.

If a VTD is operated in an IT environment, where it is needed to monitor and check the health status not only of office equipment, but also of security equipment such as IP video devices, the VTD should offer support for SNMP.

The VTD device should support SNMP in line with the requirements of this clause.

A Management Information Base (MIB) is a Simple Network Management Protocol (SNMP) specification containing definitions of management information so that video transmission devices and essential network components can be remotely monitored, configured and controlled. They are today used extensively in network elements such as routers, printers, hubs, switches and storage devices and more and more in IP Cameras, DVRs, encoders and decoders. In general there are four high level services for the management of video transmission network devices:

- faults and failures,
- alarm and events,
- status information and configuration,
- performance.

Fault and Failure management in security networks is based on root cause analysis involving remote identification and correction of network problems. Remote fault management monitors the health of the video transmission and network infrastructure, components, subsystems, and interfaces. Configuration and Status management enables the remote setup of network devices, interfaces and services. Performance management involves analysis of processing trends and network problems so that proactive actions can be taken to assure network availablility and finally the security of the protected site.

11.2 IP video MIB example

This subclause concerns recommendations

The following Figure 8 shows a high-level diagram of the MIB that is used to monitor VT devices. The organization of the MIB is defined in RFC 1155. For VSSs the private MIB 31373 is reserved and should be used.

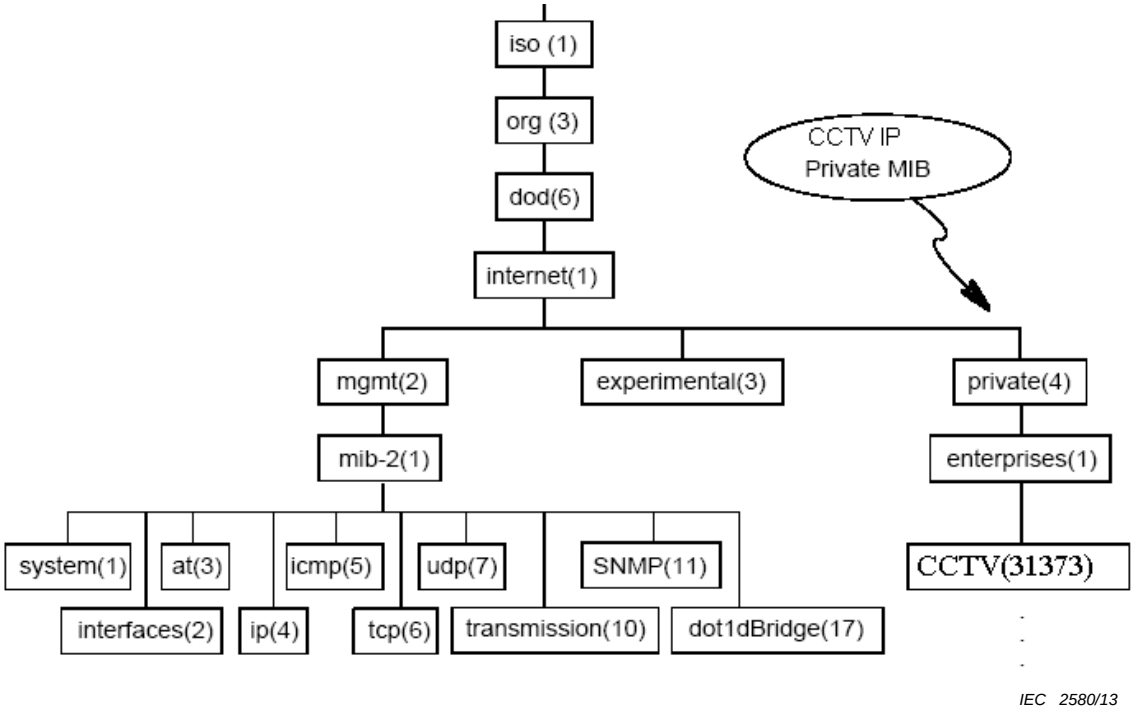


Figure 8 – MIB structure

11.3 The SNMP agent and manager for video transmission devices

This subclause is informative.

SNMP management is based on the agent/manager model described in the network management standards of the International Organization for Standardization (ISO). In this model, a network or systems manager exchanges monitoring and control information about system and network resources with distributed software components, the so-called ´agents´.

Any system or network resource that is manageable through the exchange of information is a managed resource. This can be a software resource e.g. a PC based network video recorder or digital video recorder or a hardware resource e.g. an IP camera, video encoder or decoder.

Agents typically are part of a managed resource and function as a kind of ´collection devices´ that assemble and send data about this managed resource as answer on a request from a SNMP manager. In addition, VTD agents should have the ability to issue unsolicited reports to managers when they detect certain predefined thresholds or conditions on the managed resource e.g. video loss events, detection of motion, hardware problems. In SNMP terminology, these unsolicited event messages are called trap notifications. This trap notification is a message about the occurrence of an event or the crossing of a predefined threshold, sent to a SNMP manager by a SNMP agent.

A manager is based on an information structure on properties of the managed resources provided by the agents. This is built by the Management Information Base (MIB). When new agents, e.g. with attaching a video transmission system to a network, are added and shall be included into the management of a SNMP manager, the manager shall understand the structure of this new MIB component defining the features and capabilities of the resources. These features have to be defined in an SNMP-compliant MIB and are called ´objects´. The definition of a common MIB shared by all different types of video transmission devices in a security network provides even for very heterogeneous recourses of a distributed system within the protected site a unified view and single way to manage system and network resources.

Network devices such as routers can send notifications to SNMP managers when particular events occur. For example, a SNMP agent might send a message to a SNMP manager when an error occurs.

SNMP notifications can be sent as traps or inform requests. An SNMP manager that receives an inform request acknowledges the message with an SNMP response PDU. Traps are sent only once, while an inform may be retried several times.

11.4 Performance requirements on the SNMP agent

This subclause is normative.

If a VSS is using SNMP for the health check and monitoring of VTDs, the following performance requirements are important for a reliant communication and shall be applied: For this reason any VTDs or IP video device in security applications shall comply to these requirements, even beyond of the SNMP interface defined in this standard including vendor specific MIBs.

1) The agent shall be capable of giving a SNMP-RESPONSE to a SNMP-GET with multiple variables. The agent shall be able to respond to a SNMP-GET with multiple OIDs in one SNMP packet.
2) In polling mode, the values of the OIDs shall reflect the real state of the queried video transmission device hardware within 5 s of a state transition and also be signalled by TRAP within 5 s of a state transition, if that TRAP is enabled.
3) The “Request ID” used during the query by the manager is to be used again in the response (SNMP response).
4) The response times for GETs are to be met in accordance with requirement 2) of this subclause.
5) The agent shall work in a stable manner. The stable state of the video transmission agent is characterised as follows:
   – the video transmission devices to be controlled can be operated at all times;
   – the agent always supplies a RESPONSE to all valid REQUESTs;
   – neither the agent nor the connected video transmission device executes a restart during operation without this being requested.
   – The agent’s parameter settings are retained during operation and only change because of control actions.

6) All the counters shall be zeroed when warm or cold starting the agent. The current state of the device (contained in the saved TRAP mask) is to be transferred after booting up by means of TRAP/notification.

7) If VTD system components cannot be accessed internally or the agent is not capable of providing information about these components, the integer value of 0 (undefined) shall be returned in response to a Get, GetNext and GetBulk request for the OID of these system components. At the same time, the error status shall be set to NoError. If the system is not capable of implementing a received SET request, the command shall be correctly acknowledged, although it shall not be saved. SNMP set requests are generally acknowledged (if no SNMP error occurs) with NoError and the correct Varbinds-OID (e.g. Local Mode). Trap, notification and SNMP get requests provide information relating to the successful execution of the command.

8) If an OID is obsolete, this is to be skipped during a ´walk´. In the case of a REQUEST, the SNMP error 'NOSUCHNAME' is to be used as a response, i.e. the agent behaves as though the OID does not exist.

9) To detect lost TRAPs, a global TRAP counter ("eventCounter") is implemented in the CommonVarbinds-MIB. Prior to sending a TRAP/notification, the OID even-Counter value is to be incremented by 1. The current value can be queried using the OID eventCounter.

10) The TRAP priority is sent with a TRAP and shall correspond to the defined priority of the respective event. It carries the OID of the event priority.

11) A minimum of 10 entries for each individual SNMP table defined in this standard shall be supported, exceptions shall be specified.

11.5 VSS SNMP trap requirements for event management

This subclause is normative.

Polling applications are the most common type of SNMP monitoring applications written to check the status of devices. All listed items have to be provided as managed objects through SNMP GET messages

Event management provides the ability to receive asynchronous events/traps from a video transmission device, and allows the user to manage the incidents and problems indicated by this event. Example events are fan, video loss or disk alerts

VTDs shall be able to send TRAPS or INFORMS for state changes for the following items and objects to the configured receiving address:

- auxiliaries e.g. Digital I/O;
- video input status e.g. motion, video loss, depositioning, signal tampering;
- recording;
- alarm;
- temperature, fan speed and CPU load limit passed.

12 Network security requirements

12.1 General

This clause defines a security architecture for VTD. The video transmission device shall have in the higher security grade 4 the ability to provide authentication, integrity checking and encryption on all network interfaces. The intent of this architecture is to provide peer entity, data origin, and network device authentication, as well as video data confidentiality and integrity. Other types of communication security, such as operator authentication, access control and non-repudiation, are not provided in this clause. Systems that require these services may add them to VTD in a proprietary manner.

All data communication outside secured technical room areas shall be encrypted in the security grade 4. AES with 128 bit key for symmetric and RSA with 1 024 bit key shall be provided. Native encryption shall not be accepted. The VTDs shall not store any form of passwords in clear text. All such passwords either in configuration files or a database shall be encrypted.

A VTD according to this standard shall support transport level security for the security grade 4.

12.2 Transport level security requirements for SG4 transmission

Transport level security provides a protection of all video data between a VTD client and a server. Transport Layer Security (TLS) shall be provided by a VTD for encrypted transport. The TLS protocol offers authenticated transport sessions between 2 VTDs and takes care of confidentiality and integrity of the transported data.

A VTD compliant to this standard shall support in security grade 4 TLS 1.0 according to the IETF standard RFC 2246 and TLS 1.1 according to RFC 4346. Optionally the VTD may support TLS 1.2 according to RFC 5246.

The VTD shall offer protection for the transport of all data and information concerning streaming, stream control and eventing.

The VTD client and server shall support the cipher suites TLS_RSA_WITH_AES_128_CBC_SHA and TLS_RSA_WITH_NULL_SHA from RFC 2246 and RFC 3268.

Bibliography

IEC 62676-2-3, *Video surveillance systems for use in security applications – Part 2-3: Video transmission protocols – IP interoperability implementation based on Web services*

ISO/IEC 10918 (all parts), *Information technology – Digital compression and coding of continuous-tone still Images*

ISO/IEC 10918-5, *Information technology – Digital compression and coding of continuous-tone still images: JPEG File Interchange Format (JFIF)*

ISO/IEC 14496-1, *Information technology – Coding of audio-visual objects – Part 1: Systems*

ISO/IEC 15444 (all parts), *Information technology – JPEG 2000 image coding system*

ISO 8601, *Data elements and interchange formats – Information interchange – Representation of dates and times*

ISO 19111, *Geographic information – Spatial referencing by coordinates*

ISO 19115:2003 (all parts), *Geographic information – Metadata*

ITU Recommendation H.241, *Extended video procedures and control signals for ITU-T H.300 series terminals*

SCTE 52, *Data Encryption Standard – Cipher Block Chaining Packet Encryption Specification*

SMPTE 298M-1997, *Television, Universal Labels for Unique Identification of Digital Data*

FIPS PUB 180-2, *Secure Hash Standard (SHS)*

FIPS PUB 197, *Advanced Encryption Standard (AES)*

FIPS PUB 46-3, *Specification for the Data Encryption Standard, National Institute of Standards and Tech*

FIPS PUB 81, *DES Modes of Operation, National Institute of Standards and Technology*

IETF Draft avt-rtp-h264-rcdo, *RTP Payload Format for H.264 RCDO Video*

IETF Draft avt-rtp-klv, *RTP Payload Format for SMPTE 336M Encoded Data*

IETF Draft avt-rtp-rfc3984bis, *RTP Payload Format for H.264 Video*

IETF Draft avt-rtp-svc, *RTP Payload Format for SVC Video*

IETF Draft avt-srtp-big-aes, *The use of AES-192 and AES-256 in Secure RTP*

IETF Draft HTTPMU, *HTTPU HTTP Multicast over UDP, HTTP Unicast over UDP*

IETF Draft RTP/AVPF, *Extended RTP Profile for RTCP-based Feedback (RTP/AVPF)*

IETF Draft RTP/RTX, *RTP Retransmission Payload Format*

IETF Draft, *SSDP Simple Service Discovery Protocol*

IETF RFC 052, *IAB Recommendations*

IETF RFC 792, *Internet Control Message Protocol*

IETF RFC 826, *An Ethernet Address Resolution Protocol*

IETF RFC 868, *Time Protocol*

IETF RFC 1034, *XML- Extensible Markup Language. W3C recommendation*

IETF RFC 1035, *Domain Names – Concepts and Facilities*

IETF RFC 1089, *SNMP over Ethernet*

IETF RFC 1109, *Ad-hoc Review*

IETF RFC 1155, *Structure of Management Information*

IETF RFC 1156, *Management Information Base (MIB-I)*

IETF RFC 1161, *SNMP over OSI*

IETF RFC 1187, *Bulk table retrieval*

IETF RFC 1212, *Concise MIB definitions*

IETF RFC 1214, *OSI MIB*

IETF RFC 1215, *Traps*

IETF RFC 1229, *Generic-interface MIB extensions*

IETF RFC 1305, *Network Time Protocol (Version 3) specification, implementation and analysis*

IETF RFC 1321, *The MD5 Message-Digest Algorithm, April 1992*

IETF RFC 1341, *MIME- Multipurpose Internet Mail Extensions*

IETF RFC 1738, *Uniform Resource Locators (URL)*

IETF RFC 1889, *Real Time Transport Protocol (RTP)*

IETF RFC 1901, *Community-based SNMPv2*

IETF RFC 1902, *Structure of Management Information for SNMPv2*

IETF RFC 1903, *Textual Conventions for SNMPv2*

IETF RFC 1904, *Conformance Statements for SNMPv2*

IETF RFC 1910, *User-based Security Model*

IETF RFC 2045, *Multipurpose Internet Mail Extensions (MIME) Part One Format of Internet Message Bodies*

IETF RFC 2046, *Multipurpose Internet Mail Extensions (MIME) Part Two Media Types*

IETF RFC 2104, *Keyed Hashing for Message Authentication*

IETF RFC 2190, *RTP Payload Format for H.263 Video Streams*

IETF RFC 2250, *RTP Payload Format for MPEG1/MPEG2 Video*

IETF RFC 2271, *An Architecture for Describing SNMP Management Frameworks*

IETF RFC 2272, *Message Processing and Dispatching for SNMP*

IETF RFC 2273, *SNMPv3 Applications*

IETF RFC 2274, *User-Based Security Model (USM) for SNMPv3*

IETF RFC 2275, *View-Based Access Control Model (VACM) for the SNMP*

IETF RFC 2279 UTF-8, *A transformation format of ISO 10646 (character encoding)*

IETF RFC 2387, *Format for representing content type*

IETF RFC 2396, *Uniform Resource Identifiers (URI) Generic Syntax*

IETF RFC 2429, *RTP Payload Format for the 1998 Version of ITU-T Rec. H.263 Video (H.263+)*

IETF RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*

IETF RFC 2576, *Coexistence between SNMP Versions*

IETF RFC 2616, *HTTP Hypertext Transfer Protocol 1.1*.

IETF RFC 2782, *A DNS RR for specifying the location of services (DNS SRV)*

IETF RFC 2790, *Host Resources MIB*

IETF RFC 2818, *HTTP over TLS*

IETF RFC 2863, *Interfaces Group MIB*

IETF RFC 2929, *Domain Name System (DNS)*

IETF RFC 3339, *Date and Time on the Internet Timestamps*

IETF RFC 3379, *Internet Group Management Protocol*

IETF RFC 3411, *An Architecture for Describing SNMP Management Frameworks*.

IETF RFC 3412, *Message Processing and Dispatching for SNMP*

IETF RFC 3413, *SNMP Applications*

IETF RFC 3414, *User-Based Security Model (USM) for SNMPv3*

IETF RFC 3415, *View-Based Access Control Model (VACM) for the SNMPIETF RFC 3412 Message*

Processing and Dispatching for the Simple Network Management Protocol

IETF RFC 3512, *Configuring Networks and Devices with Simple Network Management Protocol (SNMP)*

IETF RFC 3555, *MIME Type Registration of RTP Payload Formats*

IETF RFC 3556, *Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol*

IETF RFC 3584 (Best Current Practice), *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*

IETF RFC 3640, *RTP Payload Format for Transport of MPEG-4 Elementary Streams*.

IETF RFC 3711, *The Secure Real-time Transport Protocol (SRTP)*.

IETF RFC 3826, *The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP USM*

IETF RFC 3927, *Dynamic Configuration of IPv4 Link-Local addresses*

IETF RFC 3986, *Uniform Resource Identifier (URI) Generic Syntax*

IETF RFC 4122, *A Universally Unique IDentifier (UUID) URN Namespace*

IETF RFC 4571, *Framing Real-time Transport Protocol (RTP) and RTP Control Protocol (RTCP) Packets over Connection-Oriented Transport*

IETF RFC 4702, *The Dynamic Host Configuration Protocol (DHCP) Client Fully Qualified Domain Name (FQDN) Option*

IETF RFC 4855, *Media Type Registration of RTP Payload Formats*

IETF RFC 4288, *Media Type Specifications and Registration Procedures*

IETF RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2*

IETF RFC 5104, *Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF)*

IETF RFC 5371, *RTP Payload Format for JPEG 2000 Video Streams*.

IETF RFC 5372, *Payload Format for JPEG 2000 Video Extensions for Scalability & Main Header Recovery.*

IETF RFC 5590 (Proposed), *Transport Subsystem for the SNMP*

IETF RFC 5591 (Proposed), *Transport Security Model for the SNMP*

IETF RFC 5592 (Proposed), *Secure Shell Transport Model for the SNMP*

IETF RFC 5608 (Proposed), *Remote Authentication Dial-In User Service (RADIUS) Usage for SNMP Transport Models.*

IETF RFC 2222, *Simple Authentication and Security Layer (SASL)*

IETF RFC 3264, *An Offer/Answer Model with Session Description Protocol (SDP)*

IETF RFC 3376, *Internet Group Management Protocol, Version 3*

IETF STD 16 RFC 1213, *Management Information Base (MIB-II)*

IETF STD 5 RFC 1112, *Host extensions for IP multi-casting*

IETF STD 5 RFC 791, *Internet Protocol*

IETF STD 6 RFC 768, *User Datagram Protocol*

IETF STD 62 RFC 3411, *An Architecture for Describing SNMP Management Frameworks*

IETF STD 62 RFC 3412, *Message Processing and Dispatching for the SNMP*

IETF STD 62 RFC 3413, *Simple Network Management Protocol (SNMP) Application*

IETF STD 62 RFC 3414, *User-based Security Model (USM) for version 3 of the SNMPv3*

IETF STD 62 RFC 3415, *View-based Access Control Model (VACM) for the SNMP*

IETF STD 62 RFC 3416, *Version 2 of the Protocol Operations for the SNMP*

IETF STD 62 RFC 3417, *Transport Mappings for the Simple Network Management Protocol (SNMP)*

IETF STD 62 RFC 3418, *Management Information Base (MIB) for the SNMP*

IETF STD 7 RFC 793, *Transmission Control Protocol*

MISB Standard 0107, *Bit and Byte Order for Metadata in Motion Imagery Files and Streams*

MISB RP 0701, *Common Metadata System Structure (CMS)*

MISB RP 0702, *Content part of CMS*

OASIS Standard Web Services Base Notification 1.3

OASIS Standard Web Services Dynamic Discovery (WS-Discovery)

SMPTE 359M-2001, *Television and Motion Pictures, Dynamic Documents*

W3C Extensible Markup Language (XML) 1.0 (Third Edition), W3C Recommendation

W3C SOAP 1.2, Part 1 Messaging Framework

W3C SOAP, Message Transmission Optimization Mechanism

W3C SOAP, Version 1.2 Part 2 Adjuncts (Second Edition)

W3C Web Services Addressing (WS-Addressing) W3C Recommendation,

W3C Web Services Addressing 1.0 – Core

W3C Web Services Description Language (WSDL) 1.1

W3C Web Services Eventing (WS-Eventing), W3C Recommendation

W3C XML Path Language (XPath), W3C Recommendation

W3C XML Schema Part 1 Structures Second Edition, W3C Recommendation

W3C XML Schema Part 2 Datatypes Second Edition, W3C Recommendation

W3C XML-binary Optimized Packaging

W3C XML-NMSP – Namespaces in XML, W3C Recommendation

W3C XML 1.0, Extensible Markup Language (XML) 1.0 (Second Edition), W3C Recommendation

W3C XML Namespaces, Namespaces in XML, W3C Recommendation

W3C XML Information Set, XML Information Set, W3C Recommendation

W3C XML Schema: XML Schema Part 1: Structures, W3C Recommendation

W3C XML Schema: XML Schema Part 2: Datatypes, W3C RecommendationW3C WS-Addressing, Web Services Addressing 1.0 – Core, W3C Recommendation

W3C Web Services Eventing (WS-Eventing), W3C Recommendation

W3C WSDL 1.1, Web Services Description Language (WSDL) 1.1, W3C Recommendation

W3C WSDL Binding for SOAP 1.2, WSDL 1.1 Binding Extension for SOAP 1, W3C ecommendation

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

SYSTÈMES DE VIDÉOSURVEILLANCE DESTINÉS À ÊTRE UTILISÉS DANS LES APPLICATIONS DE SÉCURITÉ –

Partie 1-2: Exigences systèmes – Exigences de performances pour la transmission vidéo

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de brevet. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale CEI 62676-1-2 a été établie par le comité d'études 79 de la CEI: Systèmes d'alarme et de sécurité électroniques.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
79/433/FDIS	79/446/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Une liste de toutes les parties de la série CEI 62676, publiées sous le titre général *Systèmes de vidéosurveillance destinés à être utilisés dans les applications de sécurité*, peut être consultée sur le site web de la CEI.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de la CEI sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo *"colour inside"* qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

Le Comité d'études 79 de la CEI en charge des systèmes d'alarme et de sécurité électroniques ainsi que de nombreuses organisations gouvernementales, de laboratoires d'essai et de fabricants de matériel ont défini un cadre commun pour la transmission vidéosurveillance afin de permettre l'interopérabilité entre les produits.

