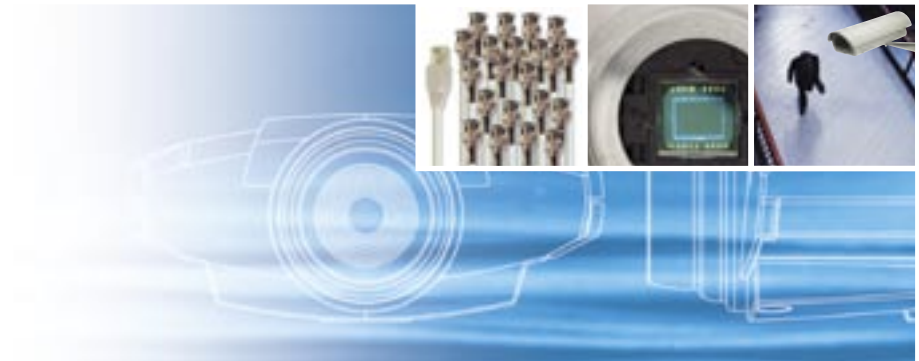




Technical guide to network video

Techniques and factors to consider for the successful deployment of IP-based security surveillance and remote monitoring applications



Welcome to the Axis technical guide to network video

The move to open video systems - combined with the benefits of networking, digital imaging, and camera intelligence - constitutes a far more effective means of security surveillance and remote monitoring than has ever been reached before. Network video provides everything that analog video offers, plus a wide range of innovative functions and features which are only possible with digital technology.

Before setting up your own system, you need to consider what features the system can provide. It is equally important to consider factors such as performance, interoperability, scalability, flexibility and future-proof functionality. This guide will walk you through these factors, helping you to achieve a solution that fully takes advantage of the potential of network video technology.

World leadership

Axis is the global market leader in network video. We have been developing solutions that add value to your network since 1984 and specifically, network video solutions since 1996. With more than 600,000 professional network video products and over 3 million networking products installed, Axis has the experience to meet your company's needs. It is this experience, combined with our cutting-edge technology that makes Axis the obvious supplier to choose when it comes to network video.



Axis specializes in professional network video solutions for security surveillance and remote monitoring. Our range of products includes network cameras, video servers, video decoders, video management software, and a full range of accessories.

Technology leadership

The core of the Axis product offering is its in-house developed IP-based technology platform, which allows the company to quickly and cost-effectively adapt its market offering to new applications and product areas. The technology enables easy installation and provides compact and powerful solutions so that equipment can be securely and rapidly connected to virtually any wired or wireless network.

Table of contents

1. Introduction to network video	7
1.1. What is network video?	7
1.2. What is a network camera?	8
1.3. What is a video server?	10
1.4. What is video management software?	10
2. The evolution of video surveillance systems	13
2.1. Analog CCTV systems using VCR	13
2.2. Analog CCTV systems using DVR	14
2.3. Analog CCTV systems using network DVR	14
2.4. Network video systems using video servers	15
2.5. Network video systems using network cameras	15
3. Image generation	17
3.1. CCD and CMOS sensors	17
3.2. Progressive scan versus interlaced video	18
3.2.1. Interlaced scanning	18
3.2.2. Progressive scanning	19
3.2.3. Example: Capturing moving objects	19
3.3. Compression	20
3.3.1. Still image compression standards	20
3.3.2. Video compression standards	21
3.4. Resolution	24
3.4.1. NTSC and PAL resolutions	24
3.4.2. VGA resolution	25
3.4.3. MPEG resolution	25
3.4.4. Megapixel resolution	26
3.5. Day and night functionality	26
4. Camera considerations	29
4.1. Using network cameras	29
4.1.1. Camera types	29
4.1.2. Lens selection	31
4.1.3. Indoor and outdoor installations	34
4.1.4. Best practices	34
4.2. Using analog cameras with video servers	36
4.2.1. Rack-mounted video servers	36
4.2.2. Standalone video servers	37
4.2.3. Video servers with PTZ and dome cameras	37
4.2.4. Video decoder	38

5. IP Network technologies	39
5.1. Ethernet	39
5.2. Power over Ethernet	40
5.3. Wireless networks	41
5.4. Data transport methods	43
5.4.1 IP addresses	43
5.4.2 IPv6	44
5.4.3 Data transport protocols for network video	44
5.4.4 Transmission methods for network video: Unicasting, Multicasting, and Broadcasting	45
5.5. Network security	45
5.5.1 Secure transmission	45
5.5.2 Security in wireless networks	47
5.5.3 Protecting single devices	48
5.6 QoS (Quality of Service)	48
5.7. More about network technologies and devices	50
6. System considerations	53
6.1. System design considerations	53
6.1.1 Bandwidth	53
6.1.2 Storage	54
6.1.3 Redundancy	56
6.1.4 System scalability	57
6.1.5 Frame rate control	57
6.2. Storage considerations	58
6.2.1 Direct attached storage	58
6.2.2 Network Attached Storage (NAS) and Storage Area Network (SAN)	59
6.2.3 RAID (Redundant Array of Independent Disks)	59
6.3. Security capabilities	60
6.4. Managing large systems	60
7. Video management	63
7.1 Hardware platforms	63
7.1.1 PC Server platforms	64
7.1.2 NVR platforms	64
7.2 Monitoring and recording	65
7.2.1 Monitoring using the web interface	65
7.2.2 Monitoring using video management software	66
7.2.3 Recording network video	66

7.3 System features	67
7.3.1 Video motion detection (VMD)	67
7.3.2 Audio	69
7.3.3 Digital inputs and outputs (I/O)	70
7.4 Integrated systems	72
8. Intelligent video systems	73
8.1 What is intelligent video?	73
8.2 Intelligent video architectures	73
8.2.1 DVRs and centralized intelligence	73
8.2.2 Network video systems and distributed intelligence	74
8.3 Typical applications	75
8.3.1 People counting	75
8.3.2 License plate recognition	75
8.3.3 D-Fence or tripwire	76
8.4 Components built on open standards	76
Quick start: Checklist when designing a network video system	77
1. Analog camera/DVR or network camera?	77
2. Making the right network camera choice	82
3. Design guides, preparing your network video project	84
4. Project tools	85
AXIS Academy	87
Contact information	93

Introduction to network video



The video surveillance industry today has a wide range of systems and devices for monitoring and safeguarding people and property. In order to understand the scope and potential of an integrated, fully digitized system, let us first examine the core components of a network video system: the network camera, the video server and video management software. When selecting an appropriate system, it is useful to compare the various available technologies in the light of the intended application area and requirements in terms of cost-effectiveness, scalability, ease of use and flexibility.

1.1. What is network video?

Network video, often referred to as IP-Surveillance for specific applications within security surveillance and remote monitoring, is a system which gives users the ability to monitor and record video over an IP network (LAN/WAN/Internet).

Unlike analog video systems, network video uses the network, rather than dedicated point-to-point cabling, as the backbone for transporting information. The term network video refers to both the video and audio sources available throughout the system. In a network video application, digitized video streams are transferred to any location in the world via a wired or wireless IP network, enabling video monitoring and recording from anywhere on the network.

Network video can be used in an almost unlimited number of applications; however, most of its uses fall into one of the following two categories:

- **Security surveillance**

Network video's advanced functionality makes it highly suited to the applications involved in security surveillance. The flexibility of digital technology enhances security personnel's ability to protect people, property and assets. Such systems are therefore an especially attractive option for companies currently using CCTV.

- **Remote monitoring**

Network video gives users the ability to gather information at all key points of an operation and view it in real-time. This makes the technology ideal for monitoring equipment, people and places both locally and remotely. Application examples include traffic and production line monitoring, and the monitoring of multiple retail locations.

The main vertical markets where network video systems have been successfully installed are:

- **Education**

Security and remote monitoring of school playground areas, hallways and classrooms.

- **Transportation**

Remote monitoring of railway stations and tracks, parking lots and garages, highways and airports.

- **Banking**

Traditional security applications in high street banks, branch offices and ATM locations.

- **Government**

For surveillance purposes, to provide safe and secure public environments.

- **Retail**

For security and remote monitoring purposes to make store management easier and more efficient.

- **Industrial**

Monitoring manufacturing processes, logistic systems, warehouse and stock control systems.

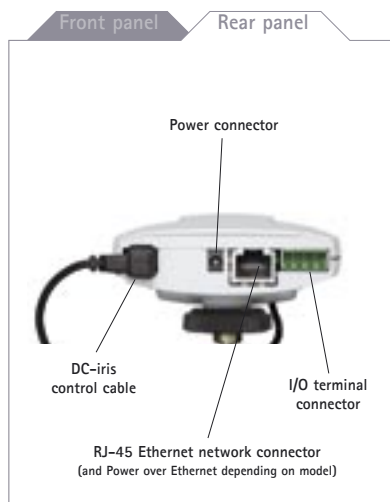
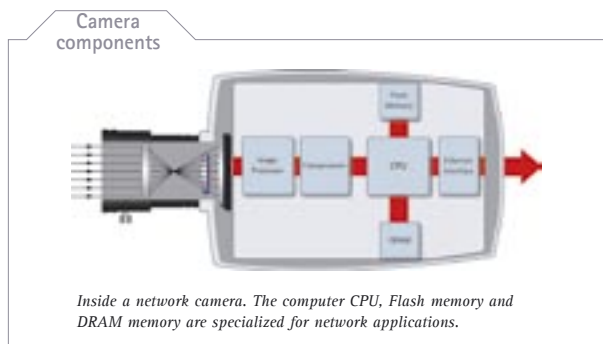
1.2. What is a network camera?

A network camera can be described as a camera and computer combined in one unit. It captures and transmits live images directly over an IP network, enabling authorized users to locally or remotely view, store, and manage video over standard IP-based network infrastructure.

Product overview

A network camera has its own IP address. It is connected to the network and has a built-in web server, FTP server, FTP client, e-mail client, alarm management, programmability, and much more. A network camera does not need to be connected to a PC, it operates independently and can be placed wherever there is an IP network connection. A web camera, on the other hand, is something totally different – it is a camera that requires connection to a PC via a USB or IEEE1394 port and a PC to operate.

In addition to video, a network camera also includes other functionalities and information being transported over the same network connection, i.e. digital inputs and outputs, audio, serial port(s) for serial data or control of pan/tilt/zoom mechanisms.



Comparing a network and an analog camera

In recent years, network camera technology has caught up to the analog camera and now meets the same requirements and specifications. Network cameras even surpass the performance of analog cameras, by offering a number of advanced functions which will be described later in this guide.

In short, an analog camera is a one-directional signal carrier which terminates at the DVR and operator level, whereas a network camera is fully bi-directional, and integrates with and drives the rest of the system to a high degree in a distributed and scalable environment. A network camera communicates with several applications in parallel, to perform various tasks, such as detecting motion or sending different streams of video.

Read more about using network cameras in chapter 4, page 29.

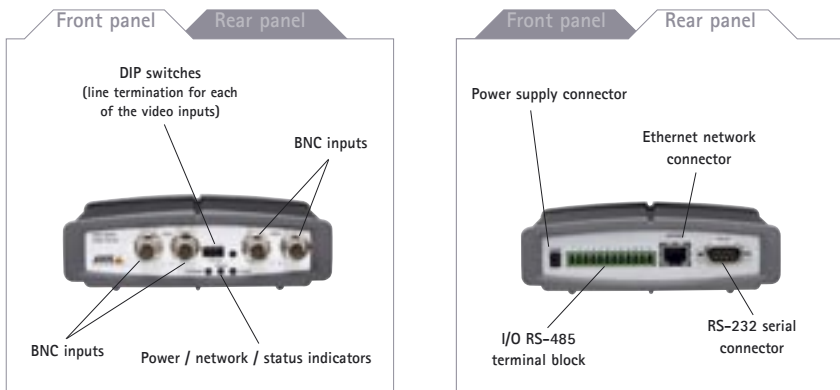
1.3. What is a video server?

A video server (sometimes called a video encoder) makes it possible to move toward a network video system without having to discard existing analog equipment. It brings new functionality to analog equipment and eliminates the need for dedicated equipment such as coaxial cabling, monitors and DVRs – the latter becoming unnecessary as video recording can be done using standard PC servers.

Product overview

A video server typically has between one and four analog ports for analog cameras to plug into, as well as an Ethernet port for connection to the network. Like network cameras, it contains a built-in web server, a compression chip and an operating system so that incoming analog feeds can be converted into digital video, transmitted and recorded over the computer network for easier accessibility and viewing.

Besides the video input, a video server also includes other functionalities and information which are transported over the same network connection: digital inputs and outputs, audio, serial port(s) for serial data or control of pan/tilt/zoom mechanisms. A video server can also be connected to a wide variety of specialized cameras, such as a highly sensitive black and white camera, a miniature or a microscope camera.



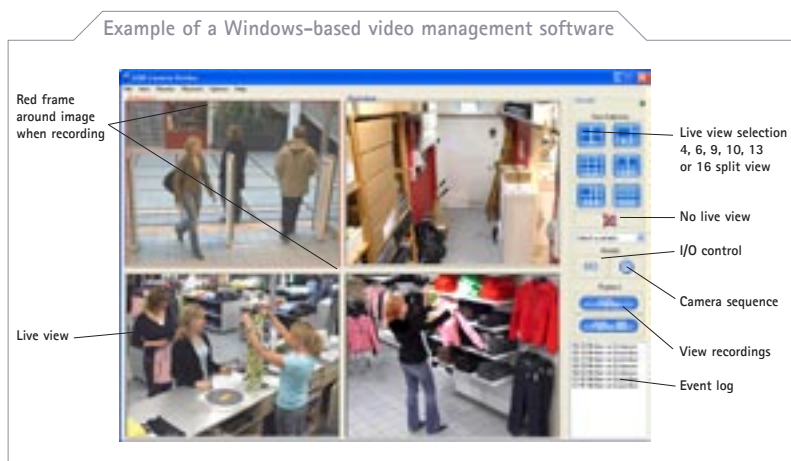
Read more about using analog cameras with video servers in chapter 4.2, page 36.

1.4. What is video management software?

Video management software running on a Windows or Unix/Linux server, supplies the basis for video management, monitoring, analysis, and recording. A wide range of software is available, based on the users' requirements. A standard web browser provides adequate viewing for many network video applications, utilizing the web interface built into the network camera or video server especially if only one or a few cameras are viewed at the same time.

To view several cameras at the same time, dedicated video management software is required. A wide range of video management software is available. In its simplest form, it offers live viewing, storing and retrieving of video sequences. Advanced software contains features like:

- Simultaneous viewing and recording of live video from multiple cameras
- Several recording modes: continuous, scheduled, on alarm and on motion detection
- Capacity to handle high frame rates and large amounts of data
- Multiple search functions for recorded events
- Remote access via a web browser, client software and even PDA client
- Control of PTZ and dome cameras
- Alarm management functions (sound alarm, pop-up windows or e-mail)
- Full duplex, real-time audio support
- Video intelligence



Read more about video management software in chapter 7.2.2, page 66.

Application development

Axis offers application software to suit different needs. In order to facilitate an even wider selection of software, it is possible for independent developers and partners to integrate Axis video products into their applications.

Axis has developed and supports a standardized instruction suite of CGI (Common Gateway Interface) programs. These instructions collectively comprise Axis' HTTP Application Programming Interface (AXIS VAPIX™ API). In their simplest form, CGI instructions for motion detection, event triggering, alarm notification via e-mail, remote video storage and so forth, can be typed directly into the URL of a web browser.

Axis also offers a Software Development Kit (SDK), which contains components and documentation to help developers integrate Axis video products in Windows applications. Furthermore, it is possible to write scripts that run on the video products, which makes it possible to tailor the functionality of network video products to meet specific needs.

More information about developer support can be found at www.axis.com/techsup/cam_servers/dev/

Axis Application Development Partner (ADP) Program

Axis' more than 300 ADP partners offer a wide range of complete software solutions that meet varying specifications and requirements for different application areas - from entry-level software to comprehensive applications covering most industry segments.



More information about Axis' ADP partners is available at www.axis.com/partner/adp_intro.htm



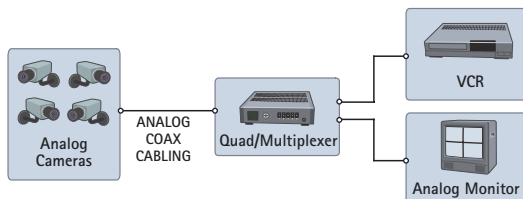
The evolution of video surveillance systems

Video surveillance systems have existed for some 25 years, starting out as 100% analog systems and gradually becoming digitized. Today's systems have come a long way from the early analog tube cameras connected to a VCR. They now use network cameras and PC servers for video recording in a fully digitized system. However, in between the fully analog and the fully digital systems, there are several solutions which are partly digital; these solutions include a number of digital components but do not represent fully digital systems.

All systems described in sections 2.2 and 2.3 below constitute partly “digital video systems”. Only the systems described in sections 2.4 and 2.5 are true network video systems, in which the video is continuously being transported over an IP network, and which are fully scalable and flexible.

2.1. Analog CCTV systems using VCR

An analog CCTV system using a VCR (Video Cassette Recorder) represents a fully analog system consisting of analog cameras with coax output, connected to the VCR for recording. The VCR uses the same type of cassettes as a home VCR. The video is not compressed, and if recording at full frame rate, one tape lasts a maximum of 8 hours. In larger systems, a quad or multiplexer can be connected in between the camera and the VCR. The quad/multiplexer makes it possible to record several cameras to one VCR, but at the cost of a lower frame rate. To monitor the video, an analog monitor is used.

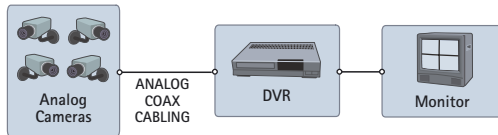


2.2. Analog CCTV systems using DVR

An analog CCTV system using a DVR (Digital Video Recorder) is an analog system with digital recording. In a DVR, the videotape is replaced with hard drives for the video recording, which requires the video to be digitized and compressed in order to store as many day's worth of video as possible. With early DVRs, hard disk space was limited – so recording duration was limited, or a lower frame rate had to be used. Recent development of hard disks means space is no longer a major problem. Most DVRs have several video inputs, typically 4, 9, or 16, which means they also include the functionality of the quad and multiplexers.

The DVR system adds the following advantages:

- No need to change tapes
- Consistent image quality

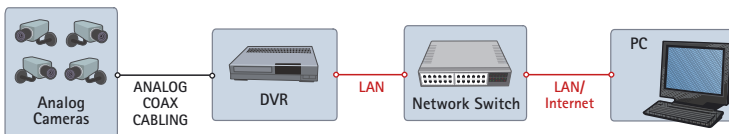


2.3. Analog CCTV systems using network DVR

An analog CCTV system using a network DVR is a partly digital system which includes a network DVR equipped with an Ethernet port for network connectivity. Since the video is digitized and compressed in the DVR, it can be transported over a computer network to be monitored on a PC in a remote location. Some systems can monitor both live and recorded video, while some can only monitor recorded. Furthermore, some systems require a special Windows client to monitor the video, while others use a standard web browser; the latter making the remote monitoring more flexible.

The network DVR system adds the following advantages:

- Remote monitoring of video via a PC
- Remote operation of the system

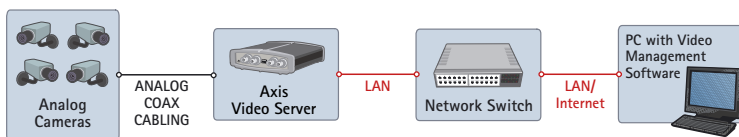


2.4. Network video systems using video servers

A network video system using video servers includes a video server, a network switch and a PC with video management software. The analog camera connects to the video server, which digitizes and compresses the video. The video server then connects to a network and transports the video via a network switch to a PC, where it is stored on hard disks. This is a true network video system.

