

ARTISAN®
TECHNOLOGY GROUP

Your **definitive** source for quality pre-owned equipment.

Artisan Technology Group
(217) 352-9330 | sales@artisantg.com | artisantg.com

Full-service, independent repair center
with experienced engineers and technicians on staff.

We buy your excess, underutilized, and idle equipment
along with credit for buybacks and trade-ins.

Custom engineering
so your equipment works exactly as you specify.

- Critical and expedited services
- In stock / Ready-to-ship
- Leasing / Rentals / Demos
- ITAR-certified secure asset solutions

Expert team | Trust guarantee | 100% satisfaction

All trademarks, brand names, and brands appearing herein are the property of their respective owners.

Visit our website - *Click HERE*

USER'S MANUAL

AXIS P5532-E PTZ Dome Network Camera

AXIS P5534-E PTZ Dome Network Camera

Notices

This manual is intended for administrators and users of the AXIS P5532-E/P5534-E PTZ Dome Network Camera, and is applicable for firmware release 5.20 and later. It includes instructions for using and managing the camera on your network. Previous experience of networking will be of use when using this product. Some knowledge of UNIX or Linux-based systems may also be beneficial for advanced users, for developing shell scripts and applications. Later versions of this document will be posted to the Axis Website, as required. See also the product's online help, available via the Web-based interface.

Liability

Every care has been taken in the preparation of this manual. Please inform your local Axis office of any inaccuracies or omissions. Axis Communications AB cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. Axis Communications AB makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Axis Communications AB shall not be liable nor responsible for incidental or consequential damages in connection with the furnishing, performance or use of this material.

Intellectual Property Rights

Axis AB has intellectual property rights relating to technology embodied in the product described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the patents listed at http://www.axis.com/patent.htm and one or more additional patents or pending patent applications in the US and other countries.

This product contains licensed third-party software. See the menu item "About" in the product's user interface for more information.

This product contains source code copyright Apple Computer, Inc., under the terms of Apple Public Source License 2.0 (see http://www.opensource.apple.com/apsl/).
The source code is available from:
http://developer.apple.com/darwin/projects/bonjour/

Equipment Modifications

This equipment must be installed and used in strict accordance with the instructions given in the user documentation. This equipment contains no user-serviceable components. Unauthorized equipment changes or modifications will invalidate all applicable regulatory certifications and approvals.

Trademark Acknowledgments

Apple, Boa, Bonjour, Ethernet, Internet Explorer, Linux, Microsoft, Mozilla, Netscape Navigator, OS/2, Real, SMPTE, QuickTime, UNIX, Windows, WWW are registered trademarks of the respective holders. Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. Axis Communications AB is independent of Sun Microsystems Inc.
UPnP™ is a certification mark of the UPnP™ Implementers Corporation.

Support

Should you require any technical assistance, please contact your Axis reseller. If your questions cannot be answered immediately, your reseller will forward your queries through the appropriate channels to ensure a rapid response. If you are connected to the Internet, you can:
- download user documentation and firmware updates
- find answers to resolved problems in the FAQ database. Search by product, category, or phrases
- report problems to Axis support by logging in to your private support area
- visit Axis Support at www.axis.com/techsup

AXIS P5532-E/P5534-E PTZ Dome Network Camera User's Manual
Rev. 1.0
Copyright© Axis Communications AB, 2010
June 2010 Part no. 39647

Contents

Notices . . . 2
Product Description . . . 4
Key features . . . 4
Overview . . . 5
Status Indicators . . . 6
Accessing the Camera . . . 7
Access from a browser . . . 7
Access from the Internet . . . 7
Setting the root password . . . 8
Video Streams . . . 11
How to stream H.264 . . . 11
Motion JPEG . . . 11
Alternative methods of accessing the video stream . . . 12
Setup Tools . . . 13
Basic Setup . . . 13
Video . . . 14
Video Stream . . . 14
Camera Settings . . . 16
Overlay Image . . . 17
Privacy mask . . . 17
Live View Config . . . 18
Layout . . . 18
PTZ (Pan Tilt Zoom) . . . 20
Preset Positions . . . 20
Guard Tour . . . 20
OSDI Zones . . . 20
Advanced . . . 21
Applications . . . 22
Events . . . 23
Event Servers . . . 23
Event Types . . . 23
Gatekeeper . . . 25
Recording List . . . 28
Continuous Recording . . . 29
System Options . . . 30
Security . . . 30
Network . . . 32
Storage . . . 37
Maintenance . . . 37
Support . . . 37
Advanced . . . 38
About . . . 39
Resetting to the Factory Default Settings . . . 39
Troubleshooting . . . 40
Checking the Firmware . . . 40
Upgrading the Firmware . . . 40
Emergency Recovery Procedure . . . 40
AXIS Support . . . 41
Symptoms, possible causes and remedial actions . . . 42
LED Indicator flash routine . . . 44
Technical Specifications . . . 45
General performance considerations . . . 47
Glossary of Terms . . . 48
Index . . . 54

Product Description

This manual applies to the following products:

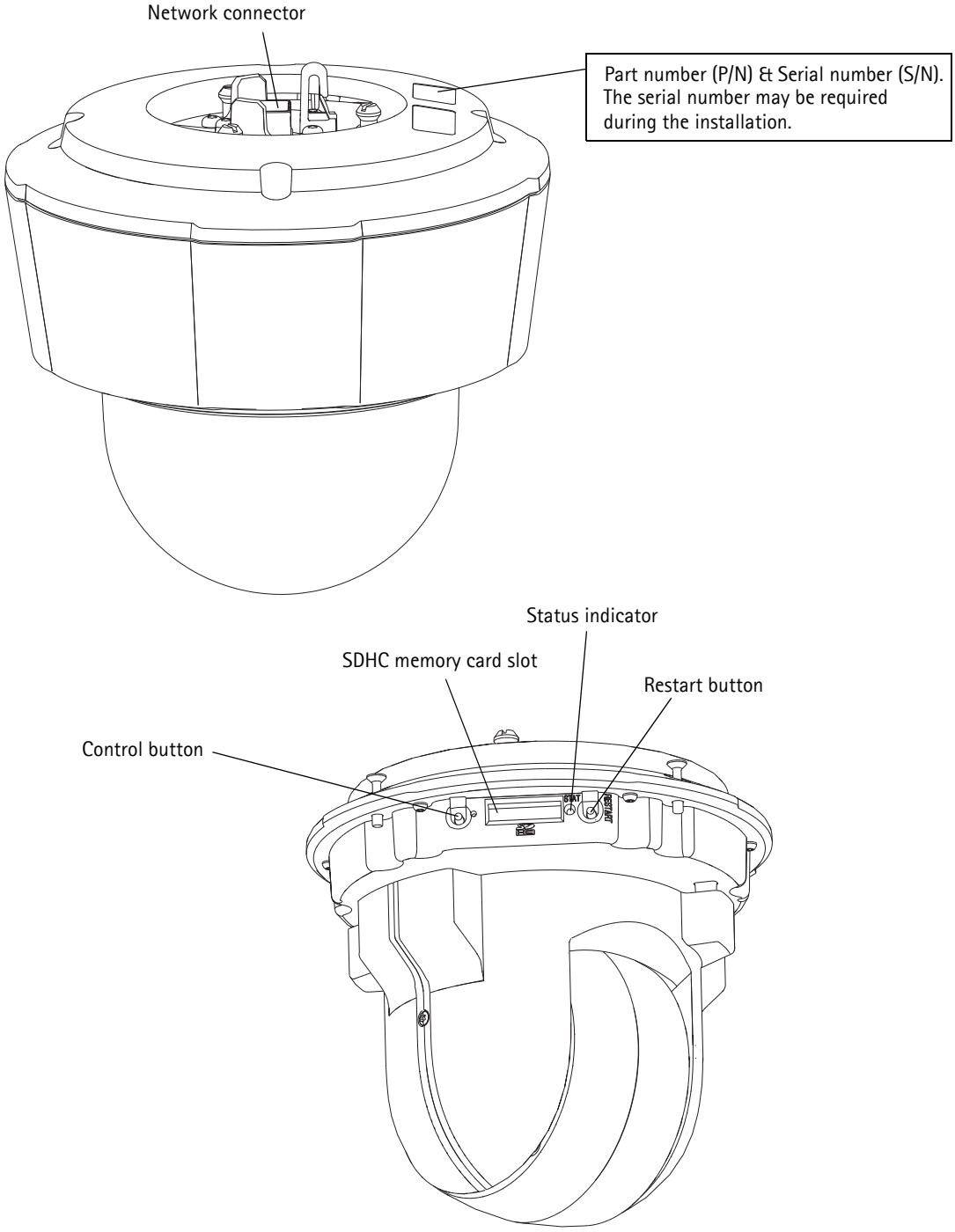
- AXIS P5532-E PTZ Dome Network Camera.
- AXIS P5534-E PTZ Dome Network Camera.

The information provided here applies to both models, except where otherwise indicated.

Key features

- **HDTV 720p**
  AXIS P5534-E offers HDTV 720p in compliance with SMPTE 296M standard of 1280 x 720 pixel resolution, full frame rate, high color fidelity and a 16:9 format. AXIS P5532-E offers D1 and 4CIF resolution (720 x 480/576 pixels).
- **Outdoor-ready**
  AXIS P5532-E/P5534-E is designed for quick and easy installation in demanding indoor and outdoor environments. There is no need to purchase and mount a separate outdoor housing. They eliminate the cost and complexity of pre-mounting a camera in an enclosure and minimizes the risk of incorrect mounting, which helps to ensure optimal camera performance.
  With an IP66 and NEMA 4X rating, it is dust tight and offer protection against high-pressure water jets. AXIS P5532-E/P5534-E have a built-in heater, fans and a removable sunshield, allowing the camera to be used in temperatures ranging from -20 °C up to 50 °C (-4 °F up to 122 °F).
- **Zoom functionality with autofocus**
  AXIS P5532-E offers a powerful 29x optical and 12x digital zoom, providing crisp, clear and rich detail of both zoomed in and zoomed out images. AXIS P5534-E offers 18x optical and 12x digital zoom in HDTV. Due to its HDTV resolution, the 18x zoom provides not only a level of detail that is comparable to a 36x-zoom, 4CIF camera, but also the extra advantage of a wider, 16:9 field of view in zoomed-in views.
- **High PoE (Power over Ethernet)**
  AXIS P5532-E/P5534-E can be powered through High PoE, which simplifies installation since only one cable is needed for carrying power, as well as video and pan/tilt/zoom controls. With High PoE, the cameras can operate even during a power failure as the network can be connected to an Uninterruptible Power Supply. A High PoE midspan is supplied with the camera.
- **Advanced Gatekeeper functionality**
  The Advanced Gatekeeper functionality enables the camera to automatically pan, tilt and zoom in when there is activity in the scene, and to return to a pre-determined position after a preset time.
- **Multiple H.264 and Motion JPEG streams**
  AXIS P5532-E/P5534-E offers the most efficient video compression format H.264 (MPEG-4 Part 10/AVC), which saves up to 80% in bandwidth and storage use compared with Motion JPEG without compromising image quality. The camera also supports Motion JPEG for increased flexibility. AXIS P5534 supports simultaneous, individually configured streams in HDTV 720p.
- **Local storage**
  The camera comes with a built-in slot for an SD/SDHC memory card, enabling several days of recordings to be stored locally without any external equipment.
- **Progressive Scan**
  Progressive scan provides full resolution images of moving objects without distortion.
- **Advanced security and network management**
  AXIS P5532-E/P5534-E offers the highest degree of security, including HTTPS encrypted video streams without affecting performance and IPv6 support in addition to IPv4. IPv6 is a requirement in many large installations.

Overview



Note:

To insert and remove an SD card, or access the camera's control and restart buttons, the sunshield and top cover must first be removed; for instructions please refer to the Installation Guide.

Network connector – RJ-45 Ethernet connector. Supports High Power over Ethernet (IEE 802.3at). Use Axis T8123 Midspan (included). Shielded cable shall be used to comply with EMC.

Control button – The control button is used for

- Connecting to an AXIS Video Hosting System service, see page 33. To connect, press and hold the button until the Status LED flashes green.
- Connecting to AXIS Internet Dynamic DNS Service, see page 33. To connect, press the button once.
- Restoring the camera to factory default settings, see Resetting to Factory Default Settings, on *Resetting to the Factory Default Settings,* on page 39.

Restart button – Press the button to restart the camera.

Serial number label – Part number (P/N) and Serial number (S/N). The serial number may be required during installation.

SDHC memory card slot – A standard or high capacity SD memory card (not included) can be used for local recording with removable storage. To insert and remove an SD card, the camera's sunshield and top cover must first be removed; for instructions please refer to the Installation Guide.

Note:

Before removal, the SD card should be unmounted to prevent corruption of recordings. To unmount the SD card, go to **Setup > System Options > Storage > SD Card** and click **Unmount**.

Status Indicators

After the startup ad self test routines the indicator flashes as follows.

Unit	Color	Description
AXIS P5532-E AXIS P5534-E	Unlit	Steady during connection/normal operation.
	Amber	Steady during system initiating. Flashes during firmware upgrade and reset to factory default.
	Amber/red	No network connection
	Red	Firmware upgrade failure.
	Green	Steady for 10 sec. after successful restart.

See also *LED Indicator flash routine,* on page 44.

Unit	LED	Color	Description
AXIS T8123	Port	Unlit	No camera connected.
		Yellow	Insufficient power for camera and heater. Check cable.
		Flashing	Power overload
		Green	Camera connected, normal behavior.
	AC input	Steady green	AC power connected.

Accessing the Camera

To install the network camera, refer to the Installation Guide supplied with your product.

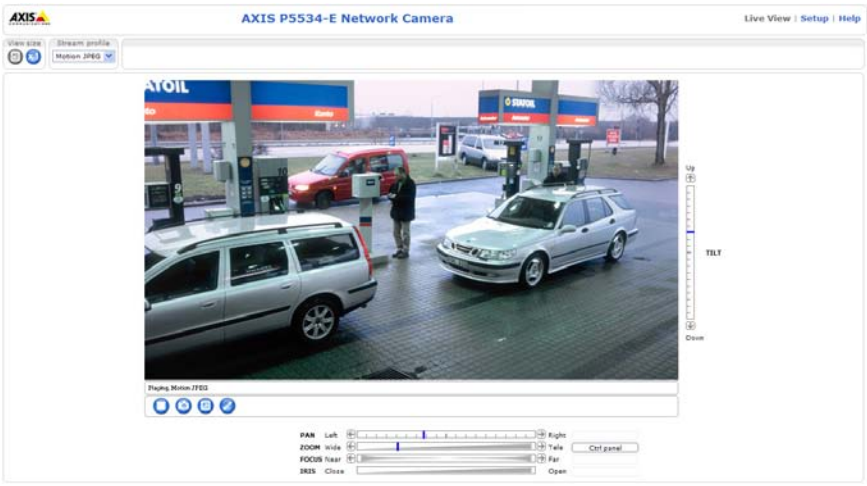
The network camera can be used with most operating systems and browsers. The recommended browsers are Internet Explorer with Windows, Safari with Macintosh and Firefox with other operating systems. See *Technical Specifications,* on page 45.

Notes:

- To view streaming video in Microsoft Internet Explorer, set your browser to allow ActiveX controls and install AXIS Media Control (AMC) on your workstation.
- QuickTime™ is also supported for viewing streaming H.264 video.
- If your computer restricts the use of additional software components, the camera can be configured to use a Java applet for viewing Motion JPEG.
- The network camera includes one (1) decoder license for viewing H.264 video streams. This is automatically installed with AMC. The administrator can disable the installation of the H.264 decoder, to prevent installation of unlicensed copies.

Access from a browser

1. Start a browser (Internet Explorer, Firefox, Safari).
2. Enter the IP address or host name of the camera in the **Location/Address** field of your browser.
   To access the camera from a Macintosh computer (Mac OS X), click on the Bonjour tab and select the network camera from the drop-down list.
3. If this is the first time you are accessing the camera, see *Setting the root password,* on page 8. Otherwise enter your user name and password, set by the administrator.
4. The camera's Live View page appears in your browser.



Note:

The layout of the Live View page may have been customized to specific requirements. Consequently, some of the examples and functions featured here may differ from those displayed on your own Live View page.

Access from the Internet

Once connected, the camera is accessible on your local network (LAN). To access the camera from the Internet you must configure your broadband router to allow incoming data traffic to the camera. To do this, enable the NAT-traversal feature, which will attempt to automatically configure the router to allow access to the camera. This is enabled from **Setup > System Options > Network > TCP/IP Advanced**.