La série de normes CEI 62676 dédiées aux systèmes de vidéosurveillance est divisée en 4 parties indépendantes:

Partie 1: Exigences systèmes

Partie 2: Protocoles de transmission vidéo

Partie 3: Interfaces vidéo analogiques et numériques

Partie 4: Directives d'application (à publier)

Chaque partie propose ses propres articles relatifs au domaine d'application, ainsi qu'aux références, définitions et exigences.

La série CEI 62676-1 comprend 2 sous-parties, respectivement numérotées 1-1 et 1-2:

CEI 62676-1-1, *Exigences systèmes – Généralités*

CEI 62676-1-2, *Exigences systèmes – Exigences de performances pour la transmission vidéo*

Cette deuxième sous-partie de la série CEI 62676-1 s'applique à la vidéotransmission. L'objet du système de transmission dans une installation VSS est d'assurer la transmission fiable des signaux vidéo entre les différents types d'équipement VSS dans des applications de sûreté, de sécurité et de surveillance.

Actuellement, les VSS équipent les réseaux de sécurité qui utilisent une infrastructure, des équipements et des connexions IT sur le site protégé proprement dit.

SYSTÈMES DE VIDÉOSURVEILLANCE DESTINÉS À ÊTRE UTILISÉS DANS LES APPLICATIONS DE SÉCURITÉ –

Partie 1-2: Exigences systèmes – Exigences de performances pour la transmission vidéo

1 Domaine d'application

La présente partie de la CEI 62676 décrit les exigences générales pour la vidéotransmission. La présente norme couvre les exigences générales pour les vidéotransmissions relatives à la performance, la sécurité et la conformité à la connectivité IP de base, fondées sur les normes internationales existantes bien connues.

Les Articles 4 et 5 de la présente norme définissent les exigences de performances minimales de la vidéotransmission pour les applications de sécurité dans les réseaux IP. Dans les applications de surveillance, les exigences relatives à la synchronisation, à la qualité et à la disponibilité sont strictes et elles sont définies dans la dernière section de la présente norme. Des recommandations relatives à l'architecture des réseaux sont fournies, ainsi que la façon dont ces exigences peuvent être satisfaites.

L'Article 6 et les articles suivants de la présente norme définissent les exigences relatives à la connectivité IP de base des dispositifs de vidéotransmission destinés à être utilisés dans les applications de sécurité. Si un dispositif de vidéotransmission est utilisé dans le domaine de la sécurité, certaines exigences de base s'appliquent. Il est nécessaire de présenter avant tout la compréhension de base de la connectivité IP exigeant que le dispositif soit conforme aux protocoles de réseaux fondamentaux. Ceux-ci peuvent être présentés sous forme d'exigences qu'il est admis d'appliquer à tous les dispositifs de sécurité IP, allant même au-delà de la vidéo IP. Pour cette raison, les exigences sont présentées dans une deuxième étape relative à la conformité des protocoles de transfert en flux continu de base utilisés dans la présente norme pour le transfert vidéo en flux continu et le contrôle de flux. Puisque les applications de sécurité nécessitent une forte disponibilité et une grande fiabilité, des moyens généraux pour la transmission d'événements de contrôle d'état et de bon fonctionnement de la vidéo sont à traiter. Ceux-ci sont définis dans les exigences générales relatives à la gestion d'événements et la gestion des dispositifs de réseaux. Dans le domaine de la sécurité, une maintenance et une mise en service correctes sont essentielles pour le fonctionnement du dispositif de vidéotransmission. La localisation des dispositifs de transfert en flux continu ainsi que leurs capacités constituent une exigence de base et sont traitées dans «découverte et description du dispositif».

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 61709, *Composants électriques – Fiabilité – Conditions de référence pour les taux de défaillance et modèles de contraintes pour la conversion*

CEI/TR 62380, *Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment* (disponible en anglais seulement)

CEI 62676-1-1, *Systèmes de vidéosurveillance destinés à être utilisés dans les applications de sécurité – Partie 1-1: Exigences systèmes – Généralités*

CEI 62676-2-1, *Systèmes de vidéosurveillance destinés à être utilisés dans les applications de sécurité – Partie 2-1: Protocoles de transmission vidéo – Exigences générales*

ISO/CEI 10646, *Technologies de l'information – Jeu universel de caractères codés sur plusieurs octets (JUC)*

ISO/CEI 13818-9, *Technologies de l'information – Codage générique des images animées et des informations sonores associées – Partie 9: Extension pour interface temps réel pour systèmes décodeurs* (disponible en anglais seulement)

ISO/CEI 14496-2, *Technologies de l'information – Codage des objets audiovisuels – Partie 2: Codage visuel*

ISO/CEI 14496-3, *Technologies de l'information – Codage des objets audiovisuels – Partie 3: Codage audio*

ISO/CEI 14496-10, *Technologies de l'information – Codage des objets audiovisuels – Partie 10: Codage visuel avancé*

UIT-T Rec. G.711, *Modulation par impulsions et codage (MIC) des fréquences vocales*

UIT-T Rec. G.726, *Modulation par impulsions et codage différentiel adaptatif (MICDA) à 40, 32, 24, 16 kbit/s*

IEEE Std 1413.1, *IEEE Guide for selecting and using reliability predictions based on IEEE 1413* (disponible en anglais seulement)

IETF RFC 1122, *Requirements for Internet Hosts – communication Layers* (disponible en anglais seulement)

IETF RFC 1157, *Simple Network Management Protocol* (disponible en anglais seulement)

IETF RFC 1441, *Introduction to version 2 of the Internet-standard Network Management Framework* (disponible en anglais seulement)

IETF RFC 2030, *Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI* (disponible en anglais seulement)

RFC 2069, *Digest Access Authentication* (disponible en anglais seulement)

IETF RFC 2131, *Dynamic Host Configuration Protocol* (disponible en anglais seulement)

IETF RFC 2246, *The TLS Protocol Version 1.0* (disponible en anglais seulement)

IETF RFC 2326:1998, *Real Time Streaming Protocol (RTSP)* (disponible en anglais seulement)

IETF RFC 2435, *RTP Payload Format for JPEG-compressed Video* (disponible en anglais seulement)

IETF RFC 2453, *RIP - Routing Information Protocol* (disponible en anglais seulement)

IETF RFC 2617, *HTTP Authentication Basic and Digest Access Authentication*, June 1999. (disponible en anglais seulement)

IETF RFC 3016, *RTP Payload Format for MPEG-4 Audio/Visual Streams* (disponible en anglais seulement)

IETF RFC 3268, *Advanced Encryption Standard (AES) Cipher suites for Transport Layer Security (TLS)* (disponible en anglais seulement)

IETF RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)* (disponible en anglais seulement)

IETF RFC 3410, *Introduction and Applicability Statements for Internet Standard Management Framework* (disponible en anglais seulement)

IETF RFC 3550, *RTP A Transport Protocol for Real-Time Applications* (disponible en anglais seulement)

IETF RFC 3551, *RTP Profile for Audio and Video Conferences with Minimal Control* (disponible en anglais seulement)

IETF RFC 3984, *RTP Payload Format for H.264 Video* (disponible en anglais seulement)

IETF RFC 4346, *The Transport Layer Security (TLS) Protocol Version 1.1* (disponible en anglais seulement)

IETF RFC 4541, *IGMP and MLD Snooping Switches* (disponible en anglais seulement)

IETF RFC 4566, *SDP Session Description Protocol* (disponible en anglais seulement)

IETF RFC 4607, *Source Specific Multicast for IP* (disponible en anglais seulement)

IETF RFC 4862, *IPv6 Stateless Address Auto configuration* (disponible en anglais seulement)

3 Termes, définitions et abréviations

Pour les besoins du présent document, les termes, définitions et abréviations suivants s'appliquent.

3.1 Termes et définitions

3.1.1
mise en mémoire tampon de gigue adaptative
mise en file d'attente de paquets dans les réseaux commutés exposés à des variations indésirables du signal de communication pour assurer la vidéotransmission continue sur un réseau pris en charge par l'aptitude «adaptative» à régler la taille du tampon de gigue sur la base de l'instabilité mesurée dans le réseau

EXEMPLE: Si l'instabilité augmente, le tampon devient plus grand et peut contenir plus de paquets; si l'instabilité diminue, le tampon devient plus petit et contient moins de paquets.

3.1.2
norme de cryptage évolué
norme de cryptage NIST, appelée également Rijndael, spécifiée comme un algorithme de cryptage symétrique public non classifié d'une taille de blocs fixe de 128 bits et d'une taille de clé de 128, 192 ou 256 bits selon la «Federal Information Processing Standards Publication 197»

3.1.3
American Standard Code for Information Interchange
norme mondiale de-facto des codes numériques utilisés par les ordinateurs pour représenter tous les caractères en majuscule et en minuscule

3.1.4
algorithme asymétrique
algorithme utilisé en cryptographie asymétrique, dans lequel une paire de clés (une clé privée et une clé publique) est utilisée pour chiffrer et déchiffrer un message pour garantir la confidentialité des communications

3.1.5
authentification
processus par lequel on vérifie l'identité d'opérateurs ou de systèmes dans un réseau

EXEMPLE: Dans les réseaux, l'authentification est couramment effectuée en utilisant des mots de passe au moment de l'accès.

3.1.6
serveur d'authentification
dispositif utilisé pour le contrôle d'accès aux réseaux

Note 1 à l'article: Il contient les noms d'utilisateur et les mots de passe qui identifient les clients au moment de l'accès ou il peut contenir les algorithmes pour l'accès. Pour un accès à des ressources spécifiques d'un réseau, le serveur peut lui-même contenir des permissions accordées à des utilisateurs et des politiques d'entreprise ou donner accès à des répertoires contenant les informations. Des protocoles tels que RADIUS, Kerberos et TACACS+, ainsi que 802.1x sont mis en œuvre dans un serveur d'authentification pour effectuer les authentifications des utilisateurs

3.1.7
authenticité
intégrité et fiabilité des données ou d'une entité; validité et conformité des informations ou identité d'un utilisateur

Note 1 à l'article: L'authenticité peut être sécurisée et vérifiée en utilisant des méthodes cryptographiques.

3.1.8
autorisation
approbation, permission ou accréditation pour un utilisateur ou un composant pour exécuter une action

3.1.9
réseau d'infrastructure
ligne à grande vitesse ou série de connexions constituant un chemin principal dans un réseau

3.1.10
couche squelette
ligne de transmission plus importante transportant des données rassemblées par des lignes de communication plus petites interconnectées avec celles-ci, par exemple une ligne ou un ensemble de lignes connectées à des réseaux locaux, afin d'augmenter significativement les distances, par exemple entre des bâtiments

3.1.11
bits par seconde
b/s
unité de mesure de la vitesse du transfert des données d'un nœud à un autre

3.1.12
pont
dispositif utilisé pour relier deux réseaux incluant la transmission de paquets de données entre eux utilisant les mêmes protocoles

3.1.13
client
composant qui entre en contact avec un serveur et en obtient des données

3.1.14
client/serveur
système de communication fournissant des services tels que des flux vidéo, le stockage, le contrôle d'accès, la gestion de communication de données et clients (stations de travail) s'abonnant à ces services

3.1.15
codec
processus de compression et de décompression ou de COdeur/DÉCodeur

3.1.16
interface de passerelle commune
CGI
méthode de communication normalisée entre un client, par exemple un navigateur Web et un serveur, par exemple un serveur Web

Note 1 à l'article: L'abréviation CGI est dérivée du terme anglais développé correspondant " Common Gateway Interface".

3.1.17
retard de compression
retard provoqué par la compression des données

3.1.18
encombrement
situation dans laquelle le trafic présent sur le réseau dépasse le débit/la capacité disponible du réseau

3.1.19
couche intérieure
partie du réseau assurant un transport optimum entre sites ou fonctionnalité du système, par exemple enregistrement

3.1.20
norme de chiffrement de données
DES
méthode d'algorithme cryptographique élaborée par le "US National Bureau Standards"

Note 1 à l'article: L'abréviation DES est dérivée du terme anglais développé correspondant " Data Encryption Standard".

3.1.21
protocole de configuration de serveur dynamique
DHCP
protocole par lequel un composant de réseau obtient une adresse IP (et d'autres informations de configuration du réseau) auprès d'un serveur sur le réseau local

Note 1 à l'article: L'abréviation DHCP est dérivée du terme anglais développé correspondant " dynamic host configuration protocol".

3.1.22
couche distribution
partie du réseau fournissant la connectivité basée sur des règles définies

3.1.23
système de noms de domaine
DNS
système traduisant les noms de domaine Internet en adresses IP

Note 1 à l'article: L'abréviation DNS est dérivée du terme anglais développé correspondant "Domain Name System".

3.1.24
double attachement
dispositif unique offrant deux interfaces de réseau ou plus

3.1.25
tampon de gigue dynamique
collecte et stockage de paquets de données vidéo pour les traiter dans des intervalles régulièrement espacés pour diminuer les distorsions sur l'affichage

3.1.26
encryptage
type de sécurité de réseau utilisée pour coder des données de façon que seule la destination prévue puisse accéder aux informations ou les décoder

3.1.27
basculement
capacité d'une application à la reprise après défaillance d'une entité par commutation automatique sur un système de secours, n'entraînant aucune perte de données ou de continuité, appelée également «basculement de fonctionnement» et souvent utilisée en parallèle

3.1.28
criminalistique
domaine de la science appliquant les technologies numériques à des questions juridiques issues d'enquêtes policières

3.1.29
trame
structure de données représentant collectivement un flux de transmission incluant des en-têtes, des données et la charge utile et procurant les informations nécessaires à la fourniture correcte des données

3.1.30
passerelle
montage matériel ou logiciel effectuant la traduction entre deux protocoles différents

3.1.31
H.261
norme de codage vidéo de l'UIT conçue à l'origine pour les lignes RNIS (Réseau Numérique à Intégration de Services) et les débits de données avec des multiples de 64 Kbit/s utilisant un protocole de transmission en temps réel (RTP)

3.1.32
H.263
norme de l'UIT prenant en charge la compression vidéo (codage) pour le transfert vidéo en flux continu par l'intermédiaire d'un protocole de transmission en temps réel (RTP) basé sur le codec H.261 et le remplaçant

3.1.33
H.264
partie 10 de la norme ISO UIT-T MPEG-4, appelée également Codage vidéo avancé (AVC) prenant en charge la compression vidéo (codage) depuis des applications de transfert en flux continu sur un réseau à faible débit binaire vers des applications vidéo HD avec un codage pratiquement sans perte pour représentation vidéo réseau

3.1.34
hôte
ordinateur situé sur un réseau constituant un référentiel pour des services disponibles à d'autres composants sur le réseau

3.1.35
remplacement à chaud
propriété d'un contrôleur permettant d'enlever et de remplacer des cartes de circuits ou d'autres dispositifs pendant que le système reste alimenté et en fonctionnement

3.1.36
HTML
langage de balisage hypertexte
langage de codage utilisé pour créer des documents hypertexte destinés à être utilisés sur le Web

Note 1 à l'article: L'abréviation HTML est dérivée du terme anglais développé correspondant " Hyper Text Mark-up Language ".

3.1.37
protocole de transfert hypertexte
HTTP
protocole orienté connexion pour transmettre des données sur un réseau ou protocole pour déplacer des fichiers hypertexte sur Internet

Note 1 à l'article: L'abréviation HTTP est dérivée du terme anglais développé correspondant "Hypertext Transfer Protocol".

3.1.38
protocole sécurisé de transfert hypertexte
HTTPS
chiffrage et authentification de communication entre un serveur et des clients

Note 1 à l'article: L'abréviation HTTPS est dérivée du terme anglais développé correspondant "Hypertext Transfer Protocol Secure".

3.1.39
protocole de message de commande Internet
ICMP
protocole d'erreur indiquant par exemple qu'un service demandé n'est pas disponible ou qu'un hôte ou un routeur peut ne pas être atteint

Note 1 à l'article: L'abréviation ICMP est dérivée du terme anglais développé correspondant " Internet Control Message Protocol".

3.1.40
identification
ID
chaîne de caractères lisible par une machine

3.1.41
IEEE 802.1x
méthode d'authentification et d'autorisation dans les réseaux IEEE-802 utilisant un serveur d'authentification, par exemple un serveur RADIUS

3.1.42
institut des ingénieurs en électricité et électronique
IEEE
association professionnelle d'ingénieurs pour l'avancement de la technologie

3.1.43
protocole Internet de gestion de groupe
IGMP
protocole de communication utilisé pour gérer les membres des groupes de multidiffusion IP

Note 1 à l'article: L'abréviation IGMP est dérivée du terme anglais développé correspondant " Internet Group Management Protocol".

3.1.44
protocole Internet
IP
protocole couche 3 de réseau dans le modèle OSI contenant des informations d'adressage et de contrôle pour permettre de router des paquets de données dans un réseau et protocole primaire de couche réseau dans la suite de protocoles TCP/IP (Protocole de contrôle de transfert/Protocole Internet) selon l'IETF RFC 791

Note 1 à l'article: L'abréviation IP est dérivée du terme anglais développé correspondant " Internet Protocol".

3.1.45
adresse IP
adresse de protocole Internet
adresse d'un ordinateur hôte utilisée dans le protocole Internet

Note 1 à l'article: L'adresse IP correspond à un nom de domaine complet. Actuellement, elle est constituée de 32 bits et est généralement représentée par une séquence de quatre décimaux (chacun d'entre eux étant compris dans une plage de 0 à 255), séparés par des points. L'adresse IP d'un ordinateur comprend habituellement deux parties: une partie correspondant au numéro de réseau du réseau auquel est relié cet ordinateur, et une partie qui identifie l'ordinateur sur son réseau. Dans la nouvelle version IPv6 du protocole Internet, l'adresse IP est constituée de 128 bits.

Note 2 à l'article: Le protocole Internet ne se limite pas à l'Internet, et peut être utilisé sur d'autres réseaux.

3.1.46
protocole Internet
IP
protocole principal utilisé conjointement avec protocole de contrôle de transfert (TCP)

VOIR: TCP/IP.

3.1.47
Images par seconde
IPS
mesure ou unité de vitesse des images transmises ou affichées pour créer un flux vidéo

Note 1 à l'article: Une vitesse de 25 IPS (PAL) ou 30 IPS (NTSC) est considérée comme de la vidéo en temps réel ou intégrale.

3.1.48
protocole Internet, version 4
IPv4
version la plus largement utilisée du protocole Internet (partie «IP» du TCP/IP)

3.1.49
protocole Internet, version 6
IPv6
successeur d'IPv4

Note 1 à l'article: Déjà déployé dans certains cas et se répandant progressivement, IPv6 fournit un nombre considérable de numéros IP disponibles, plus d'un sextillion d'adresses. IPv6 permet à tout dispositif sur la planète d'avoir son propre numéro IP.

3.1.50
gigue
variation de retard ou continuité avec laquelle les paquets arrivent à leur destination

Note 1 à l'article: ´Variation de flux reçu ou pompage de flux´.

3.1.51
kilobits par seconde
kbit/s
unité de vitesse de transmission des données

3.1.52
latence
temps qui s'écoule entre l'initialisation d'une demande de données au réseau et le début du transfert réel des données

3.1.53
commutateur couche 2
dispositif de la couche liaison de données OSI (architecture de systèmes ouverts) responsable de la transmission de données sur les liaisons physiques dans un réseau

3.1.54
dispositif couche 3
dispositif OSI qui détermine les adresses réseau, les routes pour le transport d'informations

EXEMPLE: Un routeur est un dispositif couche 3; les commutateurs peuvent avoir également une capacité de couche 3.

3.1.55
réseau local
LAN
réseau de communication desservant des utilisateurs et dispositifs dans une zone géographique limitée, par exemple un bâtiment ou une zone protégée

Note 1 à l'article: L'abréviation LAN est dérivée du terme anglais développé correspondant "Local Area Network".

3.1.56

couche d'accès local
partie des dispositifs périphériques d'accès au réseau dans le réseau et donnant accès à l'opérateur

3.1.57
ouverture de session
nom de compte utilisé pour avoir accès à un composant destiné à être utilisé en combinaison avec un mot de passe ou action de connecter un composant ou un système en fournissant des justificatifs valides (habituellement, «nom d'utilisateur» et «mot de passe»)

3.1.58
commutateur géré
commutateur pouvant être contrôlé et administré dans le réseau par l'intermédiaire de sa propre adresse IP

3.1.59
adresse de contrôle d'accès au support
adresse MAC
identifiant unique attaché aux adaptateurs de réseau agissant comme un nom pour un adaptateur particulier

Note 1 à l'article: L'abréviation MAC est dérivée du terme anglais développé correspondant "Media Access Control".

3.1.60
base d'informations de gestion
MIB
collection structurée d'informations pour service à distance utilisant le protocole SNMP (Protocole simple de gestion de réseau)

Note 1 à l'article: L'abréviation MIB est dérivée du terme anglais développé correspondant " Management Information Base".

3.1.61
extensions de courrier Internet à fonctions multiples
MIME
norme définissant le type de charge utile diffusée par flux d'un serveur à un client

Note 1 à l'article: L'abréviation MIME est dérivée du terme anglais développé correspondant " Multipurpose Internet Mail Extensions".

EXEMPLE: «video/h264» est utilisé pour la diffusion de transfert en flux continu de vidéo codée H.264.