A network video system using video servers adds the following advantages:

- Use of standard network and PC server hardware for video recording and management
- The system is scalable in steps of one camera at a time
- Off-site recording is possible
- It is future-proof since the system can easily be expanded by incorporating network cameras



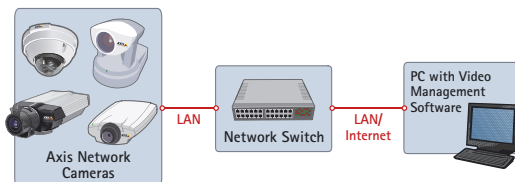
This diagram shows a true network video system, where video information is continuously transported over an IP network. It uses a video server as the cornerstone to migrate the analog security system into an IP-based video solution.

2.5. Network video systems using network cameras

A network camera combines a camera and computer in one unit, which includes the digitization and compression of the video, as well as a network connector. The video is transported over an IP-based network, via network switches, and recorded to a standard PC with video management software. This represents a true network video system, and is also a fully digital system, where no analog components are used.

A network video system using network cameras adds the following advantages:

- High resolution cameras (megapixel)
- Consistent image quality
- Power over Ethernet and wireless functionality
- Pan/tilt/zoom, audio, digital inputs and outputs over IP along with video
- Full flexibility and scalability



This diagram shows a true network video system, where the video is continuously transported over an IP network, using network cameras. This system takes full advantage of digital technology, and provides consistent image quality from the camera to the viewer, whatever their location.

Image generation

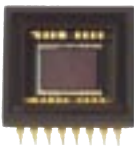
The building blocks of image quality in network video



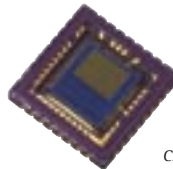
Image quality is clearly one of the most important features of any camera, if not the most important. This is especially true of security surveillance and remote monitoring applications, where lives and property may be at stake. But how can one guarantee good image quality? That is a frequently asked question when specifying a new system, which involves sourcing and installing new network cameras. Unlike traditional analog cameras, network cameras are equipped with the processing power not only to capture and present images, but also to manage and compress them digitally for network transport. Image quality can vary considerably and is dependent on several factors such as the choice of optics and image sensor, the available processing power and the level of sophistication of the algorithms in the processing chip.

This chapter covers some of the key areas that need to be considered when specifying network cameras for particular surveillance applications.

3.1. CCD and CMOS sensors



CCD sensor



CMOS sensor

The image sensor of the camera is responsible for transforming light into electrical signals. When building a camera, there are two possible technologies for the camera's image sensor:

- CCD (Charged Coupled Device)
- CMOS (Complementary Metal Oxide Semiconductor)

CCD sensors are produced using a technology developed specifically for the camera industry, while CMOS sensors are based on standard technology already extensively used in memory chips, inside PCs for example.

CCD technology

CCD sensors have been used in cameras for more than twenty years and present many quality advantages, among which a better light sensitivity than CMOS sensors. This higher light sensitivity translates into better images in low light conditions. CCD sensors are however more expensive as they are made in a non-standard process and more complex to incorporate into a camera. Besides, when there is a very bright object in the scene (such as a lamp or direct sunlight), the CCD may bleed, causing vertical stripes below and above the object. This phenomenon is called smear.

CMOS technology

Recent advances in CMOS sensors bring them closer to their CCD counterparts in terms of image quality, but CMOS sensors remain unsuitable for cameras where the highest possible image quality is required. CMOS sensors provide a lower total cost for the cameras since they contain all the logics needed to build cameras around them. They make it possible to produce smaller-sized cameras. Large size sensors are available, providing megapixel resolution to a variety of network cameras. A current limitation with CMOS sensors is their lower light sensitivity. In normal bright environments this is not an issue, while in low light conditions this becomes apparent. The result is either a very dark or a very noisy image.

3.2. Progressive scan versus interlaced video

Today, two different techniques are available to render the video: interlaced scanning and progressive scanning. Which technique is selected will depend on the application and purpose of the video system, and particularly whether the system is required to capture moving objects and to allow viewing of detail within a moving image.

3.2.1. Interlaced scanning

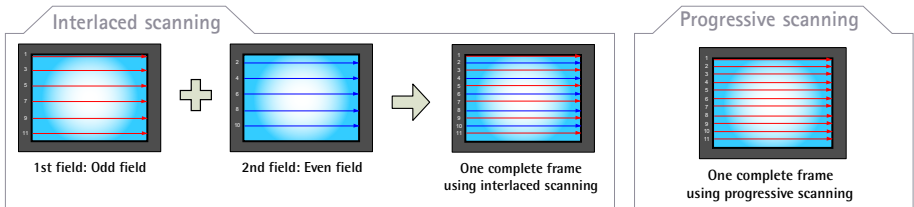
Interlaced scan-based images use techniques developed for Cathode Ray Tube (CRT)-based TV monitor displays, made up of 576 (PAL) / 480 (NTSC) visible vertical lines across a standard TV screen. Interlacing divides these into odd and even lines and then alternately refreshes them at 25/30 frames per second. The slight delay between odd and even line refreshes creates some distortion or 'jaggedness'. This is because only half the lines keeps up with the moving image while the other half waits to be refreshed.

The effects of interlacing can be somewhat compensated for by using de-interlacing. De-interlacing is the process of converting interlaced video into a non-interlaced form, by eliminating some jaggedness from the video for better viewing. This process is also called line doubling. Some network video products, such as Axis video servers, integrate a de-interlace filter which improves image quality in the highest resolution (4CIF). This feature eliminates the motion blur problems caused by the analog video signal from the analog camera.

Interlaced scanning has served the analog camera, television and VHS video world very well for many years, and is still the most suitable for certain applications. However, now that display technology is changing with the advent of Liquid Crystal Display (LCD), Thin Film Transistor (TFT)-based monitors, DVDs and digital cameras, an alternative method of bringing the image to the screen, known as *Progressive scanning*, has been created.

3.2.2. Progressive scanning

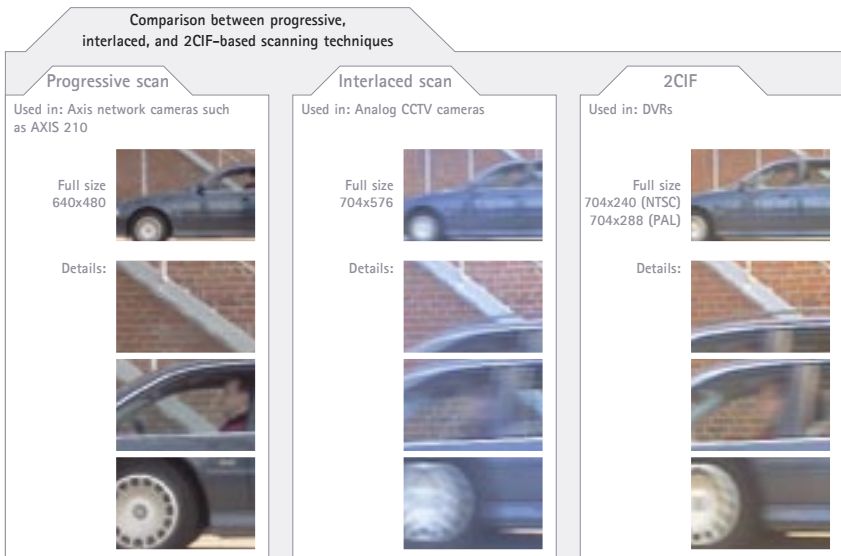
Progressive scanning, as opposed to interlaced, scans the entire image line by line every 25/30 of a second. In other words, captured images are not split into separate fields like in interlaced scanning. Computer monitors do not need to interlace to show the picture on the screen. It puts them on one line at a time in perfect order i.e. 1, 2, 3, 4, 5, 6, 7 etc. So there is virtually no "flickering" effect. As such, in a video surveillance application it can be critical in viewing detail within a moving image such as a person running away. However, a high quality monitor is required to get the best out of this type of scan.



3.2.3. Example: Capturing moving objects

When a camera captures a moving object, the sharpness of a still image will depend on the technology used. Compare these JPEG images, captured by three different cameras using progressive scan, 4CIF interlaced scan and 2CIF respectively.

- Please note the following:
- All image systems produce a clear image of the background
 - Jagged edges from motion with interlaced scan
 - Motion blur caused by the lack of resolution in the 2CIF sample
 - Only progressive scan makes it possible to identify the driver



Note: In these examples, the cameras were using the same lens. The car was driving at 20 km/h (15 mph).

3.3. Compression

Many compression standards to choose from

Image and video compression can be done either in a lossless or lossy approach. In lossless compression, each and every pixel is kept unchanged resulting in an identical image after decompression. The price to pay is that the compression ratio, i.e. the data reduction, is very limited. A well-known lossless compression format is GIF. Since the compression ratio is so limited, these formats are impractical for use in network video solutions where large amounts of images need to be stored and transmitted. Therefore, several lossy compression methods and standards have been developed. The fundamental idea is to reduce things that appear invisible to the human eye and by doing so being able to increase the compression ratio tremendously.

Compression methods also involve two different approaches to compression standards: still image compression and video compression.

3.3.1. Still image compression standards

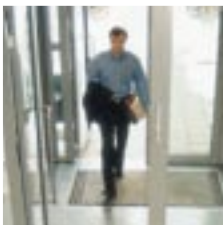
All still image compression standards are focused only on one single picture at a time. The most well known and widespread standard is JPEG.

JPEG

JPEG, a well-known image compression method, was originally standardized in the mid-1980s in a process started by the *Joint Photographic Experts Group*. With JPEG, decompression and viewing can be done from standard web browsers.

JPEG compression can be done at different user-defined compression levels, which determine how much an image is to be compressed. The compression level selected is directly related to the image quality requested. Besides the compression level, the image itself also has an impact on the resulting compression ratio. For example, a white wall may produce a relatively small image file (and a higher compression ratio), while the same compression level applied on a very complex and patterned scene will produce a larger file size, with a lower compression ratio.

The two images below illustrate compression ratio versus image quality for a given scene at two different compression levels.



Compression level "low"
Compression ratio 1:16
6% of original file size
No visible image quality degradation



Compression level "high"
Compression ratio 1:96
1% of original file size
Image quality clearly degraded

JPEG2000

Another still image compression standard is JPEG2000. It was developed by the same group that also developed JPEG. Its main target is for use in medical applications and for still image photographing. At low compression ratios, it performs similar to JPEG but at really high compression ratios it performs slightly better than JPEG. The price to pay is that the support for JPEG2000 in web browsers and image displaying and processing applications is still very limited.

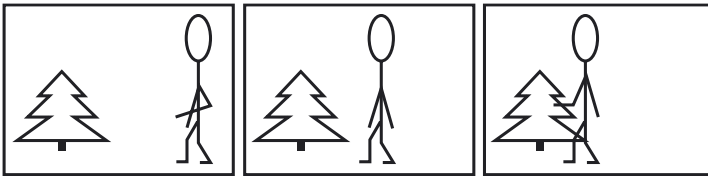
3.3.2. Video compression standards

Video as a sequence of JPEG Images – Motion JPEG (M-JPEG)

Motion JPEG is the most commonly used standard in network video systems. A network camera, like a digital still picture camera, captures individual images and compresses them into JPEG format. The network camera can capture and compress, for example, 30 such individual images per second (30 fps – frames per second), and then make them available as a continuous flow of images over a network to a viewing station. At a frame rate of about 16 fps and above, the viewer perceives motion video. We refer to this method as Motion JPEG or M-JPEG.

As each individual image is a complete JPEG compressed image, they all have the same guaranteed quality, determined by the compression level chosen for the network camera or video server.

Example of a sequence of three complete JPEG images



H.263

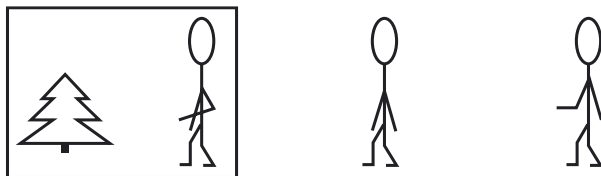
The H.263 compression technique targets a fixed bit rate video transmission. The downside of having a fixed bit rate is that when an object moves, the quality of the image decreases. H.263 was originally designed for video conferencing applications and not for video surveillance where details are more crucial than fixed bit rate.

MPEG

One of the best-known audio and video streaming techniques is the standard called MPEG (initiated by the *Motion Picture Experts Group* in the late 1980s). This section focuses on the video part of the MPEG video standards.

MPEG's basic principle is to compare two compressed images to be transmitted over the network. The first compressed image is used as a reference frame, and only parts of the following images that differ from the reference image are sent. The network viewing station then reconstructs all images based on the reference image and the "difference data".

Despite higher complexity, applying MPEG video compression leads to lower data volumes being transmitted across the network than is the case with Motion JPEG. This is illustrated on next page where only information about the differences in the second and third frames is transmitted.



Naturally, MPEG is far more complex than indicated above, often involving additional techniques or tools for parameters such as prediction of motion in a scene and identifying objects. There are a number of different MPEG standards:

- MPEG-1 was released in 1993 and intended for storing digital video onto CDs. Therefore, most MPEG-1 encoders and decoders are designed for a target bit-rate of about 1.5Mbit/s at CIF resolution. For MPEG-1, the focus is on keeping the bit-rate relatively constant at the expense of a varying image quality, typically comparable to VHS video quality. The frame rate in MPEG-1 is locked at 25 (PAL)/30 (NTSC) fps.
- MPEG-2 was approved in 1994 as a standard and was designed for high quality digital video (DVD), digital high-definition TV (HDTV), interactive storage media (ISM), digital broadcast video (DBV), and cable TV (CATV). The MPEG-2 project focused on extending the MPEG-1 compression technique to cover larger pictures and higher quality at the expense of a lower compression ratio and higher bit-rate. The frame rate is locked at 25 (PAL)/30 (NTSC) fps, just as in MPEG-1.
- MPEG-4 is a major development from MPEG-2. There are many more tools in MPEG-4 to lower the bit-rate needed to achieve a certain image quality for a certain application or image scene. Furthermore, the frame rate is not locked at 25/30 fps. However, most of the tools used to lower the bit-rate are today only relevant for non real-time applications. This is because some of the new tools require so much processing power that the total time for encoding and decoding (i.e. the latency) makes them impractical for applications other than studio movie encoding, animated movie encoding, and such like. In fact, most of the tools in MPEG-4 that can be used in a real time application are the same tools that are available in MPEG-1 and MPEG-2.

The key consideration is to select a widely used video compression standard that ensures high image quality, such as M-JPEG or MPEG-4.

MPEG-4 (Part 10)

The two groups behind H.263 and MPEG-4 joined together to form the next generation video compression standard. AVC for Advanced Video Coding, also called H.264 or MPEG-4 Part 10. The intent is to achieve very high data compression. This standard would be capable of providing good video quality at bit rates that are substantially lower than what previous standards would need, and to do so without so much of an increase in complexity as to make the design impractical or expensive to implement.

Advantages and disadvantages of Motion JPEG, MPEG-2 and MPEG-4

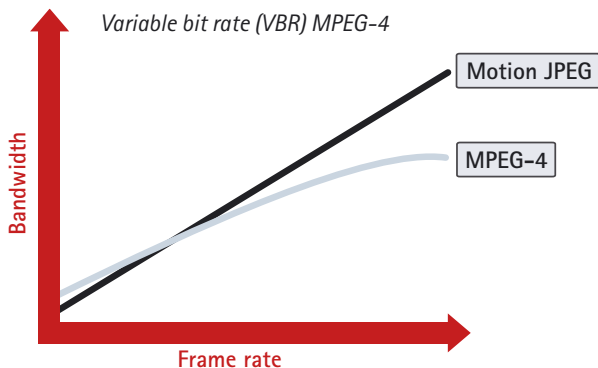
Due to its simplicity, the widely used Motion JPEG, a standard in many systems, is often a good choice. There is limited delay between image capturing in a camera, encoding, transfer over the network, decoding, and finally display at the viewing station. In other words, Motion JPEG provides low latency due to its simplicity (image compression and complete individual images), and is therefore also suitable for image processing, such as in video motion detection or object tracking. Any practical image resolution, from mobile phone display size (QVGA) up to full video (4CIF) image size and above (megapixel), is available in Motion JPEG.

The system guarantees image quality regardless of movement or image complexity, while offering the flexibility to select either high image quality (low compression) or lower image quality (high compression) with the benefit of smaller image file sizes, thus lower bit-rate and bandwidth usage. The frame rate can easily be adjusted to limit bandwidth usage, without loss of image quality.

However, Motion JPEG generates a relatively large volume of image data to be sent across the network. In this respect, MPEG has the advantage of sending a lower volume of data per time unit across the network (bit-rate) compared to Motion JPEG, except at low frame rates as described below. If the available network bandwidth is limited, or if video is to be recorded at a high frame rate and there are storage space restraints, MPEG may be the preferred option. It provides a relatively high image quality at a lower bit-rate (bandwidth usage). Still, the lower bandwidth demands come at the cost of higher complexity in encoding and decoding, which in turn contributes to a higher latency when compared to Motion JPEG.

One other item to keep in mind: Both MPEG-2 and MPEG-4 are subject to licensing fees.

The graph below shows how bandwidth use between Motion JPEG and MPEG-4 compares at a given image scene with motion. It is clear that at lower frame rates, where MPEG-4 compression cannot make use of similarities between neighboring frames to a high degree, and due to the overhead generated by the MPEG-4 streaming format, the bandwidth consumption is similar to Motion JPEG. At higher frame rates, MPEG-4 requires much less bandwidth than Motion JPEG.



About Axis' MPEG-4 support

Most Axis network video products feature advanced real-time video encoding that can deliver simultaneous MPEG-4 and Motion JPEG streams. This gives users the flexibility to maximize image quality for recording and reduce bandwidth needs for live viewing.

Axis' implementation of the MPEG-4 image compression standard follows the ISO/IEC 14496-2 standard (also known as MPEG-4 Visual or MPEG-4 Part 2). Axis network video products support the Advanced Simple Profile (ASP) up to level 5 and the possibility for Simple Profile (SP). With a wide range of settings, it is possible to configure the streams to be optimized for both bandwidth and quality. The Axis Media Control (AMC) with MPEG-4 decoder included, makes viewing of streams and integration into applications easy.

Furthermore, Axis' multicasting support enables an unlimited number of viewers without sacrificing network system performance. *Read more about multicasting in chapter 5.4.4, page 45.*

Does one compression standard fit all?

When considering this question and when designing a network video application, the following issues should be addressed:

- What frame rate is required?
- Is the same frame rate needed at all times?
- Is recording/monitoring needed at all times, or only on motion/event?
- For how long must the video be stored?
- What resolution is required?
- What image quality is required?
- What level of latency (total time for encoding and decoding) is acceptable?
- How robust/secure must the system be?
- What is the available network bandwidth?
- What is the budget for the system?

For detailed information about digital video compression techniques, please refer to Axis' white paper from www.axis.com/corporate/corp/tech_papers.htm

3.4. Resolution

Resolution in an analog or digital world is similar, but there are some important differences in how it is defined. In analog video the image consists of lines, or TV-lines, since analog video technology is derived from the television industry. In a digital system the image is made up of pixels (Picture elements).