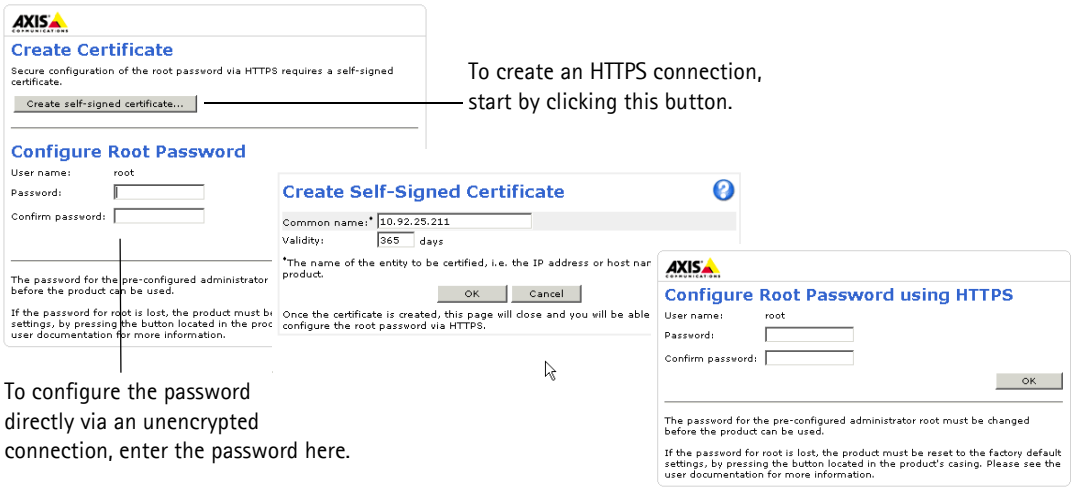
For more information, please see *NAT traversal (port mapping) for IPv4*, on page 34. See also AXIS Internet Dynamic DNS Service at www.axiscam.net For Technical notes on this and other topics, visit the Axis Support web at www.axis.com/techsup

Setting the root password

To gain access to the product, you must set the password for the default administrator user - '**root**'. This is done in the '**Configure Root Password**' dialog, which is displayed when the network camera is accessed for the first time. To prevent network eavesdropping the root password can be set via an encrypted HTTPS connection, which requires an HTTPS certificate

Note:

HTTPS (Hypertext Transfer Protocol over SSL) is a protocol used to encrypt the traffic between web browsers and servers. The HTTPS certificate ensures encrypted exchange of information.



To set the password via a standard HTTP connection, enter it directly in the first dialog shown above.

To set the password via an encrypted HTTPS connection, follow these steps:

1. Click **Create self-signed certificate**.
2. Provide the requested information and click **OK**. The certificate is created and the password can now be set securely. All traffic to and from the network camera is encrypted from this point on.
3. Enter a password and then re-enter it to confirm the spelling. Click **OK**. The password has now been configured.

Notes:

- The default administrator user name '**root**' is permanent and cannot be deleted.
- If the password for root is lost, the camera must be reset to the factory default settings. See page 39.
- If prompted, click **Yes** to install AXIS Media Control, which allows viewing of the video stream in Internet Explorer. You will need administrator rights on the computer to do this. If using Windows 7 or Windows Vista, you must also run Internet Explorer as administrator; right-click the Internet Explorer icon and select **Run as Administrator**.

The Live View page

How you customize the Live View page determines which buttons are visible. Not all the buttons described below will show up, unless configured to do so. These are configured under **Setup > Live View Config > Layout**.



View size – Click to scale the image down to 800 pixels wide or to full scale. Only available in MJPEG.



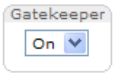
The Stream Profile drop-down list allows you to select a customized or pre-programmed stream profile on the Live View page. Stream profiles are configured under **Setup > Video > Stream Profiles**, see *Stream Profiles*, on page 16 for more information.



The **Trigger buttons** can trigger an event directly from the Live View page. The buttons are configured under **Setup > Live View Config > Layout**.



The **Snapshot** button saves a snapshot of the video image currently on display. Right-click on the video image to save it in JPEG format on your computer. This button is primarily intended for use when the AMC Media Control viewer toolbar is not available.



Enable/disable the **Gatekeeper** by selecting On or Off from the drop-down list. The Gatekeeper is configured under **Setup** > **Events** > **Gatekeeper**, see page 25.



Activate the camera's **Fan** manually with this button.



Activate the camera's **Heater** manually with this button.

AXIS Media Control viewer toolbar

The AXIS Media Control viewer toolbar is available in Internet Explorer only. See *AXIS Media Control (AMC)*, on page 12 for more information. AMC displays the following buttons:



The **Play** button connects to the Axis product and starts playing a media stream.



The **Stop** button stops the video stream.



The **Snapshot** button takes a snapshot of the current image. The location where the image is saved can be specified in the AMC Control Panel.



Click the **View Full Screen** button and the video image will fill the entire screen. Press **Esc** (Escape) on the computer keyboard to cancel full screen view.



The **Record** button is used to record the current video stream. The location where the recording is saved can be specified in the AMC Control Panel.

Pan/Tilt/Zoom Controls

The Live View page also displays the Pan/Tilt/Zoom (PTZ) controls. The administrator can enable/disable controls for specified users under **System Options > Security > Users**.

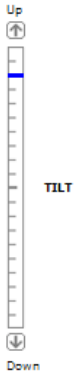
With the **PTZ Control Queue** enabled the time each user is in control of the PTZ settings is limited. Click the buttons to request or release control of the PTZ controls. The PTZ Control Queue is set up under **PTZ** > **Control Queue**.



Click the **Emulate joystick mode** button and click in the image to move the camera view in the direction of the mouse pointer.



Click the **Center mode** button and click on a position in the image to center the camera view on that position.

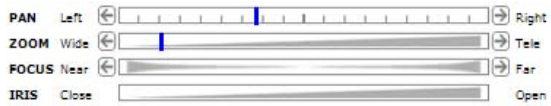


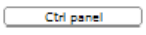
Pan and Tilt bars – Click a position directly on the bar to steer the camera view directly to the new position in one smooth movement or click on the arrows at the ends of the bars to steer the camera in steps.

Zoom bar – Click a position directly on the zoom bar to zoom all the way to the new position in one movement or click the arrows at the ends of the bar to zoom in steps.

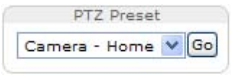
Focus bar – Click a position directly on the focus bar to set focus at a new position in one movement or click the arrows at the ends of the bar to change focus in steps.

Iris bar – Click a position directly on the iris bar to change the degree the iris opens to in one movement or click the arrows at the ends of the bar to change the iris in steps.





Click the **Ctrl panel** button to open the PTZ control panel which provides additional PTZ controls. User-defined buttons can also appear in the Control panel, see *Controls,* on page 21.



Select a **PTZ preset** position to steer the camera view to the saved position, see *Preset Positions,* on page 20.

Video Streams

The network camera provides several image and video stream formats. Your requirements and the properties of your network will determine the type you use.

The Live View page in the network camera provides access to H.264 and Motion JPEG video streams, and to the list of available stream profiles. Other applications and clients can also access these video streams/images directly, without going via the Live View page.

How to stream H.264

This video compression standard makes good use of bandwidth, and can provide high quality video streams at less than 1 Mbit/s.

Deciding which combination of protocols and methods to use depends on your viewing requirements, and on the properties of your network. The available options in Axis Media Control are:

<table>
<tr><td>Unicast RTP</td><td>This unicast method (RTP over UDP) is used for live unicast video, especially when it is important to always have an up-to-date video stream, even if some images are dropped.</td><td rowspan="3">Unicasting is used for video-on-demand transmission, so that there is no video traffic on the network until a client connects and requests the stream.

Note that there are a maximum of 20 simultaneous unicast connections.</td></tr>
<tr><td>RTP over RTSP</td><td>This unicast method (RTP tunneled over RTSP) is useful as it is relatively simple to configure firewalls to allow RTSP traffic.</td></tr>
<tr><td>RTP over RTSP over HTTP</td><td>This unicast method can be used to traverse firewalls. Firewalls are commonly configured to allow the HTTP protocol, thus allowing RTP to be tunneled.</td></tr>
<tr><td>Multicast RTP</td><td colspan="2">This method (RTP over UDP) should be used for live multicast video. The video stream is always up-to-date, even if some images are dropped.
Multicasting provides the most efficient usage of bandwidth when there are large numbers of clients viewing simultaneously. A multicast broadcast cannot however, pass a network router unless the router is configured to allow this. It is not possible to multicast over the Internet, for example. Note also that all multicast viewers count as one unicast viewer in the maximum total of 20 simultaneous connections.</td></tr>
</table>

Axis Media Control negotiates with the camera to determine the transport protocol to use. The order of priority, listed in the AMC Control Panel, can be changed and the options disabled, to suit specific requirements.

Important!

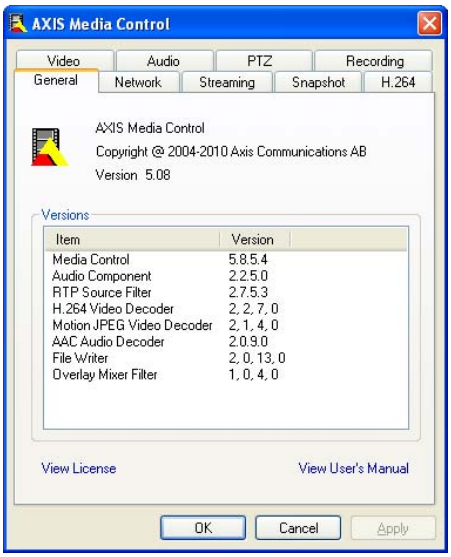
H.264 is licensed technology. The network camera includes one H.264 viewing client license. Installing additional unlicensed copies of the viewing client is prohibited. To purchase additional licenses, contact your Axis reseller.

Motion JPEG

This format uses standard JPEG still images for the video stream. These images are then displayed and updated at a rate sufficient to create a stream that shows constantly updated motion.

The Motion JPEG stream uses considerable amounts of bandwidth, but provides excellent image quality and access to every image contained in the stream. The recommended method of accessing Motion JPEG live video from the network camera is to use the AXIS Media Control (AMC) in Internet Explorer in Windows.

AXIS Media Control (AMC)



AXIS Media Control (AMC) in Internet Explorer in Windows is the recommended method of accessing live video from the network camera.

The AMC Control Panel can be used to configure various video settings. Please see the AXIS Media Control User's Manual for more information.

The AMC Control Panel is automatically installed on first use, after which it can be configured. Open the AMC Control Panel from:

- Windows Control Panel (from the Start menu)
- Alternatively, right-click the video image in Internet Explorer and click **Settings** to access the AMC window.

Alternative methods of accessing the video stream

You can also access video/images from the network camera in the following ways:

- Motion JPEG server push (if supported by the client, Firefox, for example). This option maintains an open HTTP connection to the browser and sends data as and when required, for as long as required.
- Still JPEG images in a browser. Enter the path - http://<ip>/axis-cgi/jpg/image.cgi
- Windows Media Player. This requires AXIS Media Control and the H.264 decoder to be installed. The paths that can be used are listed below in the order of preference:
  - Unicast via RTP: axrtpu://<ip>/axis-media/media.amp
  - Unicast via RTSP: axrtsp://<ip>/axis-media/media.amp
  - Unicast via RTSP, tunneled via HTTP: axrtsphttp://<ip>/axis-media/media.amp
  - Multicast: axrtpm://<ip>/axis-media/media.amp
- To access the video stream from **QuickTime™** the following paths can be used:
  - rtsp://<ip>/axis-media/media.amp
  - rtsp://<ip>/axis-media/media.3gp

<ip> = IP address

Notes: •

- The network camera supports QuickTime 6.5.1 and later.
- QuickTime adds latency to the video stream (up to 3 seconds).
- It may be possible to use other players to view the H.264 stream using the paths above, although Axis does not guarantee this.
- <ip> = IP address

Setup Tools

AXIS P5532-E/P5534-E can be configured by users with administrator or operator rights. To access the product's Setup tools, click **Setup** in the top right-hand corner of the Live View page.

- **Administrators** have unrestricted access to all settings.
- **Operators** have access to **Video & Audio**, **Live View Config**, **PTZ**, **Events** and **Recording List**.

See also the online help available by clicking on each Setup page.



Basic Setup

Basic Setup provides shortcuts to the settings that should be made before using the network camera:

1. Users, see page 30.
2. TCP/IP, see page 32.
3. Date & Time, see page 32.
4. Video Stream, see page 14.

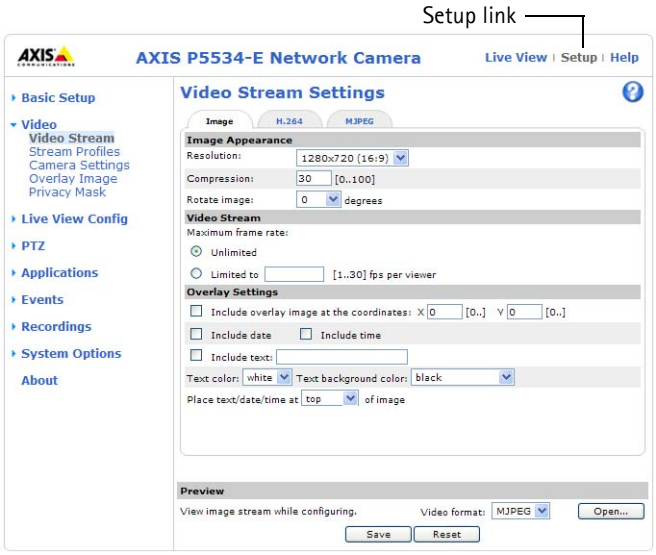
Video

Click to access the online help that explains the Setup tools.

Video Stream

The video stream settings appear under in three different tabs:

- Image
- H.264
- MJPEG



Preview

For a preview of the image before saving, select the **Video format** and click **Open**.

The **pixel counter** shows the number of pixels in an area of the image and can be used to ensure that the size of the image fulfills certain requirements, for example for face recognition. Use the mouse to move and resize the rectangle, or enter the number of pixels in the Width and Height fields and click **Apply**.

When satisfied with the settings, click **Save.**

Image

Image Appearance

Use these settings to modify the image resolution and compression. Setting the compression level affects the image quality and the amount of bandwidth required, the lower the compression, the higher the image quality with higher bandwidth requirements. The image can also be rotated.

See the online help files for more information.

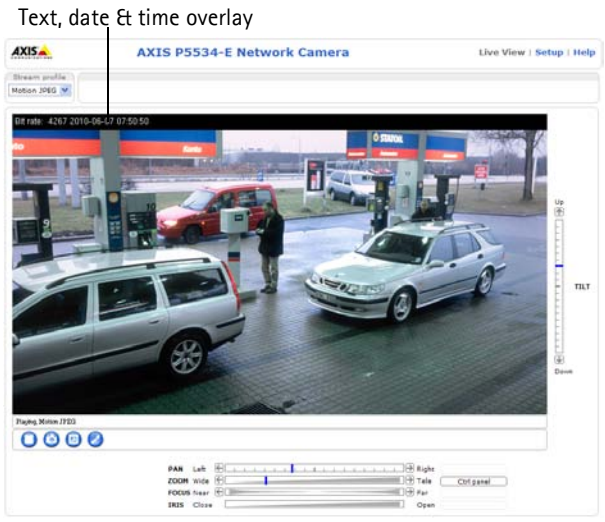
Video Stream

To avoid bandwidth problems on the network, the **frame rate** allowed to each viewer can be limited. Select the **Unlimited** radio button option to allow the highest available frame rate or select the **Limited to** radio button and enter a value (1-30) fps in the field.

Overlay Settings

To place an overlay image at specific coordinates, check the **Include overlay image at coordinates** and enter the X and Y coordinates. The overlay image must first be uploaded to the network camera, see *Overlay Image,* on page 17.

Text, date and time can also be used as an overlay. See the online help files for information on available options.



H.264

GOV Settings

The GOV structure describes the composition of the video stream and setting the GOV-length to a higher value saves considerably on bandwidth but may have an adverse effect on image quality.

Bit Rate Control

The bit rate can be set as **Variable Bit Rate** (VBR) or **Constant Bit Rate** (CBR). VBR adjusts the bit rate according to the image complexity, using up bandwidth for increased activity in the image, and less for lower activity in the monitored area.

CBR allows you to set a fixed **Target bit rate** that consumes a predictable amount of bandwidth. As the bit rate would usually need to increase for increased image activity, but in this case cannot, the frame rate and image quality are affected negatively. To partly compensate for this, it is possible to prioritize either the frame rate or the image quality whenever the bit rate needs to be increased. Not setting a priority means the frame rate and image quality are equally affected.

Note:

To determine a reasonable bit rate, go to **Setup > Video > Video Stream > Image**. Under Overlay Settings, check the **Include** checkbox and enter the code **#b** in the **Include text**: field. The current bit rate will display as a text overlay on the Live View page.