3.1.62
MJPEG
JPEG animé
norme de codage vidéo numérique ISO/CEI où chaque trame vidéo est compressée séparément en une image JPEG

3.1.63
MPEG-4
norme vidéo numérique de codage et de compression utilisant le codage intertrame pour diminuer significativement la taille du flux vidéo transmis par comparaison avec le codage intratrame seul

Note 1 à l'article: Dans le codage intertrame, une séquence vidéo est constituée de trames dites I ou clés contenant la totalité de l'image. Entre les trames clés se trouvent des trames delta qui sont codées uniquement avec les différences incrémentales. Ceci fournit souvent une compression substantielle car dans un grand nombre de séquences vidéo de surveillance, seule une petite partie des pixels est différente d'une trame à une autre.

3.1.64
multidiffusion
technique de conservation du débit diminuant l'utilisation du débit en délivrant simultanément un flux d'informations unique, ici un contenu vidéo, à plusieurs destinataires du réseau

3.1.65
basculement N+1
capacité de basculement de N applications identiques en opération en commutant automatiquement sur une instance d'application inutilisée

3.1.66
redondance N+n
capacité d'un système redondant parallèle, N représentant le nombre d'applications nécessaires pour satisfaire à la charge critique et n étant le nombre d'applications supplémentaires pour redondance

3.1.67
connectivité du réseau
connexion physique (câblée ou sans fil) et logique (protocole) d'un réseau informatique ou d'un dispositif individuel à un réseau

3.1.68
conception de réseau
façon d'agencer les divers clients et serveurs dans un réseau pour la connectivité, la performance et la sécurité

3.1.69
couche réseau
couche 3 du modèle de référence OSI, contrôlant les liaisons de communication et le routage des données sur une ou plusieurs liaisons

3.1.70
administration de réseau
services administratifs assurés dans la gestion d'un réseau, tels que la topologie du réseau et la configuration logicielle, surveillance de la performance du réseau, maintien des opérations du réseau et diagnostic et problèmes de pannes

3.1.71
performance du réseau
pour le flux de données en fonction des demandes de l'application de sécurité

Note 1 à l'article: Puisque le transfert vidéo en flux continu s'effectue principalement en temps réel, il est essentiel qu'il soit délivré en une durée spécifique.

3.1.72
topologie du réseau
motif de connexion entre nœuds dans un réseau, par exemple topologie hiérarchique

3.1.73
nœud
dispositif de communication relié à un réseau ou au point d'extrémité d'une connexion réseau tel qu'un dispositif relié à un réseau comme une station de travail, un dispositif vidéo IP, une imprimante, etc.

3.1.74
protocole relatif au temps dans le réseau
NTP
norme de synchronisation des horloges de systèmes informatiques dans les réseaux de communication par paquets

Note 1 à l'article: L'abréviation NTP est dérivée du terme anglais développé correspondant "Network Time Protocol".

Note 2 à l'article: Le NTP utilise le protocole de réseau sans connexion UDP (Protocole datagramme d'utilisateur) (voir UDP) pour permettre de transmettre de manière fiable le temps sur le réseau avec temps d'exécution de paquet variable.

3.1.75
perte de paquets
perte de paquets de données pendant la transmission sur un réseau

Note 1 à l'article: ´Fuite dans le flux´.

3.1.76
commutation de paquets
méthode utilisée pour transmettre des données sur un réseau depuis un grand nombre de sources différentes sur la même connexion, dirigées sur des routes différentes vers un grand nombre de récepteurs différents en même temps

3.1.77
paquets
structure de données représentant collectivement le flux de transmission incluant des en-têtes et des données associées à la couche réseau lorsque le protocole de communication est orienté connexion

3.1.78
topologie physique
couche physique du réseau; façon dont sont agencés les câbles; et façon dont sont connectés les composants

3.1.79
port
nombre ou identifiant pour un service particulier sur un serveur, principalement normalisé pour certains services tels que RTSP, UPnP, HTTP, etc.

3.1.80
protocole
ensemble de règles régissant la façon dont deux composants ou entités communiquent

Note 1 à l'article: Les protocoles sont utilisés à tous les niveaux de communication. Il existe des protocoles matériels et logiciels.

3.1.81
unité de données de protocole
PDU
unité de données équivalentes à la trame qui est transmise entre des couches de protocole

Note 1 à l'article: L'abréviation PDU est dérivée du terme anglais développé correspondant " Protocol Data Unit ".

3.1.82
service d'authentification à distance des utilisateurs connectés
RADIUS
protocole utilisant un serveur d'authentification pour contrôler l'accès au réseau

Note 1 à l'article: L'abréviation RADIUS est dérivée du terme anglais développé correspondant " Remote Authentication Dial-in User Service ".

3.1.83
protocole d'arbre maximal rapide
RSTP
protocole de réseau de la couche liaison garantissant une topologie sans boucle pour tout LAN ponté incluant la fonction de base pour empêcher des boucles de réseau et garantir la fonctionnalité de multidiffusion

Note 1 à l'article: L'abréviation RSTP est dérivée du terme anglais développé correspondant " Rapid Spanning Tree Protocol ".

3.1.84
redondance (réseau)
routage alternatif ou commutation de protection pour permettre une vidéotransmission fiable, par exemple par un anneau atomisé pour le mode paquet (RPR), un protocole d'arbre maximal (STP), un protocole d'arbre maximal rapide (RSTP)

Note 1 à l'article: ´Identification et remplacement d'un lien ou d'un flux rompu´.

3.1.85
demande de commentaires
RFC
normes Internet proposées et publiées, revues par le Groupe d'étude sur l'ingénierie Internet en tant que corps consensuel facilitant la discussion et éventuellement l'établissement d'une nouvelle norme (STD)

Note 1 à l'article: L'abréviation RFC est dérivée du terme anglais développé correspondant " Request For Comments ".

3.1.86
routeur
dispositif routant des informations entre des réseaux interconnectés, capable de sélectionner le meilleur chemin pour router un message en déterminant le point suivant du réseau vers lequel il convient d'acheminer un paquet allant vers sa destination finale

Note 1 à l'article: Un routeur crée et/ou maintient une table de routage spéciale contenant des informations relatives à la meilleure façon d'atteindre certaines destinations. Un routeur gère la connexion entre deux réseaux commutés par paquets ou plus en transmettant des paquets désignés par les adresses source et destination et en décidant de la route réelle pour les envoyer.

3.1.87
anneau atomisé pour le mode paquet
RPR
technologie de protocole basée sur la couche 2 MAC définie par l'IEEE 802.17 pour rétablissement rapide après défaillances et coupures de la liaison de connexion sur la couche 2

Note 1 à l'article: L'abréviation RPR est dérivée du terme anglais développé correspondant " Resilient Packet Ring ".

3.1.88
protocole de contrôle en temps réel
RTCP
protocole support pour transmission en temps réel de groupes dans un réseau

retour de qualité de service des récepteurs dans le groupe de multidiffusion et support de synchronisation de différents flux de support tels que vidéo, audio, métadonnées

Note 1 à l'article: L'abréviation RTCP est dérivée du terme anglais développé correspondant " Real-Time Control Protocol ".

3.1.89
protocole de transmission en temps réel
RTP
protocole Internet pour transmettre des données en temps réel telles que de la vidéo

Note 1 à l'article: Le RTP lui-même ne garantit pas la fourniture en temps réel des données. Il ne fournit que des mécanismes pour l'envoi et la réception de données de transfert en flux continu. Il est généralement basé sur le protocole UDP (Protocole datagramme d'utilisateur)

Note 2 à l'article: L'abréviation RTP est dérivée du terme anglais développé correspondant " Real-Time Transport Protocol ".

3.1.90
protocole de transfert en flux continu en temps réel
RTSP
norme de protocole de contrôle (RFC 2326) pour délivrer, recevoir et contrôler des flux de données en temps réel par exemple vidéo, audio et métadonnées et point d'entrée de démarrage pour négocier des transports tels que RTP, multidiffusion et monodiffusion, incluant la négociation des codecs

Note 1 à l'article: Peut être considérée comme une «commande à distance» pour contrôler des flux vidéo délivrés par un serveur.

Note 2 à l'article: L'abréviation RTSP est dérivée du terme anglais développé correspondant " Real-Time Streaming Protocol ".

3.1.91
certificat de sécurité
SC
information échangée utilisée par le protocole SSL pour établir une connexion sûre

Note 1 à l'article: L'abréviation SC est dérivée du terme anglais développé correspondant " Security Certificate ".

3.1.92
segment
section de réseau

3.1.93
serveur
programme logiciel fournissant des services à d'autres applications dans le même ordinateur ou dans d'autres ordinateurs

3.1.94
protocole simple de gestion de réseau
SNMP
ensemble de normes de communication avec des dispositifs connectés à un réseau TCP/IP pour la gestion des nœuds du réseau (serveurs, stations de travail, routeurs, commutateurs et concentrateurs, dispositifs de vidéotransmission, etc.) permettant aux administrateurs de réseaux de gérer les performances du réseau, de trouver, de résoudre des problèmes du réseau et de planifier des extensions du réseau

EXEMPLE: Les systèmes de gestion sont notifiés des problèmes des nœuds du réseau par réception de messages de pièges ou de changement provenant des dispositifs du réseau mettant en œuvre SNMP conformément à l'IETF RFC 1157, 1441, 3410.

Note 1 à l'article: L'abréviation SNMP est dérivée du terme anglais développé correspondant " Simple Network Management Protocol ".

3.1.95
protocole simple de gestion de réseau version 1
SNMPv1
protocole simple de demande/réponse pour système de gestion délivrant des requêtes à un dispositif de réseau géré qui envoie en retour une réponse conformément à l'IETF RFC 1157

3.1.96
protocole simple de gestion de réseau version 2
SNMPv2
protocole identique à SNMPv1 ajoutant et améliorant certaines opérations de protocole ainsi que l'opération de piège SNMPv2 sur la base d'un format de message différent pour le remplacement du piège SNMPv1 selon l'IETF RFC 1441

3.1.97
protocole simple de gestion de réseau version 3
SNMPv3
version du protocole SNMP (Protocole simple de gestion de réseau) ajoutant des possibilités de sécurité et de configuration à distance aux versions antérieures du SNMP incluant le modèle de sécurité basé sur l'utilisateur (USM) pour la sécurité des messages et le modèle de contrôle d'accès basé sur l'observation (VACM) pour le contrôle d'accès selon l'IETF RFC 3410

3.1.98
protocole simple relatif au temps dans le réseau
SNTP
adaptation du protocole relatif au temps dans le réseau (NTP) synchronisant les horloges d'un ordinateur sur un réseau, lorsque la précision de la mise en œuvre complète du NTP n'est pas nécessaire, selon l'IETF RFC 2030

Note 1 à l'article: L'abréviation SNTP est dérivée du terme anglais développé correspondant " Simple Network Time Protocol ".

3.1.99
point de défaillance unique
SPOF
composant d'un dispositif ou nœud d'un réseau qui, s'il tombe en panne, provoque la défaillance de la totalité du dispositif ou du réseau, normalement éliminé en ajoutant de la redondance

Note 1 à l'article: L'abréviation SPOF est dérivée du terme anglais développé correspondant " Single Point Of Failure ".

3.1.100
disponibilité six neufs
disponibilité A d'un système définie par A = MTBF/(MTBF + MTTR), décrivant le temps total de disponibilité de fonctionnement proportionnellement au temps total, qui n'est pas inférieure à 0,999 999 ou 99,999 9 %

3.1.101
protocole simple relatif au temps dans le réseau
SNTP
version simplifiée de NTP

Note 1 à l'article: L'abréviation SNTP est dérivée du terme anglais développé correspondant " Simple Network Time Protocol ".

VOIR: NTP.

3.1.102
protocole simple d'accès aux objets
SOAP
protocole de communication client-serveur utilisé pour échanger des demandes et des réponses de service «au-dessus de» HTTP (Protocole de transfert hypertexte) échangeant des données dans un format XML particulier spécifiquement conçu pour être utilisé avec SOAP

Note 1 à l'article: L'abréviation SOAP est dérivée du terme anglais développé correspondant " Simple Object Access Protocol ".

3.1.103
vitesse de transfert de données
vitesse à laquelle les informations sont transmises sur un réseau, habituellement mesurée en mégabits par seconde

3.1.104
couche de connexion sécurisée
SSL
protocole de sécurité de la couche application autorisant des communications chiffrées authentifiées sur des réseaux

Note 1 à l'article: L'abréviation SSL est dérivée du terme anglais développé correspondant "Secure Socket Layer".

3.1.105
réseau dédié au stockage
SAN
réseau ou sous-réseau à grande vitesse dont le but principal est de transférer des données entre des dispositifs de réseau et des systèmes de stockage consistant en une infrastructure de communication, fournissant des connexions physiques, une couche gestion et des éléments de stockage

Note 1 à l'article: L'abréviation SAN est dérivée du terme anglais développé correspondant " Storage Area Network ".

3.1.106
performance de transfert en flux continu
qualité du flux du réseau qui détermine comment un opérateur perçoit les informations, y compris les facteurs suivants: disponibilité, erreurs produites par le bruit, encombrement ou défaillances de composants, retard, instabilité, débit, perte

3.1.107
masque de sous-réseau
méthode permettant de diviser un grand réseau en plusieurs réseaux plus petits

Note 1 à l'article: En fonction de la classe de réseau (A, B ou C), certains nombres des bits d'adresse IP sont réservés pour l'adresse de réseau (sous-réseau) et certains pour l'adresse hôte. Les adresses de classe A par exemple utilisent 8 bits pour l'adresse de sous-réseau et 24 bits pour la partie hôte de l'adresse.

3.1.108
commutateur
dispositif connectant des dispositifs de réseau à des hôtes permettant à un grand nombre de dispositifs de partager un nombre limité de ports

3.1.109
protocole de commande de transmission/protocole Internet
TCP/IP
ensemble de protocoles définissant les réseaux et Internet en général

Note 1 à l'article: L'abréviation TCP/IP est dérivée du terme anglais développé correspondant " Transmission Control Protocol/Internet Protocol ".

3.1.110
débit (réseau)
capacité de transmission numérique permettant d'assurer la qualité exigée du flux vidéo

EXEMPLES: 1 Mbit/s jusqu'à 10 Mbit/s.

Note 1 à l'article: Dimension du tuyau de flux vidéo possible.

3.1.111
protocole de temps
protocole de réseau permettant à des clients temps d'obtenir l'heure courante à partir de serveurs de temps

3.1.112
topologie
configuration de réseau (physique) incluant des câbles et autres équipements

flux (logique) de données entre des entités logiques incluant la spécification de protocoles impliqués indépendants de l'emplacement physique

3.1.113
émetteur/récepteur
dispositif qui reçoit et envoie des signaux sur un support

3.1.114
flux de transport
TS
flux binaire de contenu habituellement en référence à un format de flux MPEG-2 AV

Note 1 à l'article: L'abréviation TS est dérivée du terme anglais développé correspondant " Transport Stream ".

3.1.115
protocole datagramme d'utilisateur
UDP
protocole sans état pour le transfert de données sans disposition pour l'acquittement des paquets reçus

Note 1 à l'article: L'abréviation UDP est dérivée du terme anglais développé correspondant " User Datagram Protocol ".

3.1.116
dispositif universel prêt à fonctionner
UPnP
architecture pour connectivité universelle du réseau poste-à-poste de dispositifs de tous les facteurs de forme

Note 1 à l'article: Elle est conçue pour établir une connectivité à base de normes souples, facile à utiliser, avec des réseaux ad-hoc ou non gérés. Il s'agit d'une architecture de réseau ouverte distribuée mettant à niveau les techniques TCP/IP et Web pour permettre une mise en réseau sans jonction en plus du contrôle et du transfert de données parmi les dispositifs en réseau.

Note 2 à l'article: L'abréviation UPnP est dérivée du terme anglais développé correspondant " Universal Plug and Play ".

3.1.117
commutateur non géré
commutateur de base ne proposant pas de capacité d'administration réseau à distance

3.1.118
identificateur uniforme de ressource
URI
adresse de ressources disponibles sur un réseau commençant par un «schéma» tel que HTTP ou RTSP

Note 1 à l'article: L'abréviation URI est dérivée du terme anglais développé correspondant " Uniform Resource Identifier".

3.1.119
localisateur uniforme de ressource
URL
adresse unique d'un fichier accessible sur Internet

Note 1 à l'article: L'abréviation URL est dérivée du terme anglais développé correspondant " Uniform Resource Locator".

Note 2 à l'article: L'URL était anciennement le localisateur universel de ressources.

3.1.120
format de transformation unicode
UTF
code de caractère préservant la totalité de la plage US-ASCII, assurant la compatibilité avec les systèmes de fichiers, les analyseurs et les autres logiciels qui sont basés sur les valeurs US-ASCII mais qui sont transparents aux autres valeurs

Note 1 à l'article: L'abréviation UTF est dérivée du terme anglais développé correspondant " Unicode Transformation Format ".

3.1.121
UTF-8
schéma de codage avec des caractères UCS-2 ou USC-4 comme nombre variable d'octets, le nombre d'octets et la valeur de chaque octet dépendant de la valeur entière assignée au caractère dans l'ISO/CEI 10646

3.1.122
dispositif de vidéotransmission
VTD
dispositif vidéo avec au moins une interface de réseau IP traitant la vidéo

Note 1 à l'article: L'abréviation VTD est dérivée du terme anglais développé correspondant " Video Transmission Device".

3.1.123
réseau étendu
WAN
réseau reliant des ordinateurs sur de grandes zones, par exemple au-delà des limites d'un site protégé unique

Note 1 à l'article: L'abréviation WAN est dérivée du terme anglais développé correspondant " Wide Area Network ".

3.1.124
station de travail
ordinateur relié à un réseau où des opérateurs interagissent avec l'affichage vidéo

3.1.125
langage de balisage extensible
XML
protocole largement utilisé pour définir des formats de données, fournissant un système très riche pour définir des structures de données complexes

3.1.126
schéma XML
définition incluant des contraintes sur les données dans un document XML

3.2 Abréviations

AAC	Advanced Audio Codec (Codec audio avancé)
AES	Advanced Encryption Standard (norme de cryptage évolué)
ARP	Address Resolution Protocol (Protocole de résolution d'adresse)
ASCII	American Standard Code for Information Interchange (Code américain normalisé pour l'échange d'information)
ATM	Automatic Teller Machine (Guichet bancaire automatique)
AVC	Advanced Video Codec (Codec vidéo avancé)
CIF	Common Intermediate Format (Format intermédiaire commun)
CPU	Central Processing Unit (Unité centrale de traitement)
DEL	Diode électroluminescente
DES	Data Encryption Standard (Norme de chiffrement de données)
DHCP	Dynamic Host Configuration Protocol (Protocole de configuration de serveur dynamique)
DNS	Domain Name System (Système de noms de domaine)
DVB	Digital Video Broadcast (Radiodiffusion vidéonumérique)
DVR	Digital Video Recorder (Magnétoscope (enregistreur vidéo) numérique)
GPS	Geo Positioning System (Système de positionnement géographique)
H.264-CBP	ISO/IEC 14496-10 et ITU H.261 Reduced complexity Baseline Profile (Profil de base de complexité réduite ISO/CEI 14496-10 et UIT H.261)
HD	High Definition (Haute définition)
HTTP	Hypertext Transfer Protocol (Protocole de transfert hypertexte)
I/O	Input / Output (Entrée/Sortie)
IANA	Internet Assigned Numbers Authority (Autorité chargée de l'assignation des numéros Internet)
ICMP	Internet Control Message Protocol (Protocole de message de commande Internet)
ID	Identification

IEEE	Institute of Electrical and Electronics Engineers (Institut des ingénieurs en électricité et électronique)
IESG	Internet Engineering Steering Group (Groupe d'orientation de génie Internet)
IETF	Internet Engineering Task Force (Groupe d'étude sur l'ingénierie Internet)
IGMP	Internet Group Multicast Protocol (Protocole Internet de gestion de groupe)
IP	Internet Protocol (Protocole Internet)
ISO	Organisation Internationale de Normalisation
IT	Information Technology (Technologie de l'information)
JPEG	Format JPEG (Joint Picture Experts Group)
LAN	Local Area Network (réseau local)
MAC	Message Authentication Code (Code d'authentification de message)
MD 5	Message Digest Algorithm Version 5 (Algorithme de condensé de message Version 5)
MIB	Management Information Base (Base d'informations de gestion)
MIME	Multipurpose Internet Mail Extensions (Extensions de courrier Internet à fonctions multiples)
MJPEG	Motion JPEG (JPEG animé)
MTBF	Mean Time Between Failures (Moyenne des temps de bon fonctionnement)
MTTR	Mean Time To Repair (Délai moyen de réparation)
NAS	Network Attached Storage (Mémoire attachée au réseau)
NTP	Network Time Protocol (Protocole relatif au temps dans le réseau)
NTSC	National Television System Committee
NVR	Network Video Recorder (Enregistreur vidéo réseau)
OASIS	Organization for the Advancement of Structured Information Standards (Organisation pour la promotion des normes d'information structurée)
OID	Object Identifier (Identificateur d'objet)
OR	Operational Requirements (Exigences de fonctionnement)
OSI	Open Systems Interconnection (Interconnexion des systèmes ouverts)
PAL	Phase Alternation Line (format de télévision) (Ligne d'alternance de phase)
PC	Personal Computer (Ordinateur personnel)
PDU	Protocol Data Unit (Unité de données de protocole)
PING	Packet Internet Groper
POS	Point of Sales (Point de vente)
PPM	Packets Per Million (Paquets par million)
PTZ	Pan / Tilt / Zoom (Panoramique/Inclinaison/ Zoom)
RFC	(Demande de commentaires) Projet de norme IETF
RPR	Resilient Package Ring (Anneau atomisé pour le mode paquet)
RSA	(système cryptographique à clé publique inventé par) Rivest, Shamir et Adleman
RTCP	Real Time Control Protocol (Protocole de transfert en flux continu en temps réel)
RTP	Real-time Transport Protocol (Protocole de transmission en temps réel)
RTSP	Real Time Streaming Protocol (Protocole de transfert en flux continu en temps réel)
SDP	Session Description Protocol (Protocole de description de session)
SMI	Structure of Management Information (Structure d'informations de gestion)
SNMP	Simple Network Management Protocol (Protocole simple de gestion de réseau)