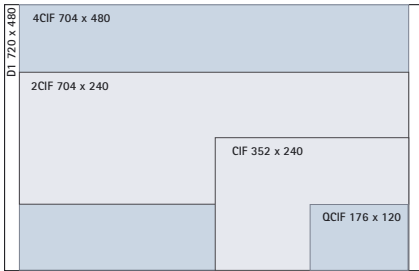
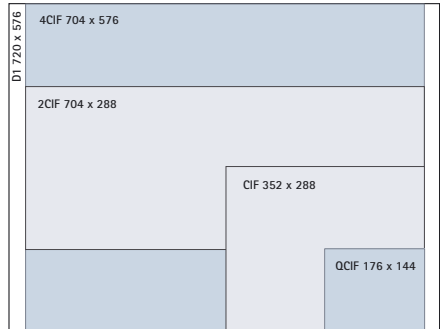
3.4.1. NTSC and PAL resolutions

In North America and Japan, the NTSC standard (National Television System Committee) is the predominant analog video standard, while in Europe the PAL standard (Phase Alternation by Line) is used. Both standards originate from the television industry. NTSC has a resolution of 480 lines, and uses a refresh rate of 60 interlaced fields per second (or 30 full frames per second). PAL has a resolution with 576 lines, and uses a refresh rate of 50 interlaced fields per second (or 25 full frames per second). The total amount of information per second is the same in both standards.

When analog video is digitized, the maximum amount of pixels that can be created is based on the number of TV lines available to be digitized. In NTSC the maximum size of the digitized image is 720x480 pixels. In PAL the size is 720x576 pixels (D1). The most commonly used resolution is 4CIF 704x576 PAL / 704x480 NTSC.

2CIF resolution is 704x240 (NTSC) or 704x288 (PAL) pixels, which means dividing the number of horizontal lines by 2. In most cases, each horizontal line is shown twice, so called "line doubling", when shown on a monitor in order to maintain correct ratios in the image. This is a way to cope with motion blur in interlace scan.

Sometimes a quarter of the CIF image is used, called QCIF short for Quarter CIF.

Image, showing different NTSC resolutions.*Image, showing different PAL resolutions.*

3.4.2. VGA resolution

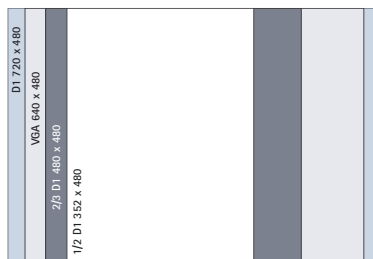
With the introduction of network cameras, 100% digital systems can be designed. This renders the limitations of NTSC and PAL irrelevant. Several new resolutions derived from the computer industry have been introduced, providing better flexibility and moreover, they are worldwide standards.

VGA is an abbreviation of Video Graphics Array, a graphics display system for PCs originally developed by IBM. The resolution is defined at 640x480 pixels. The VGA resolution is normally better suited for network cameras since the video in most cases will be shown on computer screens, with resolutions in VGA or multiples of VGA. Quarter VGA (QVGA) with a resolution of 320x240 pixels is also a commonly used format, very similar in size to CIF. QVGA is sometimes called SIF (Standard Interchange Format) resolution, easily confused with CIF. Other VGA-based resolutions are XVGA (1024x768 pixels) and 1280x960 pixels, 4 times VGA, providing megapixel resolution. *Please refer to section 3.4.4., page 26.*

3.4.3. MPEG resolution

MPEG resolution usually means one of the following resolutions:

- 704x576 pixels (PAL 4CIF)
- 704x480 pixels (NTSC 4CIF)
- 720x576 pixels (PAL or D1)
- 720x480 pixels (NTSC or D1)

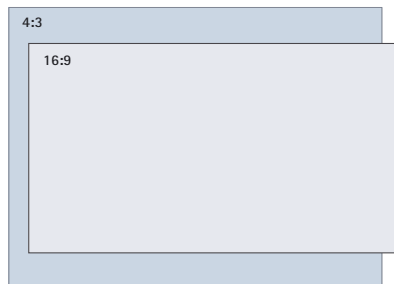
Image, showing resolutions used in MPEG:

3.4.4. Megapixel resolution

The higher the resolution, the more details can be seen in an image. This is a very important consideration in video surveillance applications, where a high-resolution image can enable a criminal to be identified. The maximum resolution of NTSC and PAL, in analog cameras, after the video signal has been digitized in a DVR or a video server, is 400,000 pixels ($704 \times 576 = 405,504$). 400,000 equals 0.4 Megapixel.

Even though the video surveillance industry has always managed to live with these limitations, new network camera technology now makes higher resolution possible. A common megapixel format is 1280×1024 , giving 1.3 megapixel resolution, 3 times higher than analog cameras. Cameras with 2 megapixel and 3 megapixel are also available, and even higher resolutions are expected in the future.

Megapixel network cameras also bring the benefit of different aspect ratios. In a standard CCTV an aspect ratio of 4:3 is used, while movies and wide-screen TV use 16:9. The advantage of this aspect ratio is that, in most images, the upper part and the lower part of the picture are of no interest, yet they take up precious pixels, and therefore bandwidth and storage space. In a network camera any aspect ratio can be used.



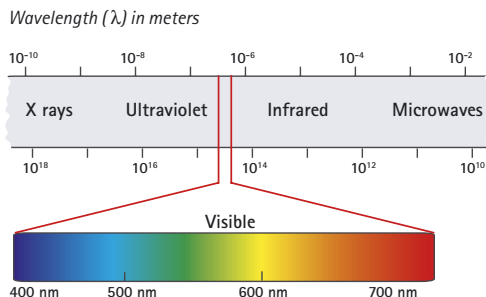
In addition, digital pan/tilt/zoom can be achieved without losing resolution, where the operator selects which part of the megapixel images should be shown. This does not imply any mechanical movement from the camera. It ensures much higher reliability.

3.5. Day and night functionality

Certain environments or situations restrict the use of artificial light, making infrared (IR) cameras particularly useful. These include low-light video surveillance applications, where light conditions are less than optimal, as well as discreet and covert surveillance situations. Infrared-sensitive cameras, which can make use of invisible infrared light, can be applied, for instance, in a residential area late at night without disturbing residents. They are also useful when the cameras should not be evident.

Light perception

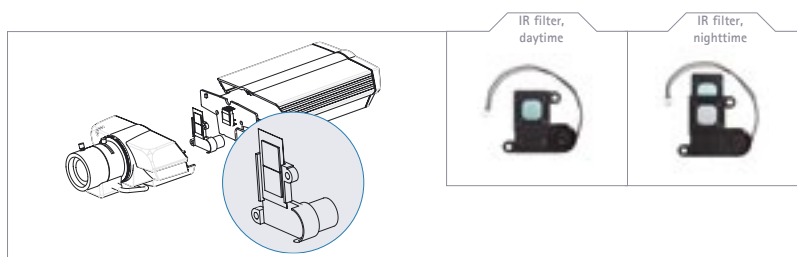
Light is a form of radiation wave energy that exists in a spectrum. The human eye can see, however, only a portion (between wavelengths of $\sim 400 - 700$ nanometers or nm). Below blue, just outside the range humans can see, is ultraviolet light, and above red is infrared light.



Infrared energy (light) is emitted by all objects: humans, animals and grass, for instance. Warmer objects such as people and animals stand out from typically cooler backgrounds. In low light conditions, for example at night, the human eye cannot perceive color and hue - only black, white and shades of gray.

How does the day and night functionality or IR-cut filter work?

While the human eye can only register light between the blue and red spectrum, a color camera's image sensor can detect more. The image sensor can sense long-wave infrared radiation and thus "see" infrared light up to 1000 nm. Allowing infrared to hit the image sensor during daylight, however, will distort colors as humans see them. This is why all color cameras are equipped with an IR-cut filter - an optical piece of glass that is placed between the lens and the image sensor - to remove IR light and to render color images that humans are used to.



As illumination is reduced and the image darkens, the IR-cut filter in a day and night camera can be removed automatically* to enable the camera to make use of IR light so that it can "see" even in a very dark environment. To avoid color distortions, the camera often switches to black and white mode, and is thus able to generate high quality black and white images. The IR-cut filter in Axis' day and night cameras can also be removed manually via the cameras' interface.

**The ability to automatically place or remove the IR cut filter in front of a camera's image sensor depends on the make of the camera.*

Camera considerations



Some basic rules apply when seeking to maximize the performance of a network video system. This chapter deals with some of these rules, in particular the choice of camera components, the positioning and installation of the camera, and factors to take into account in order to achieve the best possible image quality and detail, both indoors and outdoors. This chapter also covers best practice examples for installations which involve analog video equipment used in combination with network video.

4.1. Using network cameras

4.1.1 Camera types

If the video surveillance system to be installed is a new system, and no analog cameras exist, the best choice in most cases is to use network cameras, which are available in many different models to suit a wide variety of needs.

With such a wide variety of network cameras available today, most requirements across all vertical markets and system sizes can be accommodated. As with analog cameras, network cameras come in different models.



Fixed network cameras

Fixed cameras with a body and a lens represent the traditional camera type. In some applications it is advantageous to make the camera very visible. If this is the case then a fixed camera represents the best choice, since the camera is clearly visible, as is the direction in which it is pointing. Another advantage is that most fixed cameras have exchangeable lenses of C/CS type. For further protection fixed cameras can be installed in housings designed for indoor or outdoor installation.



Fixed dome network cameras

Fixed dome cameras, also called mini domes, essentially consist of a fixed camera pre-installed in a small dome housing. The camera can be easily directed to point in any direction. Its main benefit lies in its discreet, non-obtrusive design, as well as in the fact that it is hard to see in which direction the camera is pointing. One of the limitations is that fixed dome cameras rarely have exchangeable lenses, and even if they offer a choice of lenses, exchange opportunities are limited by the space inside the dome housing.



PTZ network cameras

Pan Tilt Zoom (PTZ) cameras have the obvious benefit of being able to pan, tilt and zoom either manually or automatically. For manual operation, a PTZ camera can, for example, be used to follow a person in a retail store. PTZ cameras are mainly used indoors and where it is desirable that the direction in which the camera is pointing can be seen. Most PTZ cameras do not have full 360 degrees pan, and are not made for continuous automatic operation, so called 'guard tours'. The optical zoom ranges from 18x to 26x.



Network dome cameras

Network dome cameras share the same benefits as the fixed dome cameras: they are fairly discreet and the direction in which they are pointing cannot be determined when looking at the camera. A network dome camera, compared to a PTZ camera, adds the ability to pan 360 degrees. It also provides mechanical robustness for continuous operation in guard tours where the camera continuously moves between say 10 presets, day in and day out. With guard tours, one camera can cover an area where 10 fixed cameras would be needed to do the same job. The main drawback is that only one location is monitored at any given time, leaving the other 9 positions un-monitored. The optical zoom normally ranges between 18x and 30x. But for installations outdoors, zoom factors above 20x normally prove impractical because of vibration and motion caused by wind.

Non-mechanical PTZ network cameras

With the introduction of network cameras, a new breed of PTZ cameras are being introduced to the market – the so-called non-mechanical PTZs. Using a megapixel sensor, the camera can cover from 140 to 360 degrees and the operator can select to pan, tilt and zoom the camera in any direction without involving any mechanical movement. The key advantage is that there is no wear and tear on moving parts. It also offers immediate movement to a new position, which in a traditional PTZ camera can take up to 1 second. The best non mechanical PTZ cameras today are using a 3 megapixel sensor. In order to ensure a good image quality, pan and tilt should be limited to 140 degrees and zoom to 3x. For higher coverage or zoom the image quality will adversely be affected.

A number of variations of the camera types described above are available, and include:

- Vandal resistant versions, depending on the protective housing used
- Weather resistant versions, depending on the protective housing used
- Day and Night versions, which means that the camera can automatically or manually switch between day mode with color video, and night mode with black and white low light image that can be enhanced by using IR illuminators. *See section 3.5, page 26.*

Once the camera is selected, the next step is to select the appropriate lenses, housings, and any other relevant components necessary in the system. The installer should also be aware of a number of common practices related to camera positioning, which will help in obtaining the best quality out of the system.

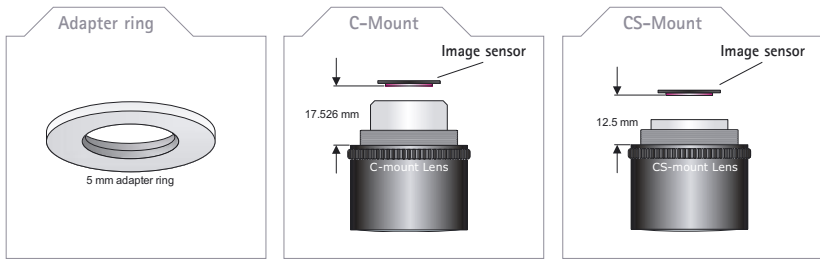
4.1.2. Lens selection

C-Mount and CS-Mount lenses

There are two main lens mount standards, called C-mount and CS-mount. They both have a 1" thread and they look the same. What differs is the distance from the lenses to the sensor when fitted on the camera:

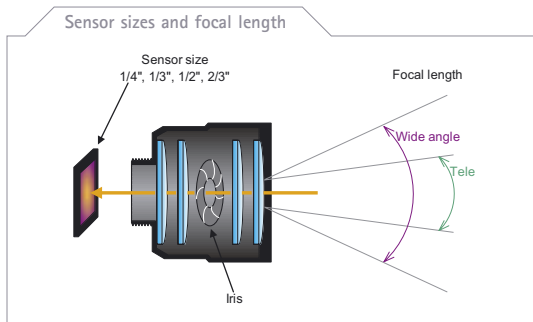
- CS-mount. The distance between the sensor and the lens should be 12.5 mm
- C-mount. The distance between the sensor and the lens should be 17.526 mm. A 5 mm spacer (C/CS adapter ring) can be used to convert a C-mount lens to a CS mount lens.

The initial standard was C-mount, while CS-mount is an update to this, allowing for reduced manufacturing cost and sensor size. Today, almost all cameras and lenses sold are equipped with a CS-mount. It is possible to mount an old C-mount lens to a camera with CS-mount by using a C/CS adapter ring. If it is impossible to focus a camera, you probably have the wrong type of lens.

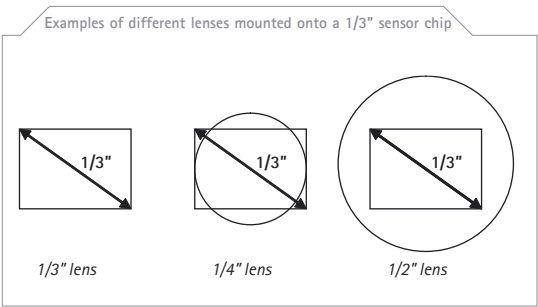


Sensor size

Image sensors are available in different sizes, such as $2/3"$, $1/2"$, $1/3"$ and $1/4"$, and lenses are manufactured to match these sizes. It is important to select a lens suitable for the camera. A lens made for a $1/2"$ sensor will work with $1/2"$, $1/3"$ and $1/4"$ sensors, but not with a $2/3"$ sensor.



If a lens is made for a smaller sensor than the one actually fitted inside the camera, the image will get black corners. If a lens is made for a larger sensor than the one actually fitted inside the camera, the angle of view will be smaller than the default angle of that lens – part of the information being “lost” outside of the chip (see illustration on next page).



Focal length requirements

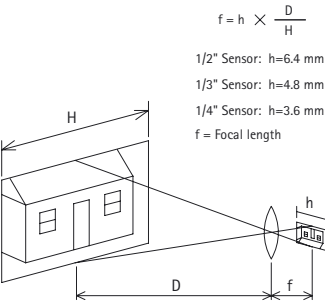
Focal length determines the horizontal field of view at particular distances – the longer the focal length, the narrower the field of view.

Lens and sensor size	1/2"	1/3"	1/4"
Focal length	12 mm	8 mm	6 mm

Examples of focal length needed to achieve an approximate 30° horizontal field of view

Most manufacturers provide simple-to-use slide and rotary calculators that calculate the lens focal length from the scene size and focal length.

To detect the presence of someone on a display, they should make up at least 10 per cent of the height of the image. To accurately identify them they should make up 30 per cent or more of the image. For this reason, it is important to check the capabilities of selected cameras and view resulting images on screen before going live.



Calculation - feet

What width of objects will be visible at 10 feet when using a camera with a 1/4" CCD sensor and a 4 mm lens?

$H = D \times h / f = 10 \times 3.6 / 4 = 9 \text{ feet}$

Calculation - meters

What width of objects will be visible at 3 meters when using a camera with a 1/4" CCD sensor and a 4 mm lens?

$H = D \times h / f = 3 \times 3.6 / 4 = 2.7 \text{ meters}$

Lens types

■ Fixed lens

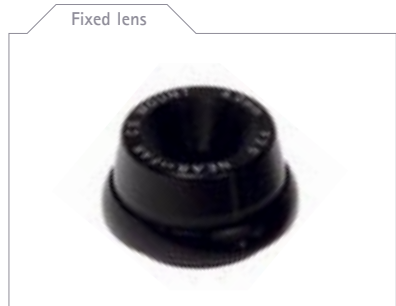
The focal length is fixed, e.g. 4 mm

■ Varifocal lens

This lens allows for the manual adjustment of the focal length (field of view). When the focal length is changed, the lens has to be refocused. The most common type is 3.5–8 mm

■ Zoom lens

The focal length can be adjusted within a range, e.g. 6 to 48 mm without affecting the focus. The lens can either be manual or motorized, so that it can be controlled remotely.



Iris

Generally network cameras control the amount of light passing to the imaging device via the iris or by adjusting the exposure time. In conventional cameras, exposure time is fixed. The role of the iris is to adjust the amount of light passing through the lens. There are different types of irises on lenses:

■ Manual iris control

The iris on a manual iris lens is usually set up when the camera is installed to suit the prevailing lighting conditions. These lenses cannot react to changes in scene illumination so the iris is set to an “average” value, which is used in conditions with varying light.

■ Automatic iris control

For outdoor conditions, and where the scene illumination is constantly changing, a lens with automatically adjustable iris is preferred. The iris aperture is controlled by the camera and is constantly changed to maintain the optimum light level to the image sensor.

- DC-controlled Iris: Connected to the output of a camera, the iris is controlled by the camera's processor
- Video-controlled Iris: The iris is controlled by video signal

Auto iris lenses are recommended for outdoor applications. The iris automatically adjusts the amount of light reaching the camera and gives best results, as well as protecting the image sensor from too much light. A small iris diameter reduces the amount of light, giving a better depth of field (focus over a greater distance). A large iris diameter, on the other hand, gives better images in low light. The iris is defined by the F-number.

F-number = Focal length / Iris diameter

The F-number of a lens is the ratio of the focal length to the effective object lens diameter. It affects the amount of light energy admitted to the sensor and plays a significant part in the resulting image.

The greater the F-number, the less light admitted to the sensor. The smaller the F-number, the more light admitted to the sensor, and hence better image quality is achieved in low-light situations. The table below shows the amount of light admitted to the image sensor at sample F-values.

F-number	f1.0	f1.2	f1.4	f1.7	f2.8	f4.0	f5.6
% of light passed	20%	14.14%	10%	7.07%	2.5%	1.25%	0.625%

In scenes with limited light, fitting a neutral density filter in the front of the lens is recommended. This works to reduce the amount of light entering the lens evenly over the whole visible spectrum and forces the iris to open fully to compensate for this. Many network cameras today offer automatic iris control to ensure that the image remains clear throughout the year and time of day as light levels constantly change.

4.1.3. Indoor and outdoor installations

Camera housings

If a camera is to be mounted outdoors or in relatively hostile environments, it needs a weatherproof or vandal-proof housing to protect it. Camera housings come in different sizes and qualities and some versions have built-in fans for cooling and/or heaters.