To preview the image stream while configuring the GOV settings and Bit rate control, select **Open** under **Preview.**

MJPEG

Sometimes the image size is large due to low light or complex scenery. Adjusting the **Maximum frame size** helps to control the bandwidth and storage used by the Motion JPEG video stream in these situations. Defining the frame size as **Default** provides consistently good image quality at the expense of increased bandwidth and storage usage during low light. Limiting the frame size optimizes bandwidth and storage usage, but may give poor image quality. To prevent increased bandwidth and storage usage, the maximum frame size should be set to an optimal value.

Stream Profiles

There are four pre-programmed stream profiles available for quick set-up. These settings can be adjusted and new, customized profiles can be created. Each profile has a descriptive name, describing its usage and/or purpose. The profiles can be accessed from the Live View page.

- To create a new stream profile, click **Add** to bring up the **Stream Profile Settings** dialog.
  1. Enter a unique name and a description for your profile.
  2. Select a **Video encoding** type (H.264 or MJPEG) from the drop-down list.
  3. Modify the stream settings under the **Image**, **H.264** and **MJPEG** tabs. See *Video Stream,* on page 14
  4. Click **OK** to save the profile.
- To copy an existing stream profile, click **Copy** and enter a new name. Change the stream profile settings as above.
- To modify an existing stream profile, click **Modify** and change the settings as above. The original settings for the pre-programmed profiles can always be restored by clicking **Restore**.
- To remove a stream profile, click **Remove**. Pre-programmed profiles cannot be removed.

Camera Settings

This page provides access to the image settings for the network camera.

Image Appearance

Color level - Select an appropriate level by entering a value in the range 0-100. Lower values mean less color saturation, whilst the value 100 gives maximum color saturation.

Brightness - The image brightness can be adjusted in the range 0-100, where a higher value produces a brighter image.

Sharpness - Controls the amount of sharpening applied to the image. A sharper image might increase image noise, especially in low light conditions. A lower setting reduces image noise, but the image would be less sharp.

White balance

White balance is used to compensate for the different colors present in different light sources, to make the colors in the image appear the same. The network camera can be set to automatically identify the light source and compensate for its color. Alternatively, the type of light source can be manually selected from the drop-down list. Please see the online help files for a description of each available setting.

Wide dynamic range

Wide dynamic range can improve the exposure when there is a considerable contrast between light and dark areas in the image.

Exposure Settings

Configure the exposure settings to suit the image quality requirements in relation to lighting, frame rate and bandwith considerations.

Exposure control - This setting is used to adapt to the amount or type of light used. **Automatic** is the default setting and can be used in most situations. The shutter speed is automatically set to produce optimum image quality.

Max exposure time - Select the maximum exposure time from the drop-down list. Increasing the exposure time will improve image quality, but may decrease the frame rate. There may also be an increase in motion blur. Checking **Allow slow shutter** decreases the shutter speed in low light to improve image brightness.

Enable Backlight compensation - Enable this option if a bright spot of light, for example a light bulb, causes other areas in the image to appear to dark.

Exposure zones - This setting determines which part of the image is used to calculate the exposure. For most situations, the **Auto** settings can be used.

IR cut filter - Set the filter to **Off** to allow the camera to "see" infrared light; it increases the light sensitivity, for example at night. The image is shown in black & white when the IR cut filter is off. Set to **Auto** to automatically switch between **On** and **Off** according to the lighting conditions.

Max gain - Measured in decibels (dB). A high level of amplification may provide a better image in very low light situations. A high gain will also increase the amount of image noise.

Image Settings

Autofocus enabled - Autofocus is enabled by default.

Image freeze on PTZ - Select **All movements** to freeze the image while the camera is moving during a pan, tilt or zoom operation. Once the camera reaches its new position the current image is shown. **Presets** freezes the image only when the camera moves between preset positions.

View Image Settings

Click **View** to view the video stream with the current configuration. Once satisfied, click **Save**.

Overlay Image

An overlay image is a static image superimposed over the video image. The overlay image can be used to provide extra information, or to mask a part of the video image. See the online help for supported image formats and sizes.

To use your own image, e.g. a logo, it must first be uploaded to the network camera. Click **Browse** and locate the image file on the computer. Click **Upload**. When uploaded, the file can be selected in the **Use overlay image** drop-down list.

To place the overlay image in the live view image, select **Include overlay image at coordinates** under **Video > Video Stream > Image**, see *Overlay Settings,* on page 14.

Once satisfied, click **Save**.

Privacy mask

A privacy mask is an area of solid color that prohibits users from viewing parts of the monitored area. Up to eight privacy masks can be used. Privacy masks cannot be bypassed via the VAPIX® Application Programming Interface (API).

Privacy Mask List

The Privacy Mask List shows all the masks that are currently configured in the network camera and if they are enabled.

Add/Edit Privacy mask

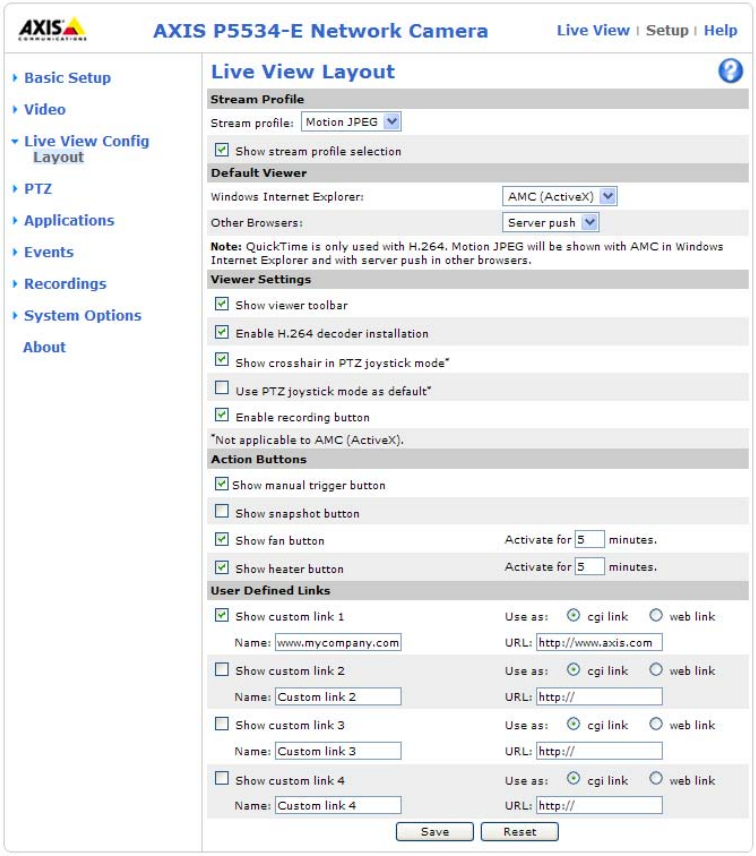
To define a new mask:

1. Click **Add mask.** A rectangle appears on the image.
2. Use the mouse to move the rectangle. To resize, click and pull the bottom right-hand corner.
3. Choose a color, black, white, gray or red, from the **Privacy mask color** drop-down list.
4. Enter a descriptive name in the **Mask name** field.
5. Click **Save**.

To edit a privacy mask, select the mask and reshape, move or change color as needed.

Live View Config

Layout



Stream Profile

From the **Stream Profile** drop-down list, select the stream profile that is to be used for the Live View page. Listed are the pre-programmed stream profiles as well as the ones created under **Video > Stream Profiles**. See *Stream Profiles,* on page 16, for more information

Default Viewer

From the drop-down lists, select the default method for viewing video images for your browser. The camera attempts to show the video images in the selected video format and viewer. If this is not possible, the camera overrides the settings and selects the best available combination.

Browser	Viewer	Description
Windows Internet Explorer	AMC	Recommended viewer in Windows Internet Explorer (H.264/Motion JPEG).
	QuickTime	H.264
	Java applet	A slower imaging alternative to AMC. Requires one of the following installed on the client: • JVM (J2SE) 1.4.2 or higher • JRE (J2SE) 5.0 or higher
	Still image	Displays still images only. Click the Refresh button in your browser to view a new image.
Other browsers	Server Push	Recommended viewer for other browsers (Motion JPEG).
	QuickTime	H.264
	Java applet	A slower imaging alternative to Server Push (Motion JPEG only).
	Still image	Displays still images only. Click the Refresh button in your browser to view a new image.

Viewer Settings

Check the **Show viewer toolbar** box to display the AXIS Media Control (AMC) or the QuickTime viewer toolbar under the video image in your browser.

The administrator can disable the installation of the H.264 decoder included with AXIS Media Control. This is used to prevent the installation of unlicensed copies. Further decoder licenses can be purchased from your Axis dealer.

Enable **Show crosshair in PTZ joystick mode** and a cross will indicate the center of the image in PTZ joystick mode.

Check **Use PTZ joystick mode as default** to enable joystick mode. The mode can be changed temporarily from the PTZ control panel.

Check **Enable recording button** to enable recording from the Live View page. The recordings are saved to the location specified in the AMC Control Panel, see *AXIS Media Control (AMC)*, on page 12.

Action Buttons

Check the boxes to display the action buttons in the Live View page.

The **manual trigger button** can be used to manually trigger and stop an event. See *Events*, on page 23.

The **snapshot button** can be used to save a snapshot from the video stream. This button is mainly intended for use with browsers other than Internet Explorer, or when not using AXIS Media Control to view the video stream. AXIS Media Control for Internet Explorer has its own snapshot button.

The **fan button** is used to manually start the camera's fan. Specify the number of minutes the fan should run for.

The **heater button** is used to manually start the camera's heater. Specify the number of minutes the heater should run for.

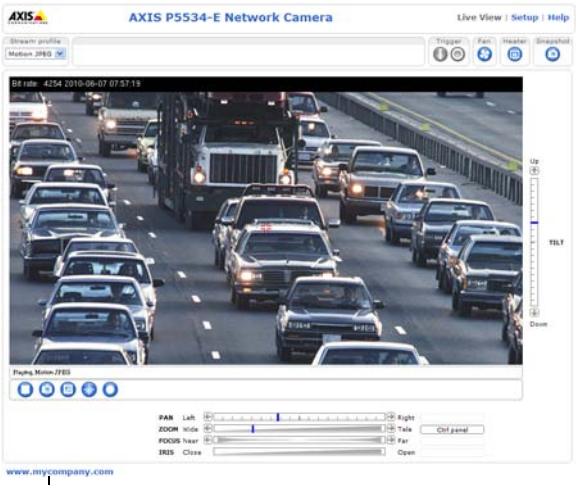
User Defined Links

User defined links can link to web pages, or can be used to run scripts or activate and control external devices connected to the network camera. Once configured, the link appear on the Live View page.

To set up a link, check the **Show custom link** box, select the cgi or web link radio button, enter the URL and a descriptive name in the provided field.

A link defined as a web link will open in a new window, while a cgi link will run for example a script in the background.

User defined CGI links can be used to issue API requests. For more information on the VAPIX Application Programming Interface (API), see the Video developer pages at Axis Web site www. axis.com/developer.

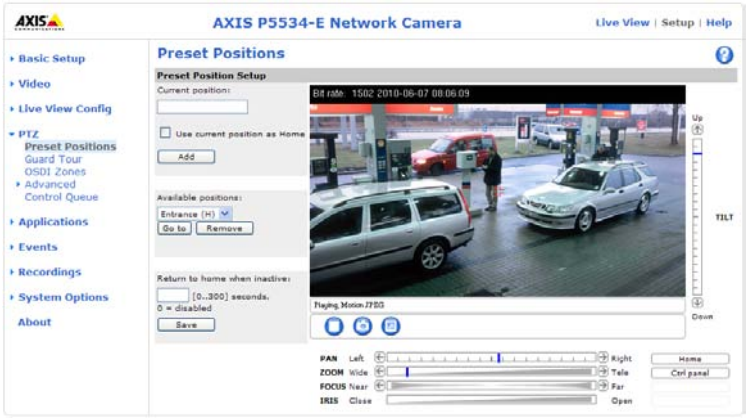


User defined link

PTZ (Pan Tilt Zoom)

Preset Positions

A preset position is a pre-defined camera view than can be used to quickly move the camera to a specific location.



From **Preset Position Setup**, use the Pan, Tilt and Zoom (PTZ) controls to steer the camera view to the required position. When satisfied with the camera's position, enter a descriptive name and click **Add**. The camera position, iris and focus settings are then saved as a preset position.

This position can be assumed at any time, by selecting the preset's name from the **Available positions** drop-down list. Preset positions can be selected in **Live View** page, from **Event Types**, **Guard Tour** and in the **Gatekeeper**.

One position can be set as the **Home** position, which is readily accessible by clicking the **Home** button in both the **Preset Positions** window and the **Live View** window. The name will have (H) added, for example, Entrance (H).

The network camera can also be configured to return to the Home position when the camera has been inactive for a specified length of time. Enter the length of time in the field **Return to home when inactive** and click **Save**. Setting the time to zero prevents the camera from automatically returning to the Home position.

The preset position name can be included in the overlay image text, see *Overlay Settings,* on page 14.

Guard Tour

A guard tour displays the video stream from different preset positions, one-by-one, in a pre-determined order or randomly, and for configurable time periods. The guard tour will keep running after the user has logged off or closed the browser.

Note:

The pause between guard tour runs must be set to at least 10 minutes.

OSDI Zones

On-Screen Direction Indicator (OSDI) Zones can be included in the overlay text (see page 14) to aid the user to navigate the camera. Each OSDI Zone is set up with coordinates and a descriptive name.

The camera uses the coordinates of the center of the image to set the lower left and upper right zone areas. First navigate to where you would like the lowermost left point of the OSDI Zone to be located. By clicking **Get** the coordinates are set. Proceed to where the upper right point of the zone should be located and click its **Get** button. Give the zone a descriptive name and click **OK**.

To include the name of the OSDI Zone in the overlay text, go to **Video > Video Stream > Overlay Settings**. Check the **Include text** box and enter the modifier **#L** in the field. See **File Naming & Date/Time Formats** in the online help for more information about modifiers.

Advanced

Limits

Define the pan, tilt, zoom and focus limits for the network camera. Movements to the left and right, up and down, can be restricted to narrow the area under surveillance. The near focus limit can be set to avoid focusing on objects too close to the camera.

Once a limit has been saved, this position cannot be exceeded by the network camera unless the values have been reset and saved to a greater value first (reset the default values of the mechanical restrictions).

Move speed sets the speed of the camera's Pan/Tilt movements. The default setting is maximum speed.

Enable proportional speed – – When using a joystick (or emulating one with the mouse), this setting can be used to reduce the maximum pan/tilt movement speed, i.e. the speed the camera moves at when the joystick is pushed all the way out in any pan/tilt direction. This is useful when the camera is zoomed in on an object and a pan/tilt movement is performed.

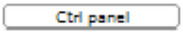
Enable Auto-flip – – The network camera will simulate continuous pan movement in the same direction, i.e. the camera will pan the full 360 degrees, even though there is a mechanical stop at ±180 degrees.

Enable movement prediction – The network camera will attempt to predict the new position in the pan movement, after compensating for the slight delay while the camera changes direction after an auto-flip. This is useful for tracking moving objects or persons when using the joystick or emulated joystick mode.

See the online help for more information.

Controls

Panel Shortcut Command Buttons can be configured to provide direct access to commands issued via the VAPIX® Application Programming Interface. The buttons will be displayed in the PTZ control panel, which is available on the Live View page by clicking the **Ctrl panel** button.



Enable/Disable controls – – Uncheck the boxes to disable the pan, tilt, zoom, focus and iris controls.

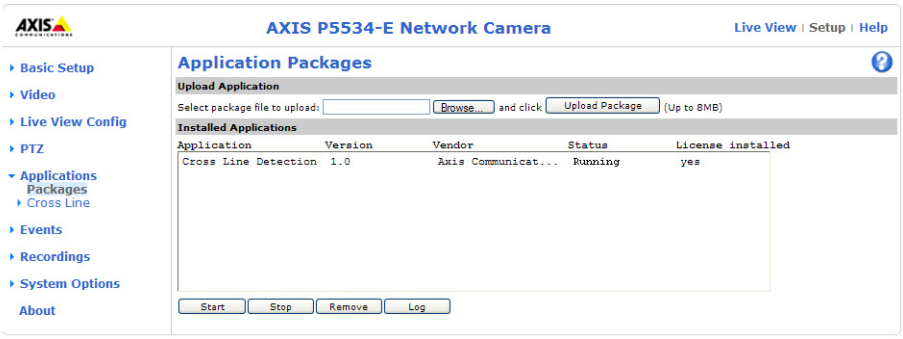
Note:

Disabling PTZ controls will affect preset positions. For example, if the tilt control is disabled, the camera cannot move to preset positions that require a tilt movement.