SNTP	Simple Network Time Protocol (Protocole simple relatif au temps dans le réseau)
SOAP	Simple Object Access Protocol (Protocole simple d'accès aux objets)
SPOF	Single Point of Failure (Point de défaillance unique)
SRTP	Secure Real-time Transport Protocol (Protocole de transmission en temps réel de sécurité)
SSL	Secure Sockets Layer (Couche de connexion sécurisée)
SSM	Source-Specific Multicast (Multidiffusion spécifique à la source)
STD	Standard (Norme)
STP	Spanning Tree Protocol (Algorithme de l'arbre recouvrant)
TCP	Transmission Control Protocol (Protocole de commande de transmission)
TCP/IP	Transmission Control Protocol / Internet Protocol (protocole de commande de transmission/protocole Internet)
TLS	Transport Layer Security (Sécurité de la couche transport)
TS	Transport Stream (Flux de transport)
TTL	Time-to-live (Durée de vie)
UCS	Universal Character Set (Jeu de caractères universel)
UDP	User Datagram Protocol (Protocole datagramme d'utilisateur)
UPnP	Universal Plug and Play (Dispositif universel prêt à fonctionner)
URI	Uniform Resource Identifier (Identificateur uniforme de ressource)
URL	Uniform Resource Locator (Localisateur uniforme de ressource)
UTC	Universal Time Coordinated (Temps universel coordonné)
UTF	Unicode Transformation Format (Format de transformation unicode)
UTF-8	8-bit Unicode Transformation Format (Format de transformation unicode 8 bits)
VACM	View-based Access Control Model (Modèle de contrôle d'accès basé sur l'observation)
VCA	Video Content Analysis (Analyse du contenu vidéo)
VSS	Video Surveillance System (Système de vidéosurveillance)
VT	Video Transmission (Vidéotransmission)
VTD	Video Transmission device (Dispositif de vidéotransmission)
W3C	World Wide Web Consortium
WAN	Wide Area Network (Réseau étendu)
WSDL	Web Services Description Language (Langage de description de services Web)
XML	eXtensible Markup Language (Langage de balisage extensible)

4 Exigences de performance

4.1 Généralités

La présente norme de vidéotransmission traite les exigences sur les dispositifs dans les applications de sécurité avec des caractéristiques différentes des applications, par exemple les stations de travail d'opérateurs intégrées, basées sur un PC (Ordinateur personnel), ainsi que d'autres. Les dispositifs vidéo de codage et décodage numérique, les stations de travail de client VSS, les mémoires vidéo, les NVR (Enregistreurs vidéo réseau) et les DVR (Magnétoscopes numériques) possèdent un ensemble de fonctions différentes pour le transfert vidéo en flux continu et la connectivité du réseau. Ces fonctionnalités sont résumées ci-dessous:

– codage de flux

– réception et décodage de flux
– enregistrement de flux
– transfert en flux continu en direct et affichage
– lecture et relecture de transfert en flux continu
– contrôle de caméra
– surveillance de bon fonctionnement et d'état
– analyse de contenu vidéo
– création et transfert en flux continu de métadonnées
– accessoires

En raison de la nature de la vidéotransmission non analogique, en particulier des réseaux vidéo IP, de l'utilisation de connexions partagées, des techniques de compression et de transfert en flux continu, les exigences suivantes doivent être appliquées:

Pour différentes applications, telles que le suivi par caméra PTZ (Panoramique/inclinaison/zoom), l'enregistrement, la détection de mouvement vidéo, la surveillance à distance, etc., il existe différentes exigences relatives aux performances des VTD (Dispositifs de vidéotransmission). La présente norme présente donc différentes classes de performance. Pour chaque application, les exigences doivent être spécifiées et inclure les classe concernant: la précision du service temps (Tableau 1), les temps d'interconnexion (Tableau 2), le partage des débits (Tableaux 3 et 4), le transfert en flux continu (Tableau 5), la gigue du réseau (Tableau 6) et la surveillance (Tableau 7).

Différentes fonctions du système peuvent avoir des classes de performance différentes.

NOTE Les classes de performance sont indépendantes des grades de sécurité.

Ces exigences ne s'appliquent pas aux interconnexions pour téléphones portables, mais doivent être appliquées aux connexions de réseau fixe sans fil et aux applications de transport, telles que les systèmes embarqués.

S'il existe des exigences minimales de performance du réseau pour le bon fonctionnement d'un VTD ou d'un VSS, celles-ci doivent être définies et documentées.

Les exigences commencent par la classe 1 la plus basse et augmentent à mesure que le numéro de classe augmente.

4.2 Services de temps réseau

4.2.1 Généralités

Le dispositif de vidéotransmission (VTD) nécessite des services de temps réseau pour une horloge en temps réel, la gestion d'événements, l'accès et pour le flux de transport vidéo (TS).

Le VTD ne doit jamais commencer le transfert vidéo en flux continu pour un enregistrement, si les exigences ci-dessous relatives à la précision de l'horodatage des trames vidéo ne peuvent pas être assurées. Ceci doit particulièrement être vérifié après démarrage ou réinitialisation après interruption d'alimentation du VTD. Sinon, l'intégrité des enregistrements de flux peut être corrompue et peut ne pas permettre la relecture correcte non seulement des séquences de trames concernées mais également d'autres enregistrements. Ceci a un impact encore plus important sur les images utilisées à des fins de preuve.

4.2.2 Horloge en temps réel

Il convient que l'horloge en temps réel du dispositif de vidéotransmission soit synchronisée avec une horloge normale utilisant le Protocole simple relatif au temps dans le réseau (SNTP) RFC 2030, Version 4 pour IPv4, IPv6 et OSI. Il convient que les adresses des serveurs SNTP

proviennent de l'option Serveur de temps du DHCP (Protocole de configuration de serveur dynamique), option (4). Le temps système le plus précis doit être utilisé comme défaut: la meilleure précision du SNTP est de 0,25 µs, tandis que l'utilisation du «Serveur de temps» selon RFC 868 ne propose comme meilleure précision que 1 s.

4.2.3 Services de temps précis pour le flux de transport

Comme option, il convient de mettre en œuvre le Protocole relatif au temps dans le réseau (NTP) (Version 3) comme détaillé dans la RFC 1305 lorsque des services de temps d'une précision de 1 ms à 50 ms suivant les exigences du Tableau 1 sont nécessaires. Il convient que les adresses IP des serveurs de temps proviennent du Serveur de temps réseau du DHCP, option (42). Il convient d'essayer en premier le protocole relatif au temps dans le réseau et seulement en cas de défaillance, on doit utiliser le Protocole simple relatif au temps dans le réseau. Une option (42) égale à zéro du serveur de temps réseau du DHCP signifie qu'aucun serveur n'est disponible et qu'il convient d'utiliser le Protocole simple relatif au temps dans le réseau.

Tableau 1 – Précision du service temps pour le flux de transport vidéo

Classe	T1	T2	T3	T4
Précision du service temps pour le flux de transport	80 ms	40 ms	5 ms	1 ms

Les horodatages du NTP dans l'en-tête du Protocole en temps réel doivent augmenter régulièrement sur les paquets consécutifs du flux du RTP. Il convient qu'ils correspondent à l'heure locale et ils doivent être réglés si nécessaire pour rester consécutifs. Après redémarrage du VTD, la resynchronisation de l'heure système peut être retardée jusqu'à 10 s pour le SNTP ou jusqu'à 15 s pour le protocole du serveur de temps (NTP).

4.3 Exigences sur le temps de la vidéotransmission

4.3.1 Généralités

Les dispositifs de vidéotransmission et leurs interconnexions doivent être conçus conformément aux exigences sur le système de la CEI 62676-1-1 en tant que partie du VSS.

4.3.2 Temps de connexion

Le temps de connexion nécessaire pour initialiser la transmission d'un flux d'une source vers un récepteur est à considérer. Ce temps doit être considéré, particulièrement dans des systèmes ou des allers et retours de caméras, un séquencement ou des tours de garde de différentes caméras sont nécessaires. Le temps de connexion initial doit être très inférieur au temps de passage de la séquence de cameras, voir Tableau 2.

Tableau 2 – Interconnexions – Exigences sur le temps

Les dispositifs de vidéotransmission doivent avoir	Classe			
	I1	I2	I3	I4
un temps de connexion initial maximum pour chaque nouvelle demande de flux vidéo de	2 000 ms	1 000 ms	500 ms	250 ms

NOTE Dans les flux de multidiffusion RTSP, une demande de trame I optimise ce temps de connexion.

4.3.3 Capacités de connexion

Si un réseau de vidéotransmission VSS est conçu et configuré de façon que des dispositifs récepteurs de vidéotransmission uniques ou multiples demandent des images vidéo et que la demande simultanée de flux d'image par tous les récepteurs possibles peut dépasser la

capacité disponible du réseau à un instant donné, le dispositif de vidéotransmission doit proposer des moyens selon le Tableau 3 suivant:

Tableau 3 – Exigences du réseau de vidéotransmission

Les dispositifs de vidéotransmission dans un réseau partagé doivent proposer des moyens pour configurer:	Classe			
	C1	C2	C3	C4
le débit de données maximal des flux vidéo pour chaque canal vidéo			X	X
le débit de données maximal pour tous les flux vidéo disponibles d'un simple dispositif			X	X
le débit de données maximal ou le nombre de flux vidéo vers tous les dispositifs clients du réseau			X	X

Tableau 4 – Exigences du réseau de vidéotransmission

Les dispositifs de vidéotransmission dans un réseau partagé doivent proposer des moyens pour:	Classe			
	P1	P2	P3	P4
affecter une priorité à certains flux par rapport à d'autres, par exemple, des flux d'enregistrement ou des alarmes sur des flux d'image en direct			X	X
affecter une priorité à certains utilisateurs par rapport à d'autres, par exemple, pour le contrôle de PTZ (Panoramique/inclinaison/zoom)			X	X

A aucun moment le récepteur de vidéotransmission ne doit permettre l'ouverture et l'initialisation de connexions avec de nouvelles sources de flux vidéo au détriment des flux vidéo déjà affichés ou enregistrés afin d'éviter toute perte de trame.

A aucun moment le récepteur de vidéotransmission ne doit permettre l'affichage de flux en direct au détriment des flux vidéo enregistrés afin d'éviter toute perte de trame.

Si la qualité de la vidéo pour la consultation en direct par un opérateur et pour l'enregistrement doit être différente, le dispositif de vidéotransmission doit proposer au minimum deux flux avec des réglages de qualité différents.

Si la qualité de la vidéo pour un enregistrement continu et pour un enregistrement d'alarme basé sur des événements doit être différente, le dispositif de vidéotransmission doit proposer un flux supplémentaire, si le réglage de qualité est différent des deux autres.

4.4 Exigences de performance sur le transfert vidéo en flux continu

4.4.1 Introduction, latence, gigue, débit

Les recommandations données dans le présent paragraphe sont informatives.

Les flux vidéo sont sensibles à l'accumulation du retard, appelée latence. Le réseau contribue à la latence de plusieurs façons:

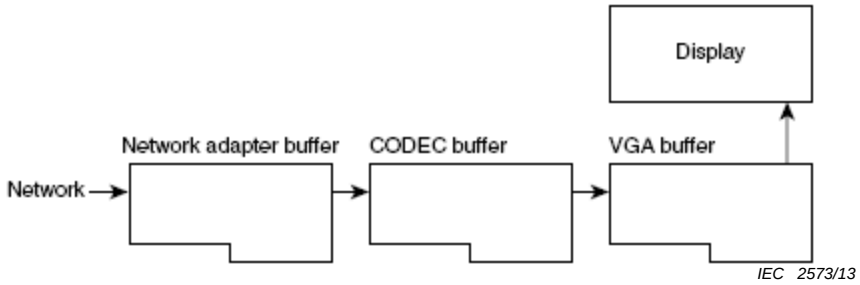
- Retard de transmission – temps nécessaire pour qu'un paquet vidéo atteigne le support donné. Le retard de transmission est déterminé par la vitesse du support de transmission et par la taille du paquet vidéo.
- Retard d'acheminement – temps nécessaire pour qu'un dispositif d'inter-réseautage (tel qu'un commutateur, un pont ou un routeur) envoie un paquet qu'il a reçu.
- Retard de traitement – temps requis par un dispositif de réseau pour rechercher la route, modifier l'en-tête et pour d'autres tâches de commutation. Dans certains cas, l'en-tête de

paquet est également à manipuler. Par exemple, le type d'encapsulation est à modifier. Chacune de ces étapes peut contribuer au retard de traitement.

- Retard de codage/décodage – temps requis pour coder et/ou décoder une image vers ou depuis un flux vidéo, influencé par la performance du VTD (Dispositif de vidéotransmission) et le type, le profil et le niveau du codec. Par exemple, le profil H.264 «Main» avec un retard de codage de 350 ms et «Baseline» avec 120 ms ou le MPEG4, peuvent proposer un retard de 110 ms et un faible retard du MPEG2 inférieur à 180 ms.
- Retard d'affichage – temps requis par l'unité de présentation pour modifier l'aspect d'un élément d'image, ne pas en tenir compte habituellement

4.4.2 Exigences sur la gigue du réseau

Si un réseau VSS envoie des données vidéo avec une latence variable, il introduit de la gigue. La technique la plus courante pour diminuer la gigue consiste à enregistrer les données vidéo entrantes dans un tampon à partir duquel elles sont affichées. Le tampon diminue l'effet de la gigue comme un amortisseur de choc.



Légende

Anglais	Français
Network	Réseau
Network adapter buffer	Tampon d'adaptation au réseau
CODEC buffer	Tampon CODEC
Display	Affichage
VGA buffer	Tampon VGA

Figure 1 – Tampon de réseau

Le besoin global est que même lorsque le trafic vidéo comporte de la gigue, l'opérateur observant les images vidéo ne doit pas être perturbé. Pour cette raison, les réseaux de sécurité vidéo doivent utiliser des techniques pour minimiser la gigue pour les flux en direct et en relecture.

Une manière de fournir une gigue et une perte de paquet minimales est d'augmenter les vitesses du réseau pour garantir un débit suffisant disponible pendant les périodes de trafic courantes et de crête.

4.4.3 Perte de paquets

Il existe différentes raisons pour la perte de paquets sur le réseau. Une perte de paquets peut être provoquée par un encombrement du réseau, lorsqu'un réseau fait l'objet d'une utilisation ou de connexions excessives ou qu'un autre trafic peut être bloquant et l'équipement d'infrastructure du réseau peut être confronté à des problèmes et présenter une défaillance. Le réseau peut être configuré d'une façon erronée, par exemple avec des adresses IP dupliquées.

Dans un paquet de transfert vidéo IP en flux continu, une perte peut avoir un impact sur la qualité de la vidéo, peut provoquer un blocage de trame, des distorsions d'image locales avec

des zones d'image manquant de netteté, des tâches, des artefacts, une pixellisation, du flou, du scintillement, des vitesses de trame décroissantes, des images figées. De plus, une perte de paquets peut également provoquer une latence et un retard excessifs pouvant conduire à des déconnexions du flux du dispositif de vidéotransmission (VTD).

NOTE Dans l'industrie de la radiodiffusion, une perte de paquets de 100 ppm ou un paquet perdu par minute pour les flux en temps réel MPEG-4 2CIF est généralement considérée comme imperceptible et de 2 ppm ou un paquet perdu par heure comme inacceptable pour l'utilisateur, conformément à la norme DVB.

L'impact d'une perte de paquets sur un transfert vidéo en flux continu dépend d'un certain nombre de facteurs incluant le pourcentage de perte de paquets, la distribution de la perte dans le temps et les capacités des VTD à traiter la perte. Dans les flux vidéo avec codage différentiel, la trame courante est prédite à partir de la vidéo transmise précédemment. Les paquets vidéo dépendent des paquets précédents. Si ces paquets n'ont pas été reçus avec succès, le paquet courant est alors inutile. Ceci est appelé propagation de perte. Cette propagation s'arrête avec l'arrivée de trames codées de manière interne (Trames I).

Le VTD doit être capable de détecter une perte de paquets et d'en compenser les effets. Le VTD doit être capable de fournir un ressenti acceptable à l'opérateur et à l'utilisateur ainsi que la perception vidéo pendant une perte de paquets. La réduction des effets visuels associés à la fourniture du flux est critique vis-à-vis de la rétention visuelle de l'utilisateur final. Au moins l'impression visuelle de la perte de paquets doit être masquée ou cachée en fonction des besoins pour satisfaire à la tâche et à l'objectif de surveillance. Un VTD doit fournir des techniques d'annulation d'erreur et de perte conformes à l'état de l'art. Le VTD doit proposer une capacité d'annulation de toute perte de paquets ou d'erreur en utilisant par exemple des informations de paquets de la vidéo codée provenant des macroblocs voisins, des trames antérieures ou futures, afin d'estimer le contenu vidéo de la trame courante.

4.4.4 Niveau de performance

Pour traiter les besoins de performance du trafic vidéo en flux continu, les exigences suivantes s'appliquent, voir Tableau 5.

Tableau 5 – Exigences de performance de transfert vidéo en flux continu et d'affichage de flux

Classe	S1	S2	S3	S4
Perte maximale	240 ppm	120 ppm	60 ppm	30 ppm
Latence unidirectionnelle maximale de flux en direct (incluant codage, mise en réseau, décodage, affichage)	600 ms	400 ms	200 ms	100 ms
Reproduction spéciale maximale (pause, échelon unique, …) Temps de réaction	400 ms	200 ms	200 ms	100 ms
Latence d'aller et retour incluant visualisation et contrôle, par exemple PTZ (Panoramique/inclinaison/zoom)	700 ms	500 ms	300 ms	200 ms
Latence d'aller et retour incluant visualisation et contrôle, par exemple PTZ lorsque le déplacement d'objets doit être surveillé et suivi	650 ms	450 ms	250 ms	150 ms

Les archives et les enregistrements vidéo de transfert en flux continu ont des exigences de performance plus faciles car ils ne sont pas sensibles au retard (la vidéo peut prendre un certain temps pour se caler) et ne sont globalement pas sensibles à la gigue (en raison du tampon d'application). Le transfert vidéo en flux continu peut contenir un contenu précieux, tel que des applications de sécurité, auquel cas il nécessite des garanties de performance.

Puisque la performance du transfert vidéo en flux continu est évaluée au mieux par l'impression visuelle, il vaut mieux soumettre à essai et vérifier les paramètres de performance d'affichage. L'exigence générale pour l'affichage du transfert vidéo en flux continu doit fournir une impression visuelle régulière à l'utilisateur final. La gigue d'affichage ne doit pas être supérieure à 1/10 de l'intervalle de vitesse de trame.

4.4.5 Gigue de paquet

La gigue de paquet crête à crête maximale est définie comme la variation de retard entre la source en direct ou en relecture du flux RTP et du dispositif d'extrémité. La gigue crête à crête, J, nécessite que l'écart du retard de réseau, d, soit limité par $-J/2 \leq d \leq +J/2$. Pour donner comme exemple une comparaison technique, le dispositif de vidéotransmission selon la classe M4 doit satisfaire à la spécification d'interface en temps réel de l'ISO/CEI 13818-9 avec une gigue de 20 ms.

Tableau 6 – Gigue de paquet de réseau de flux vidéo

Classe	M0 ms	M1 ms	M2 ms	M3 ms	M4 ms
Gigue de paquet crête à crête maximale	-	160	80	40	20

Il est nécessaire que le récepteur du VTD fournisse un tampon pour compenser la gigue spécifiée. Ceci signifie en fait qu'un VTD est tenu de comporter des tampons plus grands pour obtenir une réception et un décodage corrects de trames vidéo avec une gigue plus importante. Ce retard s'ajoute dans le tampon du récepteur du VTD qui doit être suffisamment grand pour compenser la variation des temps entre arrivées (gigue).

4.4.6 Surveillance des interconnexions

Le Tableau 7 spécifie la période maximale admise pour qu'une interconnexion ou un signal soit indisponible. Si une connexion vidéo IP pour le transfert en flux continu, le contrôle de bon fonctionnement ou une gestion d'événement présente une défaillance et que la période maximale admise est dépassée, un signal ou un message de fraude ou de défaut doit être généré comme spécifié dans la CEI 62676-1-1.

Tableau 7 – Surveillance des interconnexions

Le système doit proposer	Grade de sécurité			
	1	2	3	4
la durée maximale admise d'indisponibilité d'un dispositif			180 s	30 s
le temps de détection maximum pour la perte d'un signal en direct		8 s	4 s	2 s
L'exigence ci-dessus est destinée à déterminer si une communication est possible en surveillant la vidéocommunication pour s'assurer si elle est disponible pour acheminer un signal ou un message. La surveillance peut prendre la forme de l'écoute de l'encombrement lorsqu'un dispositif de vidéotransmission communique par l'intermédiaire d'interconnexions partagées avec d'autres dispositifs ou d'autres applications.				

NOTE Ces exigences correspondent à l'exigence 3 du Tableau 4 et à l'exigence «perte vidéo» du Tableau 5 de la CEI 62676-1-1:2013.

5 Exigences de conception du réseau de vidéotransmission IP

5.1 Généralités

Pour comprendre de quelle façon les exigences de performance du réseau vidéo IP des articles précédents sont satisfaites dans une installation, non seulement il est important de sélectionner et de configurer les composants de surveillance vidéo IP normalisés mais également de fournir une structure de réseau appropriée. Pour garantir la performance d'un réseau de vidéotransmission en fonction des exigences énumérées ci-dessus, la procédure suivante pour concevoir un réseau est recommandée:

Globalement, un VSS et ses interconnexions doivent être conçus conformément à la CEI 62676-1-1. Trois éléments importants sont à considérer lors de la conception d'un VSS effectif:

– l'infrastructure technique
– les exigences de fonctionnement (OR)
– les processus et procédures de fonctionnement

La présente section donne les détails des exigences de conception pour l'installation VSS en se concentrant sur les connexions et les communications IP.