A full list of available housings for mounting Axis network cameras outdoors and within harsh, humid and dusty environments is available at www.axis.com/products/cam_housing/

4.1.4. Best practices

To obtain high-quality images from a camera, a few basic rules apply. These are equally applicable to network cameras as to any other type of camera. Some simple tips for capturing good images:

■ Use lots of light

The most common reason for poor quality images is a lack of light. Generally, the more light, the better the images. With too little light, the images will become blurred and dull in color. Professional photographers always use strong lamps. Lux is the standard unit for measurement of the amount of light. At least 200 Lux is needed to capture good quality images. A high-quality camera might be specified to work down to 1 Lux. This means an image can be captured at 1 Lux, but not that it will be a good image. Different manufacturers use different references when they specify the light sensitivity, which makes it hard to compare cameras without looking at captured images.

Environment	Lux
Strong sunlight	100,000
Full daylight	10,000
Normal office light	500
Poorly lit room	100

■ Avoid backlight

Bright areas in the images should be avoided. Bright images might become overexposed (bright white) and objects can then appear too dark. This problem typically occurs when attempting to capture an object from behind a window.

■ Reduce the contrast

A camera adjusts the exposure to obtain an average level of light in the image. When trying to capture an image of a person standing in front of a white wall, the person generally tends to appear too dark. This problem is easily solved by substituting the background color for gray instead of white.

Recommendations for mounting a camera outdoors

■ Lenses

An auto iris lens should always be used for outdoor applications. An auto iris lens automatically adjusts the amount of light that reaches the image sensor. This optimizes the image quality and protects the image sensor from being damaged by strong sunlight.

■ Direct sunlight

Important! Direct sunlight should always be avoided in an image. Direct sunlight will "blind" the camera and permanently bleach the small color filters on the sensor chip. If possible, the camera should be positioned facing the same direction as the sun.

■ Contrast

Viewing too much of the sky results in too much contrast. The camera will adjust in order to achieve a proper light level for the sky. Consequently, the object/landscape of interest will appear too dark. One way to solve this problem is to mount the camera high above the ground; using a pole if needed. Sturdy mounting equipment should always be used to avoid vibrations caused by strong wind.

■ Reflections

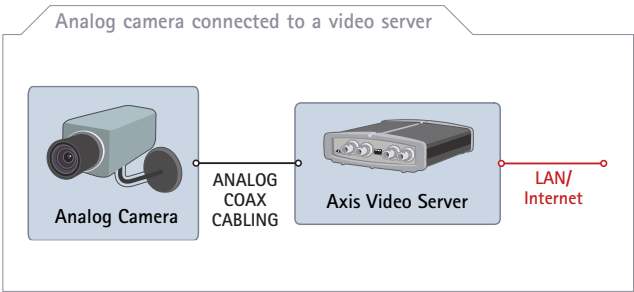
If the camera is mounted behind a glass, such as in a housing, the lens must be placed close to the glass. Otherwise, reflections from the camera and the background will appear in the image. To reduce reflection, special coatings can be applied on any glass used in front of the lens.

■ Lighting

When using cameras at night, additional external lighting may be required. This should be arranged to avoid any reflections and/or shadows. For covert security, Infrared (IR) illuminators can be used instead of normal lighting, known as "white light". IR light is imperceptible, which means that while it is sufficient for capturing images from IR cameras, it is not visible to the human eye. It is possible to connect IR-sensitive network cameras directly to the network, or to connect traditional IR-sensitive cameras to a network via a video server. *Note: Color cameras do not work with IR light. Some cameras are able to automatically switch between a daylight color mode and an IR mode useful in night vision where the image will then appear without colors. Read more about Day and Night functionality in chapter 3.5, page 26.*

4.2. Using analog cameras with video servers

Analog cameras of all types, such as fixed, dome, indoor, outdoor, fixed dome, pan/tilt/zoom, as well as specialty cameras, can all be integrated in a network video system using video servers. The coax cable from the analog camera is simply connected to the analog input on the video server, which then digitizes, compresses, and transmits the video over a local network or across the Internet. Once the video is on the network, it is identical to a video stream coming from a network camera, and ready to be integrated into network video systems. Simply put – a video server turns an analog camera into a network camera.

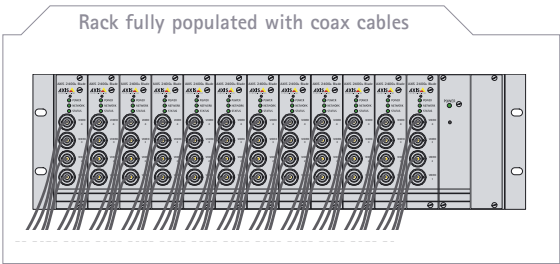


Depending on the configuration, number of cameras, camera type, and whether or not coax cabling is installed, different types of video servers can be used.

4.2.1. Rack-mounted video servers

Most companies use a dedicated control room in order to centralize equipment to one location and efficiently monitor operations in a safe and secure environment for critical information. In a building containing a large number of analog cameras, this means that vast amounts of coax cabling run to the control room.

If all coax cabling has already been installed and is available from the central room, the installation would benefit from using a video server rack which allows for a great number of blade video servers to be placed in one rack and managed centrally. The rack contains slots for up to 12 interchangeable blade video servers and provides network, serial communication and I/O connectors at the rear of each slot, as well as a common power supply. One 3U 19-inch rack can typically fit up to 48 channels with full frame rate, providing a high density solution, saving valuable rack space.



4.2.2. Standalone video servers

In a video surveillance system where investments have been made in analog cameras but coaxial cabling has not yet been installed, it is beneficial to connect a standalone video server close to analog cameras in the system. In addition to the reduced cost of the cabling to transport the video, this adds the benefit of not having reduced image quality over longer distances, which is the case with coax cabling deteriorating image quality with increased distances. A video server produces digital images, so there is no quality reduction due to distance.

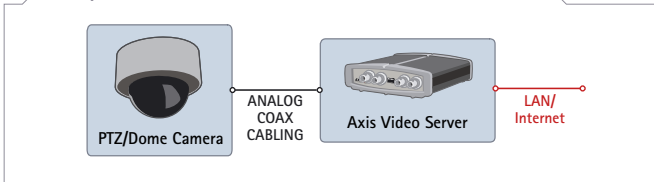
Housing with analog camera and video server installed



4.2.3. Video servers with PTZ and dome cameras

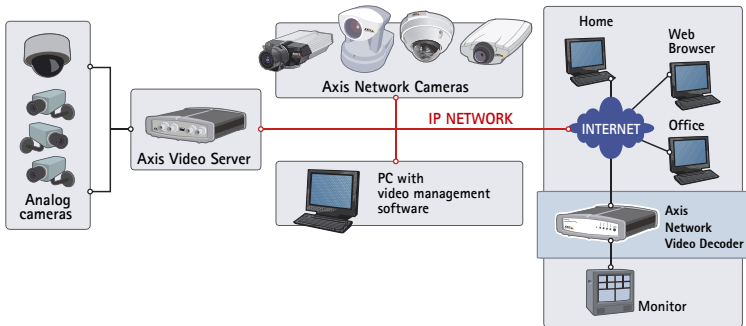
PTZ cameras can be connected to standalone video servers as well as rack-mounted video servers, using the serial port (RS232/422/485) built into the video servers. In the scenario when a single port video server is used and located close to the camera, it adds the benefit of not having to run separate serial wiring to control the PTZ mechanism. It also adds the capability of performing PTZ control over large distances using the Internet. A specific driver must be available in the video server to control a specific PTZ camera. In an Axis video server, PTZ drivers for most popular PTZ and dome cameras are available and can be uploaded to the video server. A driver located on the PC running the video management software, can also be used if the serial port is set up as a serial server, which just passes through the commands.

PTZ/Dome camera connected to an Axis Video Server



4.2.4. Video decoder

In some installations, there is a need to monitor the network video and audio streams on existing analog monitoring equipment. By using a network video decoder, the network video and audio streams are converted back to analog signals that can then be used by regular TV sets, analog monitors and video switches. Using an encoder/decoder is a very cost-effective way to transport analog video over a long distance (analog – digital – analog).



With a network video decoder, existing analog monitors can be used to receive video and audio from distant analog cameras or systems as though they were placed locally with the operator – even though they might be located in a different city.

IP Network technologies



The Internet Protocol (IP) is the most widely used computer communication protocol today. It is the base protocol used for Internet, communication such as e-mail, web and multimedia. One of the reasons for its popularity is its scalability. In other words, it works as well in very small installations as it does in very large ones and is supported by an increasingly wide range of high-performance, low-cost and industry-proven equipment and technologies.

This chapter provides an overview of the different technologies in use, based on IP, to take full advantage of a network video system.

5.1. Ethernet

In today's offices, computers are most likely to be using TCP/IP connected via an Ethernet network. Ethernet gives a fast network at a reasonable cost. Most modern computers are supplied with an integrated Ethernet interface or can easily accommodate an Ethernet network interface card (NIC).

Common Ethernet types:

10 Mbit/s (10 Mbps) Ethernet

This standard is rarely used in production networks today due to its low capacity, and has been replaced by 100 Mbit/s Ethernet since the late 90's. The most common topology used for 10 Mbit/s Ethernet was called 10BASE-T; it uses 4 wires (two twisted pairs) on a cat-3 or cat-5 cable. A hub or switch sits in the center and has a port for each node. The same configuration is used for Fast Ethernet and Gigabit Ethernet.

Fast Ethernet (100 Mbit/s)

Supporting data transfer rates of up to 100 Mbit/s, Fast Ethernet is the most common Ethernet type used in computer networks today. The main standard is called 100BASE-T. Although newer and faster than 10 Mbit Ethernet, in all other respects it is the same. The 100BASE-T standard can be subdivided into:

- 100BASE-TX: Uses twisted pair copper cabling (cat-5).
- 100BASE-FX: 100 Mbit/s Ethernet over optical fiber.

Note: most 100 Mbit network switches support both 10 and 100 Mbit to ensure backward compatibility (commonly called 10/100 network switch).

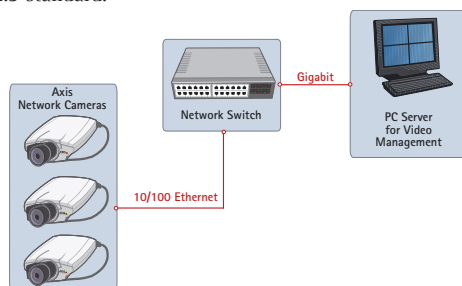
Gigabit Ethernet (1000 Mbit/s)

This is the current standard that is being endorsed for desktop computers by networking equipment vendors. The most common use today is however for backbones in between network servers and network switches. 1000 Mbit/s is widely used and it can be subdivided into:

- 1000BASE-T: 1 Gbit/s over cat-5e or cat-6 copper cabling.
- 1000BASE-SX: 1 Gbit/s over multi-mode fiber (up to 550m).
- 1000BASE-LX: 1 Gbit/s over multi-mode fiber (up to 550m). Optimized for longer distances (up to 10km) over single-mode fiber.
- 1000BASE-LH: 1 Gbit/s over single-mode fiber (up to 100km). A long-distance solution.

10 Gigabit Ethernet (10 000 Mbit/s)

This is viewed as the new choice for backbone in enterprise networks. The 10 Gigabit Ethernet standard uses seven different media types for LAN, WAN and MAN (Metropolitan Area Network). It is currently specified by a supplementary standard, IEEE 802.3ae, and will be incorporated into a future revision of the IEEE 802.3 standard.



5.2. Power over Ethernet

Power over Ethernet (PoE) is a technology that integrates power into a standard LAN infrastructure. It enables power to be provided to the network device, such as an IP phone or a network camera, using the same cable as that used for network connection. It eliminates the need for power outlets at the camera locations and enables easier application of uninterruptible power supplies (UPS) to ensure 24 hours a day, 7 days a week operation.

PoE technology is regulated in a standard called IEEE 802.3af and is designed in a way that does not degrade the network data communication performance or decrease the network reach. The power delivered over the LAN infrastructure is automatically activated when a compatible terminal is identified, and blocked to legacy devices that are not compatible. This feature allows users to freely and safely mix legacy and PoE-compatible devices, on their network.

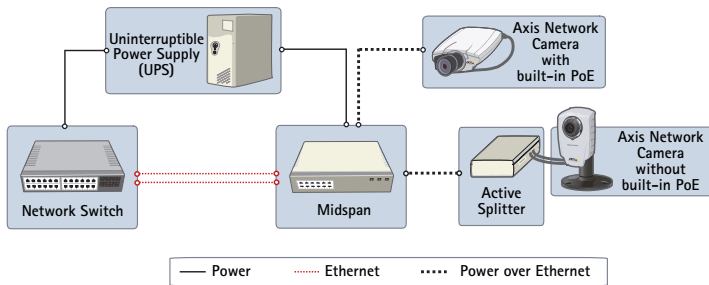
The standard provides power up to 15.4W on the switch or midspan side, which translates to a maximum power consumption of 12.9W on the device/camera side – making it suitable for indoor cameras. Outdoor cameras as well as PTZ and dome cameras have a power consumption that normally exceeds this, making PoE functionality less suitable. Some manufacturers also offer non-standard proprietary products providing suitable power for these applications as well,

but it should be noted that since these are non-standard products, no interoperability between different brands is possible. The 802.3af standard also provides support for so-called power classification, which allows for a negotiation of power consumption between the PoE unit and the devices. This means an intelligent switch can reserve sufficient, and not superfluous, power for the device (camera) – with the possible result that the switch could enable more PoE outputs.

Using Power over Ethernet

PoE works across standard network cabling (i.e. cat-5) to supply power directly from the data ports to which networked devices are connected. Today, most manufacturers offer network switches with built-in PoE support. If an existing network /switch structure is in place, customers can benefit from the same functionality by adding a so-called Midspan to the switch, which will add power to the network cable. All network cameras without built-in PoE can be integrated in a PoE system using an Active Splitter.

The following diagram shows how a network camera can receive power over a network cable and can continue to function even when there is a power failure.



5.3. Wireless networks

Even if wired networks are present in most buildings today, sometimes a non-wired solution holds substantial value to the user, financially as well as functionally. For example it could be useful in a classified building, where the installation of cables would not be possible without damaging the interior, or within a facility where there is a need to move the camera to new locations on a regular basis without having to pull new cables every time, like in retail. Another common use of wireless technology is to bridge two buildings or sites together without the need for expensive and complex ground works.

Wireless technology exists both for analog and network video systems – therefore going beyond the networking perimeter. There are two major categories for wireless communications:

- **Wireless LAN (also known as WLAN):**

A LAN is by definition a Local Area Network, i.e. over short distances and normally indoors. Nowadays, the wireless LAN standards are well defined and devices from different vendors work well together.

- **Wireless bridges**

When it is necessary to connect buildings or sites with high speed links, a point-to-point data link capable of long distances and high speeds is required. Two commonly used technologies are microwave and laser.

Wireless LAN standards

802.11a

Standard using the 5GHz band providing up to ~24 Mbps actual throughput at up to 30m/100feet in outdoor environments. Limited range of products supporting it. Theoretical bandwidth is 54Mbps.

802.11b

Standard providing up to ~5 Mbps actual throughput at up to 100m/300feet in outdoor environments. It uses the 2.4GHz band. Theoretical bandwidth is 11Mbps.

802.11g

The most commonly used standard providing improved performance compared to 802.11b. Up to ~24Mbps actual throughput at up to 100m/300feet in outdoor environments. It uses the 2.4GHz band. Theoretical bandwidth is 54Mbps.

802.11n

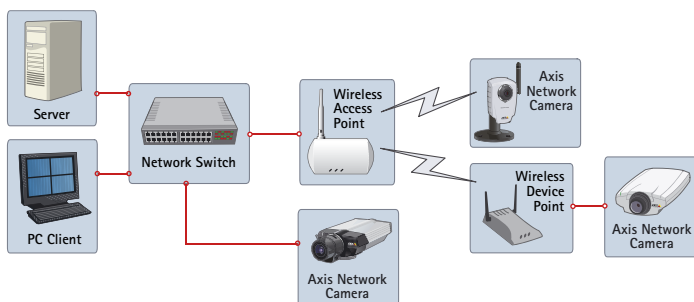
Next generation of the 802.11 Wireless LAN standard. The actual throughput will be in excess of 100Mbps.

Broadband wireless access

802.16 - WiMAX

IEEE 802.16, also known as WiMAX, is a specification for fixed broadband wireless metropolitan access networks (MANs) that use a point-to-multipoint architecture. The standard defines the use of bandwidth between the licensed 10GHz and 66GHz and sub 11GHz frequency ranges. 802.16 supports very high bit rates in both uploading to and downloading from a base station up to a distance of 50km/30 miles to handle such services as VoIP (Voice over IP).

Typical network including both wireless and wired connections



This diagram illustrates a common use of wireless technologies:

- The center point here is the network switch. To the left, a server (top) and a PC client (bottom), are connected using wired Ethernet. Next to the switch, there is a wireless access point. This device manages all the wireless devices within range.
- Two wireless devices are represented on this diagram:
 - The AXIS 207W Network Camera. This camera has built-in support for wireless communications.
 - A wireless device point. This device provides wireless communication and connects directly to the wireless access point.

It is also possible to connect the server and the PC wirelessly. But as the wireless network bandwidth is limited compared to the wired one, the goal should always be to use wired networks whenever possible.

About security in wireless networks

Due to the nature of wireless communications, everyone with a wireless device present within the area covered by the network is able to participate in the network and use shared services, hence the need for security.

Please refer to section 5.5.2, page 47, for further information about security in wireless networks.

Wireless bridges

Some solutions may also use other standards than the dominating 802.11 standard, providing increased performance and much longer distances in combination with very high security. This also includes the use of other means of Radio Frequency, such as microwave links. Another common technology is optical systems such as laser links. A microwave link can provide up to 1000Mbps for distances up to 80km/130miles. For locations outside the range of all these systems, there is also the option of satellite communication. Due to the way this system operates, transmitting up to a satellite and back down to earth, the latency can be very long (up to several seconds). This makes it less suitable for functions like manual dome control and video conferencing where low latency is preferred. If larger bandwidth is required, the use of satellite systems also becomes very costly.

5.4. Data transport methods



5.4.1. IP addresses

An IP address (Internet Protocol address) is a unique number that devices use in order to identify and communicate with each other on a network utilizing the Internet Protocol standard. An IP address consists of four numbers separated by a dot “.”, each number is in the range 0-255. For example, the address could be “192.36.253.80”.

The IP address is further split up into a network part and a host part. The boundary between the two parts is decided by a netmask or a prefix length. A netmask of 255.255.255.0 means that the first 3 bytes will be the network address and the last byte the host address. A prefix length is a different way of providing the boundary, for example the same address as the previous example has a prefix length of 24 bits (i.e. 192.36.253.80/24).

Certain blocks of addresses have been reserved for private use:

10.0.0.0/8	(netmask 255.0.0.0)
172.16.0.0/12	(netmask 255.240.0.0)
192.168.0.0/16	(netmask 255.255.0.0)

These addresses are intended for private internets. They may not be routed out on the public Internet.

5.4.2. IPv6

IPv6, or Internet Protocol version 6, is designed as an evolutionary upgrade to the Internet Protocol and will, in fact, coexist with the older IPv4 for some time. IPv6 is designed to allow the Internet to grow steadily, both in terms of the number of hosts connected and the total amount of data traffic transmitted.