Control Queue

The administrator can set up a queue for the PTZ controllers. Once set up, the **PTZ Control Queue** buttons appear on the Live View page offering one viewer exclusive control for a limited amount of time. Other users will be placed in queue.

Applications



The Application packages feature allows you to upload third party application packages for use on the network camera. Listed under **Applications > Packages** are the packages that have already been installed. Click on the name to open the menu options Settings, License and About. See the online help for more information.

Settings – Application-specific settings.

License – Some applications require a license. If there is an Internet connection Automatic Installation appears on the web page. If there is no Internet connection, visit www.axis.com from another computer to acquire a License key file. To receive the license key, you will need a license code and the camera's serial number (found on the product's label, see page 5).

About – Details about the installed application.

Upload Applications

To upload an application, browse to the package and click **Upload Package**.

Installed Applications

Uploaded applications are listed under Installed Applications together with information about the application's version, vendor, status (running or not running) and license information.

To start and stop an application, click the **Start** and **Stop** buttons.

To remove an uploaded application, select the application and click **Remove**.

Click **Log** to generate a log of the application happenings. The log is helpful when requesting support from the application's vendor.

For information on how to use the uploaded application, please refer to the documentation of the application package.

Note:

It is recommended to run one application at a time. Avoid running applications when motion detection is active.

Events

Pre-defined parameters, known as an **event** or **Event Type** can trigger certain actions in the camera. A common event type is an alarm that causes the camera to upload images. Many event types use an **Event Server**, to receive uploaded images.

An event that is triggered by a signal, such as a detection of motion or system event, is called a **triggered event**, see page 24.

A **scheduled event** runs at pre-programmed times.

An **Action** refers to what happens when the event occurs.

This section describes how to configure the camera to perform certain actions when events occur.

Event Servers

Event servers are used to receive uploaded image files and/or notification messages. To set up Event Server connections in your camera, go to **Setup > Events > Event Servers** and enter the required information for the server type.

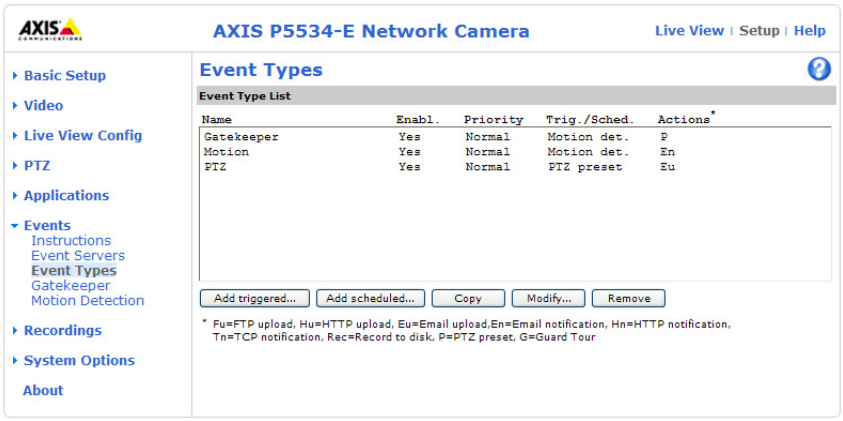
Server type	Purpose	Information required
FTP Server	• Receives uploaded images	• Descriptive name • Network address and Upload path • User Name and Password
HTTP Server	• Receives notification messages • Receives uploaded images	• Descriptive name • URL (IP address or host name) • User Name and Password • Proxy settings
TCP Server	• Receives notification messages	• Descriptive name • Network address (IP address or host name) • Port number

For details on each setting, see the online help available from each web page.

When the setup is complete, the connection can be tested by clicking the **Test** button (the connection test takes approximately 10 seconds).

Event Types

An **Event Type** describes how and when the camera is to perform certain actions.



Example: If somebody passes in front of a camera and an event has been configured to detect and respond to motion, the camera can record and save images to an FTP server, and can send a notification e-mail to an e-mail address. Images can be sent as e-mail attachments.

Triggered Event

A triggered event can be activated by:

- A manual trigger - using the manual trigger button on the Live View page or through the VAPIX® Application Programming Interface (API)
- An application trigger - a third party application installed on the camera.
- Movement in a motion detection window
- On boot - for example after power loss
- Temperature - when the temperature of the camera rises or falls outside the operating range
- Pan Tilt Zoom - when the camera stops at a preset position
- Disk full - when the local storage disk (SD memory card) has less than 1MB of free memory left
- Fan malfunction

How to set up a triggered event

The following example describes how to set up the camera to upload images when a door is opened.

1. Click **Add triggered** on the **Event types** page. The **Triggered Event Type Setup** page appears
2. Enter a descriptive **Name** for the event, such as Door open.
3. Set the **Priority** - High, Normal or Low.
4. Set the **Respond to Trigger** parameters to define when the event is active, for example, after office hours.
5. Select the trigger alternative from the **Triggered by** drop-down list. For example, motion detection.
6. Set the **When Triggered** parameters, that is, define what the camera will do if the main door is opened. To upload images, select **Save stream** and enter the required information. See *Save stream,* on page 24.
7. Click **OK** to save the event in the **Event Types** list.

Please see the online help for descriptions of each available option.

Note:

Up to 10 event types can be configured in the camera, and up to three of these can be configured to upload images. File names can be formatted according to specific requirements. See File Naming & Date/Time Formats in the online help .

Save stream

To upload images to an FTP or HTTP server, save the video stream to the local storage card or to send images by email, check the **Save stream** box.

Image frequency – Set the image frequency to a desired frame rate. The frame rate will be the best possible, but might not be as high as specified, especially if uploading via a slow connection.

Pre-trigger and Post-trigger buffers
This function is very useful when checking to see what happened immediately before and/or after a trigger, for example, 20 seconds before and/or after a door was opened. All uploaded images are JPEG images.

Include pre-trigger buffer - Images stored internally in the server from the time immediately preceding the trigger. Check the box to enable the pre-trigger buffer and specify the buffer length in seconds, minutes or hours.

Include post-trigger buffer - Contains images from the time immediately after the trigger. The post-trigger buffer is configured in the same way as the pre-trigger buffer.

Notes

- Pre-trigger and Post-trigger buffers will be lost if the connection to the event server fails
- The maximum length of the pre-/post-buffer depends on the video image size and selected frame rate
- If the pre- or post-buffer is too large for the camera's internal memory, the frame rate is reduced and individual images may be missing. If this occurs, an entry is created in the unit's log file

Continue image upload (unbuffered) - Upload video images for a fixed length of time or for as long as the trigger is active.

Select type – Upload images to an FTP or HTTP server, send images by e-mail or save the video stream to the local storage disk.

Create folder – Images uploaded to FTP and HTTP servers can be saved to designated folders. Folders can for example be named using the current date and time, see File Naming & Date/Time formats in the online help .

Base file name – Used to name all uploaded images. Add a suffix or use your own file format to give the images unique names, see File Naming & Date/Time formats in the online help .

Use stream profile – Select the stream profile to upload, send as e-mail or save to the local disk. When saving to the local disk, the video format (JPEG or H.264) must first be selected.

Scheduled Event

A **Scheduled event** can be activated at preset times, in a repeating pattern on selected weekdays.

How to set up a scheduled event

The following example describes how to configure the camera to save images from pre-programmed time periods.

1. Click **Add scheduled** on the **Event Types** page.
2. Enter a descriptive **Name** for the event, such as Scheduled e-mail upload.
3. Set the **Priority** (High, Normal or Low).
4. Set the **Activation Time** parameters (24h clock) for the event. For example, select **Recurrence pattern** and let the event start on Sundays at 13.00 with a duration of 12 hours.
5. Set the **When Activated** parameters, that is, define what the camera should do when the event is active. To upload images, select **Save stream** and enter the required information. See *Save stream,* on page 24.
6. Click **OK** to save the Event in the Event Types list.

Please see the online help for descriptions of each available option.

Gatekeeper

The Gatekeeper monitors an area such as an entrance gate and can pan, tilt, zoom in and take a snapshot of, for example, a face, triggered by movement in the area. The camera will then automatically return to the Home position and continue to overview the monitored area. Follow the online instructions to configure Gatekeeper.

Motion Detection

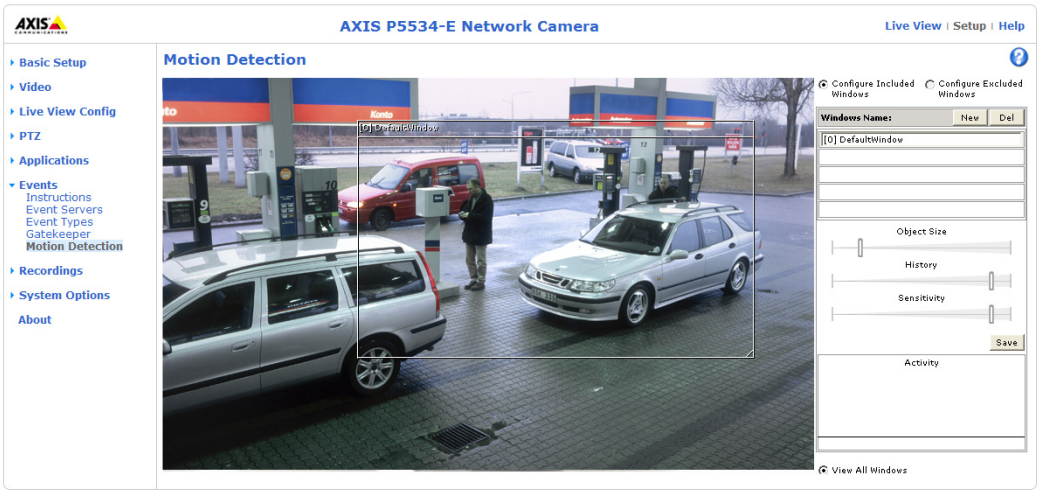
Motion detection is used to generate an alarm whenever movement occurs (or stops) in the video image. Up to 10 Include and Exclude windows can be configured.

- **Included** windows target specific areas within the whole video image
- **Excluded** windows define areas within an Include window that should be ignored (areas outside Include windows are automatically ignored)

Once configured, the motion detection windows appear in the list of available triggers, for triggering events. See *How to set up a triggered event*, on page 24.

Note:

Using the motion detection feature may decrease the camera's overall performance.



Set up a motion detection include window

The following example describes how to configure the camera for motion detection.

1. Go to **Setup > Events > Motion Detection.**
2. Create a new motion detection window:
   a. Using AXIS Media Control (Internet Explorer): Select the radio button **Configure Included Windows** and click **New**. Select the new window in the list of windows and enter a descriptive name.
   b. Using the Java applet: Click **Add Window**. Select the **Include** radio button and enter a descriptive name in the field.
3. Adjust the size (drag the bottom right-hand corner) and position (click on the text at the top and drag to the desired position) of the active window.
4. Adjust the **Object Size**, **History** and **Sensitivity** profile sliders (see table below for details). Any detected motion within an active window is then indicated by red peaks in the **Activity** window (the active window has a red frame).
5. Click **Save**.

> To exclude parts of the Include window, select the **Exclude** option and position the Exclude window as required, within the Include window.

To delete an Include or Exclude window:

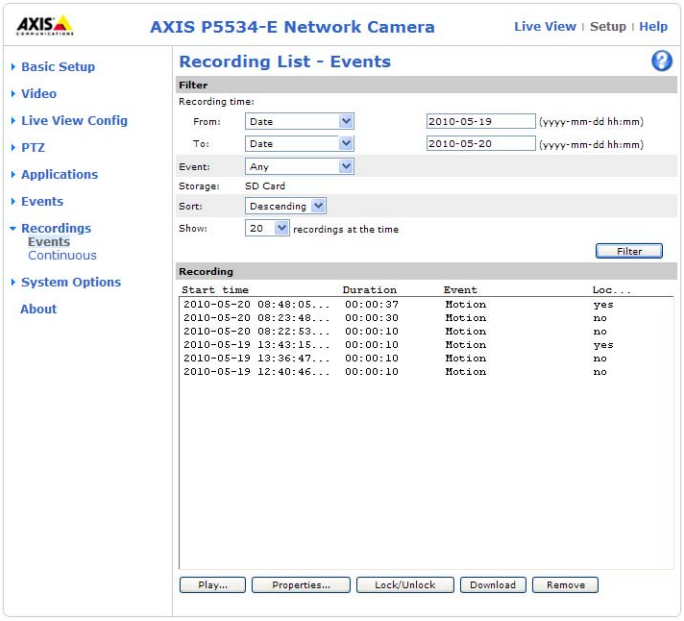
a. Using AXIS Media Control (Internet Explorer): Select the window in the list ow windows and click **Del**.
b. Using the Java applet: Select the window and click on the cross in the upper right corner.

Please see the online help for descriptions of each available option.

	Object Size	History	Sensitivity
High level	Only very large objects trigger motion detection	An object that appears in the region will trigger the motion detection for a long period	Ordinary colored objects on ordinary backgrounds will trigger the motion detection
Low level	Even very small objects trigger motion detection	An object that appears in the region will trigger motion detection for only a very short period	Only very bright objects on a dark background trigger motion detection
Default value	Low	High	High

- Avoid triggering on small objects in the video image by setting the **object size** level to high.
- Use several small Motion Detection windows rather than one large window, if triggers on small movements or objects are desired.
- To reduce the number of triggers if there is a lot of movement during a short period of time, select a high **history** level.
- To only detect flashing light, select low **sensitivity**. In other cases, a high **sensitivity** level is recommended.

Recording List



The **Recording List** web page contains a list of recordings made to the SD memory card. It shows each recording's start time, length, the event type, and indicates if the recording is locked so that it can neither be deleted nor recorded over.

To view a recording, select it from the list and click **Play**.

For detailed recording and video information, select an individual recording from the list and click **Properties**.

Use the **Lock/Unlock** button to define whether a recording can be removed or recorded over, or if the recording is important and needs to be saved for future use. Locking the recording can help prevent its accidental removal.

Recordings can be downloaded in a zip file containing a minimum of three files of which the .mkv or Matroska file is the actual recording. Select one or more recordings and click **Download**.

The **Remove** button is used to delete unlocked recordings.

Recordings are made to the SD memory card once an event has been set up on under **Setup > Event Types > Add triggered /Add scheduled > Save stream > Select type.** Select Local Storage from the drop-down list.

See **System Options > Storage > SD Card** to mount, format and monitor the status and available recording space of the SD memory card.

Please refer to the Installation Guide supplied with the product for instructions on how to insert and remove the SD memory card.

Notes:

- The SD memory card is optional and not included in the product.
- To play recordings in Windows Media Player download and install AXIS Matroska File Splitter from www.axis.com/techsup/software

Filter

Use the filter to narrow down the list according to certain criteria such as a particular time frame.

Recording time – Filter out a group of recordings based on their start and end dates or times. The recording date and time is listed according to the device's time zone. If the local time zone is different than the device's time zone, you will need to consider that the filter is done by the local time zone. **First recording/Now** are the default settings. Use **Date** if you want to specify a certain date or date and time for when the recording started.

Event – Select a group of recordings based on what type of event triggered the recording.

Storage – Select a group of recordings based on where the recordings are stored.

Sort – Select whether the filtered recording list should be sorted in ascending or descending order of start time.

Show – Select how many recordings to view in the window at one time.

See the online help files for more information.

Continuous Recording

The camera can be configured to continuously save video to an SD Card. Configure continuous recordings for different stream profiles.

Recording Settings

The **Enabled** box must be checked to record continuously. Select a **Stream Profile** in the drop-down list and click **Save** to apply the new settings.

Note:

The recording will be restarted and all previous continuous recordings will be removed if Disk or Stream profile is changed.

Recording

Start time – Shows the time the current continuous recording began. If no continuous recording is taking place the status will show as Not started.

Duration – Shows the length of the current continuous recording. Click **Restart** to start a new recording. Note that all previous continuous recording data will be removed.

From – To play or download the recording from a point in time, enter the year, month, day and the time in hours and minutes. The time set here is also used for naming the file.

Duration – Enter the amount of the recording to play or download in hours and minutes.

To view a selected continuos recording, click **Play**.

To download a selected continuos recording, click **Download**. The package downloaded is a zip file containing a minimum of 3 files, of which the .mkv or Matroska file is the actual recording.

See the online help files for more information.

System Options

Security

Users

User access control is enabled by default. An administrator can set up other users, by giving them user names and passwords. It is also possible to allow anonymous viewer login, which means that anybody may access the Live View page, as described below:

The **user list** displays the authorized users and user groups (levels):

Viewer	Provides the lowest level of access, which only allows access to the Live View page.
Operator	An operator can view the Live View page, create and modify events, and adjust certain other settings. Operators have no access to System Options.
Administrator	An administrator has unrestricted access to the Setup tools and can determine the registration of all other users.

HTTP/RTSP Password Settings - Select the type of password. You may need to allow unencrypted passwords if there are viewing clients that do not support encryption, or if you recently upgraded the firmware and the existing clients do support encryption, but need to log in again, and be configured to use this functionality.