5.2 Vue d'ensemble

Les deux éléments de conception les plus importants sont la détermination du nombre de serveurs et de sources de transfert vidéo en flux continu (c'est-à-dire, les dispositifs de codage vidéo IP) et du nombre de récepteurs ou clients (interfaces d'utilisateurs, stations de travail, dispositifs d'enregistrement, décodeurs), car ils définissent la charge qui peut varier considérablement. Ces deux facteurs sont étroitement liés et influent l'un sur l'autre. Une combinaison de ces deux éléments a un impact sur la réussite de la conception d'un système.

5.3 Planification d'un réseau numérique

5.3.1 Généralités

Pour une conception correcte d'un réseau, suivre les étapes suivantes:

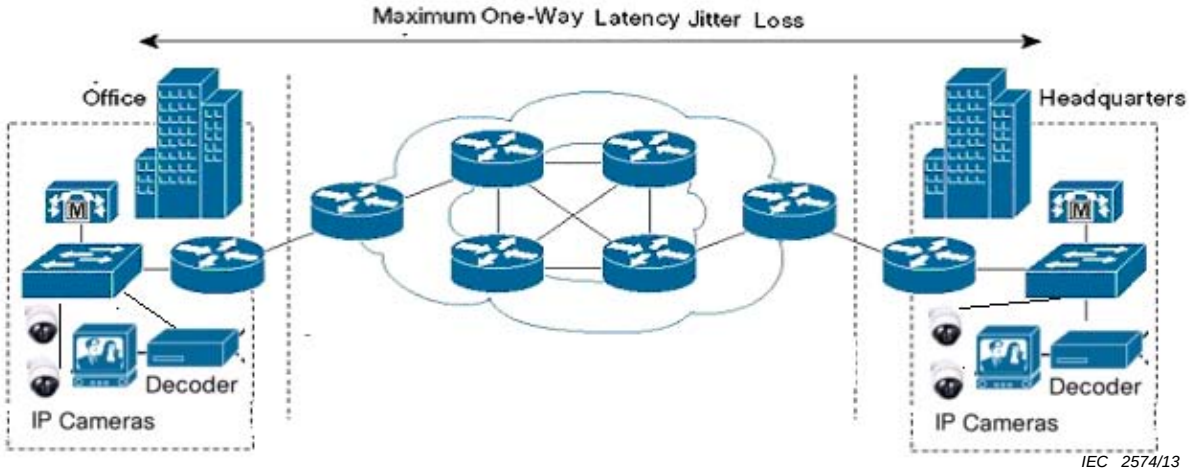
1) Représenter les connexions logiques nécessaires de l'infrastructure de réseau physique prévue
2) Définir une topologie adaptée à la connectivité requise
3) Planifier la redondance du réseau
4) Définir les données de trafic de base du réseau en se basant sur un flux vidéo continu avec la résolution visuelle requise pour l'enregistrement et l'affichage de scènes statiques et en déplacement
5) Simuler le trafic du flux vidéo pour vérifier ces données de base
6) Définir les besoins de capacité des données de flux vidéo moyenne et de crête en se basant sur la vidéo demandée par l'utilisateur pour les stations de travail, les enregistrements de flux vidéo en continu et les enregistrements vidéo de mouvement ou d'alarme
7) Définir un nombre pour la simultanéité moyenne et maximale des sources de transfert en flux continu, appelé facteur sélectif
8) Identifier chaque exigence de débit de liaison du réseau dans les couches accès, distribution et intérieure
9) Identifier les engorgements potentiels. Les liens de WAN (Réseau étendu) peuvent être des engorgements de trafic vidéo IP
10) Examiner soigneusement l'infrastructure matérielle du réseau pour garantir une prise en charge d'une extension immédiate et future des besoins de capacité de surveillance ou de transfert vidéo en flux continu
11) Documenter précisément la topologie du réseau, la capacité réellement utilisée et la capacité maximale.

5.3.2 Exigences critiques pour la performance du transfert vidéo IP en flux continu

5.3.2.1 Généralités

Pour prendre en charge le trafic vidéo, des normes et des chiffres de performance de qualité équivalente doivent être satisfaits pour des services de transfert vidéo en flux continu acceptables (voir Figure 1). Quatre facteurs, à savoir le débit, la latence, la gigue et la perte de paquets, sont critiques du point de vue du réseau. La gestion de chacun d'entre eux détermine l'efficacité avec laquelle le réseau prend en charge le trafic vidéo IP. Une approche est spécifiée dans la présente norme, où une conception de réseau convenable et une gestion globale du système garantissent la qualité et la performance du flux vidéo.

Un cinquième facteur «autre routage», appelé «commutation de protection» est également une considération importante pour faciliter la protection d'un VSS critique et du trafic de l'opérateur.



Légende

Anglais	Français
Maximum One-Way Latency Jitter Loss	Perte de gigue de latence maximale unidirectionnelle
Office	Bureau
Decoder	Décodeur
IP cameras	Caméras IP
Headquarters	Direction

Figure 2 – Latence de réseau, gigue, perte

5.3.2.2 Débit: planification de capacité de flux

Avant d'appliquer des données associées à la vidéo sur un réseau, l'opérateur est tenu de vérifier que le réseau peut prendre en charge toutes les applications existantes (le cas échéant) ainsi que le débit de données exigé, associé à la qualité de vidéo devant être transportée sur le réseau. Calculer d'abord les exigences minimales de débit de données pour chaque nœud vidéo majeur. La somme représente l'exigence minimale de débit de données pour un lien spécifique quelconque. Cette valeur ne doit pas consommer plus de 75 % du débit de données total disponible sur cette liaison. Cette règle des 75 % suppose qu'une partie du débit de données est nécessaire pour le trafic à surdébit. Des exemples de trafic à surdébit comportent les mises à jour du protocole de routage et l'entretien, ainsi que des applications supplémentaires telles que la gestion et le trafic de configuration VSS.

5.3.2.3 Performance de transfert en flux continu et gestion de flux

L'une des exigences essentielles pour le déploiement de la vidéo IP est l'aptitude à offrir un service de qualité équivalent au VSS analogique sur coaxial existant, en tant que moyen pour débit vidéo et une qualité très supérieurs. La qualité vidéo perçue est très sensible à trois critères de performance essentiels dans un réseau par paquets numérique, en particulier le retard, la perte de paquets, le débit binaire pouvant être atteint (influant sur le niveau de compression et les artefacts, la résolution et la vitesse de trame). Par sa nature, IP fournit un service au mieux et ne donne aucune garantie concernant les critères essentiels énumérés ci-dessus.

5.3.3 Disponibilité

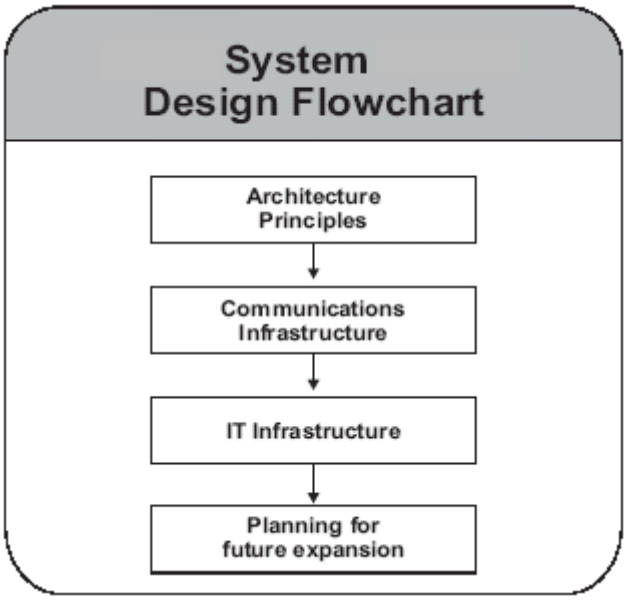
La disponibilité requise peut être obtenue dans un réseau vidéo IP en utilisant des matériels et réseaux redondants, équilibrés en charge et partagés. Il est nécessaire que la connexion

d'un codeur vidéo, de la passerelle d'accès, de la passerelle de jonction et de l'enregistreur vidéo réseau soit insensible aux défaillances. Les types de fonctionnalité souvent utilisés pour obtenir une insensibilité aux défaillances comportent:

– des circuits redondants
– des connexions de réseaux redondants
– une redondance N+n
– la possibilité de remplacement à chaud
– la capacité de basculement pour tous les composants
– la capacité de basculement N+1 pour un composant parmi N composants identiques
– aucun point de défaillance isolé, à l'exception des caméras et du codage
– des dispositifs vidéo source à deux ports réseau tels que des caméras ou des codeurs IP
– une configuration, un logiciel et un micrologiciel pouvant être modifiés et mis à jour sans perte de service.

D'autres aménagements de protection du trafic du réseau tels que RSTP selon IEEE 802.1w doivent fournir une convergence d'arbre maximal après une modification de topologie ou une défaillance du réseau en moins de 1 seconde. Le STP (Protocole d'arbre maximal) doit répondre dans un délai de 30 s à 50 s.

5.4 Principes supplémentaires d'architecture



IEC 2575/13

Légende

Anglais	Français
System Design Flowchart	Organigramme de conception du système
Architecture Principles	Principes de l'architecture
Communications Infrastructure	Infrastructure de communication
IT Infrastructure	Infrastructure IT
Planning for future expansion	Prévision pour extension future

Figure 3 – Conception du système

L'architecture doit être basée sur les principes suivants:

1) composants fonctionnels du système séparés afin d'assurer fiabilité et redondance

2) garantie d'un environnement contrôlé pour la fiabilité des dispositifs et le confort des opérateurs
3) compréhension des paramètres de conception en fonctionnement normal et lors d'une deuxième étape dans des situations d'alarme ou de pointe, lorsque les temps de réponse des événements sont plus importants que prévu. Lorsque la taille de l'installation VSS augmente, les charges de pointe tendent vers une moyenne par rapport au temps et aux sites
4) autres principes (voir Figure 3)

5.5 Conception d'un réseau

5.5.1 Petit réseau monodiffusion

La Figure 4 ci-dessous représente un LAN avec trois stations de travail de vidéosurveillance A, B et C, un serveur vidéo D, une imprimante réseau E et un routeur F. Ce réseau est utilisé pour prendre en charge un petit système de surveillance avec jusqu'à 30 canaux vidéo IP.

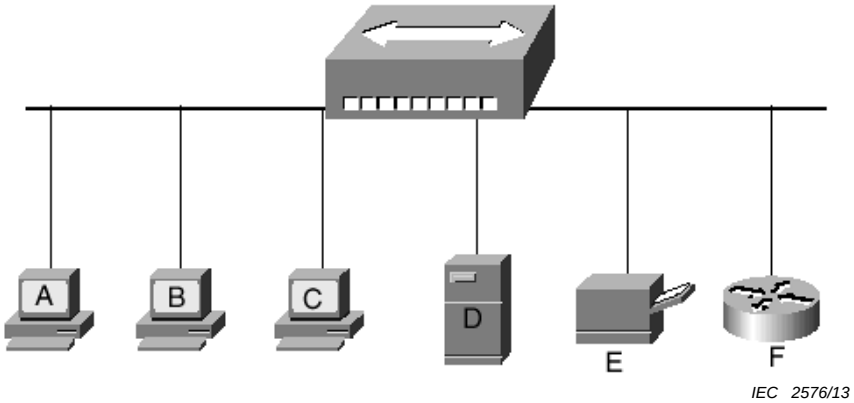
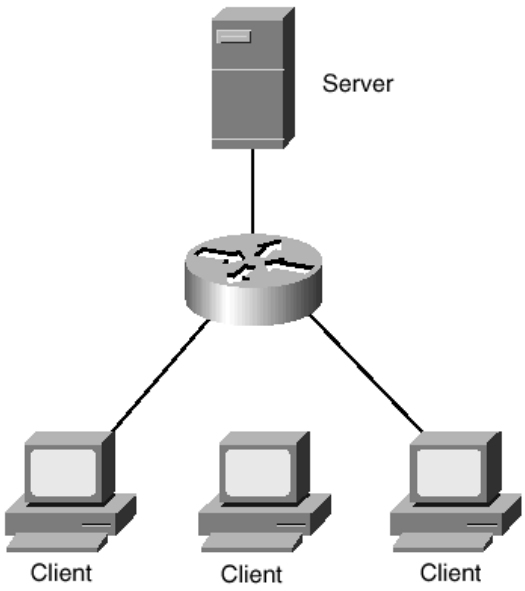


Figure 4 – Petit réseau

5.5.2 Petit réseau vidéo multidiffusion

La Figure 5 ci-dessous représente un LAN avec trois stations de travail fixes, un serveur vidéo, un commutateur de réseau multidiffusion et plus de 30 caméras. Ce réseau est utilisé pour prendre en charge un petit système de surveillance multidiffusion avec plus de 30 canaux vidéo IP et plusieurs opérateurs et clients surveillant les mêmes sources vidéo la majeure partie du temps.



Légende

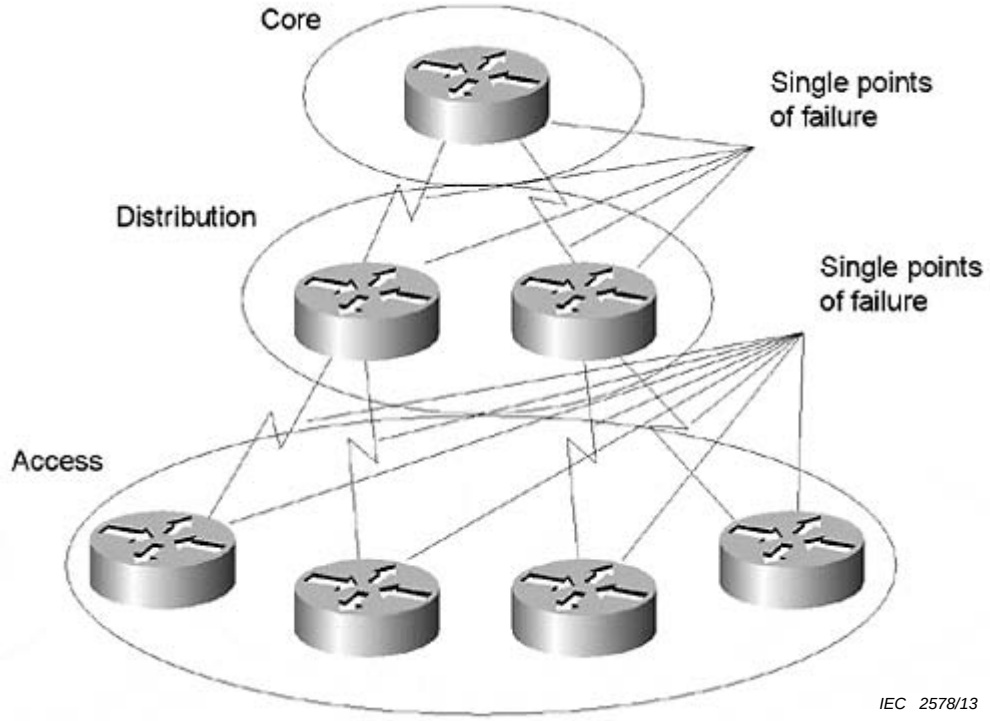
Anglais	Français
Server	Serveur
Client	Client

Figure 5 – Réseau multidiffusion

5.5.3 Réseau VSS hiérarchique

Une conception de réseau hiérarchique comporte les trois couches suivantes de la Figure 6:

- la couche squelette ou couche intérieure assurant un transport optimum entre sites ou fonctionnalité du système, par exemple, enregistrement
- la couche distribution assurant la connectivité
- la couche d'accès local reliant les dispositifs de vidéotransmission dans le réseau et fournissant l'accès à l'opérateur



Légende

Anglais	Français
Core	Couche intérieure
Distribution	Distribution
Access	Accès
Single points of failure	Points de défaillance uniques

Figure 6 – Réseau hiérarchique

Les réseaux vidéo IP de plus grande taille doivent être basés sur le modèle de réseau hiérarchique. Ce modèle divise un réseau en trois couches: les couches intérieure, distribution et d'accès.

La couche d'accès est responsable de la connexion des dispositifs au réseau. Ces caractéristiques par définition ont généralement une grande densité de ports et/ou l'aptitude à prendre en charge le dispositif physique périphérique ou les défis «dernier kilomètre».

La couche distribution est la couche où sont appliquées les politiques. C'est dans celle-ci que doivent être prises les décisions de listes d'accès et de routage intensif pour le CPU (par opposition à une simple route par défaut ou passerelle par défaut). La conception de la couche distribution est basée sur la concentration des dispositifs d'accès en composants avec des ressources de traitement importantes de façon à pouvoir appliquer les règles définies.

La couche intérieure constitue le «squelette» du réseau. Son travail consiste simplement à déplacer de grandes quantités de paquets de flux vidéo provenant de sources vidéo multiples A vers un récepteur vidéo B, aussi rapidement que possible et avec le moins de manipulations possibles.

Les couches intérieure et distribution sont simplement séparées en différents commutateurs dans les grands réseaux. Dans les environnements vidéo IP plus petits, très souvent un commutateur exécute à la fois les tâches de la couche intérieure et de la couche distribution.

5.5.4 Planification de la capacité d'un réseau vidéo IP effectif

Les ingénieurs, les consultants et les administrateurs de réseau IP vidéo caractérisent la capacité d'un réseau par la quantité de trafic que le réseau peut traiter par conception. L'explication de la capacité d'un réseau dans les systèmes vidéo IP devient davantage une mesure du nombre de flux vidéo simultanés que le réseau peut traiter. Ce concept de «**charge de pointe**», volume de flux vidéo maximum supposé que le réseau doit être capable de traiter, constituera la base du processus de planification de capacité. Pendant la **planification de capacité**, on doit considérer ce qui suit:

- le nombre de codeurs/caméras sur le réseau
- les codecs vidéo et leur performance dans la solution VSS
- l'existence d'un trafic de données sur le réseau
- l'enregistrement décentralisé ou centralisé et l'analyse du contenu vidéo
- la connectivité avec la mémoire réseau, les enregistreurs vidéo, les détecteurs de mouvement vidéo
- le nombre de flux prévus des codeurs et le nombre de clients que chacun prend en charge
- le nombre d'utilisateurs et de clients opérateurs vidéo dans le réseau
- la conception d'un réseau local (LAN) et/ou d'un réseau étendu (WAN) existants
- l'infrastructure matérielle du réseau existant et sélectionné
- la redondance du réseau
- le débit en réserve disponible dans le réseau

5.5.5 Interconnexions sans fil

Lorsqu'on utilise des interconnexions sans fil, les facteurs ci-dessous doivent être considérés:

1) emplacement des antennes pour garantir une communication fiable avec les autres composants du système;
2) possibilité pour que d'autres matériels RF interfèrent avec le matériel d'interconnexion du VSS;
3) proximité de grands objets métalliques par rapport à l'antenne de l'installation;
4) possibilité d'intrus qui interfèrent avec l'interconnexion ou la bloquent.

5.6 Remplacement et redondance

5.6.1 Conception d'un réseau redondant

La redondance fournit d'autres routes autour de points de défaillance uniques (SPOF).

La conception de réseaux redondants tente de satisfaire aux exigences de disponibilité des réseaux en dupliquant les liaisons de réseau et les dispositifs d'interconnectivité. La redondance élimine la possibilité d'avoir un point de défaillance unique sur le réseau. Le but est de dupliquer tout composant requis dont la défaillance pourrait désactiver des applications critiques. Le composant peut être un commutateur matriciel vidéo analogique, un routeur intérieur, une caméra, un codeur ou un décodeur vidéo, une alimentation, une ligne de jonction de réseau, un magnétoscope numérique et ainsi de suite.

Etant donné que la redondance est coûteuse à déployer et à maintenir, il convient que les topologies redondantes ne soient mises en œuvre qu'en cas de nécessité. Un niveau de redondance ne doit être sélectionné que conformément aux exigences de fonctionnement concernant la fiabilité et la faisabilité. La redondance ajoute de la complexité à la topologie du réseau. La redondance pour les caméras peut être traitée par une caméra PTZ (Panoramique/inclinaison/zoom) capable de naviguer sur la scène de plusieurs caméras statiques ou par le positionnement de caméras, lorsque le champ de vision d'une caméra fait partie de la caméra suivante avec un niveau de qualité moindre.

Un point de défaillance unique est un dispositif, une interface sur un dispositif ou une liaison quelconque, pouvant empêcher le VSS d'effectuer une certaine tâche de surveillance s'il tombe en panne. Les réseaux qui suivent un modèle hiérarchique puissant ont tendance à comporter un grand nombre de points de défaillance uniques en raison de l'importance accordée aux points de récapitulation et aux points d'entrée entre les couches du réseau. Dans un réseau hiérarchique strict par exemple, tel que celui qui est représenté sur la Figure 6, chaque dispositif et chaque liaison est un point de défaillance unique.