The most obvious improvement in IPv6 over the IPv4 is that IP addresses are lengthened from 32 bits to 128 bits. This extension anticipates considerable future growth of the Internet, providing for an unlimited (for all intents and purposes) number of networks and systems. For instance, IPv6 is intended to provide each cell phone and mobile electronic device its own address.

5.4.3. Data transport protocols for network video

The most common protocol for transmitting data on computer networks today is the TCP/IP Protocol suite. TCP/IP acts as a “carrier” for many other protocols – A good example is HTTP (Hyper Text Transfer Protocol) used to browse web pages on servers around the world using the Internet.

TCP/IP protocols and ports used for network video

Common protocols and their port numbers used for the transfer of network video include:

Protocol	Transport Protocol	Port	Common usage	Network video usage
FTP File Transfer Protocol	TCP	21	Transfer of files over the Internet/intranets	Transfer of images or video from network camera/video server to a FTP server or to an application
SMTP Send Mail Transfer Protocol	TCP	25	Protocol for sending e-mail messages	A network camera/video server can send images or alarm notifications using its built-in e-mail client
HTTP Hyper Text Transfer Protocol	TCP	80	Used to browse the web, i.e to retrieve web pages from web servers	The most common way to transfer video from a network camera/video server where the network video device essentially works as a web server making the video available for the requesting user or application server
HTTPS Hypertext Transfer Protocol over Secure Socket Layer	TCP	443	Used to access web pages securely using encryption technology	Secure transmission of video from network cameras/video servers can also be used to authenticate the sending camera using X.509 digital certificates
RTP Real Time Protocol	UDP/TCP	Not defined	RTP standardized packet format for delivering audio and video over the Internet. Often used in streaming media systems or videoconferencing	A common way of transmitting MPEG based network video Transmission can be either unicast (one to one) or multicast (one to many)
RTSP Real Time Streaming Protocol	TCP	554	Used to setup and control multimedia sessions over RTP	

The TCP/IP protocol suite's most used transport protocols are the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP). TCP provides a reliable, connection-based transmission channel; it handles the process of breaking large chunks of data into smaller packets, suitable for the physical network being used, and ensures that data sent from one end is received on the other. UDP, on the other hand, is a connectionless protocol and does not guarantee the delivery of data sent, thus leaving the whole control mechanism and error-checking to the application itself.

In general TCP is used when reliable communication is preferred over transport latency. TCP's reliability through retransmission may introduce significant delays. UDP on the other hand provides no retransmissions of lost data and therefore does not introduce further delays.

5.4.4. Transmission methods for network video: Unicasting, Multicasting, and Broadcasting

There are different methods for transmitting data on a computer network:

- *Unicast* - the sender and the recipient communicate on a point-to-point basis. Data packets are sent addressed solely to one recipient and no other computers on the network will need to process this information.
- *Multicast* - communication between a single sender and multiple receivers on a network. Multicast technologies are used to reduce network traffic when many receivers want to view the same source simultaneously, by delivering a single stream of information to hundreds of recipients. The biggest difference compared with unicasting is that the video stream only needs to be sent once. Multicasting (i.e IP-Multicasting) is commonly used in conjunction with RTP transmissions.
- *Broadcast* - a one-to-everybody transmission. On a LAN, broadcasts are normally restricted to a specific network segment and are not in practical use for network video transmissions.

5.5. Network security



There are several ways to provide security within a wired or wireless network and between different networks and clients. Everything, from the data sent over the network to the actual use and accessibility of the network, can be controlled and secured.

5.5.1. Secure transmission

Providing secure transmission of data is like using a courier to bring a valuable and sensitive document from one person to another. When the courier arrives to the sender, he would normally be asked to prove his identity. Once this is done, the sender would decide if he is the one he claims to be, and if he can be trusted. If everything seems to be correct, the locked and sealed briefcase would be handed over to him, and he would deliver it to the receiver. At the receiver, the same identification procedure would take place, and the seal would be verified as “unbroken”. Once the courier had left, the receiver would unlock the briefcase and take out the document to read it.

A secure communication is created in the same way, and is divided into three different steps:

Authentication

This initial step is for the user or device to identify itself to the network and the remote end. This is done by providing some kind of identity to the network/system, like a username and password, an X509 (SSL) certificate, and using the 802.1x standard.

Authorization

The next step is to have this authentication authorized and accepted, that is verifying whether the device is the one it claims to be. This is done by verifying the provided identity within a database or list of correct and approved identities. Once the authorization is completed, the device is fully connected and operational in the system.

A closer look at IEEE 802.1x authentication

Pushed by the wireless community looking for stronger security methods, the 802.1x standard is among the most popular authentication methods in use today: IEEE 802.1X provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails.

How it works

Clients and servers in an 802.1x network authenticate each other with the help of digital certificates provided by a Certification Authority. These are then validated by a third-party entity, such as an authentication server called a RADIUS server, one example of which is Microsoft Internet Authentication Service.

The Axis network video device presents its certificate to the network switch, which in turn forwards it to the RADIUS server. The RADIUS server validates or rejects the certificate and responds to the switch, which then allows or denies network access accordingly, on a preconfigured port.

This makes it possible to leave network sockets open and available: the access point will not connect you into the network until proper identity is provided.

Privacy

The final step is to apply the level of privacy required. This is done by encrypting the communication, which prevents others from using/reading the data. The use of encryption could provide a substantial decrease in performance, depending on the kind of implementation and encryption used.

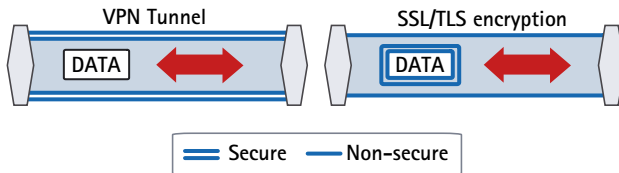
Privacy can be achieved in several ways. Two of the more commonly used methods are VPN and SSL/TLS (also known as HTTPS):

■ VPN (Virtual Private Network)

A VPN creates a secure tunnel between the points within the VPN. Only devices with the correct “key” will be able to work within the VPN. Network devices between the client and the server will not be able to access or view the data. With a VPN, different sites can be connected together over the Internet in a safe and secure way.

■ SSL/TLS

Another way to accomplish security is to apply encryption to the data itself. In this case there is no secure tunnel like with the VPN solution, but the actual data sent is secured. There are several different encryption techniques available, like SSL, WEP and WPA, the later two being used in wireless networks. When using SSL, also known as HTTPS, the device or computer will install a certificate into the unit, which can be issued locally by the user or by a third-party body such as Verisign.



5.5.2. Security in wireless networks

Due to the nature of wireless communications, everyone with a wireless device present within the area covered by the network is able to participate in the network and use shared services, hence the need for security.

WEP

WEP (Wireless Equivalent Privacy) adds RSA RC4-based encryption to the communication, and prevents people without the correct key to access the network.

The problem with WEP is that it has several flaws that make it vulnerable to attacks, therefore it is not able to provide basic levels of security. The main flaws in WEP are the static encryption key and the short initialization vector. Since it is easy to attack WEP with inexpensive off-the-shelf equipment, wireless networks should not rely on WEP for security.

WPA

WPA (WiFi Protected Access) resolves the main flaws with WEP. With WPA, the key is changed for every frame transmitted using Temporal Key Integrity Protocol (TKIP). The Initialization vector length is increased from 24 to 48 bits. WPA is considered as the base level of security for wireless networks.

For even higher security WPA2 should be used. WPA2 uses Advanced Encryption Standard (AES) instead of TKIP. AES is the best encryption available for wireless networks today. WPA2 also includes 802.1x authentication (see section about 802.1x).

5.5.3. Protecting single devices

Security also means protecting single devices against intrusions, such as unauthorized users trying to gain access to the unit, or viruses and similar unwanted items.

Access to PCs or other servers can be secured with user names and passwords, which should be at least 6 characters long (the longer the better), combining numbers and figures (mixing lower and upper cases). In the case of a PC, tools like finger scanners and smart cards can also be used to increase security and speed up the login process.

To secure a device against viruses, worms and other unwanted items, a virus scanner of good quality with up-to-date filters is recommended. This should be installed on all computers. Operating systems should be regularly updated with service packs and fixes from the manufacturer.

When connecting a LAN to the Internet, it is important to use a firewall. This serves as a gatekeeper, blocking or restricting traffic to and from the Internet. It can also be used to filter information passing the firewall or to restrict access to certain remote sites.

5.6. QoS (Quality of Service)

Nowadays, fundamentally different networks are merging into one IP network. For example, telephone and video (CCTV) networks are migrating towards IP. In these networks, you will need to control the way to share network resources to fulfill the requirements of each service. One solution is to let the network routers and switches behave differently on different kinds of services (voice, data, video) as the traffic passes through the network. This technique is called Differentiated Services (DiffServ). By using QoS, different network applications can co-exist on the same network, without consuming each other's bandwidth.

Definition

The term Quality of Service refers to a number of technologies to guarantee a certain quality to different services on the network. Quality can be, for instance, a maintained level of bandwidth, low latency, no packet losses, etc. The main benefits of a QoS-aware network can be summarized as:

- The ability to prioritize traffic and thus allow critical flows to be served before flows with lesser priority.
- Greater reliability in the network, thanks to the control of the amount of bandwidth an application may use, and thus control over bandwidth races between applications.

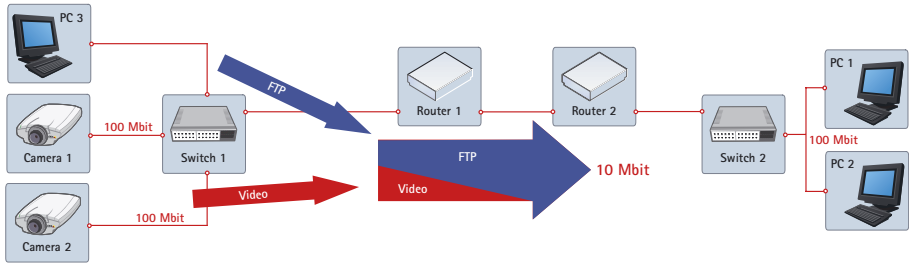
QoS and network video: requirements

To use QoS in a network with network video products, the following requirements must be met:

- All network switches and routers must include support for QoS. This is important to achieve end-to-end QoS functionality.
- The network video products must be QoS-enabled.

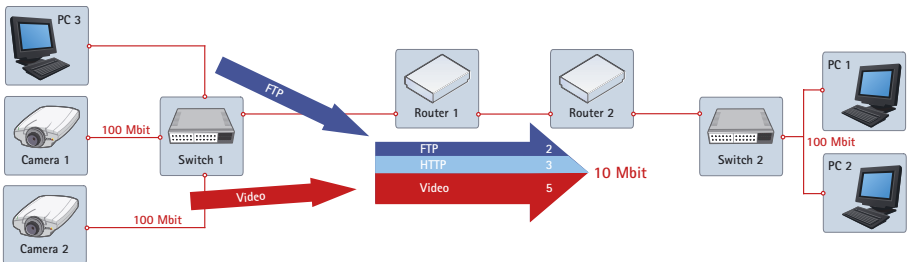
A QoS scenario

Figure 1: ordinary (non-QoS aware) network



In this example, PC1 is watching two video streams from cameras Camera 1 and Camera 2, with each camera streaming at 2.5 Mbps. Suddenly, PC2 starts a file transfer from PC3. In this scenario, the file transfer will try to use the full 10 Mbps capacity between the routers 1 and 2, whilst the video streams will try to maintain their total of 5 Mbps. The amount of bandwidth given to the surveillance system can no longer be guaranteed and the video frame rate will probably be reduced. At worst, the FTP traffic will consume all the available bandwidth.

Figure 2: QoS aware network



The router 1 has been configured to devote up to 5 Mbps of the available 10 Mbps for streaming video. FTP traffic is allowed to use 2 Mbps, and HTTP and all other traffic can use a maximum of 3 Mbps. Using this division, video streams will always have the necessary bandwidth available. File transfers are considered less important and get less bandwidth, but there will still be bandwidth available for web browsing and other traffic. Note that these maximums only apply when there is congestion on the network. If there is unused bandwidth available, this can be used by any type of traffic.

About Pan Tilt Zoom (PTZ) traffic

PTZ traffic is often regarded as critical and requires low latency to guarantee fast responses to movement requests. This is a typical case in which QoS can be used to provide the necessary guarantees. The QoS control of PTZ traffic in Axis network video products is handled by the ActiveX viewer AXIS Media Control (AMC), which is automatically installed the first time the Axis product is accessed from Microsoft Internet Explorer.

5.7. More about network technologies and devices

Hubs, switches and bridges

These devices are essentially used as connection boxes to allow several pieces of equipment to share a single Ethernet connection. Usually 5-24 devices can be connected to one hub. If more devices are used, another hub can be added. To speed up the network, you can use switched hubs that allow several data packets to be transmitted simultaneously.

Gateways and routers

Gateways and Routers are essentially packet forwarders that operate at layer 3 (i.e. the IP layer). Forwarding decisions are made based on IP addresses and IP routing tables. A gateway makes it possible to connect two networks of different technologies into one network. For example, an Ethernet network can be connected with a Token-Ring network.

NAT routers

All devices connecting directly to the Internet must have a unique public IP address. Public IP addresses are sold by Internet Service Providers (ISPs). A device called a Network Address Translator (NAT) makes it possible to connect a LAN with private addresses to the Internet by translating internal private addresses into public addresses.

Gateways

Gateways provide a convenient way to create a local network. A gateway works as a combined router, switch and NAT and is available from many manufacturers.

DHCP servers

It takes time to manage the IP addresses for large numbers of devices on a network. To reduce this administration time and keep the number of IP addresses to a minimum, a DHCP server can be used. This type of server automatically issues network devices with IP addresses when they connect to the network.

Domain Name Servers

In larger networks a Domain Name Server (DNS) is included. This is literally a 'name' server. It associates and remembers given names to corresponding IP addresses. For example, a network camera monitoring a door is more easily remembered and accessed by the word 'door' than it is by its IP address, such as 192.36.253.80.

Firewall

A firewall is designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. For example, using firewalls,

one can make sure that video terminals are able to access the cameras while communication from other computers with the cameras will be blocked.

DDNS and dynamic IP addresses

Dynamic DNS is a method of keeping a domain name linked to a changing IP address as not all computers use static IP addresses. Typically, when a user connects to the Internet, the user's ISP assigns an unused IP address from a pool of IP addresses, and this address is used only for the duration of that specific connection. This method of dynamically assigning addresses extends the usable pool of available IP addresses. A dynamic DNS service provider uses a special program that runs on the user's computer, contacting the DNS service each time the IP address provided by the ISP changes and subsequently updating the DNS database to reflect the change in IP address. In this way, even though a domain name's IP address will change often, other users do not have to know the changed IP address in order to connect with the other computer.

In a network video application, a camera watching an entrance door is more easily remembered as "door.camera.axis.com" for instance. But when using DHCP, the camera's IP address may change over time. So a static mapping between "door.camera.axis.com" into the camera's IP address "192.36.253.80" may not be valid after a while. DDNS provides the solution: every time the camera changes IP address, it will contact the DNS server and update the mapping.

"Hi Mr. DNS server, I am door.camera.axis.com and I just got a new IP address 192.168.10.33. Please update my mapping."



SNMP

SNMP (Simple Network Management Protocol) is a set of protocols for managing complex networks – and for remotely controlling and managing network-attached devices.

IPSec

"IP Security" (IPSec) consists of a set of protocols to support secure exchange of packets at the IP layer. IPSec has been deployed widely to implement Virtual Private Networks (VPNs).

UPnP

Universal Plug and Play (UPnP) is a networking architecture that provides compatibility among networking equipment, software and peripherals of the 400+ vendors that are part of the Universal Plug and Play Forum. UPnP works with wired or wireless networks and can be supported on any operating system. Simply, it allows devices to connect seamlessly and to simplify the implementation of networks in the home and corporate environments.

UPnP is a common way for instance to discover network cameras. When you connect a camera for the first time, it may get an address from the DHCP server which you have no idea of what this address is. With UPnP you can search for camera devices and see them pop up.

For further information about network technologies and devices, please visit www.axis.com/products/video/about_networkvideo/

System Considerations



These days, video systems are no longer limited to recording and storing huge volumes of information passively (most of which is useless); they can actually evaluate a situation and take action accordingly.

With all these new capabilities, and the many methods available to manage video, it is key to consider your application needs and level of functionality. Once you have made an assessment of your needs, a number of factors should be taken into account to set up a system that takes advantage of the full potential of network video. These factors are explored below.

6.1. System design considerations

6.1.1. Bandwidth

Network video products utilize network bandwidth based on their configuration. Bandwidth usage depends on:

- Image resolution
- Compression ratio
- Frame rate
- Complexity of the scene

The following technologies are among those that enable management of bandwidth consumption:

- **Switched networks:** By using network switching—a common networking technique today—the same physical computer and video surveillance network can be separated into two autonomous networks. Even though these networks remain physically connected, the network switch logically divides them into two virtual and independent networks.
- **Faster networks:** As the price of switches and routers continues to fall, Gigabyte networks become an affordable option. The trend towards faster networks increases the potential value of remote monitoring over networks.

- **Event driven frame rate:** a rate of up to 25/30 fps on all cameras at all times is above the level required for many applications. With the configuration capabilities and built-in intelligence of the network camera/video server, frame rates under normal conditions can be set lower, e.g. 5-6 fps, dramatically decreasing bandwidth consumption. In the event of an alarm, if motion detection is triggered, the recording frame rate speed can automatically be increased. In many cases the camera will only send video over the network if the video is worth recording; the rest of the time nothing is being transferred.

Calculating bandwidth needs

A bandwidth calculator helps to determine the bandwidth a network video product will use, based on the image size and frame rate. It also calculates how much space a recorded image sequence would require.

Example of a network camera's bandwidth calculator



To calculate specific bandwidth needs, a bandwidth calculator is available from the Axis web site at www.axis.com/products/video/design_tool/

6.1.2. Storage

The emergence of network video systems calls for increased use of storage. This raises a number of questions, ranging from how much hard disk is needed to how to build a redundant storage system. The different methods of storage design are covered in section 6.4, page 61.

Calculating storage needs

Factors to consider when calculating storage needs:

- Number of cameras
- Number of hours per day the camera will be recording
- How long the data must be stored
- Motion detection (Event) only or continuous recording
- Other parameters such as frame rate, compression, image quality and complexity

Note that the calculation examples below are examples only and do not take into consideration any overhead or other technical issue that may result in a higher file size than mentioned below. The calculation example does not consider storage space for the operating system or video management software.

JPEG/Motion JPEG

For JPEG/Motion JPEG consisting of individual files, storage requirements vary by changing the frame rate, resolution and compression: Cameras 1, 2 and 3 in the table below have different storage requirements according to their fps (frames per second) and resolution settings.

Calculation:

Image size x frames per second x 3600s = KB per hour / 1000 = MB per hour

MB per hour x hours of operation per day / 1000 = GB per day

GB per day x requested period of storage = Storage need

Camera	Resolution	Image size (KB)	Frames per second	MB/hour	Hours of operation	GB/day
No. 1	CIF	13	5	234	8	1,9
No. 2	CIF	13	15	702	8	5,6
No. 3	4CIF	40	15	2160	12	26

Total for the 3 cameras and 30 days of storage = 1002 GB

MPEG-4

In MPEG-4, the images are part of a continuous data stream, i.e. not individual files. It is the bit rate - measuring the amount of video data transmitted - that determines the corresponding storage requirements. The bit rate is a result of specific frame rate, resolution and compression, as well as the level of motion in the scene.