User Settings

- Check the box to enable **anonymous viewer login** to allow any viewer direct access to the Live View page.
- Check the box to enable **anonymous PTZ control login** to allow anonymous users to join a queue for gaining control of the PTZ controls.
- **Enable Basic Setup** - Before using the network camera, there are certain settings that should be made, most of which require Administrator access privileges. To quickly access these settings, use the **Basic Setup** in the menu. All settings are also available from the standard setup links in the menu. **Basic Setup** is enabled by default but can be disabled and removed from the menu.

IP Address Filter

Enable **IP Address Filtering** to allow or deny access to the network cameras**.** Once enabled, the IP addresses in the list are allowed or denied access according to the choice made in the drop-down list **Allow/Deny the following IP addresses.**

The administrator can add up to 256 IP address entries to the list (a single entry can contain multiple IP addresses). The users from these IP addresses need to be specified in the user list with the appropriate access rights. This is done from **Setup > System Options > Security > Users**.

HTTPS

The network cameras support encrypted browsing using HTTPS.

A **self-signed certificate** can be used until a Certificate Authority-issued certificate has been obtained. Click the **Create self-signed Certificate** button to install a self-signed certificate. Although self-signed certificates are free and offer some protection, true security is only implemented after the installation of a signed certificate issued by a Certificate Authority.

A signed certificate can be obtained from an issuing Certificate Authority by clicking the **Create Certificate Request** button. When the signed certificate is returned, click the **Install signed certificate** button to import the certificate. The properties of any certificate request currently resident in the camera or installed can also be viewed by clicking **Properties**. The HTTPS Connection Policy must also be set in the drop-down lists to enable HTTPS in the camera.

For more information, refer to the online help .

IEEE 802.1X

IEEE 802.1X is a standard for port-based Network Admission Control providing secure authentication of wired and wireless network devices. IEEE 802.1X is based on EAP (Extensible Authentication Protocol).

To access a network protected by IEEE 802.1X, devices must authenticate themselves. The authentication is performed by a third-party entity called an authentication server, typically a RADIUS server, examples of which are FreeRADIUS and Microsoft Internet Authentication Service. In Axis implementation, the network device and the authentication server authenticate themselves with the help of digital certificates using EAP-TLS (Extensible Authentication Protocol - Transport Layer Security). The certificates are provided by an Certification Authority (CA). You need:

- a CAcertificate to validate the identity of the authentication server
- a CA-signed client certificate and a private key to authenticate the network device.

To allow the network device to access a network protected by IEEE 802.1X:

1. Obtain a CA certificate, a client certificate and a client private key (contact your network administrator).
2. Go to **Setup > System Options > Security > IEEE 802.1X** and upload the CA certificate, the client certificate and the client private key.
3. Under **Settings**, select the EAPOL version, provide your EAP identity and private key password.
4. Check the box to enable IEEE 802.1X and click **Save**.

Certificates

CA Certificate – The CA certificate is used to validate the identity of the authentication server. Enter the path to the certificate directly, or locate the file using the **Browse** button. Then click **Upload**. To remove a certificate, click **Remove**.

Client Certificate/Client private key – The client certificate and private key are used to authenticate the network device. They can be uploaded as separate files or in one combined file (e.g. a PFX file or a PEM file). Use the Client private key field if uploading one combined file. For each file, enter the path to the file, or locate the file using the **Browse** button. Then click **Upload**. To remove a file, click **Remove**.

Settings

Eapol version – Select the EAPOL version (1 or 2) as used in your network switch.

Eap identity – Enter the user identity (maximum 16 characters) associated with your certificate.

Private key password – Enter the password (maximum 16 characters) for the private key.

Enable IEEE 802.1X – Check the box to enable the IEEE 802.1X protocol.

Date & Time

Current Server Time

Displays the current date and time (24h clock). The time can be displayed in 12h clock format in the overlay (see below).

New Server Time

Select your **time zone** from the drop-down list. If you want the server clock to automatically adjust for daylight savings time, select the **Automatically adjust for daylight saving time changes** option.

Note:

The time zone setting only apply when the device's time is synchronized with an NTP server.

From the **Time Mode** section, select the preferred method to use for setting the time:

- **Synchronize with computer time** - Sets the time from the clock on your computer.
- **Synchronize with NTP Server** - The camera will obtain the time from an NTP server.
- **Set manually** - This option allows you to manually set the time and date.

Note:

If using a host name for the NTP server, a DNS server must be configured under **TCP/IP** settings.
See *Basic TCP/IP Settings*, below.

Date & Time Format Used in Images

Specify the formats for the date and time (12h or 24h) displayed in the video streams. Use the predefined formats or use your own custom date and time formats. See **File Naming & Date/Time Formats** in the online help for information on how to create your own date and time formats.

Network

Basic TCP/IP Settings

The camera supports both IP version 4 and IP version 6. Both versions may be enabled simultaneously, and at least one version must always be enabled. When using IPv4, the IP address for the camera can be set automatically via DHCP, or a static IP address can be set manually. If IPv6 is enabled, the network cameras receive an IP address according to the configuration in the network router. There are also options for using AXIS Internet Dynamic DNS Service and AVHS (AXIS Video Hosting System). For more information on setting the IP address, please refer to the Installation Guide supplied with the product.

Network Settings

Click the **View** button for an overview of the IP configuration of the network camera.

IPv4 Address Configuration

Check the **Enable IPv4** box option to enable IPv4.

Obtain IP address via DHCP - Dynamic Host Configuration Protocol (DHCP) is a protocol that lets network administrators centrally manage and automate the assignment of IP addresses on a network. DHCP is enabled by default. Although a DHCP server is mostly used to set an IP address dynamically, it is also possible to use it to set a static, known IP address for a particular MAC address.

Note:

DHCP should only be enabled if using dynamic IP address notification, or if your DHCP server can update a DNS server, which then allows you to access the network camera by name (host name). If DHCP is enabled and you cannot access the unit, run AXIS IP Utility to search the network for connected Axis products or reset the network camera to factory default settings and then perform the installation again.

Use the following IP address – To use a static IP address for the network camera, check the radio button and then make the following settings:

- **IP address** - Specify a unique IP address for your network camera. (To check if the IP address you intend to use is available or not, click the **Test** button)
- **Subnet mask** - Specify the mask for the subnet the network camera is located on
- **Default router** - Specify the IP address of the default router (gateway) used for connecting devices attached to different networks and network segments.

IPv6 Address Configuration

Check the **Enable IPv6** box to enable IPv6. Other settings for IPv6 are configured in the network router.

Services

Enable ARP/Ping setting of IP address - The IP address can be set using the ARP/Ping method, which associates the unit's MAC address with an IP address. Check this box to enable the service. Leave disabled to prevent unintentional resetting of the IP address.

Notes:

- The ARP/Ping service is automatically disabled two minutes after the unit is started, or as soon as an IP address is set. In order to reset the IP address, the camera must be restarted to activate ARP/Ping for an additional two minutes.
- Pinging the unit is still possible when this service is disabled.

AXIS Video Hosting System (AVHS)

AVHS used in conjunction with an AVHS service provides easy and secure Internet access to live and recorded video accessible from any location. For more information and help to find a local AVHS Service Provider go to www.axis.com/hosting

Enable AVHS – Enabled by default, if AVHS is not to be used this option can be disabled.

- **One-click enabled –** Press the camera's control button (see Hardware overview, on page 5) to connect to an AVHS service over the Internet. Once registered, Always is enabled and the cameras stays connected to the AVHS service. If the camera is not registered within 24 hours from when the button is pressed, the camera will disconnect from the AVHS service.
- **Always –**The camera will constantly attempt to connect to the AVHS service over the Internet. Once registered, the camera will stay connected to the service. This option can be used when the camera is already installed and it is not convenient to use the one-click installation.

AXIS Internet Dynamic DNS Service – Enable this option to use AXIS Internet Dynamic DNS service to assign a host name for easy access to your network camera (requires access to the Internet).

Click **Settings** to register the camera with AXIS Internet Dynamic DNS service, or to modify the existing settings. The domain name currently registered at AXIS Internet Dynamic DNS service for your product can at any time be removed.

For more information, please refer to www.axiscam.net and to the online help .

Advanced TCP/IP Settings

DNS Configuration

DNS (Domain Name Service) provides the translation of host names to IP addresses on your network.

Obtain DNS server address via DHCP – Automatically use the DNS server settings provided by the DHCP server. Click the **View** button to see the current settings.

Use the following DNS server address - Enter the desired DNS server by specifying the following:

- **Domain name** - Enter the domain(s) to search for the host name used by the network camera. Multiple domains can be separated by semicolons (;). The host name is always the first part of a Fully Qualified Domain Name, for example, **myserver** is the host name in the Fully Qualified Domain Name **myserver.mycompany.com** where mycompany.com is the Domain name.
- **DNS servers** - Enter the IP addresses of the primary, and secondary DNS servers.
  Note: This is not mandatory with regard to secondary DNS servers.

NTP Configuration

Obtain NTP server address via DHCP - Check this radio button to automatically look up and use the NTP server settings as provided by DHCP. Click the **View** button to see the current settings.

Use the following NTP server address – To create manual settings, check this radio button and enter the host name or IP address of the NTP server.

Host Name Configuration

The network cameras can be accessed using a host name, instead of an IP address. The host name is usually the same as the assigned DNS Name.

Link-Local IPv4 Address

This is enabled by default and assigns the network cameras an additional IP address for use with UPnP™. The camera can have both a Link-Local IP and a static/DHCP-supplied IP address at the same time - these will not affect each other.

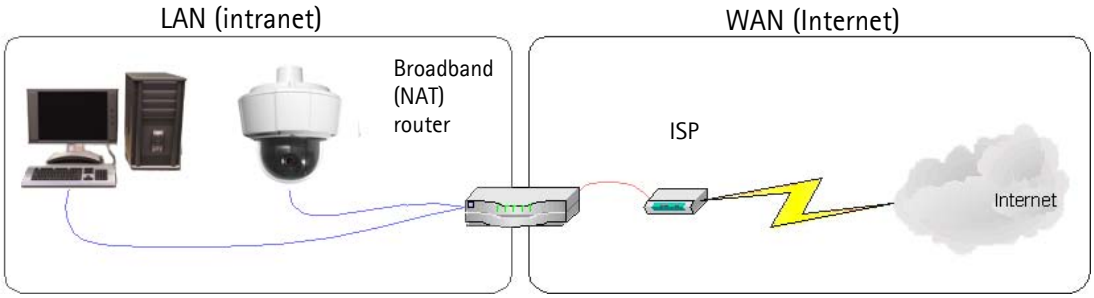
HTTP and HTTPS

The default HTTP/HTTPS port numbers (80 and 443 respectively) can be changed to any port within the range 1024-65535. This is useful for simple security port mapping, for example.

NAT traversal (port mapping) for IPv4

A broadband router allows devices on a private network (LAN) to share a single connection to the Internet. This is done by forwarding network traffic from the private network to the "outside", that is, the Internet. Security on the private network (LAN) is increased since most broadband routers are pre-configured to stop attempts to access the private network (LAN) from the public network/Internet.

Use **NAT traversal** when your network cameras are located on an intranet (LAN) and you wish to make it available from the other (WAN) side of a NAT router. With NAT traversal properly configured, all HTTP traffic to an external HTTP port in the NAT router is forwarded to the camera.



Notes:

- For NAT traversal to work, this must be supported by the broadband router. The router must also support UPnP™.
- The broadband router has many different names: "NAT router", "Network router", Internet Gateway", "Broadband sharing device" or "Home firewall" but the essential purpose of the device is the same.

Enable/Disable - When enabled, the network camera attempts to configure port mapping in a NAT router on your network, using UPnP™. Note that UPnP™ must be enabled in the camera (see **System Options > Network > UPnP**).

Use manually selected NAT router - Select this option to manually select a NAT router and enter the IP address for the router in the field provided.

If a router is not manually specified, the network cameras automatically search for NAT routers on your network. If more than one router is found, the default router is selected.

Alternative HTTP port - select this option to manually define an external HTTP port. Enter the port number in the field provided. If no port is entered here a port number is automatically selected when NAT traversal is enabled.

Notes:

- An alternative HTTP port can be used/be active even if NAT traversal is disabled. This is useful if your NAT router does not support UPnP and you need to manually configure port forwarding in the NAT router.
- If you attempt to manually enter a port that is already in use, another available port is automatically selected.
- When the port is selected automatically it is displayed in this field. To change this enter a new port number and click **Save**.

FTP

The FTP server running in the network cameras enables the upload of new firmware, and user applications. Check the box to enable the service.

RTSP

The RTSP protocol allows a connecting client to start an H.264 stream. Check the box to enable the server and enter the RTSP port number to use. The default setting is 554. Note that H.264 video streams will not be available if this service is not enabled.

SOCKS

SOCKS is a networking proxy protocol. The network camera can be configured to use a SOCKS server to reach networks on the other side of a firewall/proxy server. This functionality is useful if the network camera is located on a local network behind a firewall, and notifications, uploads, alarms, and such need to be sent to a destination outside the local network (such as the Internet). See the online help for more information.

Quality of Service (QoS)

Quality of Service (QoS) guarantees a certain level of a specified resource to selected traffic on a network. Quality can be defined as a maintained level of bandwidth, low latency, and no packet losses. 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.

The QoS in Axis network video products marks the data packets for various types of network traffic originating from the product. This makes it possible for network routers and switches to reserve a fixed amount of bandwidth for these types of traffic. The network camera marks the following types of traffic:

- video
- event/alarm
- management network traffic

QoS Settings

For each type of network traffic supported by your Axis network video product, enter a DSCP (Differentiated Services Codepoint) value. This value is used to mark the traffic's IP header. When the marked traffic reaches a network router or switch, the DSCP value in the IP header tells the router or switch the type of treatment to apply to this type of traffic, for example, how much bandwidth to reserve for it. Note that DSCP values can be entered in decimal or hex form, but saved values are always shown in decimal.

For more information on Quality of Service, please see the Axis support web at www.axis.com/techsup

SMTP (email)

Enter the host names (or IP addresses) and port numbers for your primary and secondary mail servers in the fields provided, to enable the sending of notifications and image email messages from the camera to predefined addresses via SMTP.

If your mail server requires authentication, check the box for **Use authentication to log in to this server** and enter the necessary information. See the online help for more information.

SNMP

The Simple Network Management Protocol (SNMP) allows remote management of network devices. An SNMP community is the group of devices and management station running SNMP. Community names are used to identify groups.

Depending on the level of security required, select the version of SNMP to use.

SNMP v1/v2

Select either SNMP V1 that includes no security, or SNMP v2c that uses very simple security.

The community name can be specified as a password for read or read/write access to all supported SNMP objects. The community is the group of network devices using SNMP. The default password for the **Read Community** is **public** and the default password for the **Write community** is **write**.

Traps for SNMP v1/v2

Traps are used by the camera to send messages to a management system for important events or status changes.

If **Enable traps** is selected, enter the email address where the trap message is to be sent as well as the **Trap community** that should receive the message.

There are four types of traps available for the network camera.

- Cold start
- Warm start
- Link up
- Authentication failed

SNMP v3

SNMP v3 provides encryption and secure passwords. HTTPS must be enabled. To use traps with SNMP v3 an SNMP v3 management application is required.

If the **Enable SNMP v3** option is enabled, provide the Initial user password. Note that the initial password is activated only when HTTPS is enabled and can only be set once.

If HTTPS is enabled, SNMP v1 and SNMP v2c should be disabled.

When SNMP configuration is ready, click **Save** to use the new settings or **Reset** to return to the default values.

UPnP™

The network camera includes support for UPnP™. UPnP™ is enabled by default, and the network camera then is automatically detected by operating systems and clients that support this protocol.

RTP/H.264

These settings are the port range, IP address, port number, and Time-To-Live value to use for the video stream(s) in multicast H.264 format. Only certain IP addresses and port numbers should be used for multicast streams. For more information, please see the online help .

Bonjour

The network camera includes support for Bonjour. When enabled, the camera is automatically detected by operating systems and clients that support this.

Storage

SD Card

The **Disk Management** window is used to set up and manage local storage. it is used to connect memory cards for recording video, monitoring a disk's status, enabling automatic cleanup and preventing a memory card's memory from being overwritten.

Storage Device

Storage device is used to identify and monitor the status of the SD card. it shows the size of the SD card and how much free space is available for storage. It is also used to mount and format SD cards for local storage.

Storage Device Settings

Storage device settings is used to configure removal of recorded video. Automatic disk cleanup can be enabled and set up according to a schedule, and an SD card can be locked to prevent storage removal.

Maintenance

Maintain Server

Restart - The camera is restarted without changing any settings.