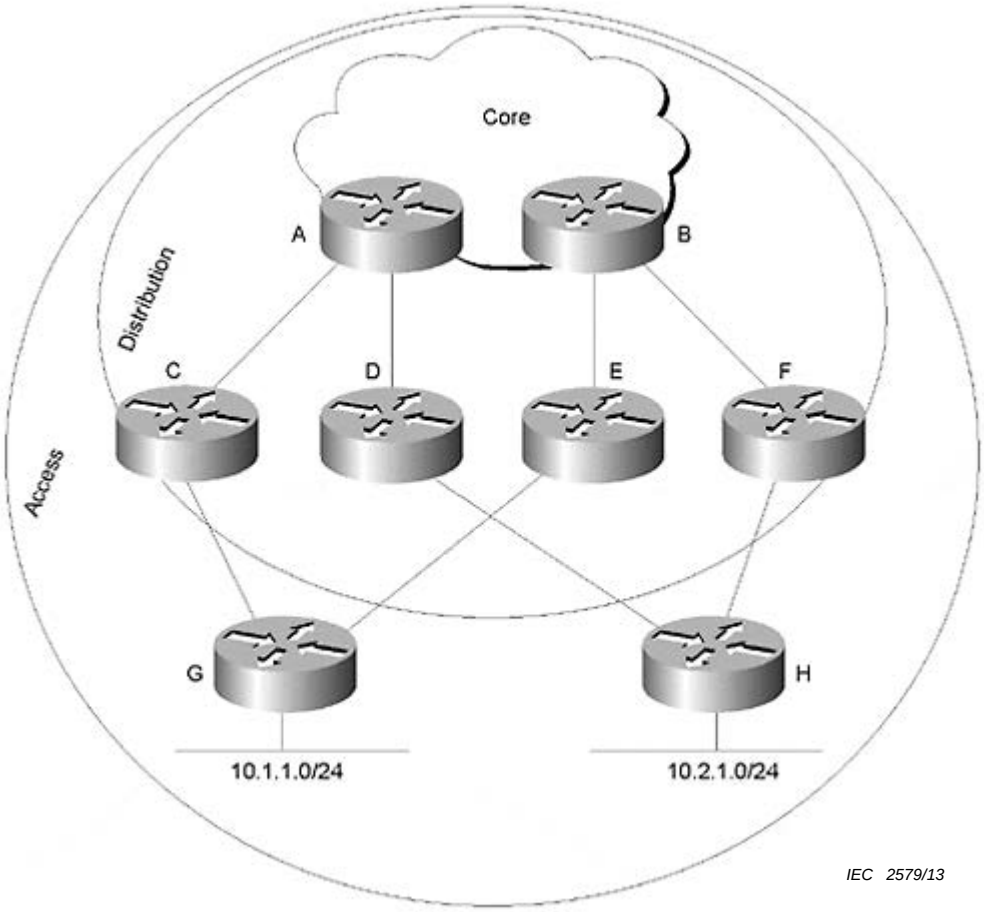
Il existe différentes conceptions pour assurer la redondance dans la **couche intérieure**. Si la totalité du réseau intérieur se trouve dans un bâtiment ou sur un petit site protégé, chaque routeur est connecté à deux LAN à grande vitesse, routeurs A et B à la Figure 7.

Si les routeurs intérieurs ne se trouvent pas tous dans un bâtiment ou dans un site protégé, les options deviennent plus limitées.

Les deux méthodes les plus courantes pour assurer la redondance au niveau de la **couche distribution** sont le double attachement et les liaisons de secours vers d'autres routeurs de la couche distribution.

Les dispositifs de la **couche d'accès** à double attachement constituent la façon la plus courante d'assurer la redondance vers des emplacements distants dans un site protégé mais il est également possible d'interconnecter des dispositifs de la couche d'accès pour assurer la redondance.

Sur la Figure 7, le Routeur G et le Routeur H sont des routeurs de la couche d'accès à double attachement avec le circuit de secours connecté à différentes branches de la couche distribution.



Légende

Anglais	Français
Core	Couche intérieure
Distribution	Distribution
Access	Accès

Figure 7 – Réseau redondant

5.6.2 Disponibilité

Les exigences de fonctionnement (OR) requièrent manifestement un niveau de disponibilité du réseau vidéo.

La moyenne des temps de bon fonctionnement (MTBF) des composants doit être considérée lors de la conception du réseau, ainsi que le délai moyen de réparation (MTTR). La conception d'une redondance logique dans le réseau est aussi importante qu'une redondance physique. L'ensemble VSS doit avoir une MTBF minimale de 16 000 h en se basant sur la CEI/TR 62380, la CEI 61709, et l'IEEE 1413.1-2002.

5.7 Enregistrement réseau centralisé et décentralisé et analytique du contenu vidéo

Un réseau VSS peut inclure toutes les variantes possibles d'enregistrement centralisé et d'analytique de contenu vidéo (VCA) ou d'enregistrement décentralisé et de VCA à l'emplacement de la caméra.

Un grand nombre de facteurs influent sur la décision d'enregistrement centralisé ou décentralisé et de VCA. Si, par exemple, le réseau couvre plusieurs bâtiments, l'enregistrement doit être situé dans chaque bâtiment. Cependant, une consultation et une évaluation centrales des données vidéo enregistrées sont plus faciles dans un environnement d'enregistrement centralisé. Un enregistrement centralisé est réalisé lorsque les dispositifs de stockage sont connectés au commutateur intérieur, il en est de même pour le VCA centralisé. L'ensemble du réseau doit être capable de transporter les données vidéo enregistrées ou les flux à analyser.

Un enregistrement ou un VCA décentralisé est réalisé lorsque les dispositifs de stockage ou de VCA sont connectés au commutateur de la couche d'accès. Le réseau est segmenté en «zones de trafic». Les données vidéo enregistrées ou analysées restent dans les sous-réseaux et n'inondent pas le réseau. Si un enregistrement ou un VCA décentralisé est réalisé, les commutateurs d'accès doivent être conçus pour le trafic attendu.

Du point de vue de l'IT, la solution centralisée sera toujours préférée. Une solution centralisée est plus facile à gérer, à sauvegarder et plus facile à dimensionner. De plus, tous les logiciels et matériels de gestion sont concentrés, par exemple dans le centre de contrôle ou dans une partie du bâtiment. «En périphérie» on ne trouve que des caméras et décodeurs. L'inconvénient de l'enregistrement ou VCA centralisé est qu'il nécessite des commutateurs centraux très puissants (et coûteux). Un autre inconvénient est que les solutions de redémarrage après défaillance sont complexes. Si le commutateur central présente une défaillance, l'ensemble du système s'arrête de fonctionner lorsqu'il n'y a pas de basculement. La solution décentralisée offre une meilleure stabilité. Lorsqu'un commutateur ou un segment de réseau présente une défaillance, l'enregistrement et le VCA dans les autres segments ne sont pas affectés. L'extensibilité de l'enregistrement décentralisé est limitée. Lorsqu'on ajoute de nouvelles caméras à tous les segments du réseau, il se peut que les mémoires du segment soient trop petites et doivent être remplacées. Dans une solution centralisée, il suffit de remplacer ou d'agrandir le dispositif de mémoire centrale. Un enregistrement direct sur un NVR (Enregistreur vidéo réseau) ou une mémoire attachée au réseau (NAS) est entièrement indépendant des commutateurs. Tant que le codeur et le dispositif mémoire sont actifs et fonctionnent, l'enregistrement se poursuit. Par conséquent un certain nombre de petits dispositifs mémoire sont toutefois nécessaires, pouvant être beaucoup plus coûteux qu'un grand dispositif mémoire.

Un inconvénient du VCA centralisé est que l'analyse est effectuée sur le flux vidéo transmis, qui est compressé avec la résolution et la vitesse de trames données, ce qui inclut des artefacts.

6 Exigences générales IP

6.1 Généralités

Le but du présent article est de spécifier les exigences et les protocoles de base du réseau, avec une préférence pour les normes existantes bien connues et bien acceptées. Cette spécification d'interface est rédigée pour fournir l'ensemble d'exigences minimum pour le transfert vidéo en flux continu et les protocoles support entre serveurs de VTD (Dispositif de vidéotransmission) et clients. Dans l'ensemble, le réseau IP doit prendre en charge les DNS, IPv4, DHCP, TTL et IPv6, de manière facultative.

6.2 IP – Couche ISO 3

Toutes les entités d'un dispositif de vidéotransmission doivent être capables de mettre en œuvre l'IP (Protocole Internet) en tant que protocole de couche 3. Pour garantir l'interopérabilité avec les réseaux TCP/IP existants, les entités doivent mettre en œuvre l'IPv4, comme défini dans la RFC 791. La prise en charge de l'IPv6 comme défini dans la RFC 2460 est facultative.

NOTE Dans le restant de ce texte, toutes les références à l'IP («IP» seul) sont interprétées comme IPv4.

6.3 Adressage

Le fondement de la mise en réseau est l'adressage IP. Chaque VTD doit comporter un protocole de configuration du serveur dynamique (DHCP) client et rechercher un serveur de DHCP lorsque le dispositif est connecté au réseau pour la première fois. Si aucun serveur de DHCP n'est disponible, dans un réseau dit non géré, le dispositif doit s'affecter lui-même une adresse. Si, au cours de la transaction de DHCP, le dispositif reçoit un nom de domaine, par exemple par l'intermédiaire d'un serveur DNS (Système de noms de domaine) ou par l'intermédiaire d'un acheminement de DNS, il convient que le dispositif utilise ce nom dans les opérations suivantes du réseau; sinon, il convient que le dispositif utilise son adresse IP.

Le présent article définit les exigences de conformité de la configuration IP par rapport à la CEI 62676-1-2 sur les VTD. Les exigences principales sont énumérées ci-dessous.

Configuration IP

Le dispositif de vidéotransmission doit avoir au moins une interface réseau assurant la connectivité IP avec le réseau et permettant un échange de vidéo et de données entre des dispositifs de vidéotransmission, par exemple entre un serveur et une vidéotransmission client.

Il doit être possible de réaliser une configuration IP statique sur le dispositif de vidéotransmission en utilisant une interface de configuration réseau ou locale.

Adressage IPv4

Il convient que le dispositif de vidéotransmission prenne en charge la configuration IP dynamique d'une adresse de liaison locale conformément à la RFC 3927.

Le dispositif de vidéotransmission peut prendre en charge tout mécanisme supplémentaire de configuration IP.

Adressage IPv6

Un dispositif de vidéotransmission prenant en charge IPv6 doit prendre en charge une configuration IP sans état conformément à la RFC 4862 ou doit prendre en charge une configuration IP dynamique conformément à la RFC 3315 ou les deux.

DHCP (Protocole de configuration de serveur dynamique)

Le dispositif de vidéotransmission doit prendre en charge une configuration IP dynamique conformément à la RFC 2131.

La méthode d'assignation préférentielle d'une adresse IP sur une entité s'effectue par l'intermédiaire du DHCP selon la RFC 2131. Chaque nœud prenant en charge cette couche doit posséder une fonction pour obtenir les informations de détermination d'adresse en utilisant un serveur de DHCP. Pour le fonctionnement, il est fortement recommandé de déployer un serveur de DHCP dans un réseau vidéo IP.

La présente norme ne spécifie aucune méthode de détermination d'adresse IP dynamique autre que le DHCP.

6.4 Protocole de message de commande Internet (ICMP)

6.4.1 Généralités

Des messages ICMP sont envoyés dans plusieurs situations: par exemple, lorsqu'un datagramme ne peut pas atteindre sa destination, lorsque la passerelle n'a pas la capacité de

mise en mémoire tampon pour acheminer un datagramme et lorsque la passerelle peut diriger l'hôte pour envoyer le trafic sur une route plus courte.

6.4.2 Exigences de diagnostic

Pour faciliter le dépannage, les entités du système doivent mettre en œuvre la commande «PING» selon l'ICMP (RFC 792). Selon la RFC 1122, tout hôte doit accepter une demande d'écho et fournir en retour une réponse d'écho.

Tout hôte réseau doit être capable d'envoyer des paquets de «demandes d'écho» ICMP (Protocole de message de commande Internet) à la cible de vidéotransmission et d'écouter les retours de «réponse d'écho» ICMP. Ceci fournit une capacité de diagnostic précieuse.

Tous les clients de vidéotransmission doivent être conformes à la RFC 1122 de sorte que tout hôte doit accepter une demande d'écho et fournir en retour une réponse d'écho.

Selon la demande/réponse d'écho de la RFC 792, chaque hôte doit mettre en œuvre une fonction de serveur d'écho ICMP (Protocole de message de commande Internet) qui reçoit des demandes d'écho et envoie les réponses d'écho correspondantes. Une demande d'écho ICMP destinée à une adresse de diffusion IP ou de multidiffusion IP doit être éliminée en silence.

L'adresse source IP dans une réponse d'écho ICMP doit être la même que l'adresse de destination spécifique du message de demande d'écho ICMP correspondant. Les données reçues dans une demande d'écho ICMP doivent être entièrement incluses dans la réponse d'écho résultante.

6.5 Diagnostics

Pour effectuer un diagnostic et une maintenance plus faciles du réseau de vidéotransmission et de ses dispositifs, il convient que le VTD signale l'état de la connexion réseau de base par l'intermédiaire de voyants tels que des DEL (Diodes électroluminescentes) à proximité du connecteur de réseau, dont il convient qu'ils indiquent l'état de fonctionnement et les indications de défaillances et de dysfonctionnements possibles:

Si aucune autre spécification n'est fournie pour un VTD, il convient que les couleurs suivantes des voyants représentent l'état de connexion du réseau énuméré: il convient qu'un voyant vert allumé signale l'état d'une connexion de réseau à 10 Mb, un voyant vert et orange pour 100 Mb, un voyant orange pour 1 Gb. Il convient qu'un clignotement du ou des voyants chaque seconde représente une transmission de données en cours. Si aucune connexion ne peut être établie, il convient de ne pas allumer le ou les voyants. Il convient qu'un voyant rouge allumé signale le processus de démarrage d'un VTD. Durant une mise à jour de micrologiciel, il convient que le voyant clignote rapidement en rouge. Il convient qu'un clignotement rouge chaque seconde signale une défaillance ou un défaut du VTD tel qu'une alimentation coupée, des ventilateurs coupés, une configuration ou un micrologiciel corrompus.

6.6 Multidiffusion IP

6.6.1 Généralités

Si un VTD prend en charge la multidiffusion, il doit alors fonctionner conformément à la RFC 1112. Si un VTD ne prend pas en charge la multidiffusion conformément à la présente norme, il doit être clairement spécifié que le «VTD ne prend pas en charge la multidiffusion». Tous les dispositifs multidiffusion doivent prendre en charge les extensions de multidiffusion spécifique à la source (SSM) selon la RFC 4607. L'utilisation d'une multidiffusion toute source (lorsque l'adresse IP source n'est pas spécifiée) n'est pas recommandée. Pour une multidiffusion spécifique à la source, la configuration d'adressage doit satisfaire à la RFC 4607 (plage 232/8).

6.6.2 Exigences du Protocole Internet de gestion de groupe (IGMP)

6.6.2.1 Généralités

Il convient que les VTD soient capables de générer des messages IGMP pour rejoindre/quitter un groupe de multidiffusion. Il convient que la version minimale d'IGMP mise en œuvre soit la version 3 conformément à la RFC 3376.

6.6.2.2 Surveillance de réseau IGMP

Les dispositifs de couche 2 (c'est-à-dire, les commutateurs de réseau) doivent être capables de prendre en charge la «surveillance de réseau IGMP» selon la RFC 4541 et ne doivent pas inonder un trafic multidiffusion sans discrimination parmi toutes leurs interfaces en cas de disponibilité d'un interrogateur IGMP (Protocole Internet de gestion de groupe).

7 Exigences sur le transfert vidéo en flux continu

7.1 Généralités

Il existe actuellement un grand nombre de mises en œuvre incompatibles de transfert vidéo en flux continu et de contrôle de flux, bien que des normes soient utilisées. Dans le présent article, des exigences générales pour l'application des normes existantes au transfert vidéo en flux continu sont présentées.

L'article suivant contient les exigences concernant l'utilisation du transport de flux vidéo dans les VTD. Les exigences sont organisées dans un paragraphe qui couvre les exigences communes à tous les transports vidéo et des paragraphes qui couvrent les exigences pour des protocoles de transports vidéo spécifiques, par exemple RTP (Protocole de transmission en temps réel) et d'autres.

Les clients et serveurs de vidéotransmission doivent prendre en charge une interface réseau IP pour le transport du contrôle de session et des données vidéo.

Les données de contrôle et les données vidéo doivent être envoyées en utilisant TCP/IP selon la STD 7 RFC 793 et/ou UDP/IP selon la STD 6 RFC 768. Une vue d'ensemble de la pile de protocoles se trouve à la Figure 2 de la présente norme.

7.2 Protocole de transport

7.2.1 Généralités

Les dispositifs de vidéotransmission doivent prendre en charge UDP (Protocole datagramme d'utilisateur) et/ou TCP (Protocole de commande de transmission).

NOTE La série CEI 62676-2 définit un protocole, la façon dont une demande du VTD circule dans le mode sélectionné UDP ou TCP.

Le transport vidéo nécessite un comportement en temps réel, fourni dans les réseaux IP par les protocoles de transmission en temps réel (RTP). Le protocole RTP prévoit une prise en charge du réordonnancement, de la suppression de la gigue et de la synchronisation des supports. Tous les flux de support transférés par le protocole RTP doivent être conformes aux RFC 3550, RFC 3551, RFC 3984, RFC 3016 et JPEG sur RTP conformément à la série CEI 62676-2.

Le profil RTP/UDP est l'option la plus simple et la plus largement prise en charge dans les systèmes de transfert vidéo en flux continu actuels. Un dispositif de VT (Vidéotransmission) doit prendre en charge le protocole RTP/UDP et il convient par ailleurs qu'il prenne en charge la multidiffusion RTP/UDP. Le protocole RTP via le TCP constitue un autre moyen de transport des supports et un VTD peut prendre en charge cette option conformément à la

norme RFC 4571. RTSP/RTP sur TCP fournit l'option de transport fiable. De plus, RTSP/RTP sur TCP permet la traversée de traducteurs et pare-feu d'adresse réseau.

Le protocole de contrôle RTP (RTCP) fournit un retour d'information sur la performance de transfert en flux continu assurée par le protocole RTP et la synchronisation de différents flux de supports. Le protocole RTCP doit être conforme à la norme RFC 3550.

Tous les dispositifs et clients doivent prendre en charge le RTSP conformément à la norme RFC 2326 pour l'initiation de session et la commande de lecture. Le RTSP doit utiliser le protocole TCP comme protocole de transport, et le port TCP par défaut pour le trafic RTSP est 554. Le protocole de description de session (SDP) doit servir à fournir des informations sur les flux de support et doit être conforme à la norme RFC 4566.

7.2.2 JPEG sur RTP

JPEG sur RTP doit être fondamentalement conforme à la RFC 2435. Cette mise en œuvre ne prend en charge que les tables de Huffman par défaut, le rapport d'aspect est limité à 1:1 et 1:2 et la taille d'image est limitée à 2 040 x 2 040 pixels en raison du champ de bits limité de l'en-tête RTP/JPEG.

Pour les images JPEG ayant d'autres rapports d'aspect, par exemple PAL ou NTSC et pour les capteurs d'image de 4 mégapixels et plus, un en-tête d'extension RTP doit être inclus après l'en-tête normalisé d'origine selon la RFC 3550. L'extension d'en-tête doit être ignorée par les VTD ne prenant pas en charge ces caractéristiques. Sur des récepteurs de VTD incompatibles, ceci peut avoir pour effet que le flux est décodé mais présente par exemple le mauvais rapport d'aspect.

7.2.3 JPEG sur HTTP

Si un VTP prend en charge JPEG sur HTTP, il doit être conforme à la RFC 2453.

Le transfert en flux continu HTTP (Protocole de transfert hypertexte) sépare chaque image en réponses HTTP individuelles. Le transfert en flux continu RTP crée des paquets d'une séquence d'images JPEG pouvant être reçus par les clients de VTD. Un type MIME (Extensions de courrier Internet à fonctions multiples) spécial «multipart/x-mixed-replace;boundary=» doit signaler au VTD de recevoir plusieurs parties comme réponse, séparées par une limite spéciale, qui est définie par le type MIME. La connexion TCP (Protocole de commande de transmission) est active tant que le récepteur du VTD demande de nouvelles trames et que le serveur du VTD fournit des trames.

7.3 Documentation et spécification

7.3.1 Généralités

La spécification du VTD et de son interface de transfert vidéo en flux continu doit indiquer le nombre de clients et/ou de serveurs de VTD capables d'être connectés pour un transfert vidéo en flux continu en direct et/ou en relecture. Si nécessaire, la vitesse de trame et la qualité du flux vidéo doivent également être spécifiées.

La présente norme définit le protocole RTP Payload Formats For interoperability purposes (Formats de charge utile à des fins d'interopérabilité), l'ensemble admis d'options de transfert en flux continu de supports et les formats pour les données vidéo, audio et les métadonnées basées sur le protocole RTP.

Au moins une des spécifications de transfert vidéo en flux continu suivantes doit être prise en charge pour des raisons de compatibilité:

- JPEG sur RTP
- MPEG-4 conformément à l'ISO/CEI 14496-2

- H.264 conformément à l'ISO/CEI 14496-10

et les codecs audio suivants:

- G.711 conformément à l'UIT-T G.711
- G.726 conformément à l'UIT-T G.726
- AAC conformément à l'ISO/CEI 14496-3

7.3.2 Formats de charge utile non conformes, propriétaires et spécifiques au fournisseur

En plus des charges utiles conformes énumérées, les VTD peuvent prendre en charge des formats de charge utile RTP non conformes ou propriétaires. Celles-ci sont utilisées lorsque le format vidéo en temps réel est propriétaire et n'est pas destiné à faire partie d'un quelconque système normalisé. Ces formats propriétaires doivent toutefois être correctement documentés et enregistrés, en raison de

– l'utilisation dans des environnements normalisés tels que SDP (Protocole de description de session). Il est nécessaire que RTP soit configuré en considérant les profils RTP utilisés, les formats de charge utile et leurs types de charge utile. Pour ce faire, il existe un besoin de noms enregistrés garantissant que les noms ne sont pas en conflit avec d'autres formats.
– l'intégration de dispositifs vidéo de tierces parties: les formats de charge utile RTP sont utilisés pour prendre en charge des formats propriétaires. Une spécification écrite du format économisera du temps et de l'argent pour les deux parties collaborant entre elles: l'interopérabilité est beaucoup plus facile à obtenir.
– la garantie de l'interopérabilité entre différentes mises en œuvre sur différentes plates-formes.

Pour éviter des collisions de noms, un registre central conserve la trace des noms des types de supports enregistrés utilisés par différents formats de charge utile RTP. Lorsque des formats propriétaires arrivent, ceux-ci doivent être enregistrés dans le stockeur du fournisseur. Tous les enregistrements spécifiques à un fournisseur utilisent des noms de sous-types qui commencent par «vnd.<vendor- name>». Il n'est pas requis d'enregistrer à l'IANA (Internet Assigned Numbers Authority (Autorité chargée de l'assignation des numéros Internet)) tous les noms qui utilisent des noms se trouvant dans les stockeurs du fournisseur. L'enregistrement est toutefois recommandé s'il est utilisé dans des environnements publics.