Calculation:

Bit rate / 8(bits in a byte) x 3600s = KB per hour / 1000 = MB per hour

MB per hour x hours of operation per day / 1000 = GB per day

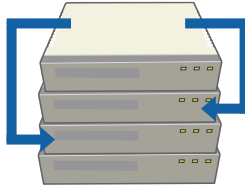
GB per day x requested period of storage = Storage need

Camera	Resolution	Bit Rate (kBit/s)	Frame per second	MB/hour	Hours of operation	GB/day
No. 1	CIF	170	5	76,5	8	0,6
No. 2	CIF	400	15	180	8	1,4
No. 3	4CIF	880	15	396	12	5

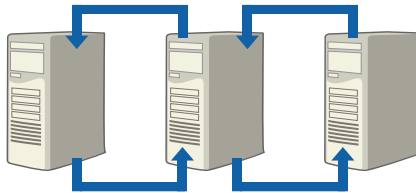
Total for the 3 cameras and 30 days of storage = 204 GB

6.1.3. Redundancy

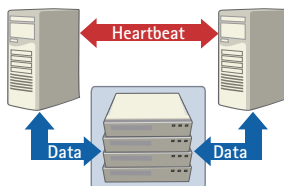
- **Hard disk RAID (Redundant Array of Independent Disks)** is essentially a method to span data over multiple hard disk drives with enough redundant data on all disks so that the data can be recovered from the remaining disks in case of a disk failure. *For further information about RAID storage, please refer to page 59.*



- **Data replication** is a common feature of many network operating systems: file servers in the network are configured to replicate data among each other.



- **Tape backup** is an alternative or complementing method. There is a variety of software and hardware equipment available on the market and backup policies normally include taking tapes off-site as prevention against fire or theft.
- **Server clustering:** Many server clustering methods exist, a common one for database servers and mail servers is when two servers are working with the same storage device, commonly a RAID system: when one server fails, the other one (which is configured identically) takes over the application – these servers regularly even share the same IP address – making the so called fail-over completely transparent for the user.



- **Multiple video recipients:** A common method to ensure disaster recovery and off-site storage in network video is to simultaneously send the video to two different servers located in separate locations. These servers can of course in their turn be equipped with RAID, work in clusters or replicate their data with servers even further away.

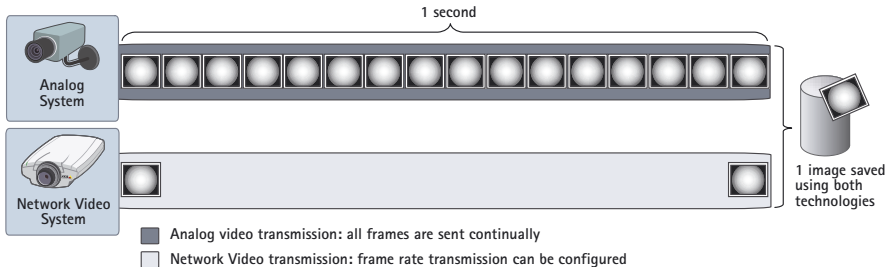
6.1.4. System scalability

Scalability varies according to the type of system chosen, and must therefore be considered at the design stage of a video system.

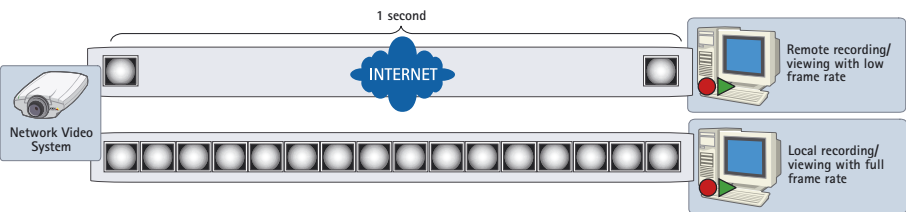
- **Scalability steps:** A DVR system is usually supplied with 4, 9 or 16 camera inputs, therefore becomes scalable in steps of 4, 9 or 16. If a system includes 15 cameras, this is not an issue, but it becomes a problem if 17 cameras are needed. Adding one single camera would generate the need for an additional DVR. Network video systems are far more flexible, and can be scaled in steps of one camera at a time.
- **Number of cameras per recorder:** In a network video system, a PC server records and manages the video. The PC server can be selected according to the performance needed. Performance is often specified as number of frames per second, total for the system. If 30 fps is needed for each camera, one server may only record 25 cameras. If 2 fps is sufficient, 300 cameras can be managed by one server. This means that the performance of the system is used efficiently and can be optimized.
- **Size of system:** For larger installations, a network video system is easy to scale. When higher recording frame rates or longer recording times are needed, more processing and/or memory capacity can be added to the PC server managing the video. Even more simply, another PC server can be added, located either at a central location, or at remote locations.

6.1.5. Frame rate control

Network video allows for “frame rate control” – as opposed to analog video where “all video is sent from the camera all the time”. Frame rate control in network video systems means that the network camera/video server only sends images at the specified frame rate – no unnecessary frames are transferred over the network. The network camera/video server or video management software can be configured to raise this frame rate if for example activity is detected.



It is also possible to send video with different frame rates to different recipients – a benefit especially when using low bandwidth links to remote locations.

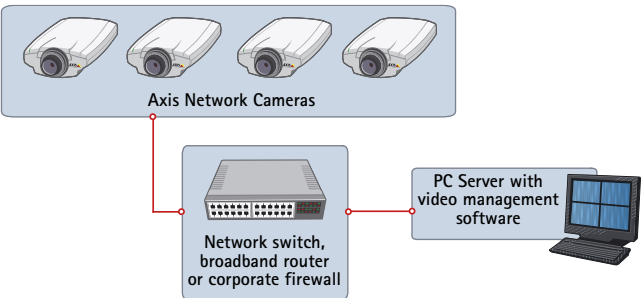


6.2. Storage considerations

Different hard disk solutions

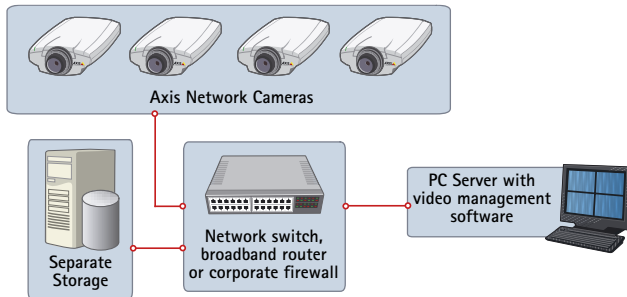
There are two ways to approach hard disk storage: one is to have the storage attached to the actual server running the application. The other is a detached storage solution where the storage is separate from the server running the application.

6.2.1. Direct attached storage



This is probably the most common solution for hard disk storage in small to medium-sized installations. The hard disk is located in the same PC that runs the video management software (application server). Space availability is determined by the PC and the number of hard disks it can hold. Most PCs can hold 2 disks, some up to 4 disks. Each disk can be up to approximately 300 Gbyte. This gives a total hard disk capacity of approximately 1.2 Tbyte.

6.2.2. Network Attached Storage (NAS) and Storage Area Network (SAN)



In applications where the amount of stored data and management requirements exceed the limitations of direct attached storage, a separate storage system is implemented. These systems are Network Attached Storage (NAS) and Storage Area Network (SAN).

NAS

Network Attached Storage provides a single storage device which is directly attached to a LAN and offers shared storage to all clients on the network. A NAS device is simple to install and easy to administer, providing a low-cost solution for storage requirements, but limited throughput for incoming data.

SAN

A Storage Area Network is a high-speed special-purpose network for storage, connected to one or more servers via fiber. Users can access any of the storage devices on the SAN through the servers, and the storage is scalable to over hundreds of Tbytes. Centralized data storage reduces the administration required and provides a high performance flexible storage pool for use by multi-server environments.

The difference between the two is that NAS is a storage device where the whole file is stored on one single hard disk, whereas SAN consists of a number of devices where the file can be stored block by block on multiple hard disks. This type of hard disk configuration allows for very large and scalable hard disk solutions where large amounts of data can be stored with a high level of redundancy. There are solutions of both types available for video management software.

6.2.3. RAID (Redundant Array of Independent Disks)

RAID is a method of arranging standard, off-the-shelf hard drives in such a way that the operating system sees them as one large logical hard disk.

There are different levels of RAID offering different levels of redundancy; from practically no redundancy at all to a full “hot swappable” mirrored solution where there is no disruption to the operation of the system and no lost data in the event of hard disk failure.

The most common RAID levels are listed in the table below.

RAID Level	Characteristics
RAID-0	Data is being striped (divided) over two or several hard disks, for improved read/write speed but no redundancy.
RAID-1	Also known as disk mirroring. At least two disks duplicate data. No striping. Both disks can be read at the same time. Write performance as for single disk storage.
RAID-5	Includes a rotating parity array, allowing all read and write operations to be overlapped. Stores parity information for reconstruction of any lost data. RAID-5 requires at least 3, and runs with up to 16 disks in the array.

6.3. Security capabilities

With any video surveillance system privacy is an important consideration. Video intelligence and network cameras can be put to work to alleviate some of these concerns. Unlike analog CCTV cameras that only send out one single video stream that can be tapped into, a network camera can encrypt the video being sent over the network to make sure it cannot be viewed or tampered with. The system can also be set up to authenticate the connection using encrypted certificates that only accept a specific network camera, thus eliminating the possibility of anyone hacking into the line.

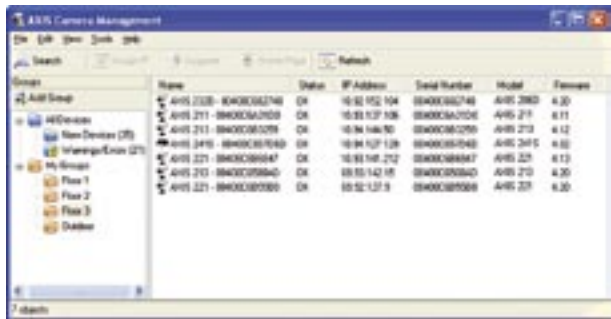
To mitigate against the threat of manipulating of digital images, it is now possible to use techniques such as time stamping and watermarking. The creation of audit trails makes it possible to know who has seen what images and whether any edits have been made by those individuals.

With watermarking, the network camera adds encrypted watermarks to the video data stream. These watermarks contain the time, location and user information as well as information about which alarms were linked to a specific recording sequence. Digital watermarks are designed to be completely invisible to viewers. This is achieved by scattering the watermark information randomly throughout the file in such a way that they cannot be identified and manipulated by unauthorized users.

6.4. Managing large systems

Network video products have a built-in web server which makes them accessible from the network. This built-in web server offers live viewing as well as authorized access to internal settings for configuration and firmware upgrades. For a system with a few network cameras or video servers, the built-in web server will prove sufficient in most instances. Larger systems may however require higher specification management tools.

Based on standard network protocols, a management tool can automatically find and display new devices on the network, even those without a valid IP address. By using a well-defined API such as the AXIS VAPIX™ API, the management tool can also display basic properties of the devices it has found including the model's name and current firmware version. It also helps you set the IP addresses, shows connection status of local and remote video devices, and enables configuration and firmware upgrades of multiple units sequentially or in parallel. The use of a centralized management tool not only makes system maintenance easy, but also lowers overall maintenance costs.



AXIS Camera Management, scalable to hundreds of cameras, enables easy IP setting and installation of Axis network video products and is able to perform such tasks as configuration and multiple firmware upgrades.

Video Management



Network cameras are only ever as good as the selection and configuration of the video management systems that control them. Systems should enable users to monitor, analyse and store video output effectively. The chapter compares a ‘PC Server platform’ approach with an ‘NVR platform’ approach using a dedicated device such as a Network Video Recorder (NVR) for managing network video output. This chapter also covers options for building event management, motion detection and audio capability into systems.

Systems based on a network video platform are suitable for integration to other systems such as access control or building management, and the information from those systems can be used to trigger functions in the network video system, for example to store images related to events.

7.1. Hardware platforms

There are two different types of platforms for network video management: PC Server platforms and NVR platforms (Network Video Recorder). Both types are based on PCs but there are some noticeable differences.

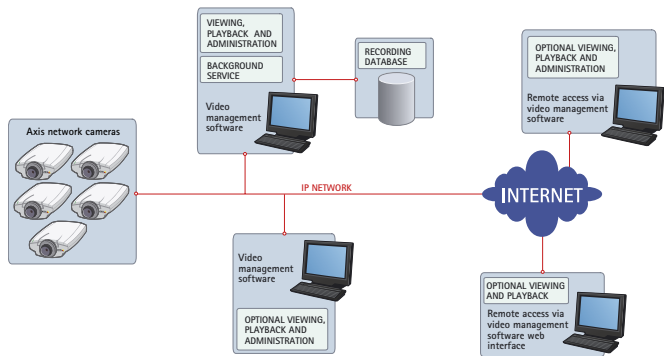
A PC Server platform solution on the other hand runs on ‘off the shelf’ hardware where hardware components have been selected to obtain the maximum performance. With a PC Server platform solution it is possible to leverage on standard components, such as increased or external storage, additional remote operator stations and to run additional software in parallel to the video application, such as firewalls and virus protection.

The most obvious difference between an NVR platform and a PC Server platform type solution is that an NVR comes as a hardware box with the video management functionality pre-installed. By definition, it is dedicated to its specific tasks of recording, analyzing and playing back of network video. NVRs do not allow for any other applications to reside on them. The NVR hardware itself is ‘locked’ to this application and the unit can very rarely be altered to accommodate anything outside its original specification.

Systems designed on a network platforms are fully scalable. Cameras and licenses can be added one by one and the system hardware can be expanded to meet increased performance requirements. This platform is suitable for system scenarios where a large number of cameras are deployed or when the IT department has standard specifications on the server hardware and software allowed on the network.

7.1.1. PC Server platforms

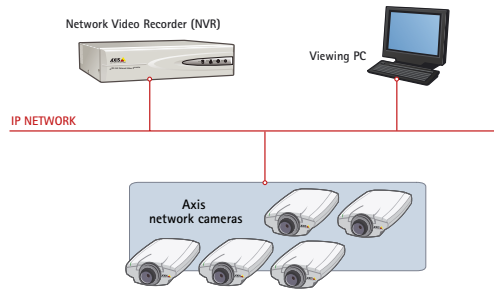
A PC Server platform solution, as mentioned above, runs on off-the-shelf hardware, where hardware components have been selected to achieve the maximum performance for the specific design of the system, such as detached storage or dual processor systems.



As the PC Server platform system is based on standard hardware components it is possible to still use the end user's preferred choice of hardware as well as their existing suppliers of IT equipment and maintenance services.

7.1.2. NVR platforms

An NVR has some similarities to a Digital Video Recorder (DVR) in relation to recording and playback. A DVR is in fact a hybrid system that can accommodate analog cameras and store the video on a hard disk in digital format. An NVR is a true digital system that receives digital images/video streams over the network and records them on a hard disk in a digital format. Some DVRs have a rudimentary interface to the network that offers remote viewing capabilities. An NVR does not have a dedicated monitor and keyboard. All viewing and management of the NVR takes place remotely over the network via a PC.



An NVR is designed to offer optimal performance for up to a set number of cameras, which makes it less scalable than a PC Server platform system. This makes the unit suitable for smaller system configurations where the number of cameras stays within the limits of the NVR design capacity. An advantage is that an NVR is less complex to install in comparison to a PC Server platform.

7.2. Monitoring and recording

Video management of a network video system includes *video monitoring*, which can be conducted from a web browser or specific video management software, and *video recording*, which can be conducted from video management software installed on a PC or using a Network Video Recorder.

7.2.1. Monitoring using the web interface

In a network video system, video can be viewed from any point on the network provided there is access to a web browser. Each camera has a built-in web server with an IP address, so to view the images on a PC, one simply opens a web browser and types in the camera's IP address in the Address/Location field:



Once the computer has established the connection, the network camera's 'start page' is automatically displayed in the web browser. This start page will display live video feeds from the camera along with hyperlinks for changing the camera set-up, such as image resolution, network and e-mail settings – unless the system is set up with security/password limitations.

7.2.2. Monitoring using video management software

Even though video can be viewed directly from a standard web browser, video management software can be installed if more flexible viewing options, as well as the ability to store and manage video, are required. A wide variety of software solutions exist on the market, which range from independent solutions for a single PC, to advanced client/server-based software providing support for multiple simultaneous users. Common functionality includes video monitoring, event management functions and alerts to alarm events via siren or e-mail for instance.

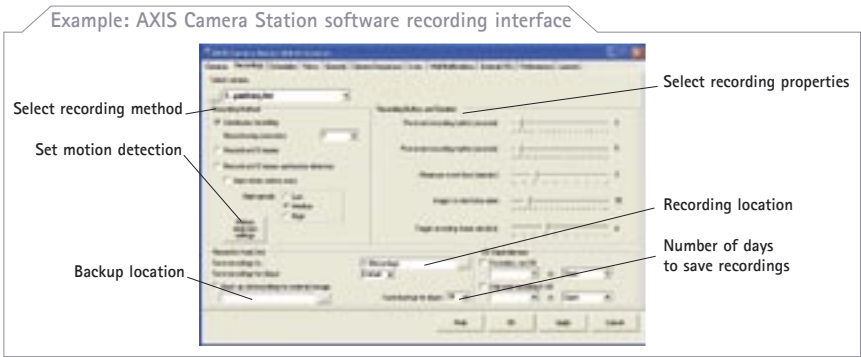


7.2.3. Recording network video

There are several ways to record network video:

For simple recordings, the network camera's built-in functionality can be used to record images or video, based on scheduled or triggered events. These images are then uploaded to an FTP server or to the hard drive of a computer.

For advanced recording and event management, video management software serves as the core of professional video surveillance systems. The software is installed on a PC and can be an independent solution or a client/server-based application for multiple simultaneous users. From the software interface, operators can, for example, record video continuously, on schedule, on alarm and/or on motion detection or search for recorded events.



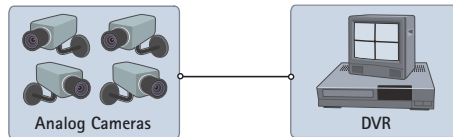
7.3. System features

7.3.1. Video motion detection (VMD)

Video Motion detection (VMD) is a way of defining activity in a scene by analyzing image data and differences in series of images.

VMD in DVR systems

Cameras are connected to the DVR, which performs the VMD on each video stream. This allows the DVR to decrease the amount of recorded video, to prioritize recordings and to use motion in a specific area of the image as a search term when searching for events. The downside of this method is that performing VMD is a CPU intensive process and performing VMD on many channels puts a heavy strain on the DVR system.

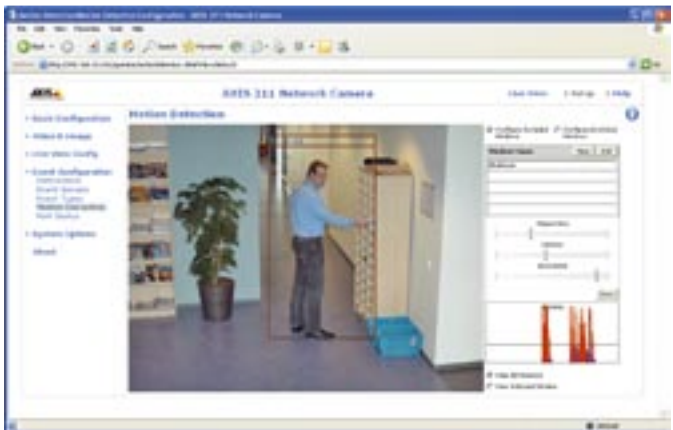
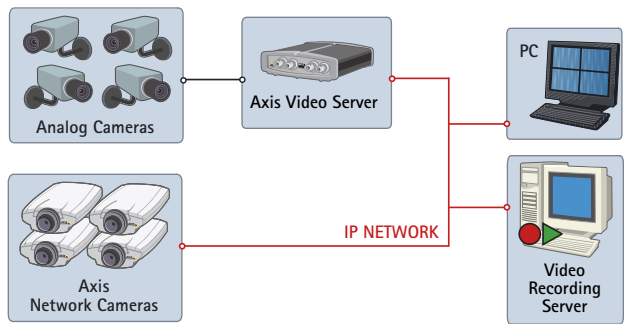


VMD in network video systems

VMD as an integrated function of network cameras or video servers offers substantial advantages over the scenario mentioned above – the most significant being that the VMD is processed in the network camera or video server itself. This alleviates the workload for any recording devices in the system and makes “event-driven surveillance” possible. In that case, no video (or only video with low frame rate) is sent to the operator or recording system unless activity is detected in the scene.