Restore - The unit is restarted and most current settings are reset to factory default values. The settings that do not reset are:

- the boot protocol (DHCP or static)
- the static IP address
- the default router
- the subnet mask
- the product interface language
- the system time
- the 802.1x settings

Default - The default button should be used with caution. Pressing this returns the camera's settings to the factory default values (including the IP address).

Dome Status - Click the test button to check the pan, tilt, zoom mechanics and camera for errors. If you receive an error message, contact Axis Customer Services at www.axis.com/techsup

Upgrade Server

See *Upgrading the Firmware*, on page 40.

Support

Support Overview

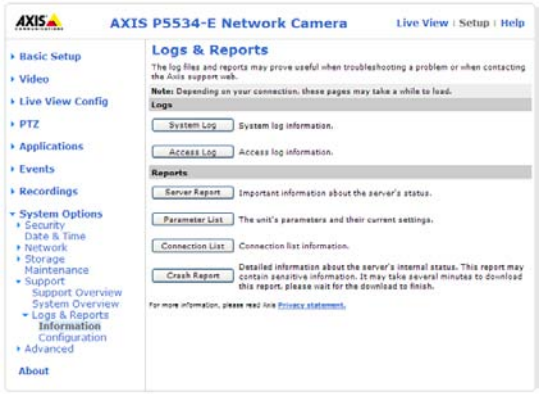
The **Support Overview** page provides valuable information on troubleshooting and contact information, should you require technical assistance.

System Overview

System Overview is an overview of the camera's status and settings. Information that can be found here includes the camera's firmware version, IP address, security, event and image settings and recent log items. Many of the captions are also links to the proper **Setup page** to conveniently make adjustments in the camera's settings.

Logs & Reports

When contacting Axis support, please be sure to provide a valid Server Report with your query. The Access Log is automatically included in the server report.



Information

the **Server Report** and **Parameter List** may prove useful when troubleshooting a problem or when contacting the Axis support.

- **System Log** - Provides information about system events.
- **Access Log** - By default, the Access Log lists all failed attempts to access the camera but can be configured to list all connections to the camera, whether successful or not. Go to **Support > Logs & Reports > Configuration** and select the desired level of information from the list. See *Configuration,* on page 38 for more information.
  The Access Log is useful for various purposes such as tracking all access to the camera, simple web attraction tracking, system analysis and troubleshooting.
- **Server Report** - Provides information about the server status and should always be included when requesting support.
- **Parameter List** - Shows the unit's parameters and their current settings.
- **Connection List** - Lists all clients that are currently accessing video. It is also used for system analysis and troubleshooting.
- **Crash Report** - Generates an archive with debugging information. Note that the report takes several minutes to generate.

Configuration

From the drop-down lists, select the level of information to be added to the **System Log** and **Access Log** files and the permitted size of the log files.

The default information level for the Access Log is set to Critical & Warnings, i.e. failed connections. However, in an error situation and when requesting support, set it to the highest information level - Critical & Warnings & Info.

For the **Log Level for Email**, select from the drop-down list the level of information to send as email and enter the destination email address.

Advanced

Scripting

Scripting is an advanced function that enables you to customize and use scripts.

Caution!

Incorrect scripting may cause unexpected behavior or even cause loss of contact with the unit. If a script does cause problems, reset the unit to its factory default settings. A backup file may be of use to return the unit to its latest configuration.

Axis strongly recommends that you do not use this function unless you understand the consequences. Note that Axis support does not provide assistance for problems with customized scripts.

For more information, please visit the Developer pages at www.axis.com/developer

File upload

Files (e.g. web pages and images) can be uploaded to the network camera and used as custom settings. Uploaded files are accessed through http://<ip address>/local/<user>/<filename> where <user> is the selected user access group (viewer, operator or administrator) for the uploaded file.

Plain Config

Plain Config is for the advanced user with experience of Axis network camera configuration. All parameters can be set and modified from this page. Help is available from the standard help pages.

About

Here you can find basic information about your network camera. You can also view third party software licenses.

Resetting to the Factory Default Settings

To reset the camera to the original factory default settings, go to the **System Options > Maintenance** web page (as described in *Maintenance,* on page 37). Alternatively, use the **Control button** and the **Power switch** on the side of the camera as described below:

Using the control and restart buttons

This will reset all parameters, including the IP address, to the Factory Default settings:

1. Remove the top cover, for instructions please refer to the Installation Guide supplied with the camera.
2. Press and hold the control and restart buttons at the same time.
3. Release the restart button but continue to hold down the control button.
4. Continue to hold down the control button until the status indicator flashes amber at regular intervals (this may take up to 15 seconds).
5. Release the control button.
6. When the Status indicator changes to green (which may take up to 1 minute), the process is complete and the camera has been reset. The unit now has the default IP address 192.168.0.90
7. Replace the top cover.
8. Re-assign the IP address, see the Installation Guide for instructions.

Troubleshooting

Checking the Firmware

Firmware is software that determines the functinality of network cameras. One of your first actions when troubleshooting a problem should be to check the current firmware version. The latest version may contain a correction that fixes your particular problem. The current firmware in your camera is displayed on the page **Setup > Basic Setup** or under **About**.

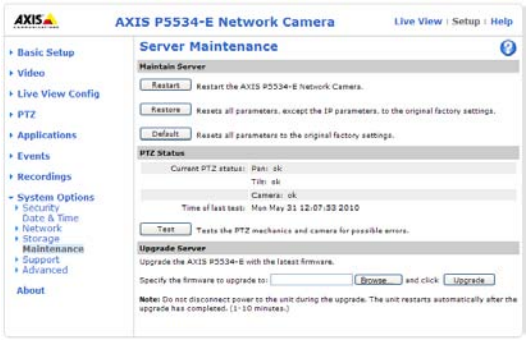
Upgrading the Firmware

When you upgrade your camera with the latest firmware from the Axis web site, your camera receives the latest available functionality. Always read the upgrade instructions and release notes available with each new release, before updating the firmware.

Note:

Preconfigured and customized settings are retained for use when the new firmware is running (providing that the features are available in the new firmware) although this is not guaranteed by Axis Communications.

1. Save the firmware file to your computer. The latest version of the firmware is available free of charge from the Axis web site at http://www.axis.com/techsup
2. Go to **Setup > System Options > Maintenance** in the camera's web pages.
3. In the **Upgrade Server** section, click **Browse** to locate the desired firmware file on your computer. Click **Upgrade**.



Note:

- After starting the upgrade process, you should always wait at least 5-10 minutes before restarting the camera, even if you suspect the upgrade has failed.
- Your dealer reserves the right to charge for any repair attributable to faulty upgrading by the user.
- AXIS Camera Management can be used for multiple upgrades. Please see the Axis website at www.axis.com for more information.

Emergency Recovery Procedure

If power or the network connection to the camera is lost during the upgrade, the process will fail and the unit becomes unresponsive. A flashing red status indicator indicates a failed upgrade. To recover the unit, follow the steps below. The serial number is found on the label on the product casing and is included on an extra label included in the package.

1. **Unix/Linux** - From the command line, type the following:
   arp -s <IP address of camera> <Serial number> temp
   ping -s 408 <IP address of camera>

   Windows - From a command/DOS prompt, type the following:
   arp -s <IP address of camera> <Serial number>
   ping -l 408 -t <IP address of camera>
2. If the unit does not reply within a few seconds, restart it and wait for a reply. Press CTRL+C to stop Ping.
3. Open a browser and type in the camera's IP address. In the page that appears, use the **Browse** button to select the upgrade file to use, for example, axisq6032_e.bin. Then click the **Load** button to restart the upgrade process.
4. After the upgrade is complete (1-10 minutes), the unit automatically restarts and shows a steady green (for about 10 seconds) on the status indicator before returning to its normal unlit status.
5. Reinstall the camera, for more information, see the Installation Guide provided with the product.

If the emergency recovery procedure does not get the camera up and running again, contact Axis support at www.axis.com/techsup

AXIS Support

If you contact Axis Customer Services, please help us to resolve your problems expediently by providing a Server Report and a brief description of the problem.

The Server Report contains important information about the server and its software, as well as a list of the current parameters. The Access log files are also included in the Server Report. Go to **Setup > System Options > Support > Support Overview** to generate a Server Report.

Symptoms, possible causes and remedial actions

Problems setting the IP address	
When using ARP/Ping	Try the installation again. The IP address must be set within two minutes after power has been applied to the camera. Ensure the Ping length is set to 408. See the Installation Guide.
The camera is located on a different subnet	If the IP address intended for the camera and the IP address of your computer are located on different subnets, you will not be able to set the IP address. Contact your network administrator to obtain an appropriate IP address.
The IP address is being used by another device	Disconnect the camera from the network. Run the Ping command (in a Command/DOS window, type **ping** and the **IP address** of the unit). If you receive: **Reply from <IP address>: bytes = 32; time = 10 ms.....** - this means that the IP address may already be in use by another device on your network. You must obtain a new IP address and reinstall the unit. If you receive: **Request timed out** - this means that the IP address is available for use with your camera. In this case, check all cabling and reinstall the unit.
The camera cannot be accessed from a web browser	
Cannot log in	When HTTPS is enabled, ensure that the correct protocol (HTTPS or HTTPS) is used when attempting to log in. You may need to manually type http or https in the browser's address field.
The IP address has been changed by DHCP	If the camera and client are on the same network. Run AXIS IP Utility to locate the camera. Identify the camera using its model or serial number. Alternatively: 1) Move the camera to an isolated network or to one with no DHCP or BOOTP server. Set the IP address again, using AXIS IP Utility or the ARP Ping command. 2) Access the unit and disable BOOTP and DHCP in the TCP/IP settings. Return the unit to the main network. The unit now has a fixed IP address that will not change. 3) As an alternative to 2), if dynamic IP address via DHCP or BOOTP is required, select the required service and then configure IP address change notification from the network settings. Return the unit to the main network. The unit will now have a dynamic IP address, but will notify you if the address changes.
Other networking problems	Test the network cable by connecting it to another network device, then Ping that device from your workstation. See instructions above.
Camera is accessible locally, but not externally	
Broadband router configuration	To configure your broadband router to allow incoming data traffic to the camera, enable the NAT-traversal feature which will attempt to automatically configure the router to allow access to the camera. This is enabled from **Setup > System Options > Network > TCP/IP Advanced**. Note that the router must support UPnP™.
Firewall protection	Check the Internet firewall with your system administrator.
Default routers required	Check if you need to configure the default router settings.
Problems with the H.264 format	
No H.264 displayed in the client	Check that the correct network interface is selected in the AMC control panel (streaming tab).
	Check that the relevant H.264 connection methods are enabled in the AMC control panel applet (streaming tab).
	In the AMC Control Panel, select the H.264 tab and click the button Set to default H.264 decoder.
No multicast H.264 displayed in the client.	Check with your network administrator that the multicast addresses used by the camera are valid for your network.
	Check with your network administrator to see if there is a firewall preventing viewing.
Multicast H.264 only accessible by local clients.	Check if your router supports multicasting, or if the router settings between the client and the server need to be configured. The TTL (Time To Live) value may need to be increased.
Poor rendering of H.264 images.	Color depth set incorrectly on clients. Set to 16-bit or 32-bit color.
	In text overlays are blurred, or if there are other rendering problems, you may need to enable Advanced Video Rendering from the H.264 tab in the AMC Control Panel.
	Ensure that your graphics card is using the latest device driver. The latest drivers can usually be downloaded from the manufacturer's web site.
Color saturation is different in H.264 and Motion JPEG	Modify the settings for your graphics adapter. Please see the adapter's documentation for more information.

Lower frame rate than expected	Reduce number of applications running on the client computer.
	Limit the number of simultaneous viewers.
	Check with the system administrator that there is enough bandwidth available. See also the online help.
	Check in the AMC control panel applet (H.264 tab) that video processing is not set to Decode only I frames.
	Lower the image resolution.
Why do I not get 30 frames per second?	See *General performance considerations,* on page 47
Image degeneration	Decrease the GOV length, see the online help for more information.
The status indicator flashes red and the camera is inaccessible	
A firmware upgrade has been interrupted or the firmware has in some other way been damaged.	See *Emergency Recovery Procedure,* on page 40.
No images are displayed on web page	
Problem with AXIS Media Control (*Internet Explorer only*)	To enable the updating of video images in Internet Explorer, set your browser to allow ActiveX controls. Also, make sure that AXIS Media Control is installed on your workstation.
Installation of additional ActiveX component restricted or prohibited	Configure your camera to use a Java applet for updating the images under **Live View Config > Layout > Default Viewer** for Internet Explorer. See the online help for more information.
Video/Image problems, general	
Image too dark or too light.	Check the video image settings. See the online help on Video Stream and Camera Settings
Missing images in uploads	This can occur when trying to use a larger image buffer than is actually available. Try lowering the frame rate or the upload period.
Slow image update	Configuring pre-buffers, motion detection, high-resolution images, high frame rates will affect the performance of the camera.
Poor performance	Poor performance may be caused by heavy network traffic, multiple users accessing the unit, low performance clients, use of features such as motion detection, event handling and image rotation other than 180 degrees.
Image not clear	Check that the dome cover is clean. Do not clean a dome cover that looks clean to the eye and never polish the surface. Excessive cleaning can damage the surface. For general cleaning of a dome cover it is recommended to use a non-abrasive, solvent-free neutral soap or detergent with water and a soft cloth. Rinse well with clean lukewarm water. Dry with a soft cloth to prevent water spotting. Never use harsh detergents, gasoline, benzene or acetone etc. and avoid cleaning in direct sunlight or at elevated temperatures.
Poor quality snapshot images	
Screen incorrectly configured on your workstation	In Display Properties, configure your screen to show at least 65000 colors, that is, at least 16-bit. Using only 16 or 256 colors will produce dithering artifacts in the image.
Overlay/Privacy mask is not displayed	
Incorrect size or location of overlay or privacy mask.	The overlay or privacy mask may have been positioned incorrectly or may be too large. Refer to **Overlay Image Settings** in the online help for more information.
Browser freezes	
Netscape 7.x or Mozilla 1.4 (or later) can sometimes freeze on a slow computer	Lower the image resolution.
Problems uploading files	
Limited space	There is only limited space available for the upload of your own files. Try deleting existing files to free up space.
Motion Detection triggers unexpectedly	
Changes in luminance	Motion detection is based on changes in luminance in the image. This means that if there are sudden changes in the lighting, motion detection may be triggered mistakenly. Lower the sensitivity setting to avoid problems with luminance.
Storage/Disk management problems	
Video cannot be recorded	Check that the SD Card is not write protected (i.e., Read only).
SD Card cannot be mounted	If the SD Card cannot be mounted, reformat it and then click **Mount**.

For further assistance, please contact your reseller or check the support pages on the Axis web site at www.axis.com/techsup

LED Indicator flash routine

Case	Color	Description
Normal boot sequence	Unlit	Power on RFL check*
	Amber	Kernel booting System initiating
	Green	Shows steady green for 10 sec. for normal operation after restart.
	Unlit	Steady connection/normal operation
Hard Factory Default	Unlit	Power on RFL check*
	Amber	Steady - Kernel booting Flashes - Firmware restore Steady - System initiating
	Green	Shows steady green for 10 sec. for normal operation after restart.
	Unlit	Steady connection/normal operation
Flash Upgrade	Unlit	Steady connection/normal operation
	Amber	Flashes - Firmware upgrade
	Unlit	Reset RFL check*
	Amber	Steady - Kernel booting Flashes - Firmware restore Steady - System initiating
	Green	Shows steady green for 10 sec. for normal operation after restart.
	Unlit	Steady connection/normal operation
No Network	Unlit	Power on RFL check*
	Amber	Kernel booting System initiating
	Amber/red	Flashes - No network
	Green	Shows steady green for 10 seconds for normal operation after restart
	Unlit	Steady connection/normal operation
AXIS DynDNS	Unlit	Steady connection/normal operation
	Green	Flashes- Dyn DNS connecting Steady - DynDNS connection successful
	Unlit	Steady connection/normal operation
AVHS	Unlit	Steady connection/normal operation
	Green	Flashes - Initiating
	Amber	Flashes - Connection successful
	Unlit	Steady connection/normal operation
Bad Checksum	Red	Flashes - RFL check* failed See *Emergency Recovery Procedure*, on page 40.

* RFL (Resident Firmware Loader) check is a checksum method used to ensure that the software loading and starting the firmware works correctly.