Les nouveaux types de supports de charge utile RTP peuvent être enregistrés dans l'arborescence de normes par d'autres entités normatives. Les exigences relatives à l'organisation sont soulignées dans le document d'enregistrement de type de support (RFC 4855 et RFC 4288). Cet enregistrement nécessite une demande à l'IESG (Internet Engineering Steering Group (Groupe directeur sur l'ingénierie Internet)), qui garantit que le modèle d'enregistrement est acceptable.

L'enregistrement du nom de la charge utile RTP est requis pour éviter une collision de noms dans le futur. On peut trouver la liste de tous les types de supports déjà enregistrés à l'IANA (http://www.iana.org/assignments/media-types/video).

Les extensions spécifiques à un fournisseur doivent utiliser la gamme de types de charge utile 77 à 95, qui est marquée comme «non assignée».

7.3.3 Réception de formats de charge utile RTP non pris en charge

Un format de charge utile RTP pour un codec est un ensemble de règles qui définissent la façon dont les trames vidéo du codec sont mises dans des paquets RTP. Ceci est habituellement défini par un IETF RFC (ou pour les formats de charge utile plus récents, un IETF Internet-Draft).

Par défaut, le client du VTD ignore toute sous-session dont il ne comprend pas le format de charge utile RTP (car s'il ne connaît pas le format de charge utile RTP, il ne sait pas comment extraire les données du flux RTP entrant).

Le client du VTD ne doit pas être influencé négativement par des flux vidéo incompatibles avec des codecs ou des formats vidéo inconnus ou corrompus.

Les extensions spécifiques à un fournisseur doivent utiliser la gamme de types de charge utile 77 à 95, qui est marquée comme «non assignée».

7.4 Transfert en flux continu de métadonnées

7.4.1 Généralités

Dans les réseaux de vidéosurveillance, il est nécessaire de transporter des données supplémentaires, en plus du flux vidéo, appelées métadonnées. ATM/POS-, VCA-, GPS-, Geolocation, Number Plates, Access Control Cardholder IDs sont certains des types de métadonnées les plus courants. Il existe généralement trois alternatives pour transporter des actifs de métadonnées avec le contenu vidéo réel:

– multiplexage: transfert en flux continu combiné contenant de la vidéo et des métadonnées (non recommandé);
– flux séparés de métadonnées et de données vidéo;
– flux de métadonnées multiples (un pour chaque type de métadonnées) et un flux de données vidéo.

Le transfert en flux continu combiné/multiplexé présente plusieurs inconvénients, car l'approche de flux combiné dépend du format de charge utile spécifique, fournissant la section d'en-tête auxiliaire où peuvent être transportées les métadonnées. Certains formats de charge utile RTP, par exemple pour les flux élémentaires MPEG-4 (RFC 3640), mais d'autres formats de charge utile utilisés en vidéosurveillance ne fournissent pas la section «auxiliary». Ceci est contraire aux exigences d'interopérabilité. Outre l'économie de surdébit de traitement en ne traitant qu'un seul flux, un certain surdébit est apporté en raison du (dé)multiplexage de la vidéo et des métadonnées.

Les utilisateurs finals s'attendent à ce que les métadonnées soient fournies sans perte d'information ou avec une perte d'information de faible niveau. Un mécanisme basé sur RTP doit donc être utilisé et il est ici spécifié, comment permettre l'arrivée des métadonnées dans le bon ordre et avec détection et indication de perte. Les métadonnées doivent être transmises sur une session RTP séparée dans leur propre format de charge utile.

7.4.2 Documents XML en tant que charge utile

7.4.3 Généralités

Si des formats de données complexes sont à transférer en flux continu sous forme de métadonnées, nécessitant un système très riche de structures de données complexes, les documents XML doivent être transmis sous la forme de charge utile RTP.

Dans une session RTSP, la description SDP pour les métadonnées de type et de sous-type de contenu «application» doit être utilisée comme type de charge utile dynamique.

```
SDP Example:

Client->Server: DESCRIBE rtsp://140.10.2.3/VideoChannel/1/h264 RTSP/1.0
CSeq: 1

Server->Client: RTSP/1.0 200 OK
CSeq: 1
Content-Type: application
```

```
Content-Length: XXX
```

Le flux de métadonnées lui-même est ensuite transporté par RTP.

XML doit être transféré en flux continu directement, un document XML après l'autre, par l'intermédiaire de RTP. Pour la synchronisation avec le flux vidéo, un horodatage RTP doit être utilisé avec le temps d'occurrence. Seuls les horodatages en UTC (Temps universel coordonné) doivent être utilisés dans le flux de métadonnées. Cette charge utile de métadonnées XML pure doit signaler par le nœud racine XML «<?xml version="1.0" encoding="UTF-8"?> et le namespace (espace de nom) xmlns XML utilisé tel que"`http://www.xxx.org/ver10/schema`" ou "urn:yyy-org" qu´un flux de documents XML suit.

NOTE Un schéma de métadonnées XML et namespace pour les applications de vidéosurveillance est défini dans la CEI 62676-2-3.

8 Exigences sur le contrôle de flux vidéo

8.1 Généralités

Il existe actuellement un grand nombre de mises en œuvre incompatibles de transfert vidéo en flux continu et de contrôle de flux, bien que des normes soient utilisées. Dans le présent article, des exigences générales pour l'application des normes existantes au contrôle de flux vidéo sont présentées.

Dans le présent article, l'utilisation du Protocole de transfert en flux continu en temps réel (RTSP) conformément à la RFC 2326 pour les dispositifs de vidéotransmission capables de transfert en flux continu en direct et/ou en lecture est spécifiée.

Le RSTP est un protocole au niveau application pour le contrôle de la fourniture de données avec des propriétés en temps réel. L'utilisation du RTSP pour les VSS est spécifiée.

L'établissement d'une session se réfère à la méthode par laquelle un client de vidéotransmission obtient la description de session initiale. La description de session initiale peut être par exemple un URL sur le contenu.

Un exemple de requête valide d'un client de vidéotransmission est:

```
rtsp://140.10.10.22:554/VideoChannel/1/h264/1/trackID=1
```

8.2 Utilisation de RTSP dans les dispositifs de vidéotransmission

8.2.1 Généralités

Transfert vidéo en flux continu en direct

Le flux en direct est caractérisé comme l'équivalent de la VSS analogique classique. Les flux vidéo réels sont généralement délivrés en mode multidiffusion. Ceci signifie que la présentation est linéaire et qu'il n'y a pas de support pour un fonctionnement en mode spécial tel que la pause, l'avance rapide et équivalent. L'affichage est un flux continu de données et d'événements et non à la demande.

Relecture incluant les modes spéciaux

Le transfert vidéo en flux continu en relecture avec les modes spéciaux est caractérisé comme l'équivalent du transfert vidéo en flux continu en direct, en ajoutant la prise en charge du fonctionnement en mode spécial tel que la pause, le retour, l'avance rapide et équivalent.

Les flux vidéo réels sont donc délivrés en mode monodiffusion seulement. La présentation est également un flux continu d'événements.

8.2.2 Utilisation de RTSP avec multidiffusion

Il est possible de façon facultative d'utiliser le RTSP pour relier des multidiffusions de transfert en flux continu en direct.

NOTE En principe, une multidiffusion ne prend pas en charge le fonctionnement en mode spécial, il ne peut donc pas être utilisé.

De façon spécifique, les pare-feu sont capables de vérifier le port d'entrée utilisé, c'est-à-dire que ceci leur permet d'ouvrir les ports et d'effectuer tout acheminement nécessaire sur les ports. De plus, il peut être utile que le serveur vidéo RTSP puisse compter le nombre de clients vidéo inscrits.

Lorsqu'aucune indication n'est donnée par le RTSP concernant le fait de savoir si le mode de fourniture est monodiffusion ou multidiffusion conformément à la RFC 2326, le flux vidéo par défaut doit être délivré en mode multidiffusion.

Pour tout VTD, le nombre maximum de flux monodiffusion pris en charge doit être spécifié.

8.3 Exigences de suivi des normes RTSP

8.3.1 Généralités

Les exigences RTSP suivantes s'appliquent aux dispositifs de vidéotransmission:

Le dispositif de vidéotransmission doit prendre en charge le Protocole de transfert en flux continu en temps réel (RTSP) conformément à l'IETF RFC 2326: les clients et les serveurs de vidéotransmission RTSP doivent mettre en œuvre toutes les caractéristiques requises pour la mise en œuvre minimale du RTSP décrites à l'Annexe D de la RFC 2326:1998.

8.3.2 Interfaces de transfert en flux continu et de contrôle de vidéo IP de haut niveau

Si d'autres interfaces éventuelles, basées par exemple sur les services Web ou les requêtes HTTP, proposent l'initialisation du transfert en flux continu et la récupération d'un flux vidéo URI (Identificateur uniforme de ressource), ceci doit s'effectuer en plus des méthodes définies dans le présent article. Il doit toujours être possible de se référer à un URI en fonction des exigences du présent article.

Les VTD proposant une interface de haut niveau pour le transfert en flux continu et le contrôle de flux doivent également prendre en charge l'interface de contrôle de flux vidéo minimum présentée dans ce qui suit, y compris leurs exigences minimales:

8.3.3 Méthode RTSP minimum et mise en œuvre de l'en-tête

Le récepteur de transmission vidéo RTSP doit mettre en œuvre les méthodes obligatoires PLAY, OPTIONS, DESCRIBE, SETUP, TEARDOWN dans la direction de l'émetteur vidéo (R->T). Le numéro de port par défaut pour un serveur RTSP de VTD est 554. Tous les clients et serveurs doivent mettre en œuvre toutes les caractéristiques requises pour la mise en œuvre minimale du RTSP décrites à l'Annexe D de la RFC 2326:1998.

8.3.4 Authentification RTSP

La documentation des VTD doit spécifier les méthodes prises en charge pour l'authentification. Un VTD doit prendre en charge l´une des deux méthodes ´basic-´ ou ´digest-authentication´ pour l'interface RTSP et l'interface HTTP. Dans tous les cas, il est nécessaire que l'authentification soit mise en œuvre conformément à la RFC 2617 – HTTP authentication: Basic and Digest Access Authentication. Les serveurs RTSP prenant en charge

l'authentification «HTTP digest» doivent la mettre en œuvre conformément à la RFC 2069. L'authentification digest access est recommandée dans les systèmes de grade de sécurité 3 et 4, en raison de la plus grande sécurité fournie. La gamme de noms d'utilisateurs, comptes et mots de passe valides pour accéder à une session RTSP est configurée dans le VTD.

9 Exigences sur la découverte et la description de dispositif

Tout dispositif de VT doit proposer un moyen pour être détecté dans le réseau et proposer une description concernant ses propriétés et capacités vidéo.

Un VTD est tenu de proposer des protocoles de découverte et description de dispositif dans un réseau vidéo IP. Le VTD doit prendre charge au moins l'une des deux méthodes suivantes: WS-Discovery et/ou Zeroconf.

Dans la présente norme, seule la prise en charge de base de cette fonctionnalité est exigée. De plus, dans la série CEI 62676-2, une mise en œuvre de protocole détaillée est exigée et définie pour ces deux méthodes de découverte et de description de dispositif.

10 Exigences sur la gestion d'événement

Un VTD est tenu de proposer des protocoles pour signaler le bon fonctionnement et les événements associés à la source vidéo. Conformément à la CEI 62676-1-1, un VTD doit signaler une perte de signal vidéo, du bruit dans le signal, un signal trop lumineux, trop sombre et la suppression de la caméra. La notification de mouvement et autre événement d'analyse de contenu vidéo dans l'image vidéo doit être effectuée par le même moyen. Il est généralement nécessaire que ces états soient signalés par l'intermédiaire de l'interface vidéo IP d'une manière définie par des valeurs, attributs ou événements normalisés, pour qu'un client de VTD connaisse exactement l'état détaillé de tout serveur de VTD indépendamment du type de dispositif, du fabricant ou du logiciel d'intégration.

Dans la présente norme, seule la prise en charge de base de cette fonctionnalité de gestion d'événement est exigée. Dans la série CEI 62676-2, des méthodes et des mises en œuvre de protocole détaillé de gestion d'événement sont exigées et définies.

Les exigences supplémentaires suivantes pour la gestion de dispositif s'appliquent si un VTD est utilisé dans un réseau IT (Technologie de l'information) ou dans un environnement de réseau de bureau:

11 Exigences sur la gestion des dispositifs de réseau

11.1 Généralités

Le présent paragraphe concerne les recommandations.

Les deux disciplines des réseaux IT et des réseaux de sécurité convergent de plus en plus. Les utilisateurs finals tels que les administrateurs sont de plus en plus responsables à la fois de l'équipement IT, des dispositifs de sécurité et de leurs réseaux d'interconnexion.

Si un système de surveillance vidéo IP est actionné dans un environnement IT, il vaut mieux proposer des services de gestion pour les dispositifs de vidéotransmission utilisant des protocoles types pour ce type de réseaux. Les réseaux industriels, de bureau ou dans un environnement IT utilisent déjà le Protocole simple de gestion de réseau (SNMP) pour surveiller et gérer leur infrastructure d'information. Ceci permet à l'utilisateur final, par exemple un administrateur de réseau incluant des dispositifs de réseau de bureau et de sécurité, de surveiller par exemple la mise en œuvre et le fonctionnement convenables de l'ensemble du matériel par un moyen unique en un point d'extrémité basé sur un protocole unique:

Il convient par conséquent que les VTD incluent la possibilité de communiquer avec des systèmes de gestion d'entreprise basés sur le Protocole simple de gestion de réseau (SNMP). Il convient que les VTD proposent la possibilité d'intégration dans un système de gestion conforme SNMP fournissant par exemple à un administrateur une vue unique des diverses ressources de transmissions logicielles et matérielles de ce système de réseau vidéo distribué complexe.

Si un VTD est utilisé dans un environnement IT où il est nécessaire de surveiller et de contrôler le bon fonctionnement non seulement du matériel de bureau, mais également du matériel de sécurité, tel que les dispositifs vidéo IP, il convient que le VTD propose une prise en charge du SNMP.

Il convient que le VTD prenne en charge le SNMP conformément aux exigences du présent article.

Une base d'informations de gestion (MIB) est une spécification de Protocole simple de gestion de réseau (SNMP) contenant des définitions d'information de gestion telles que les dispositifs de vidéotransmission et les composants essentiels du réseau puissent être surveillés, configurés et contrôlés à distance. Ils sont aujourd'hui largement utilisés dans les éléments de réseau tels que les routeurs, les imprimantes, les concentrateurs, les commutateurs et les dispositifs de stockage et de plus en plus dans les caméras IP, les DVR (Magnétoscopes numériques), les codeurs et les décodeurs. Il existe en général quatre services de haut niveau pour la gestion des dispositifs de réseau de vidéotransmission:

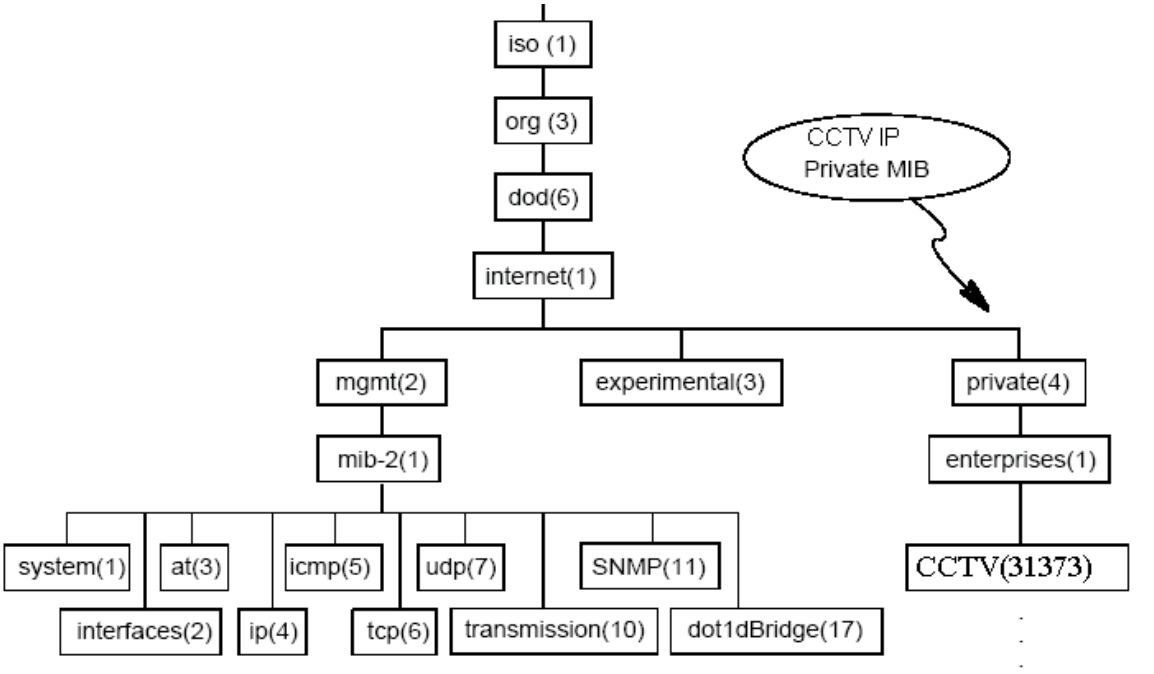
- défauts et défaillances,
- alarmes et événements,
- information d'état et configuration,
- performance

La gestion des défauts et défaillances dans les réseaux de sécurité est basée sur l'analyse des causes profondes impliquant une identification à distance et la correction des problèmes du réseau. La gestion des défauts à distance surveille le bon fonctionnement de la vidéotransmission et de l'infrastructure du réseau, des composants, des sous-systèmes et des interfaces. La configuration et la gestion d'état permettent la mise en service à distance des dispositifs de réseau, interfaces et services. La gestion de performance implique l'analyse des tendances de traitement et des problèmes de réseau de façon à pouvoir entreprendre des actions proactives pour garantir la disponibilité du réseau et enfin la sécurité du site protégé.

11.2 Exemple MIB de vidéo IP

Le présent paragraphe concerne les recommandations.

La Figure 8 suivante représente un schéma de haut niveau de la MIB qui est utilisée pour surveiller les dispositifs de VT. L´organisation de la MIB est définie dans la RFC 1155. Pour les VSS, la MIB 31373 privée est réservée et il convient de l'utiliser.



IEC 2580/13

Légende

Anglais	Français
CCTV IP Private MIB	MIB privée CCTV IP

Figure 8 – Structure MIB

11.3 Agent et gestionnaire SNMP pour les dispositifs de vidéotransmission

Le présent paragraphe est informatif.

La gestion SNMP (Protocole simple de gestion de réseau) est basée sur le modèle agent/gestionnaire décrit dans les normes de gestion de réseau de l'Organisation internationale de normalisation (ISO). Dans ce modèle, un réseau ou un gestionnaire de système échange des informations de surveillance et de contrôle concernant les ressources du système et du réseau avec des composants logiciels distribués, appelés «agents».

Tout système ou ressource de réseau gérable par l'échange d'informations est une ressource gérée. Celle-ci peut être une ressource logicielle telle qu'un enregistreur vidéo réseau basé sur un PC (Ordinateur personnel) ou un magnétoscope numérique ou une ressource matérielle telle qu'une caméra IP, un codeur ou un décodeur vidéo.

Les agents font généralement partie d'une ressource gérée et fonctionnent comme un type de «dispositif de collecte» qui recueille et envoie des données concernant cette ressource gérée comme réponse à une demande d'un gestionnaire SNMP. De plus, il convient que les agents de VTD aient la possibilité de délivrer des rapports non demandés par les gestionnaires lorsqu'ils détectent certains seuils ou conditions prédéfinis sur la ressource gérée tels que des événements de perte vidéo, la détection de mouvement, des problèmes matériels. Dans la terminologie SNMP, ces messages d'événements non demandés sont appelés notifications de piège. Cette notification de piège est un message concernant l'apparition d'un événement ou le franchissement d'un seuil prédéfini, envoyé à un gestionnaire SNMP par un agent de même nature.

Un gestionnaire est basé sur une structure d'informations concernant les propriétés des ressources gérées fournies par les agents. Celui-ci est construit par la Base d'informations de gestion (MIB). Lorsque de nouveaux agents sont ajoutés, par exemple avec le raccordement d'un système de vidéotransmission à un réseau, et doivent être inclus dans la gestion d'un gestionnaire SNMP, le gestionnaire doit comprendre la structure de ce nouveau composant

de la MIB définissant les caractéristiques et les possibilités des ressources. Ces caractéristiques sont à définir dans une MIB conforme SNMP et sont appelées «objets». La définition d'une MIB commune partagée par tous les types différents de dispositifs de vidéotransmission dans un réseau de sécurité fournit, même pour des ressources très hétérogènes d'un système distribué au sein du site protégé, une vue unifiée et une manière unique de gérer les ressources du système et du réseau.

Les dispositifs de réseau tels que les routeurs peuvent envoyer des notifications aux gestionnaires de SNMP lorsque des événements particuliers se produisent. Par exemple, un agent SNMP peut envoyer un message à un gestionnaire SNMP lorsqu'une erreur se produit.

Les notifications SNMP peuvent être envoyées comme des pièges ou des demandes d'informations. Un gestionnaire SNMP qui reçoit une demande d'information acquitte le message avec une PDU (Unité de données de protocole) de réponse SNMP. Les pièges ne sont envoyés qu'une seule fois, tandis qu'une information peut être relancée plusieurs fois.

11.4 Exigences de performance de l'agent SNMP (Protocole simple de gestion de réseau)

Le présent paragraphe est normatif.

Si un VSS utilise le protocole SNMP pour le contrôle de bon fonctionnement et la surveillance des VTD, les exigences de performance suivantes sont importantes pour une communication fiable, et doivent être appliquées: Pour cette raison, tout VTD ou dispositif vidéo IP dans des applications de sécurité doit être conforme à ces exigences, même au-delà de l'interface SNMP définie dans la présente norme incluant des MIB spécifiques au fournisseur.