VMD data with information about the activity can also be included in the video stream to simplify activity searches in recorded material. VMD can also reside in the video management software, thus providing VMD functionality to network cameras that do not originally embed this feature.

VMD with network video equipment



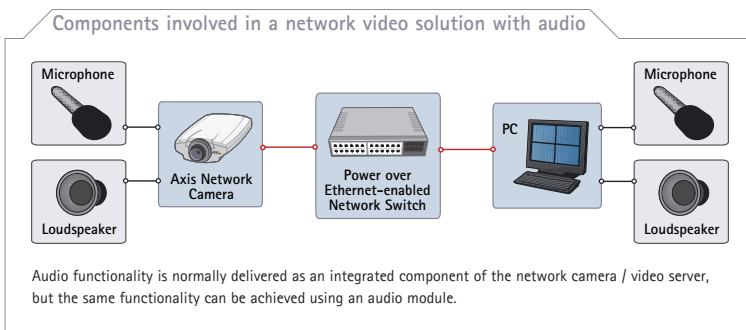
Advantages of local VMD in the "endpoint" (network camera and video server compared with systems using central analyzing such as DVRs)

- Conserves bandwidth
- Reduces CPU load on recording server
- Saves storage space
- The camera can interact with others systems using I/O Ports (for example triggering alarms)

7.3.2. Audio

Audio can easily be integrated into network video as the network can carry any type of data, which reduces the need for extra cabling – as opposed to analog systems where an audio cable must be installed from endpoint to endpoint. A network camera captures audio at the camera, integrating it into the video stream, and then sending it back for monitoring and/or recording over the network.

This makes it possible to use audio from remote locations. For instance, monitoring personnel at a company's headquarters can interact with "surveillance scenes" at remote branch offices. They can inform possible perpetrators that they are under surveillance and listen in on situations using the audio as an additional confirmation method. Audio can also be used in network cameras or video servers as an independent detection method, which triggers video recordings and alarms when audio levels above a certain threshold are detected.



Audio transmission

Audio can be compressed and transmitted as an integrated part of the video stream, if MPEG-1/MPEG-2/MPEG-4 or any of the H.x video conferencing standards are used. It can also be transmitted in parallel if using a still image standard, such as JPEG. However if synchronized audio and video is prioritized, MPEG is the preferred choice. Nonetheless, there are many situations where synchronized audio is less important or even undesirable (for example if audio is to be monitored but not recorded).

Audio compression

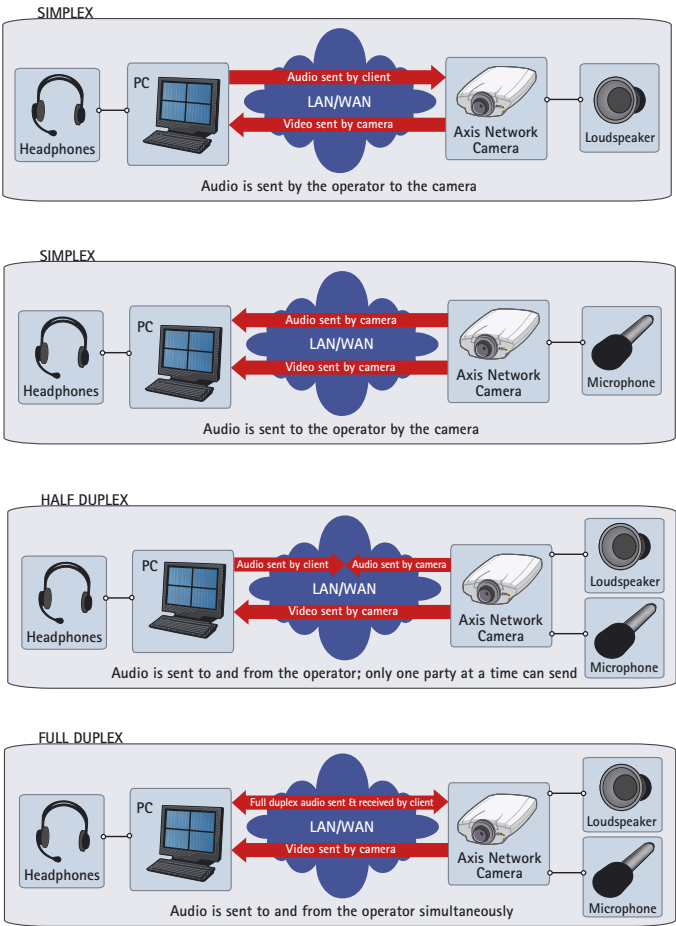
Digital audio compression allows for efficient transmission and storage of audio data. As with video, there are many audio compression techniques, which offer different levels of compressed audio quality. In general, higher compression levels introduce more latency. Audio in digital form offers many advantages, for example high noise immunity, stability, and reproducibility. It also allows for efficient implementation of many audio post-processing functions, such as noise filtering and equalization.

Popular audio compression formats include:

- G.711 PCM providing high quality audio at 64kbit/s bit rate
- G.726 ADPCM providing audio at 32 or 24kbit/s bit rate
- MP3 (which stands for ISO-MPEG Audio Layer-3), a popular format geared towards music, with bit rates around 100 kbit/s
- Standard MPEG-4 audio using AAC LC compression (Advanced Audio Coding Low Complexity profile), 16 kHz sampling with a bit rate of 40 kbit/s.

Audio modes

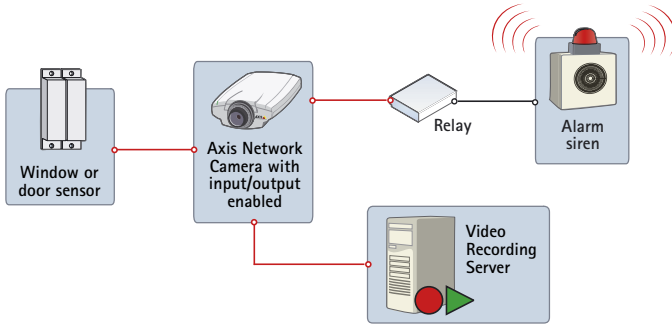
When using Axis network cameras, there are several audio modes to choose from:



7.3.3. Digital inputs and outputs (I/O)

A unique feature of network video products, is their integrated digital inputs and outputs that are manageable over the network. The output can be used to trigger mechanisms either from a remote PC or automatically, using the camera's built-in logic, while inputs can be configured to respond to external sensors such as PIRs or push button initiating video transfers.

The I/Os can be used in conjunction with alarm sensors for instance, to eliminate unnecessary transfers of video, unless the sensor attached to the camera triggers.



I/O usage example - A camera attached to a window switch and to an alarm system/siren

Digital inputs

The range of devices that can be connected to a network camera's input port is almost infinite. The basic rule is that any device that can toggle between an open and closed circuit can be connected to a network camera or a video server.

Examples of alarm devices and their usage

Device type	Description	Usage
Door contact	Simple magnetic switch detecting opening of doors or windows	When circuit is broken (door is opened) the camera can take action sending full motion video and notifications
Passive infrared detector (PIR)	A sensor that detects motion based on heat emission	When motion is detected, the PIR breaks the circuit and the camera can take action sending full motion video and notifications
Glass break detector	An active sensor that measures air pressure in a room and detects sudden pressure drops (can be powered by the camera)	When an air pressure drop is detected, the detector breaks the circuit and the camera can take action sending full motion video and notifications

Digital outputs

The output port's main function is to allow the camera to trigger external devices, either automatically or by remote control from a human operator or a software application.

Example of devices that can be connected to the output port

Device type	Description	Usage
Door relay	A relay (solenoid) that controls the opening and closing of door locks	The locking/unlocking of an entrance door can be controlled by a remote operator (over the network)
Siren	Alarm siren configured to sound when alarm is detected	The camera can activate the siren either when motion is detected using the built-in VMD or using "information" from the digital input
Alarm/intrusion system	Alarm security system continuously monitoring a normally closed or normally open alarm circuit	The camera can act as an integrated part of the alarm system serving as a sensor and enhancing the alarm system with event triggered video transfers

7.5. Integrated systems

In a network video system, all devices are connected to an IP network – enabling the use of a cost-efficient infrastructure to transport video for recording or monitoring. It also enables integration with other systems for increased functionality and easier operation. Examples of systems which can be integrated include:

- **Access control:** Using a video surveillance system with integrated access control systems, means for example that video can be captured at all doors when someone enters or exits a facility. Additionally all pictures in the badging system can be accessible to the operator of the video surveillance system, for quick identification of employees or visitors.
- **Building management systems (BMS):** Video can be integrated into building management systems, like heating, ventilation, and air conditioning systems (HVAC). The I/O ports of the network cameras can be used to provide input to the system, or the cameras used to detect motion in meeting rooms for instance, and control heating or lights to save energy.
- **Industrial control systems:** A visual verification is often required in complex industrial automation systems. Instead of the operator having to leave the control panel to visually check a part of the process, he or she can view network video using the same interface. Also in some sensitive clean room processes, or in facilities with dangerous chemicals, video surveillance is the only way to have visual access to the process. The same goes for electrical grid systems with a substation in a very remote location.

Intelligent video systems



These days lots of video is being recorded, however not properly analyzed, due to lack of time. This has led to the development of Intelligent Video (IV) applications. New IV systems are now being developed for taking video data of number plates and digitizing the plate for cross checking with a database. People counting and trip wire are other examples of IV applications. Being able to offer this sort of intelligence in the edge device itself offers major advantages, which include analysis of raw data and reduced workload of staff. The intelligent network camera is never idle. It is constantly on guard, waiting for an impulse to start recording. The motion detection feature may be used for tailored alarm settings, in order to suit each specific environment and event intensity.

8.1 What is intelligent video?

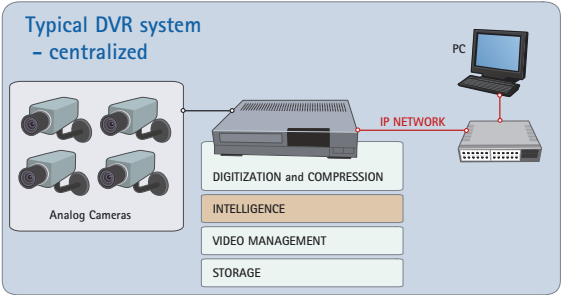
Intelligent Video is about turning raw video data into actionable information. Provision of intelligence through surveillance will therefore support potential quality decision-making in time critical situations. New business opportunities such as people counting will occur; see *chapter 8.3.1., page 75*.

8.2 Intelligent video architectures

8.2.1 DVRs and centralized intelligence

One solution for traditional CCTV systems being centrally monitored, is to take surveillance videos direct from the analog cameras into the IV-enabled DVR. The DVR will perform the intelligent analysis (people counting or car license plate extraction for example) before taking the remaining data, digitizing, compressing and recording it, and distributing resulting alarms and video output to authorized operators.

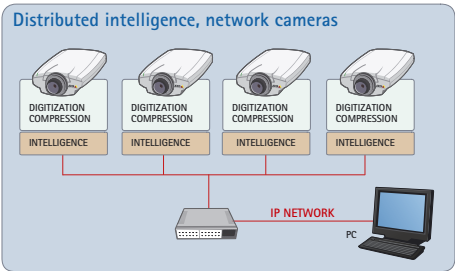
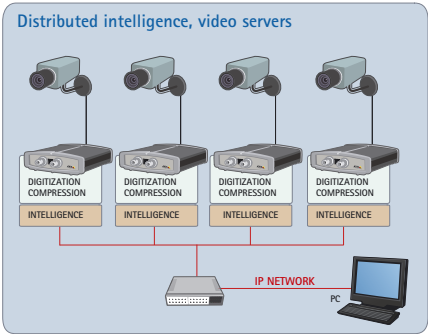
This approach is fine for systems that offer adequate capacity for uncompressed live video output to be transmitted to a central point. It is also appropriate for systems where the numbers of cameras are constant, as each DVR can only carry a specific number of cameras, and each unit is very costly.



8.2.2 Network video systems and distributed intelligence

A better and scalable alternative, compared to analog-based systems, is to rely on video servers attached to analog cameras locally to make the analysis of the video stream, and digitize and compress before passing information via the network for monitoring and storage.

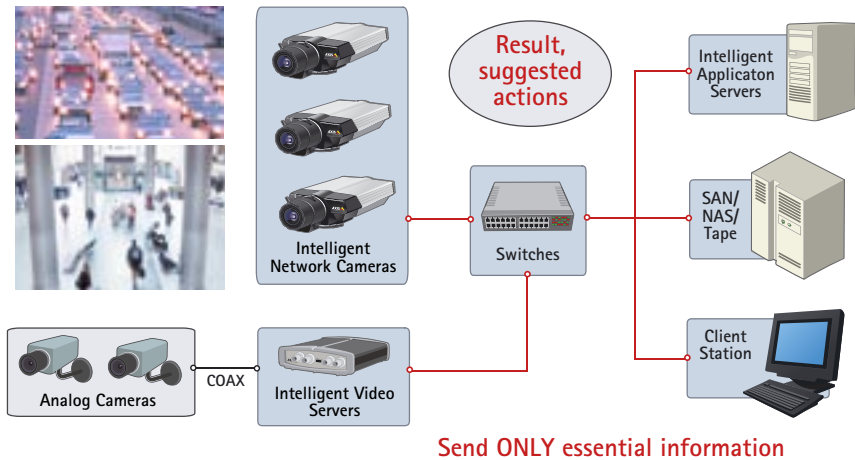
The advantages of this approach are several. The first is that digitization and compression are done locally and then existing network infrastructure combined with the Internet itself can be used for low cost transmission of intelligent data. It is possible, for example, for only video data triggered by motion detection and accompanied by an alert message to be sent on to a centralized monitoring station for further action and analysis, possibly through use of more sophisticated IV applications. The load on the infrastructure and people involved falls dramatically.



A “distributed” approach enables intelligence to reside in “edge devices,” as shown above in the network camera itself, or in the video server. The information can, at an appropriate time, be channeled to either a centralized server or to specific clients who need to conduct specific actions.

From a basic configuration, it is possible to join specifically compiled intelligence in order to govern operators tasked to a particular job. As organizations look to enhance their video systems, different types of distributed IV applications may be combined. The network distributed intelligence approach is limitless in scalability and thereby future-proof in regards to future expanding building blocks.

8.3 Typical Applications



8.3.1 People counting

In a retail store there could be a network video device installed at each of the three public entrances.

Network video devices can be fitted with a people counting module, which records numbers of people passing through each door directly into a central business unit. Separate devices provide views of point of sale displays. Network cameras may trigger on motion and will stream this video down to a central unit, and onto an IV operator for analysis of 'dwell times'. High volumes of people buzzing around, combined with long dwell times provide a picture of the display success. This information ultimately aids the store's overall profitability.

Other important store issues are: "When do queuing levels start to impact the customer experience? Is a particular line going faster than anticipated? Is there frustration around a new layout in a store?"

Network video systems can therefore serve multiple purposes: for business intelligence purposes helping retailers to increase sales and profitability through analysis of customer behavior; for improving the customer experience through analysis of queuing times and observing reaction of waiting customers, helping support decisions to open new tills as queue times reach levels where they begin to detract from the customer experience.

8.3.2 License plate recognition

Intelligent parking is a successful application based on license plate recognition. A problem may be that clients lose their long term parking tickets and question the administration of the specific parking lot. Lots of time and energy are spent on finding the correct fee. The new system offers monthly bills and non questionable parking tickets.

Another issue is the use of parking lots for letting stolen vehicles “cool off”. The police authorities welcome the new intelligent gate keepers that records entry times and statistics of which cars reside in each parking location. It prohibits both housing of stolen cars at other city locations as well as tampering with cars parked at an “intelligent house”. The IV application serves multiple purposes. Owners of cars, authorities and the parking administration are among the winners.

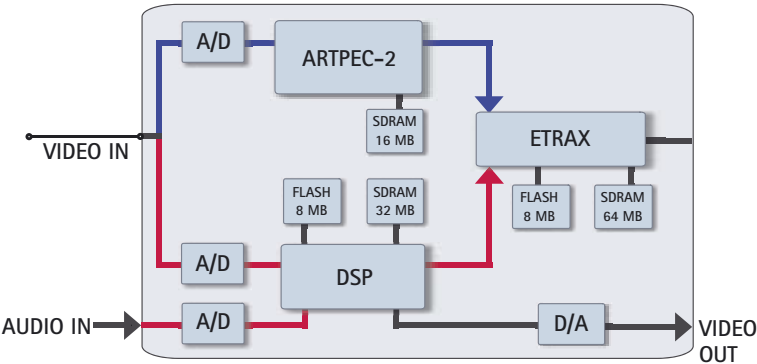
8.3.3 D-fence or tripwire

A “trip-wire” application helps prohibit break-in attempts with limited security officers on duty. The application is designed to offer a virtual line or lines, restricting passage in one specific direction. In other words, employees or security personnel may leave a building but not re-enter without consulting the alarm administrator.

Tailoring the virtual trip wires, offers great potential. This means that intelligent video systems can configure surveillance systems so they only collect video data when specific parameters exist and when anomalies to normal movements are detected. The key point here is that systems can be set up to deliver far more targeted and specific information.

8.4 Components built on open standards

New modules are being integrated into network video devices to fully enable powerful intelligent video applications. The IV-enabled one port video server called the AXIS 242S IV contains an additional Digital Signal Processing (DSP) chip. This chip is fully dedicated to the processing of data associated with IV applications.



In order to be commercially attractive and optimize software compatibility and usability, Axis technology strategy has been built on an open platform. The platform provides more possibilities to capitalize on our partner program that constantly offers cutting edge software technology for future intelligent analytics.

Quick start: Checklist when designing a network video system

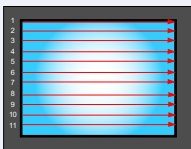
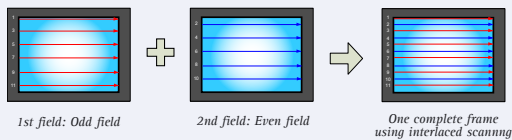
1. Analog camera or network camera?

Network cameras have fully caught up with analog camera technology and now meet the same requirements and specifications and, as you have read in the guide, network cameras surpass analog camera performance in some important areas.

Below is a summary of 10 of these most important functional differences between today's network cameras and analog cameras, and why these factors are important to understand before deploying or extending your video system.

(1) End to interlace problems

As we have seen in chapter 3.2, an analog camera at high resolution (4CIF) has a significant problem with interlacing, creating blurry images. A network camera, which employs "progressive scan" technology that better suits depicting moving objects, provides crystal clear images even with a high degree of motion.



One complete
frame using
progressive scan



(2) Power over Ethernet increases savings and reliability

Not available for analog cameras, Power over Ethernet (PoE) means that networking devices get power from a PoE-enabled switch or midspan over the same standard Cat-5 or Cat-6 cable that transmits data and video. Since the IEEE 802.3af standard is in place, all equipment is compatible, maximizing the benefits for all end users. In a surveillance application, PoE provides an additional benefit: cameras can get centralized backup power from the server room, so in the event of a power failure they will continue to operate.



(3) Megapixel resolution

Analog cameras are stuck at NTSC/PAL specifications, with a resolution corresponding to 0.4 megapixel at 4CIF. A network camera's higher resolution provides more detail and can cover larger areas, ensuring high image accuracy, crucial in security applications.



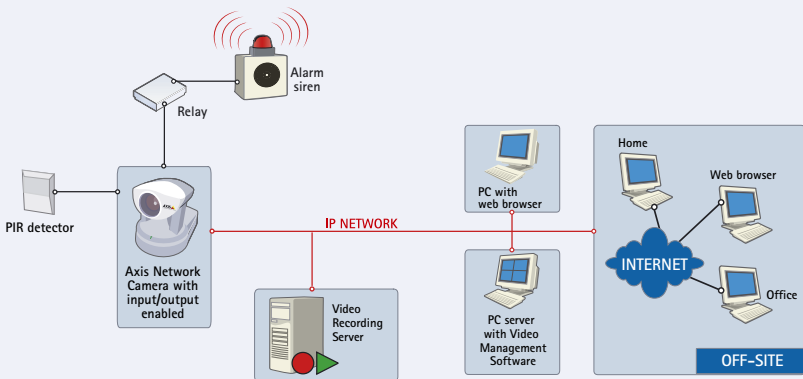
(4) Intelligence at the camera level

Intelligence at the camera level empowers a much more productive and effective means of video surveillance than is possible with a DVR or other centralized systems. The network camera also solves another emerging dilemma: the shortage of computing power to analyze more than a few channels in real time. Network cameras have purpose-built, highly integrated hardware that excels in image analysis tasks, thus enabling installation of large-scale intelligent video systems.



(5) Integrated PTZ and input/output control

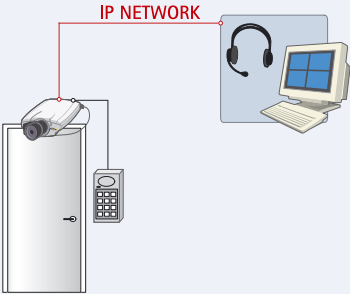
With an analog PTZ camera, the serial communication that controls PTZ movement requires cabling separate from the video signal. This is costly and cumbersome. Network camera technology enables PTZ control over the same network that transports the video. What's more, network cameras can integrate input and output signals such as alarms and controlling locks. This all adds up to less cable, less money, and increased functionality and integration potential.



Example: Typical I/O use – Integration with alarm

(6) Integrated audio

With an analog system, audio is not possible unless separate audio lines are run to the DVR. A network camera solves this by capturing audio at the camera, synchronizing it with the video or even integrating it into the same video stream.



Example: Communicate and open a door remotely

(7) Secure communication

With an analog camera, the video signal is transported over a coax cable without any encryption or authentication. A network camera can encrypt the video being sent over the network to make sure it cannot be viewed or tampered with. The system can also be set up to authenticate the connection using encrypted certificates that only accept a specific network camera, thus eliminating the possibility of anyone hacking into the line. The network camera can also add encrypted “watermarks” to the video data stream with information on image, time, location, users, alarms and more, in order to secure an evidence trail.

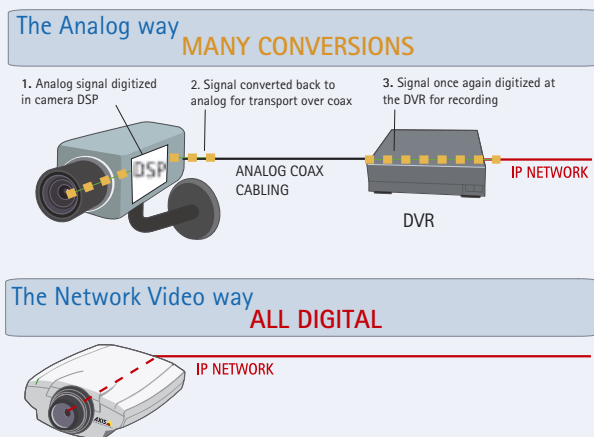
(8) Flexible, cost-effective infrastructure choices

Analog video is typically transmitted by expensive coax where distance will influence image quality. Adding power, inputs/outputs and audio further complicates this situation. Network video systems surmount these obstacles at much lower cost and with many more options. A network camera produces digital images, so there’s no quality reduction due to distance. IP-based networking is an established, standardized technology meaning the resulting costs are comparatively low. Unlike analog systems, IP-based video streams can be routed around the world, using a variety of interoperable infrastructure.



(9) A true digital solution

The CCD sensor in an analog camera generates an analog signal that is digitized by an A/D converter to make possible the image improving function in a DSP. The signal is then converted back to analog for transport over a coax cable. Finally, at the DVR the signal is once again digitized for recording. That makes a total of three conversions, and with every conversion image quality is lost. In the network camera system, images are digitized once and they stay digital for the duration—no unnecessary conversions and no image degradation.



(10) Lower total cost of ownership

It stands to reason that all the advanced features described above come at a cost. The initial price for a network camera can indeed be higher, if one compares only the camera. But compare the cost per channel, and the network video system quickly becomes comparable with an analog system anchored by a DVR. In many system configurations, the upfront cost for a video surveillance system based on network cameras is even lower, when compared to analog options. This lower total cost for the network camera system is mainly a result of back end applications and storage that can be run on industry standard, open systems-based servers, and not on proprietary solution like a DVR. This radically reduces management and equipment costs, in particular for larger systems where storage and servers are a significant portion of the total solution cost. Additional cost savings come from the infrastructure used. IP-based networks such as the Internet, LANs and various connection methods such as wireless can be leveraged for other applications across the organization and are much less expensive alternatives than traditional coax and fiber.

2. Making the right network camera choice

Many vendors have entered the network video market. This means you are probably facing an increasing number of choices, accompanied by a lot of often confusing or contradictory information. When evaluating what network camera to buy, how do you make a good, informed decision?

Following are 10 important factors to think about when you have decided to add network cameras to your security operation.

(1) High image quality

When assessing a network camera's image quality, be sure to research these questions: What is the light sensitivity? Level of image clarity? Does it have a high quality lens? And what is the image quality when there is motion in the image? A datasheet tells part of the story, but make sure to field test a few of the camera choices to make the datasheet information real for your application.

(2) Part of a wide product portfolio

When choosing your network video vendors, go with those who maintain a full product line including fixed cameras, fixed domes, and PTZ dome cameras. This way, one or two companies can satisfy your needs now and well into the future when you're ready to expand and to upgrade functionality to megapixel, wireless and/or audio. If you have analog cameras to upgrade, make sure that your chosen company's product portfolio also includes video servers (encoders), video decoders, housings, and other related equipment.

(3) Extensive application support and ease of integration

Is the network camera you are looking at part of a closed system where you have limited or possibly only one choice of video management software? Make sure to select a network camera that has open interfaces (an Application Programming Interface or API) and multiple software applications from which to choose. Certain leading companies have hundreds of such alliances. Your choice of network camera should never limit your options or functionalities. Open, multi vendor systems will always prevail in the long run.

(4) Compression fully compliant with JPEG and MPEG-4 standards

Make certain the camera follows JPEG and MPEG-4 standards 100%. You would be surprised to find that many vendors, who claim compliance with a standard, do not yet adhere 100% to that standard. 99% compliance means no compliance. Full adherence ensures the flexibility to use video for many different applications. It also guarantees that you can view the video 10 years from now or longer. Also, if a company is following the MPEG-4 standard, ask if the licensing fees are paid, and how many licenses are included with each product. If fees are not paid by the vendor, either the compression is not following the standard, or you will need to pay for licenses after the purchase.

(5) Tools for managing large deployments

Like all intelligent network devices, network cameras have an IP address and built-in firmware. Many vendors provide upgrades free of charge. When making a purchase decision, you have to consider the cost to set IP addresses and eventually update all the cameras in the facility. The network camera maker should have tools to manage these processes and their estimates for cost and downtime should be clear and measurable upfront. Among the maker's tools should also be the capability to automatically locate all network video devices and monitor the status of those devices.

(6) Extensive networking functionality and security

In the same way that high image quality is essential, a camera's networking functionality is just as important. Plugging into an Ethernet connection with an IP address is only a basic functionality; all network cameras can boast the same. You need to consider other factors: What about DHCP (Dynamic Host Configuration Protocol), used by many organizations to manage IP addresses? What about security in the form of encryption or HTTPS? Also, an important litmus test is the attitude of your IT department. Are they happy with putting a particular network camera on the network? They are the experts. They'll be able to determine if the camera provides adequate network functionality and security.

(7) Progressive Scan sensor

Progressive scan capability is found only in network cameras, but not all network cameras have this functionality. It consistently produces the best results in clarity and recognizing important details. Consider: when you press "pause" on a DVD, why is the picture quality better than a paused VHS tape? That's right: progressive scan.

(8) Power over Ethernet (PoE)

This might seem like a small check-off item on the feature list, but think of it this way: Wouldn't you like to save hundreds of dollars per camera? Even for an installation with 50 or 100 cameras that's a considerable savings. For end users with hundreds of cameras, this translates to a lot of money. Make sure the camera's Power over Ethernet feature is in accordance with the IEEE 802.3af standard. This will give you the freedom to select from a wide array of network switches from companies such as Cisco, Nortel, NetGear, and others.

(9) Distributed intelligence

Intelligent video has become a hot buzzword. The technology will evolve and improve greatly over the next few years, but it only becomes scalable if the intelligence is located at the camera. The reason is that video intelligence requires a large amount of processing power, and if that power is not in the camera, just a few cameras will quickly overload the PC servers. When intelligence is located in an edge device like the camera, the camera is able to decide when to send and therefore process the video.

(10) Vendor history and focus

As we've discussed, it is important to make network camera decisions based on the assumption of future growth and the need for added features and functionality. This means your network camera manufacturer is going to be a partner for a long time.

Consider:

What is the makers installed base of network cameras and other networking products? Is the company profitable? Does the company focus just on network camera technology, or are network cameras only a fraction of the company's business? What about local representation and support? Is the company a global player and does it demonstrate proficiency in a number of languages? How about reference installs? You want to choose a camera from a market leader to ensure that innovation, support, upgrades, and a product path are going to be there for the long term. Don't sacrifice future security just to save a little money upfront.

3. Design guides, preparing your network video project

(1) Define the scene and type of network video products required

- **Scene:** What kind of scene do you want to monitor? How important is it?

This will help you determine the features you'd like to have in a network camera, such as video quality, light sensitivity and type of lens.

- **Lighting conditions:** level of indoor and/or outdoor light sensitivity required

Axis offers network cameras for indoor use, as well as ones for both indoor/outdoor conditions. Indoor/outdoor cameras have varifocal lens that automatically adjust the lens' iris. Day/night cameras, which provide color images during daytime and black & white images during night time are also available. Check details on the network camera's light sensitivity both in indoor and/or outdoor environments. Light is measured in "lux".

- **Distance from position of camera to object being monitored**

This determines the type of camera and type of lens (normal, telephoto, wide-angle) to use, as well as the placement of the camera(s). Certain Axis network cameras have lenses that are replaceable.

- **Angle of view needed:** wide, narrow, general or detailed coverage (determine how much of the scene you need to see)

Network cameras come with fixed angle and focus, as well as variable ones that allow remote pan/tilt/zoom capability, which enables a wider area of coverage.

- **High or low traffic**

The higher the traffic, perhaps the more cameras are needed.

(2) Determine your application needs: features, recording and storage needs

- **Application**

Simple remote viewing, intelligent surveillance system with advanced event management, input/output triggers, audio component?

- **Viewing and recording needs**

Determine when and how often you need to view and record: day, night and/or weekends? Schedule the needs for every scene.

- **Calculate storage requirements**

- **Calculate bandwidth requirements**

(3) Determine your network needs (LAN/WAN, wireless)

- Assess network use of current LAN: what are you or the company using it for?
- Assess network use of current WAN links
- Determine the pattern of congestion levels over a given period
- Do you need to add new equipment to the network, e.g. switches, or use existing infrastructure and equipment?
- Do you need to subscribe to additional ISPs for redundancy?
- Is distributed storage needed?

10 most important questions to ask

- Are there currently analog cameras installed?
- Will new cameras be added?
- How many cameras will there be in total?
- Do you understand the cost structure of an IP-based system?
- Are electrical power outlets at camera locations an issue?
- Are there cameras at remote sites?
- Are the IT and Security departments working together?
- Has your IT department standardized on a PC platform?
- Does your IT department provide 24/7 support for systems on their network?
- Is your IT department involved with purchase decisions?

4. Project tools



Axis Network Video Design Tools CD: A variety of tools that will help you design your network video project

Axis has developed a variety of tools that will help you design your network video project: The Axis Network Video Design Tools CD guides you through the factors and settings to consider for the successful deployment of a network video installation. It includes a lens calculator, an image and video clip gallery, as well as the new AXIS Design Tool, a simulation-based calculation tool which helps determine the bandwidth and storage needs for specific network video projects.

Multilingual format: English, Dutch, French, German, Italian, and Spanish.
To order your free personal copy, visit www.axis.com/free_cd



Learn Network Video with the Leaders

The market is changing fast! Get yourself up to speed with the latest advances in network video at the AXIS Academy.

Deploying a brand new network video system, or migrating an existing surveillance system from analog to a networked system, is a process which involves many decisions. All the technical guides and manuals in the world are no substitute for in-depth discussions with experts, in person training, and hands-on labs. That's what you get when joining an AXIS Academy training. As new technologies and possibilities in video surveillance continue to emerge at a fast pace, the AXIS Academy gives you an opportunity to update your knowledge and thereby stay on top of the latest developments in the area. It's also the place to go for valuable tips and insights based on Axis' extensive experience.

Seminars and hands-on classes exploring a variety of network video related matters
Network video started at Axis. We invented and launched the first network camera back in 1996, and we continue to lead what has become a huge market as network video systems replace analog systems at an accelerating rate. The AXIS Academy brings this unique perspective to seminars and hands-on classes, offering different levels and modules depending on your existing knowledge. Topics such as camera optics, video intelligence, best practices in network design, and camera selection are all included. We explore the strengths and weaknesses of different installation scenarios. Discussions are tailored to participants' needs, whether you design, sell, service, integrate, or operate network video systems. Through interactive, dynamic sharing of experiences, the best possible system strategies can be worked out.

Join the AXIS Academy now and anticipate future opportunities

Attending an AXIS Academy course is an investment that pays off threefold: in time, money, and peace of mind. You gain an understanding of how to make the most of a network video solution, whether it's for security surveillance or remote monitoring. And, as technologies and your system needs change, the AXIS Academy remains a resource you can count on to remain up-dated and indeed, to help you anticipate future opportunities.

To book your place in an upcoming AXIS Academy class, or for general information, please contact your local Axis office.



Notes

Notes

Notes

Notes

Contact information

CORPORATE HEADQUARTERS, SWEDEN

Head office, Lund
Axis Communications AB
Emdalavägen 14
SE-223 69 Lund
Tel: +46 46 272 18 00
Fax: +46 46 13 61 30
www.axis.com/request

AUSTRALIA

Melbourne
Axis Communications Pty Ltd
Level 25, 367 Collins Street
Melbourne VIC 3000
Australia
Tel: +613 9221 6133
www.axis.com/request

CANADA

Toronto
Axis Communications Canada
117 Lakeshore Road E,
Suite 304
Mississauga, ON L5G 4T6
Canada
Tel: +1 978 614 2000
www.axis.com/request

CHINA

Shanghai
Axis Communications Ltd
Rm. 001, 6/F, Novel Building
887 Huai Hai Zhong Rd.
Shanghai 200020
Tel: +86 21 6431 1690
Fax: +86 21 6433 8264
www.axis.com/request

FRANCE, BELGIUM, LUXEMBURG

Paris
Axis Communications S.A.
7-9 avenue Aristide Briand
94230 Cachan
Tel: +33 1 49 69 15 50
Fax: +33 1 49 69 15 59
www.axis.com/request

Support:
Tel: +33 1 49 69 15 50
E-mail: support-fr@axis.com

GERMANY, AUSTRIA, SWITZERLAND

Munich
Axis Communications GmbH
Lilienthalstr. 25
DE-85399 Hallbergmoos
Tel: +49 811 555 08 0
Fax: +49 811 555 08 69
www.axis.com/request

Support:
Tel: +49 1805 294 77 8

ITALY

Torino
Axis Communications
Via Roma 47
10025 Pino Torinese
Torino
Tel/Fax: +39 011 841 321
www.axis.com/request

JAPAN

Tokyo
Axis Communications K.K.
Shinagawa East One Tower
13F
2-16-1 Konan
Minato-ku Tokyo 108-0075
Tel: +81 3 6716 7850
Fax: +81 3 6716 7851
www.axis.com/request

KOREA

Seoul
Axis Communications Korea
Co., Ltd.
Rm 407, Life Combi B/D.
61-4 Yoido-dong
Yeongdeungpo-Ku
Seoul
Tel: +82 2 780 9636
Fax: +82 2 6280 9636
www.axis.com/request

THE NETHERLANDS

Rotterdam
Axis Communications BV
Benelux
Glashaven 38
NL-3011 XJ Rotterdam
Tel: +31 10 444 34 34
Fax: +31 10 750 46 99
www.axis.com/request

Support:
Tel: +31 10 444 34 34

SINGAPORE

Axis Communications
(S) Pte Ltd
541 Orchard Road
#18-03/04 Liat Towers
Singapore 238881
Tel: +65 6 836 2777
Fax: +65 6 836 3106
www.axis.com/request

SPAIN

Madrid
Axernet Communications S.A.
Sector Oficinas 31, 1
ES-28760 Tres Cantos
Tel: +34 91 803 46 43
Fax: +34 91 803 54 52
www.axis.com/request

Support:
Tel: +34 91 803 46 43

TAIWAN

Taipei
Axis Communications Ltd
8F-11, 101 Fushing North
Road
Taipei
Tel: +886 2 2546 9668
Fax: +886 2 2546 1911
www.axis.com/request

UNITED KINGDOM

Hertfordshire
Axis Communications (UK) Ltd.
Suite 2, Ladygrove Court
Hitchwood Lane
Preston, Nr Hitchin
Hertfordshire SG4 7SA
Tel: +44 870 162 0047
Fax: +44 870 777 8620
www.axis.com/request

Support:
Tel: +44 870 162 0048

UNITED STATES

Boston
Axis Communications Inc.
100 Apollo Drive
Chelmsford, MA 01824
Tel: +1 978 614 2000
Fax: +1 978 614 2100
www.axis.com/request

Support:
Tel: 800 444 2947

San Diego
9191 Towne Centre Drive
Suite #420
San Diego, CA 92122
Tel: +1 978 614 2000
www.axis.com/request

Support:
Tel: 800 444 2947

About Axis

Axis increases the value of network solutions. The company is an innovative market leader in network video and print servers. Axis' products and solutions are focused on applications such as security surveillance, remote monitoring and document management. The products are based on in-house developed chip technology, which is also sold to third parties.

Axis was founded in 1984 and is listed on the Stockholmsbörsen (XSSE: AXIS) Attract 40-list. Axis operates globally with offices in 16 countries and in cooperation with distributors, system integrators and OEM partners in 70 countries. Markets outside Sweden account for more than 95% of sales. Information about Axis can be found at www.axis.com

www.axis.com