Technical Specifications

Function/group	Item	Specification
Camera	Models	**AXIS P5532-E** 60 Hz, **AXIS P5532-E** 50 Hz **AXIS P5534-E** 60 Hz, **AXIS P5534-E** 50 Hz
	Image sensor	**AXIS P5532-E**: 1/4" Progressive scan CCD **AXIS P5534-E**: 1/3" Progressive scan CCD 1.3 Megapixel
	Lens	**AXIS P5532-E:** • Zoom 3.6 mm – 104.4 mm • F1.4 – 3.7 • Autofocus • Automatic day and night functionality • Horizontal angle of view: 53.1° – 2.0°
		AXIS P5534-E: • Zoom 4.7 mm – 84.6 mm • F1.6 – 2.8 • Autofocus • Automatic day and night functionality • Horizontal angle of view: 55.2° – 3.2°
	Light sensitivity	**AXIS P5532-E:** • Color: 0.5 lux at 30 IRE F1.4 • B/W: 0.01 lux at 30 IRE F1.4
		AXIS P5534-E • Color: 0.74 lux at 30 IRE F1.6 • B/W: 0.04 lux at 30 IRE F1.6
	Shutter time	**AXIS P5532-E** • 1/30000 s to 1 s (60 Hz) • 1/30000 s to 1/0.75 s (50 Hz)
		AXIS P5534-E 1/10000 s to 1/4 s
	Pan/Tilt/Zoom	• E-flip, auto-flip • 100 preset positions • Pan: 360° (with auto-flip), 0.2 – 300°/s • Tilt: 180°, 0.2 - 300°/s • **AXIS P5532**: 29x optical zoom and 12x digital zoom, total 348x zoom • **AXIS P5534**: 18x optical zoom and 12x digital zoom, total 216x zoom
	Pan/Tilt/Zoom functionalities	Guard Tour, control queue On-screen directional indicator
Video	Video compression	• H.264 (MPEG-4 Part 10/AVC, Baseline profile) • Motion JPEG
	Resolutions	**AXIS P5532-E** D1 720x480 to 176x120 (60 Hz) D1 720x576 to 176x144 (50 Hz)
		AXIS P5534-E HDTV 720p 1280x720 to 320x180)
	Frame rate H.264	Up to 30/25fps (60/50 Hz) in all resolutions
	Frame rate Motion JPEG	Up to 30/25fps (60/50 Hz) in all resolutions
	Video streaming	• Multiple, individually configurable streams in H.264 and Motion JPEG • Controllable frame rate and bandwidth • VBR/CBR H.264
	Image settings	• Wide Dynamic Range (WDR), manual shutter time, compression, color, brightness, sharpness, white balance, exposure control, exposure zones, backlight compensation, fine tuning of behavior at low light • **AXIS P5532-E**: Electronic Image Stabilization (EIS), noise reduction • Rotation 0°, 180° • Text and image overlay • Privacy mask • Image freeze on PTZ

Function/group	Item	Specification
Network	Security	Password protection, IP address filtering, HTTPS encryption, IEEE 802.1X network access control*, digest authentication, user access log *This product includes software developed by the Open SSL Project for use in the Open SSL Tool kit (www.openssl.org)
	Supported protocols	IPv4/v6, HTTP, HTTPS*, SSL/TLS*, QoS Layer 3 DiffServ, FTP, SMTP, Bonjour, UPnP, SNMPv1/v2c/v3(MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS, etc. *This product includes software developed by the Open SSL Project for use in the Open SSL Tool kit (www.openssl.org)
System Integration	Application Programming Interface	Open API for software integration, including VAPIX® from Axis Communications, specification available at www.axis.com Support for AXIS Video Hosting System (AVHS) with One-Click Camera Connection
	Intelligent video	Video motion detection, Advanced Gatekeeper
	Alarm triggers	Video motion detection, external input, PTZ preset, temperature, memory card full
	Alarm events	• File upload via FTP, HTTP and email • Notification via email, HTTP and TCP • External output activation • Go to PTZ preset • Run guard tour • Recording to local storage
	Video buffer	96 MB pre- and post alarm
	Video access from web browser	• Camera live view • Video recording to file (ASF) • Customizable HTML pages • Windows 7, Windows Vista, XP, Server 2003, Server 2008 • DirectX 9c or higher • For other operating systems and browers see www.axis.com/techsup
	Installation, management and maintenance	• AXIS Camera Management tool on CD and web-based configuration • Configuration of backup and restore • Firmware upgrades over HTTP or FTP, firmware available at www.axis.com
General	Casing	IP66-rated, metal casing (aluminum) Acrylic (PMMA) clear dome cover Sunshield (PC/ASA))
	Processors, memory	ARTPEC-3, 256 MB RAM, 128 MB Flash Battery backed-up real-time clock
	Power	• High Power over Ethernet (High PoE) IEEE 802.3at, max 30 W • AXIS T8123 High PoE Midspan 1-port included: 100-240 V AC
	Connectors	• RJ-45 10BASE-T/100BASE-TX PoE • IP66-rated RJ-45 connector kit included
	Local storage	SD/SDHC memory card slot (card not included)
	Operating conditions	• Operating conditions camera unit -20°C to 50 °C (-4°F to 122 °F) • Humidity up to 93% RH (non-condensing) • Operating conditions midspan -10°C to 55 °C (14°F to 131 °F)
	Storage conditions	• Storage conditions camera unit -40°C to 70 °C (-40°F to 158 °F)

Function/group	Item	Specification
	Approvals	• EN 55022 Class B, EN 61000-3-2 • EN 61000-3-3 • EN 61000-6-1, EN 61000-6-2, EN 55024 • FCC Part 15 Subpart B Class B • ICES-003 Class B • VCCI Class B • C-tick AS/NZS CISPR 22 • KCC Class B • IP66 • NEMA 4X • IEC 60721-4-3 Class 3K3, 3M3, EN/IEC 60068-2 • EN 60950-1 (IEC 60950-1) • Midspan: EN 60950-1, GS, UL, cUL, UL-AR, CE, VCCI, CB, KCC
	Dimensions (HxWxD)	195 mm x 210 mm x 210 mm (7.7" x 8.4". x 8.4")
	Weight	2.0 kg (4.4 lb.)
	Included accessories	AXIS T8123 High Power of Ethernet Midspan 1-port, IP66-rated RJ45 connector kit, clear and smoked dome cover, Installation Guide, CD with User's Manual, recording software, installation and management tools, Windows decoder 1-user license
	Video management software (not included)	AXIS Camera Station - Video management software for viewing and recording up to 50 cameras See www.axis.com/products/video/software/ for more software applications via partners
	Optional accessories	• AXIS T91A Mounting accessories • AXIS T8310 Video Surveillance Control Board • AXIS Camera Station • AXIS T90A Illuminators • Multi-user decoder license pack

General performance considerations

When setting up your system, it is important to consider how various settings and situations will affect performance. Some factors affect the amount of bandwidth (the bit rate) required, others can affect the frame rate, and some affect both. If the load on the CPU reaches its maximum, this will also affect the frame rate.

The following factors are among the most important to consider:

- High image resolutions and/or lower compression levels result in larger images. Bandwidth affected.
- Access by large numbers of Motion JPEG and/or unicast H.264 clients. Bandwidth affected.
- Simultaneous viewing of different streams (resolution, compression) by different clients. Effect on frame rate and bandwidth.
- Accessing both Motion JPEG and H.264 video streams simultaneously. Frame rate and bandwidth affected.
- Heavy usage of event settings affects the camera's CPU load. Frame rate affected.
- Enabled motion detection. Frame rate and bandwidth affected.
- Heavy network utilization due to poor infrastructure. Bandwidth affected.
- Viewing on poorly performing client PCs lowers perceived performance. Frame rate affected.

Glossary of Terms

ActiveX - A standard that enables software components to interact with one another in a networked environment, regardless of the language(s) used to create them. Web browsers may come into contact with ActiveX controls, ActiveX documents, and ActiveX scripts. ActiveX controls are often downloaded and installed automatically as required.

Angle - The field of view, relative to a standard lens in a 35mm still camera, expressed in degrees, e.g. 30°. For practical purposes, this is the area that a lens can cover, where the angle of view is determined by the focal length of the lens. A wide-angle lens has a short focal length and covers a wider angle of view than standard or telephoto lenses, which have longer focal lengths.

ARP (Address Resolution Protocol) - This protocol is used to associate an IP address to a hardware MAC address. A request is broadcast on the local network to discover the MAC address for an IP address.

ARTPEC (Axis Real Time Picture Encoder) - This chip is used for image compression.

ASIC (Application Specific Integrated Circuit) - A circuit designed for a specific application, as opposed to a general purpose circuit, such as a microprocessor.

Aspect ratio - A ratio of width to height in images. A common aspect ratio used for television screens and computer monitors is 4:3. High-definition television (HDTV) uses an aspect ratio of 16:9.

Autoiris (DC-Iris) - This special type of iris is electrically controlled by the camera, to automatically regulate the amount of light allowed to enter.

Bitmap - A bitmap is a data file representing a rectangular grid of pixels. It defines a display space and color for each pixel (or 'bit') in the display space. This type of image is known as a 'raster graphic.' GIFs and JPEGs are examples of image file types that contain bitmaps.

Because a bitmap uses this fixed raster method, it cannot easily be rescaled without losing definition. Conversely, a vector graphic image uses geometrical shapes to represent the image, and can thus be quickly rescaled.

Bit rate - The bit rate (in kbit/s or Mbit/s) is often referred to as speed, but actually defines the number of bits/time unit and not distance/time unit.

Bonjour - Also known as zero-configuration networking, Bonjour enables devices to automatically discover each other on a network, without having to enter IP addresses or configure DNS servers. Bonjour is a trademark of Apple Computer, Inc.

Broadband - In network engineering terms, this describes transmission methods where two or more signals share the same carrier. In more popular terminology, broadband is taken to mean high-speed data transmission.

CCD (Charged Coupled Device) - This light-sensitive image device used in many digital cameras is a large integrated circuit that contains hundreds of thousands of photo-sites (pixels) that convert light energy into electronic signals. Its size is measured diagonally and can be 1/4", 1/3", 1/2" or 2/3".

CGI (Common Gateway Interface) - A specification for communication between a web server and other (CGI) programs. For example, a HTML page that contains a form might use a CGI program to process the form data once it is submitted.

CIF (Common Intermediate Format) - CIF refers to the analog video resolutions 352x288 pixels (PAL) and 352x240 pixels (NTSC). See also *Resolution*.

Client/Server - Client/server describes the relationship between two computer programs in which one program, the client, makes a service request from another program, the server, which fulfils the request. Typically, multiple client programs share the services of a common server program. A web browser is a client program that requests services (the sending of web pages or files) from a web server.

CMOS (Complementary Metal Oxide Semiconductor) - A CMOS is a widely used type of semiconductor that uses both negative and positive circuits. Since only one of the circuit types is on at any given time, CMOS chips require less power than chips using just one type of transistor. CMOS image sensors also allow processing circuits to be included on the same chip, an advantage not possible with CCD sensors, which are also much more expensive to produce.

Codec - In communications engineering, a codec is usually a coder/decoder. Codecs are used in integrated circuits or chips that convert e.g. analog video and audio signals into a digital format for transmission. The codec also converts received digital signals back into analog format. A codec uses analog-to-digital conversion and digital-to-analog conversion in the same chip.

Codec can also mean compression/decompression, in which case it is generally taken to mean an algorithm or computer program for reducing the size of large files and programs.

Compression - See *Image compression*.

CVBS - analog video format (composite video).

DC-Iris (Autoiris) - This special type of iris is electrically controlled by the camera, to automatically regulate the amount of light allowed to enter.

DHCP (Dynamic Host Configuration Protocol) - DHCP is a protocol that lets network administrators automate and centrally manage the assignment of Internet Protocol (IP) addresses to network devices in a network.

DHCP uses the concept of a 'lease' or amount of time that a given IP address will be valid for a computer. The lease time can vary, depending on how long a user is likely to require the network connection at a particular location.

DHCP also supports static addresses for e.g. computers running web servers, which need a permanent IP address.

DNS (Domain Name System) - DNS is used to locate and translate Internet domain names into IP (Internet Protocol) addresses. A domain name is a meaningful and easy-to-remember name for an Internet address. For example the domain name www.example.com is much easier to

remember than 192.0.34.166. The translation tables for domain names are contained in Domain name servers.

Domain Server - Domains can also be used by organizations who wish to centralize the management of their (Windows) computers. Each user within a domain has an account that usually allows them to log in to and use any computer in the domain, although restrictions may also apply. The domain server is the server that authenticates the users on the network.

Duplex - See *Full-duplex*.

Ethernet - Ethernet is the most widely installed local area network technology. An Ethernet LAN typically uses special grades of twisted pair wires. The most commonly installed Ethernet systems are 10BASE-T and 100BASE-T10, which provide transmission speeds up to 10 Mbps and 100 Mbps respectively.

ETRAX (Ethernet Token Ring AXIS) - Axis' own microprocessor.

Factory default settings - These are the settings that originally applied for a device when it was first delivered from the factory. If it should become necessary to reset a device to its factory default settings, this will, for many devices, completely reset any settings that were changed by the user.

Firewall - A firewall works as a barrier between networks, e.g. between a Local Area Network and the Internet. The firewall ensures that only authorized users are allowed to access the one network from the other. A firewall can be software running on a computer, or it can be a standalone hardware device.

Focal length - Measured in millimeters, the focal length of a camera lens determines the width of the horizontal field of view, which in turn is measured in degrees.

FTP (File Transfer Protocol) - An application protocol that uses the TCP/IP protocols. It is used to exchange files between computers/devices on networks.

Frame - A frame is a complete video image. In the 2:1 interlaced scanning format of the RS-170 and CCIR formats, a frame is made up of two separate fields of 262.5 or 312.5 lines interlaced at 60 or 50 Hz to form a complete frame, which appears at 30 or 25 Hz. In video cameras with a progressive scan, each frame is scanned line-by-line and not interlaced; most are also displayed at 30 and 25 Hz.

Frame rate - The frame rate used to describe the frequency at which a video stream is updated is measured in frames per second (fps). A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

Full-duplex - Transmission of data in two directions simultaneously. In an audio system this would describe e.g. a telephone systems. Half-duplex also provides bi-directional communication, but only in one direction at a time, as in a walkie-talkie system. See also *Simplex*.

Gain - Gain is the amplification factor and the extent to which an analog amplifier boosts the strength of a signal. Amplification factors are usually expressed in terms of power. The decibel (dB) is the most common way of quantifying the gain of an amplifier.

Gateway - A gateway is a point in a network that acts as an entry point to another network. In a corporate network for example, a computer server acting as a gateway often also acts as a proxy server and a firewall server. A gateway is often associated with both a router, which knows where to direct a given packet of data that arrives at the gateway, and a switch, which furnishes the actual path in and out of the gateway for a given packet.

GIF (Graphics Interchange Format) - GIF is one of the most common file formats used for images in web pages. There are two versions of the format, 87a and 89a. Version 89a supports animations, i.e. a short sequence of images within a single GIF file. A GIF89a can also be specified for interlaced presentation.

GOV (Group Of VOPs) - A group of VOPs is the basic unit of an H.264 video stream. The GOV contains different types and numbers of VOPs (I-VOPs, P-VOPs) as determined by the GOV length and GOV structure. See also *VOP*.

GOV length - The GOV length determines the number of images (VOPs) in the GOV structure. See also *GOV* and *VOP*.

GOV structure - The GOV structure describes the composition of an H.264 video stream, as regards the type of images (I-VOPs or P-VOPs) included in the stream, and their internal order. See also *GOV* and *VOP*.

H.264 - A standard for video compression, also known as MPEG-4 Part 10.

Half-duplex - See *Full-duplex*.

HDTV - High-definition television, high resolution digital video.

HTML (Hypertext Markup Language) - HTML is the set of "markup" symbols or codes inserted in a file intended for display in web browser. The markup tells the browser how to display the page's words and images for the user.

HTTP (Hypertext Transfer Protocol) - HTTP is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the web. The HTTP protocol runs on top of the TCP/IP suite of protocols.

Hub - A (network) hub is used to connect multiple devices to the network. The hub transmits all data to all devices connected to it, whereas a switch will only transmit the data to the device it is specifically intended for.

IEEE 802.11 - A family of standards for wireless LANs. The 802.11 standard supports 1 or 2 Mbit/s transmission on the 2.4 GHz band. IEEE 802.11b specifies an 11 Mbit/s data rate on the 2.4 GHz band, while 802.11a allows up to 54 Mbit/s on the 5 GHz band.

Image compression - Image compression minimizes the file size (in bytes) of an image. Two of the most common compressed image formats are JPEG and GIF.

Interlacing - Interlaced video is video captured at 50 pictures (known as fields) per second, of which every 2 consecutive fields (at half height) are then combined into 1 frame.

Interlacing was developed many years ago for the analog TV world and is still used widely today. It provides good results when viewing motion in standard TV pictures, although there is always some degree of distortion in the image.

To view interlaced video on e.g. a computer monitor, the video must first be de-interlaced, to produce progressive video, which consists of complete images, one after the other, at 25 frames per second. See also *Progressive scan*.

IP (Internet Protocol) - The Internet Protocol is a method transmitting data over a network. Data to be sent is divided into individual and completely independent "packets." Each computer (or host) on the Internet has at least one address that uniquely identifies it from all others, and each data packet contains both the sender's address and the receiver's address.

The Internet Protocol ensures that the data packets all arrive at the intended address. As IP is a connectionless protocol, which means that there is no established connection between the communication end-points, packets can be sent via different routes and do not need to arrive at the destination in the correct order.

Once the data packets have arrived at the correct destination, another protocol - Transmission Control Protocol (TCP) - puts them in the right order. See also *TCP*.

IP Address - An IP address is simply an address on an IP network used by a computer/device connected to that network. IP addresses allow all the connected computers/devices to find each other and to pass data back and forth.

To avoid conflicts, each IP address on any given network must be unique. An IP address can be assigned as fixed, so that it does not change, or it can be assigned dynamically (and automatically) by DHCP.

An IP address consists of four groups (or quads) of decimal digits separated by periods, e.g. 130.5.5.25. Different parts of the address represent different things. Some part will represent the network number or address, and some other part will represent the local machine address.

See also *IP (Internet Protocol)*.

I-VOP - See *VOP*.

JPEG (Joint Photographic Experts Group) - Together with the GIF file format, JPEG is an image file type commonly used on the web. A JPEG image is a bitmap, and usually has the file suffix '.jpg' or ".jpeg." When creating a JPEG image, it is possible to configure the level of compression to use. As the lowest compression (i.e. the highest quality) results in the largest file, there is a trade-off between image quality and file size.

kbit/s (kilobits per second) - A measure of the bit rate, i.e. the rate at which bits are passing a given point. See also *Bit rate*.

LAN (Local Area Network) - A LAN is a group of computers and associated devices that typically share common resources within a limited geographical area.

Linux - Linux is an open source operating system within the UNIX family. Because of its robustness and availability, Linux has won popularity in the open source community and among commercial application developers.

Local storage - If a camera or video encoder supports local storage, an SD card can be inserted into the SD card slot to locally record and store a video stream.

MAC address (Media Access Control address) - A MAC address is a unique identifier associated with a piece of networking equipment, or more specifically, its interface with the network. For example, the network card in a computer has its own MAC address.

Manual iris - This is the opposite to an autoiris, i.e. the camera iris must be adjusted manually to regulate the amount of light allowed to reach the image sensor.

Mbit/s (Megabits per second) - A measure of the bit rate, i.e. the rate at which bits are passing a given point. Commonly used to give the 'speed' of a network. A LAN might run at 10 or 100 Mbit/s. See also *Bit rate*.

Monitor - A monitor is very similar to a standard television set, but lacks the electronics to pick up regular television signals.

Motion JPEG - Motion JPEG is a simple compression/decompression technique for networked video. Latency is low and image quality is guaranteed, regardless of movement or complexity of the image. Image quality is controlled by adjusting the compression level, which in turn provides control over the file size, and thereby the bit rate.

High-quality individual images from the Motion JPEG stream are easily extracted. See also JPEG.

Megapixel - See *Pixel*.

MPEG (Moving Picture Experts Group) - The Moving Picture Experts Group develops standards for digital video and audio compression. It operates under the auspices of the International Organization for Standardization (ISO). The MPEG standards are an evolving series, each designed for a different purpose.

MPEG-2 - MPEG-2 is the designation for a group of audio and video coding standards, and is typically used to encode audio and video for broadcast signals, including digital satellite and Cable TV. MPEG-2, with some modifications, is also the coding format used by standard commercial DVD movies.

Multicast - Bandwidth-conserving technology that reduces bandwidth usage by simultaneously delivering a single stream of information to multiple network recipients.

Network connectivity - The physical (wired or wireless) and logical (protocol) connection of a computer network or an individual device to a network, such as the Internet or a LAN.

NTSC (National Television System Committee) - NTSC is the television and video standard in the United States. NTSC delivers 525 lines at 60 half-frames/second.

NWay - A network protocol that automatically negotiates the highest possible common transmission speed between two devices.

PAL (Phase Alternating Line) - PAL is the dominant television standard in Europe. PAL delivers 625 lines at 50 half-frames/second.

Ping - Ping is a basic network program used diagnostically to

check the status of a network host or device. Ping can be used to see if a particular network address (IP address or host name) is occupied or not, or if the host at that address is responding normally. Ping can be run from e.g. the Windows Command prompt or the command line in UNIX.

Pixel - A pixel is one of the many tiny dots that make up a digital image. The color and intensity of each pixel represents a tiny area of the complete image.

PoE (Power over Ethernet) - Power over Ethernet provides power to a network device via the same cable as used for the network connection. This is very useful for IP-Surveillance and remote monitoring applications in places where it may be too impractical or expensive to power the device from a power outlet.

PPP (Point-to-Point Protocol) - A protocol that uses a serial interface for communication between two network devices. For example, a PC connected by a phone line to a server.

PPTP (Point-to-Point Tunneling Protocol) - A protocol (set of communication rules) that allows corporations to extend their own corporate network through private "tunnels" over the public Internet. In this way a corporation can effectively use a WAN (Wide Area Network) as a large single LAN (Local Area Network). This kind of interconnection is known as a virtual private network (VPN).

Pre/post alarm images - The images from immediately before and after an alarm. These images are stored in a buffer for later retrieval.

Progressive scan - Progressive scan, as opposed to interlaced video, scans the entire picture, line by line every sixteenth of a second. In other words, captured images are not split into separate fields as in interlaced scanning.

Computer monitors do not need interlace to show the picture on the screen, but instead show them progressively, 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. In a surveillance application, this can be critical when viewing detail within a moving image, such as a person running. A high-quality monitor is required to get the best from progressive scan. See also *Interlacing*.

Protocol - A special set of rules governing how two entities will communicate. Protocols are found at many levels of communication, and there are hardware protocols and software protocols.

Proxy server - In an organization that uses the Internet, a proxy server acts as an intermediary between a workstation user and the Internet. This provides security, administrative control, and a caching service. Any proxy server associated with a gateway server, or part of a gateway server, effectively separates the organization's network from the outside network and the local firewall. It is the firewall server that protects the network against outside intrusion.

A proxy server receives requests for Internet services (such as web page requests) from many users. If the proxy server is also a cache server, it looks in its local cache of previously downloaded web pages. If it finds the page, it is returned to the user without forwarding the request to the Internet. If the page is not in the cache, the proxy server, acting as a client on behalf of the user, uses one of its own IP addresses to request the page from another server over the Internet. When the requested page is returned, the proxy server forwards it to the user that originally requested it.

P-VOP - See *VOP*.

Resolution - Image resolution is a measure of how much detail a digital image can hold: the greater the resolution, the greater the level of detail. Resolution can be specified as the number of pixel-columns (width) by the number of pixel-rows (height), e.g. 320x240.

Alternatively, the total number of pixels (usually in megapixels) in the image can be used. In analog systems it is also common to use other format designations, such as CIF, QCIF, 4CIF, etc.

RTCP (Real-Time Control Protocol) - RTCP provides support for real-time conferencing of groups of any size within an intranet. This support includes source identification and support for gateways like audio and video bridges as well as multicast-to-unicast translators.

RTCP offers quality-of-service feedback from receivers to the multicast group as well as support for the synchronization of different media streams.

RTP (Real-Time Transport Protocol) - RTP is an Internet protocol for the transport of real-time data, e.g. audio and video. It can be used for media-on-demand as well as interactive services such as Internet telephony.

RTSP (Real Time Streaming Protocol) - RTSP is a control protocol, and a starting point for negotiating transports such as RTP, multicast and Unicast, and for negotiating codecs.

RTSP can be considered a 'remote control' for controlling the media stream delivered by a media server. RTSP servers typically use RTP as the protocol for the actual transport of audio/video data.

Router - A device that determines the next network point to which a packet should be forwarded on its way to its final destination. A router creates and/or maintains a special routing table that stores information on how best to reach certain destinations. A router is sometimes included as part of a network switch. See also *switch*.

Server - In general, a server is a computer program that provides services to other computer programs in the same or other computers. A computer running a server program is also frequently referred to as a server. In practice, the server may contain any number of server and client programs. A web server is the computer program that supplies the requested HTML pages or files to the client (browser).

Sharpness - This is the control of fine detail within a picture. This feature was originally introduced into color TV sets that used notch filter decoders. This filter took away all high frequency detail in the black and white region of the picture. The sharpness control attempted to put some of that detail back in the picture. Sharpness controls are mostly superfluous in today's high-end TVs. The only logical requirement for it nowadays is on a VHS machine.

Simplex - In Simplex operation, a network cable or communications channel can only send information in one direction.

SMTP (Simple Mail Transfer Protocol) - SMTP is used for sending and receiving e-mail. However, as it is 'simple,' it is limited in its ability to queue messages at the receiving end, and is usually used with one of two other protocols, POP3 or IMAP. These other protocols allow the user to save messages in a server mailbox and download them periodically from the server.

SMTP authentication is an extension of SMTP, whereby the client is required to log into the mail server before or during the sending of email. It can be used to allow legitimate users to send email while denying the service to unauthorized users, such as spammers.

SNMP (Simple Network Management Protocol) - SNMP forms part of the Internet Protocol suite, as defined by the Internet Engineering Task Force. The protocol can support monitoring of network-attached devices for any conditions that warrant administrative attention.

Sockets - Sockets are a method for communication between a client program and a server program over a network. A socket is defined as 'the endpoint in a connection.' Sockets are created and used with a set of programming requests or 'function calls' sometimes called the sockets application programming interface (API).

SSL/TSL (Secure Socket Layer/Transport Layer Security) These two protocols (SSL is succeeded by TSL) are cryptographic protocols that provide secure communication on a network. SSL is commonly used over HTTP to form HTTPS, as used e.g. on the Internet for electronic financial transactions. SSL uses public key certificates to verify the identity of the server.

Subnet/subnet mask - A subnet is an identifiably separate part of an organization's network. Typically, a subnet may represent all the machines at one geographic location, in one building, or on the same local area network (LAN). Having an organization's network divided into subnets allows it to be connected to the Internet with a single shared network address.

The subnet mask is the part of the IP address that tells a network router how to find the subnet that the data packet should be delivered to. Using a subnet mask saves the router having to handle the entire 32-bit IP address; it simply looks at the bits selected by the mask.

Switch - A switch is a network device that connects network segments together, and which selects a path for sending a unit of data to its next destination. In general, a switch is a simpler and faster mechanism than a router, which requires knowledge about the network and how to determine the route. Some switches include the router function. See also *Router*.

TCP (Transmission Control Protocol) - TCP is used along with the Internet Protocol (IP) to transmit data as packets between computers over the network. While IP takes care of the actual packet delivery, TCP keeps track of the individual packets that the communication (e.g. requested a web page file) is divided into, and, when all packets have arrived at their destination, it reassembles them to re-form the complete file.

TCP is a connection-oriented protocol, which means that a connection is established between the two end-points and is maintained until the data has been successfully exchanged between the communicating applications.

Telnet - Telnet is a simple method with which to access another network device, e.g. a computer. The HTTP protocol and the FTP protocols allow you to request specific files from remote computers, but do not allow you logon as a user of that computer. With Telnet, you log on as a regular user with whatever privileges you may have been granted for specific applications and data residing on that computer.

UDP (User Datagram Protocol) - UDP is a communications protocol that offers limited service for exchanging data in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP). The advantage of UDP is that it is not required to deliver all data and may drop network packets when there is e.g. network congestion. This is suitable for live video, as there is no point in re-transmitting old information that will not be displayed anyway.

Unicast - Communication between a single sender and a single receiver over a network. A new connection is established for each new user.

URL (Uniform Resource Locator) - An "address" on the network.

Varifocal lens - A varifocal lens provides a wide range of focal lengths, as opposed to a lens with a fixed focal length, which only provides one.

VPN (Virtual Private Network) - This creates a secure "tunnel" between the points within the VPN. Only devices with the correct "key" will be able to work within the VPN. The VPN network can be within a company LAN (Local Area Network), but different sites can also be connected over the Internet in a secure way. One common use for VPN is for connecting a remote computer to the corporate network, via e.g. a direct phone line or via the Internet.

VOP (Video Object Plane) - A VOP is an image frame in an H.264 video stream. There are several types of VOP:

- An I-VOP is complete image frame.

- A P-VOP codes the differences between images, as long as it is more efficient to do so. Otherwise it codes the whole image, which may also be a completely new image.

WAN (Wide-Area-Network) - Similar to a LAN, but on a larger geographical scale.

W-LAN (Wireless LAN) - A wireless LAN is a wireless local area network that uses radio waves as its carrier: where the network connections for end-users are wireless. The main network structure usually uses cables.

Web server - A web server is a program, which allows web browsers to retrieve files from computers connected to the Internet. The web server listens for requests from web browsers and upon receiving a request for a file sends it back to the browser.

The primary function of a web server is to serve pages to other remote computers; consequently, it needs to be installed on a computer that is permanently connected to the Internet. It also controls access to the server whilst monitoring and logging server access statistics.

WEP (Wireless Equivalent Privacy) - A wireless security protocol, specified in the IEEE 802.11 standard, which is

designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to that usually expected of a wired LAN. Security is at two different levels; 40-bit and 128-bit encryption. The higher the bit number, the more secure the encryption.

WPA-PSK (Wi-Fi Protected Access - Pre-Shared Key) - This wireless encryption method uses a pre-shared key (PSK) for key management. Keys can usually be entered as manual hex values, as hexadecimal characters, or as a Passphrase. WPA-PSK provides a greater degree of security than WEP.

YPbPr - analog video signal for component video.

Zoom lens - A zoom lens can be moved (zoomed) to enlarge the view of an object to show more detail.

Index

A
Access Log 38
Action Buttons 9, 19
Administrator 13, 30
Alarm 26
AMC 7
ARP/Ping 33
Axis Media Control viewer Toolbar 9

B
Backlight compensation 16
Backup 37
Bit Rate 15
Bonjour 7, 37
Brightness 16
Buffer Size 24
Buffers 24

C
Color level 16
Connection List 38
Constant Bit Rate 15
Continuous Recording 29
Control Queue 21

D
Date & Time 32
Default Viewer 18
Disk full 24
DNS Configuration 33
DNS Server 33, 34
Domain Name 34

E
Emergency recovery 40
Enable ARP/Ping 33
Event Servers 23
Event Types 23
Events 23
Exposure Settings 16
Exposure zones 16

F
Factory Default Settings 39
Fan 9, 24
Firmware 40
Frame Rate 14
FTP 35
FTP Server 23

G
Gatekeeper 25
GOV Settings 15
Guard Tour 20

H
H.264 14, 15
Heater 9
Host Name 34
HTTP Server 23
HTTPS 8, 30, 34

I
IEEE 802.1X 31
Image freeze on PTZ 17
IP Address Filtering 30
IPv4 32, 34
IPv6 33
IR cut filter 17

L
LED 44
LED Indicator 6, 44
Live View 9
Live View Config 18
Local storage 4
Logs & Reports 38

M
Mask 17
MJPEG 14, 15
Motion Detection 26
Motion detection 24

N
NAT traversal 7, 34
Network Settings 32
NTP Configuration 34
NTP Server 32

O
Operator 30
OSDI Zones 20
Overlay Settings 14

P
Pan Tilt Zoom 24
Pan/Tilt/Zoom Controls 10
Parameter List 38
Password Settings 30
Port Status 28
Post-trigger Buffer 24
Pre-trigger Buffer 24
Proportional speed 21
PTZ control panel 10

Q
QoS 35
QuickTime 11, 18

R
Recording List 28

Recovery 40
Referrals 30
Restore 37
RTSP 35

S
Scheduled Event 25
Security 30
Self-signed certificate 8
Server Report 38
Server Time 32
Sharpness 16
SMTP 36
Snapshot button 9
SNMP 36
Storage 37
Storage Device 37
Support 37, 41
System Log 38
System Options 30

T
TCP Server 23
TCP/IP Settings 32
Time Mode 32
Troubleshooting 40

U
Upgrade Server 37
UPnP 34, 36
Users 30

V
Variable Bit Rate 15
Video Stream 14
Viewer 30

W
White balance 16
Wide dynamic range 16

Artisan Technology Group is an independent supplier of quality pre-owned equipment

Gold-standard solutions

Extend the life of your critical industrial, commercial, and military systems with our superior service and support.

We buy equipment

Planning to upgrade your current equipment? Have surplus equipment taking up shelf space? We'll give it a new home.

Learn more!

Visit us at **artisantg.com** for more info on price quotes, drivers, technical specifications, manuals, and documentation.

Artisan Scientific Corporation dba Artisan Technology Group is not an affiliate, representative, or authorized distributor for any manufacturer listed herein.

We're here to make your life easier. How can we help you today?

(217) 352-9330 | sales@artisantg.com | artisantg.com

ARTISAN® TECHNOLOGY GROUP