1) L'agent doit être capable de fournir une SNMP-RESPONSE à un SNMP-GET avec des variables multiples. L'agent doit être capable de répondre à un SNMP-GET avec des OID (Identificateurs d'objet) multiples dans un paquet SNMP.
2) En mode de scrutation, les valeurs des OID doivent représenter l'état réel des circuits du dispositif de vidéotransmission demandé en moins de 5 s d'une transition d'état et également être signalées par TRAP (piège) en moins de 5 s d'une transition d'état, si ce TRAP est activé.
3) Le «Request ID» utilisé pendant l'interrogation du gestionnaire est à réutiliser dans la réponse (réponse SNMP).
4) Il est nécessaire que les temps de réponse pour les GET soient satisfaits conformément à l'exigence 2) de ce paragraphe.
5) L'agent doit fonctionner d'une manière stable. L'état stable de l'agent de vidéotransmission est caractérisé comme suit:
   – les dispositifs de vidéotransmission à contrôler peuvent être actionnés à tout moment;
   – l'agent fournit toujours une RÉPONSE à toutes les REQUÊTES valides;
   – ni l'agent, ni le dispositif de vidéotransmission connecté n'exécutent un redémarrage pendant le fonctionnement sans que cela soit demandé;
   – les réglages des paramètres de l'agent sont conservés pendant le fonctionnement et ne varient qu'en raison des actions de contrôle.
6) Tous les compteurs doivent être mis à zéro lors d'un démarrage à chaud ou à froid de l'agent. L'état courant du dispositif (contenu dans le masque TRAP sauvegardé) est à transférer après redémarrage au moyen de TRAP/notification.
7) Si on ne peut pas accéder aux composants de système de VTD de manière interne ou si l'agent n'est pas capable de fournir des informations concernant ces composants, la valeur entière 0 (non définie) doit être retournée en réponse à une requête Get, GetNext et GetBulk pour l'OID (Identificateur d'objet) de ces composants de système. En même temps, l'état d'erreur doit être fixé à NoError. Si le système n'est pas capable de mettre en œuvre une requête SET reçue, la commande doit être correctement acquittée, bien que l'on ne doive pas la sauvegarder. Les requêtes SNMP sont généralement acquittées (si

aucune erreur SNMP ne se produit) avec NoError et le Varbinds-OID correct (par exemple, en mode local). Les requêtes Trap, notification et SNMP get fournissent des informations concernant la réussite de l'exécution de la commande.

8) Si un OID est périmé, celui-ci est à ignorer pendant un «walk». Dans le cas d'une REQUÊTE, l'erreur SNMP «NOSUCHNAME» est à utiliser comme réponse, c'est-à-dire que l'agent se comporte comme si l'OID n'existait pas.

9) Pour détecter les TRAP perdus, un compteur global de TRAP («eventCounter») est mis en œuvre dans CommonVarbinds-MIB. Avant d'envoyer une TRAP/notification, la valeur d'even-Counter de l'OID est à incrémenter d'une unité. La valeur courante peut être demandée en utilisant eventCounter de l'OID.

10) TRAP priority est envoyé avec un TRAP et doit correspondre à la priorité définie de l'événement respectif. Elle comporte l'OID de la priorité d'événement.

11) 10 entrées au minimum pour chaque table individuelle de SNMP définie dans la présente norme doivent être prises en charge, les exceptions doivent être spécifiées.

11.5 Exigences concernant le Trap SNMP VSS pour la gestion d'événements

Le présent paragraphe est normatif.

Les applications de scrutation sont le type le plus courant d'applications de surveillance SNMP écrites pour contrôler l'état des dispositifs. Tous les éléments énumérés sont à fournir en tant qu'objets gérés par l'intermédiaire de messages SNMP GET.

La gestion d'événements donne la possibilité de recevoir des événements/pièges asynchrones depuis un dispositif de vidéotransmission et permet à l'utilisateur de gérer les incidents et les problèmes indiqués par cet événement. Des exemples d'événements sont des alertes de ventilation, perte vidéo ou disque.

Les VTD doivent être capables d'envoyer des TRAPS ou INFORMS pour les changements d'état pour les éléments et objets suivants, vers l'adresse de réception configurée:

- accessoires, par exemple E/S numérique;
- état de l'entrée vidéo tel que le mouvement, la perte vidéo, le dépositionnement, la falsification de signal;
- enregistrement;
- alarme;
- dépassement de la limite de température, de vitesse du ventilateur et de charge de CPU.

12 Exigences de sécurité du réseau

12.1 Généralités

Le présent article définit une architecture de sécurité pour le VTD. Le dispositif de vidéotransmission doit avoir, pour le grade de sécurité le plus élevé 4, la possibilité de fournir une authentification, un contrôle d'intégrité et un chiffrement de toutes les interfaces de réseau. Le but de cette architecture est de fournir une authentification de l'entité homologue, de l'origine des données et du dispositif réseau, ainsi que la confidentialité et l'intégrité des données vidéo. D'autres types de sécurité de communication tels que l'authentification de l'opérateur, le contrôle d'accès et la non répudiation, ne sont pas prévus dans le présent article. Les systèmes nécessitant ces services peuvent les ajouter au VTD d'une manière propriétaire.

Toutes les communications de données en dehors des zones de la pièce technique sécurisée doivent être chiffrées avec le degré de sécurité 4. L'AES (Norme de cryptage évoluée) avec une clé de 128 bits pour la symétrie et le RSA avec une clé de 1 024 bits doivent être prévus. Le chiffrement natif ne doit pas être accepté. Les VTD ne doivent stocker aucune forme de

mot de passe en texte clair. Tous ces mots de passe, soit dans des fichiers de configuration, soit dans une base de données, doivent être chiffrés.

Un VTD selon la présente norme doit prendre en charge le niveau de sécurité de transport pour le degré de sécurité 4.

12.2 Exigences de sécurité au niveau transport pour la transmission SG4

La sécurité au niveau transport fournit une protection de toutes les données vidéo entre un client et un serveur de VTD. La sécurité de la couche transport (TLS) doit être assurée par un VTD pour le transport chiffré. Le protocole TLS fournit des sessions de transport authentifiées entre deux VTD et tient compte de la confidentialité et de l'intégrité des données transportées.

Un VTD conforme à la présente norme doit prendre en charge le degré de sécurité 4 TLS 1.0 conformément à la norme IETF RFC 2246 et TLS 1.1 conformément à la RFC 4346. De manière facultative, le VTD peut prendre en charge TLS 1. 2 conformément à la RFC 5246.

Le VTD doit proposer une protection pour le transport de toutes les données et informations concernant le transfert en flux continu, le contrôle de flux et la gestion d'événement.

Le client et le serveur de VTD doivent prendre en charge les séries de chiffrement TLS_RSA_WITH_AES_128_CBC_ SHA et TLS_RSA_WITH_NULL_SHA de la RFC 2246 et la RFC 3268.

Bibliographie

CEI 62676-2-3, *Systèmes de vidéosurveillance destinés à être utilisés dans les applications de sécurité – Partie 2-3: Protocoles de transmission vidéo – Mise en œuvre de l'interopérabilité IP sur la base des services Web*

ISO/CEI 10918 (toutes les parties), *Technologies de l'information – Compression numérique et codage des images fixes à modelé continu*

ISO/CEI 10918-5, *Technologies de l'information – Compression numérique et codage des images fixes à modelé continu: Format d'échange de fichiers JPEG (JFIF)*

ISO/CEI 14496-1, *Technologies de l'information – Codage des objets audiovisuels – Partie 1: Systèmes* (disponible en anglais seulement)

ISO/CEI 15444 (toutes les parties), *Technologies de l'information – Système de codage d'images JPEG 2000*

ISO 8601, *Eléments de données et formats d'échange – Échange d'information – Représentation de la date et de l'heure*

ISO 19111 (toutes les parties), *Information géographique – Système de références spatiales par coordonnées* (disponible en anglais seulement)

ISO 19115:2003, *Information géographique – Métadonnées*

Recommandation UIT H.241, *Extended video procedures and control signals for ITU-T H.300 series terminals*

SCTE 52, *Data Encryption Standard – Cipher Block Chaining Packet Encryption Specification* (disponible en anglais seulement)

SMPTE 298M-1997, *Television, Universal Labels for Unique Identification of Digital Data* (disponible en anglais seulement)

FIPS PUB 180-2, *Secure Hash Standard (SHS)* (disponible en anglais seulement)

FIPS PUB 197, *Advanced Encryption Standard (AES)* (disponible en anglais seulement)

FIPS PUB 46-3, *Specification for the Data Encryption Standard, National Institute of Standards and Tech.* (disponible en anglais seulement)

FIPS PUB 81, *DES Modes of Operation, National Institute of Standards and Technology* (disponible en anglais seulement)

IETF Draft avt-rtp-h264-rcdo, *RTP Payload Format for H.264 RCDO Video* (disponible en anglais seulement)

IETF Draft avt-rtp-klv, *RTP Payload Format for SMPTE 336M Encoded Data* (disponible en anglais seulement)

IETF Draft avt-rtp-rfc3984bis, *RTP Payload Format for H.264 Video* (disponible en anglais seulement)

IETF Draft avt-rtp-svc, *RTP Payload Format for SVC Video* (disponible en anglais seulement)

IETF Draft avt-srtp-big-aes, *The use of AES-192 and AES-256 in Secure RTP* (disponible en anglais seulement)

IETF Draft HTTPMU, *HTTPU HTTP Multicast over UDP, HTTP Unicast over UDP* (disponible en anglais seulement)

IETF Draft RTP/AVPF, *Extended RTP Profile for RTCP-based Feedback (RTP/AVPF)* (disponible en anglais seulement)

IETF Draft RTP/RTX, *RTP Retransmission Payload Format* (disponible en anglais seulement)

IETF Draft SSDP, *Simple Service Discovery Protocol* (disponible en anglais seulement)

IETF RFC 052, *IAB Recommendations* (disponible en anglais seulement)

IETF RFC 792, *Internet Control Message Protocol* (disponible en anglais seulement)

IETF RFC 826, *An Ethernet Address Resolution Protocol* (disponible en anglais seulement)

IETF RFC 868, *Time Protocol* (disponible en anglais seulement)

IETF RFC 1034, *XML- Extensible Markup Language. W3C recommendation* (disponible en anglais seulement)

IETF RFC 1035, *Domain Names – Concepts and Facilities* (disponible en anglais seulement)

IETF RFC 1089, *SNMP over Ethernet* (disponible en anglais seulement)

IETF RFC 1109, *Ad-hoc Review* (disponible en anglais seulement)

IETF RFC 1155, *Structure of Management Information* (disponible en anglais seulement)

IETF RFC 1156, *Management Information Base (MIB-I)* (disponible en anglais seulement)

IETF RFC 1161, *SNMP over OSI* (disponible en anglais seulement)

IETF RFC 1187, *Bulk table retrieval* (disponible en anglais seulement)

IETF RFC 1212, *Concise MIB definitions* (disponible en anglais seulement)

IETF RFC 1214, *OSI MIB* (disponible en anglais seulement)

IETF RFC 1215, *Traps* (disponible en anglais seulement)

IETF RFC 1229, *Generic-interface MIB extensions* (disponible en anglais seulement)

IETF RFC 1305, *Network Time Protocol (Version 3) specification, implementation and analysis* (disponible en anglais seulement)

IETF RFC 1321, *The MD5 Message-Digest Algorithm, April 1992* (disponible en anglais seulement)

IETF RFC 1341, *MIME- Multipurpose Internet Mail Extensions* (disponible en anglais seulement)

IETF RFC 1738, *Uniform Resource Locators (URL)* (disponible en anglais seulement)

IETF RFC 1889, *Real Time Transport Protocol (RTP)* (disponible en anglais seulement)

IETF RFC 1901, *Community-based SNMPv2* (disponible en anglais seulement)

IETF RFC 1902, *Structure of Management Information for SNMPv2* (disponible en anglais seulement)

IETF RFC 1903, *Textual Conventions for SNMPv2* (disponible en anglais seulement)

IETF RFC 1904, *Conformance Statements for SNMPv2* (disponible en anglais seulement)

IETF RFC 1910, *User-based Security Model* (disponible en anglais seulement)

IETF RFC 2045, *Multipurpose Internet Mail Extensions (MIME) Part One Format of Internet Message Bodies* (disponible en anglais seulement)

IETF RFC 2046, *Multipurpose Internet Mail Extensions (MIME) Part Two Media Types* (disponible en anglais seulement)

IETF RFC 2104, *Keyed Hashing for Message Authentication* (disponible en anglais seulement)

IETF RFC 2190, *RTP Payload Format for H.263 Video Streams* (disponible en anglais seulement)

IETF RFC 2250, *RTP Payload Format for MPEG1/MPEG2 Video* (disponible en anglais seulement)

IETF RFC 2271, *An Architecture for Describing SNMP Management Frameworks* (disponible en anglais seulement)

IETF RFC 2272, *Message Processing and Dispatching for SNMP* (disponible en anglais seulement)

IETF RFC 2273, *SNMPv3 Applications* (disponible en anglais seulement)

IETF RFC 2274, *User-Based Security Model (USM) for SNMPv3* (disponible en anglais seulement)

IETF RFC 2275, *View-Based Access Control Model (VACM) for the SNMP* (disponible en anglais seulement)

IETF RFC 2279 UTF-8, *A transformation format of ISO 10646 (character encoding)* (disponible en anglais seulement)

IETF RFC 2387, *Format for representing content type* (disponible en anglais seulement)

IETF RFC 2396, *Uniform Resource Identifiers (URI) Generic Syntax* (disponible en anglais seulement)

IETF RFC 2429, *RTP Payload Format for the 1998 Version of ITU-T Rec. H.263 Video (H.263+)* (disponible en anglais seulement)

IETF RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification* (disponible en anglais seulement)

IETF RFC 2576, *Coexistence between SNMP Versions* (disponible en anglais seulement)

IETF RFC 2616, *HTTP Hypertext Transfer Protocol 1.1* (disponible en anglais seulement)

IETF RFC 2782, *A DNS RR for specifying the location of services (DNS SRV)* (disponible en anglais seulement)

IETF RFC 2790, *Host Resources MIB* (disponible en anglais seulement)

IETF RFC 2818, *HTTP over TLS* (disponible en anglais seulement)

IETF RFC 2863, *Interfaces Group MIB* (disponible en anglais seulement)

IETF RFC 2929, *Domain Name System (DNS)* (disponible en anglais seulement)

IETF RFC 3339, *Date and Time on the Internet Timestamps* (disponible en anglais seulement)

IETF RFC 3379, *Internet Group Management Protocol* (disponible en anglais seulement)

IETF RFC 3411, *An Architecture for Describing SNMP Management Frameworks* (disponible en anglais seulement)

IETF RFC 3412, *Message Processing and Dispatching for SNMP* (disponible en anglais seulement)

IETF RFC 3413, *SNMP Applications* (disponible en anglais seulement)

IETF RFC 3414, *User-Based Security Model (USM) for SNMPv3* (disponible en anglais seulement)

IETF RFC 3415, *View-Based Access Control Model (VACM) for the SNMPIETF RFC 3412 Message* (disponible en anglais seulement)

Processing and Dispatching for the Simple Network Management Protocol (disponible en anglais seulement)

IETF RFC 3512, *Configuring Networks and Devices with Simple Network Management Protocol (SNMP)* (disponible en anglais seulement)

IETF RFC 3555, *MIME Type Registration of RTP Payload Formats* (disponible en anglais seulement)

IETF RFC 3556, *Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol* (disponible en anglais seulement)

IETF RFC 3584 (Best Current Practice), *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework* (disponible en anglais seulement)

IETF RFC 3640, *RTP Payload Format for Transport of MPEG-4 Elementary Streams* (disponible en anglais seulement)

IETF RFC 3711, *The Secure Real-time Transport Protocol (SRTP)* (disponible en anglais seulement)

IETF RFC 3826, *The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP USM* (disponible en anglais seulement)

IETF RFC 3927, *Dynamic Configuration of IPv4 Link-Local addresses* (disponible en anglais seulement)

IETF RFC 3986, *Uniform Resource Identifier (URI) Generic Syntax* (disponible en anglais seulement)

IETF RFC 4122, *A Universally Unique IDentifier (UUID) URN Namespace* (disponible en anglais seulement)

IETF RFC 4571, *Framing Real-time Transport Protocol (RTP) and RTP Control Protocol (RTCP) Packets over Connection-Oriented Transport* (disponible en anglais seulement)

IETF RFC 4702, *The Dynamic Host Configuration Protocol (DHCP) Client Fully Qualified Domain Name (FQDN) Option* (disponible en anglais seulement)

IETF RFC 4855, *Media Type Registration of RTP Payload Formats* (disponible en anglais seulement)

IETF RFC 4288, *Media Type Specifications and Registration Procedures* (disponible en anglais seulement)

IETF RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2* (disponible en anglais seulement)

IETF RFC 5104, *Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF)* (disponible en anglais seulement)

IETF RFC 5371, *RTP Payload Format for JPEG 2000 Video Streams* (disponible en anglais seulement)

IETF RFC 5372, *Payload Format for JPEG 2000 Video Extensions for Scalability & Main Header Recovery* (disponible en anglais seulement)

IETF RFC 5590 (Proposed), *Transport Subsystem for the SNMP* (disponible en anglais seulement)

IETF RFC 5591 (Proposed), *Transport Security Model for the SNMP* (disponible en anglais seulement)

IETF RFC 5592 (Proposed), *Secure Shell Transport Model for the SNMP* (disponible en anglais seulement)

IETF RFC 5608 (Proposed), *Remote Authentication Dial-In User Service (RADIUS) Usage for SNMP Transport Models* (disponible en anglais seulement)

IETF RFC 2222, *Simple Authentication and Security Layer (SASL)* (disponible en anglais seulement)

IETF RFC 3264, *An Offer/Answer Model with Session Description Protocol (SDP)* (disponible en anglais seulement)

IETF RFC 3376, *Internet Group Management Protocol, Version 3* (disponible en anglais seulement)

IETF STD 16 RFC 1213, *Management Information Base (MIB-II)* (disponible en anglais seulement)

IETF STD 5 RFC 1112, *Host extensions for IP multi-casting* (disponible en anglais seulement)

IETF STD 5 RFC 791, *Internet Protocol* (disponible en anglais seulement)

IETF STD 6 RFC 768, *User Datagram Protocol* (disponible en anglais seulement)

IETF STD 62 RFC 3411, *An Architecture for Describing SNMP Management Frameworks* (disponible en anglais seulement)

IETF STD 62 RFC 3412, *Message Processing and Dispatching for the SNMP* (disponible en anglais seulement)

IETF STD 62 RFC 3413, *Simple Network Management Protocol (SNMP) Application* (disponible en anglais seulement)

IETF STD 62 RFC 3414, *User-based Security Model (USM) for version 3 of the SNMPv3* (disponible en anglais seulement)

IETF STD 62 RFC 3415, *View-based Access Control Model (VACM) for the SNMP* (disponible en anglais seulement)

IETF STD 62 RFC 3416, *Version 2 of the Protocol Operations for the SNMP* (disponible en anglais seulement)

IETF STD 62 RFC 3417, *Transport Mappings for the Simple Network Management Protocol (SNMP)* (disponible en anglais seulement)

IETF STD 62 RFC 3418, *Management Information Base (MIB) for the SNMP* (disponible en anglais seulement)

IETF STD 7 RFC 793, *Transmission Control Protocol* (disponible en anglais seulement)

MISB Standard 0107, *Bit and Byte Order for Metadata in Motion Imagery Files and Streams* (disponible en anglais seulement)

MISB RP 0701, *Common Metadata System Structure (CMS)* (disponible en anglais seulement)

MISB RP 0702, *Content part of CMS* (disponible en anglais seulement)

OASIS Standard Web Services Base Notification 1.3 (disponible en anglais seulement)

OASIS Standard Web Services Dynamic Discovery (WS-Discovery) (disponible en anglais seulement)

SMPTE 359M-2001, *Television and Motion Pictures, Dynamic Documents* (disponible en anglais seulement)

W3C Extensible Markup Language (XML) 1.0 (Third Edition), W3C Recommendation (disponible en anglais seulement)

W3C SOAP 1.2, Part 1 Messaging Framework (disponible en anglais seulement)

W3C SOAP, Message Transmission Optimization Mechanism (disponible en anglais seulement)

W3C SOAP, Version 1.2 Part 2 Adjuncts (Second Edition) (disponible en anglais seulement)

W3C Web Services Addressing (WS-Addressing) W3C Recommendation (disponible en anglais seulement)

W3C Web Services Addressing 1.0 – Core (disponible en anglais seulement)

W3C Web Services Description Language (WSDL) 1.1 (disponible en anglais seulement)

W3C Web Services Eventing (WS-Eventing), W3C Recommendation (disponible en anglais seulement)

W3C XML Path Language (XPath), W3C Recommendation (disponible en anglais seulement)

W3C XML Schema Part 1 Structures Second Edition, W3C Recommendation (disponible en anglais seulement)

W3C XML Schema Part 2 Datatypes Second Edition, W3C Recommendation (disponible en anglais seulement)

W3C XML-binary Optimized Packaging (disponible en anglais seulement)

W3C XML-NMSP – Namespaces in XML, W3C Recommendation (disponible en anglais seulement)

W3C XML 1.0, Extensible Markup Language (XML) 1.0 (Second Edition), W3C Recommendation (disponible en anglais seulement)

W3C XML Namespaces, Namespaces in XML, W3C Recommendation (disponible en anglais seulement)

W3C XML Information Set, XML Information Set, W3C Recommendation (disponible en anglais seulement)

W3C XML Schema: XML Schema Part 1: Structures, W3C Recommendation (disponible en anglais seulement)

W3C XML Schema: XML Schema Part 2: Datatypes, W3C RecommendationW3C WS-Addressing, Web Services Addressing 1.0 – Core, W3C Recommendation (disponible en anglais seulement)

W3C Web Services Eventing (WS-Eventing), W3C Recommendation (disponible en anglais seulement)

W3C WSDL 1.1, Web Services Description Language (WSDL) 1.1, W3C Recommendation (disponible en anglais seulement)

W3C WSDL Binding for SOAP 1.2, WSDL 1.1 Binding Extension for SOAP 1, W3C Recommendation (disponible en anglais seulement)

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch