IP Camera Overview

Basics

An Internet protocol camera, or IP camera, is a type of digital video camera commonly employed for surveillance, and which unlike analog closed circuit television (CCTV) cameras can send and receive data via a computer network and the Internet. Although most cameras that do this are webcams, the term "IP camera" or "netcam" is usually applied only to those used for surveillance.

There are two kinds of IP cameras:

Centralized IP cameras, which require a central Network Video Recorder(NVR) to handle the recording, video and alarm management.

Decentralized IP cameras, which do not require a central Network Video Recorder (NVR), as the cameras have recording function built-in and can thus record directly to any standard storage media, such as SD cards, NAS (network attached storage) or a PC/Server.

Potential advantages:

- Two-way audio via a single network cable allows users to communicate with what they are seeing (e.g. gas station clerk assisting a customer on how to use the pay pumps)
- Flexibility: IP cameras can be moved around anywhere on a network (wireless).
- Distributed intelligence: with IP cameras, video analytics can be placed in the camera itself allowing ability in analytics solutions.[3]
- Transmission of commands for PTZ (pan, tilt, zoom) cameras via a single network.
- Encryption & authentication: IP cameras offer secure data transmission through encryption and authentication methods such as WPA, WPA2, TKIP, AES.
- Remote accessibility: live video from selected cameras can be viewed from any computer, anywhere, and also from many mobile smartphones and other devices. Remote accessibility also prevents police officers from confiscating video and audio evidence that you can use against them
- IP cameras are able to function on a wireless network.
- PoE - Power over Ethernet: Modern IP cameras have the ability to operate without a power supply. They can work with the PoE-protocol.
- IP camera communication signals are not just electronic voltage, it is numerically decoded as bits and bytes with security features and TCP/IP protocol.
- Depending on the equipment and system installed, there is no limit to the number of devices that can be placed on the network.

Potential disadvantages

- Higher initial cost per camera
- High network bandwidth requirements

HD 1080P/2MP	30 fps	H.264	Expect 4 Mbps per camera
CIF/0.07MP	5 fps	H.264	Expect 125 Kbps per camera
HD 1080P/2MP	30 fps	MJPEG	Expect 12 Mbps per camera

- Can have challenges capturing images in low-light or backlight situations (this is true for most IP cameras)
- If the video is transmitted over the public Internet rather than a private IP LAN, the system becomes open to a wider audience of hackers and hoaxers.

(http://www.campussafetymagazine.com/article/Your-IP-Video-Surveillance-Cheat-Sheet-The-Basics)

Internet protocol (IP) video uses the computer network infrastructure to transmit security video to recording and viewing stations and dispatch centers. In IP video systems, network cameras output a digitally encoded signal that can be transmitted over the network as data for viewing, storage and integration with other security solutions. Video management systems or software (VMS) allows the user to view the live video, call up recorded video, control the cameras connected to the network and many other functions.

Security

- Update Your Camera's Firmware: Most modern IP security cameras feature user upgradeable firmware. If a security vulnerability is found, the IP security camera manufacturer will often fix the vulnerability by issuing a firmware update. Usually, you can update your camera's firmware from the admin console via a web browser. You should frequently check your IP security camera manufacturer's website for updated firmware so that you can make sure the version you are using doesn't contain an unpatched vulnerability that could be exploited by hackers and Internet voyeurs.
- Keep Your Cameras Local: If you don't want your camera feeds to end up on the Internet, then don't connect them to the Internet. If privacy is your top priority then you should keep your cameras on a local network and assign them non-routable internal IP addresses (i.e 192.168.0.5 or something similar). Even with non-routable IP addresses your cameras could still be exposed by camera software that sets up port forwarding or uses UPNP to expose your cameras to the Internet. Check your IP camera's website to learn how to setup your cameras in local-only mode.
- Password Protect Your Cameras: Many IP cameras don't have password protection for video feeds turned on by default. They probably think that you would rather get your cameras up and running and secure them later. Unfortunately a lot of people forget to go back and add password protection after the initial setup and end up leaving the cameras wide open for all to access. Most cameras offer at least some form of basic authentication. It may not be super

robust, but at least it is better than nothing at all. Protect your camera feeds with a username and a strong password and change it periodically.

- Rename the Default Admin Account and set a new Admin Password: Your camera's default admin name and password, set by the manufacturer, is usually available by visiting their website and going to the support section for your camera model. If you haven't changed the admin name and password then even the most novice hacker can quickly look up the default password and view your feeds and/or take control of your camera.
- If Your Camera is Wireless, Turn on WPA2 Encryption: If your camera is wireless capable, you should only join it to a WPA2-encrypted wireless network so that wireless eavesdroppers can't connect to it and access your video feeds.
- Don't put IP Cameras Where They Don't Belong: Don't put an IP security camera inside areas of your house where you wouldn't feel comfortable being seen by strangers. Even if you think you've secured your cameras in every way possible, there is always the possibility of getting blind-sided by a Zero-Day vulnerability that hasn't been found by your manufacturer yet. You don't want to be the star of someone else's sick reality show so when in doubt, leave the camera out.

Set-up/Ports used

(https://answers.yahoo.com/question/?qid=20100312074318AA1leiy) Firewall security features built into some routers may prevent users from accessing the IP cam over the Internet. Your router connects to the Internet over a series of “ports”.

Sometimes the default ports used by the IP cam are blocked from access over the Internet, therefore, these ports need to be made accessible. This is achieved using the Port Forwarding function on your router. The ports used by the camera must be opened through the router for remote access to your IP cam. Check your router’s user manual for specific instructions on how to open and route ports on you router. You can also find instructions for how to do this on your specific router on the following website: http://www.portforward.com/ Important: Some ISPs block access to port 80 and other commonly used Internet ports. Check with your ISP in order to open the appropriate ports. If your ISP does not pass traffic on port 80, you will need to change the camera’s default port number from 80 to a different number such as 8000.

- (http://www.networkwebcams.co.uk/blog/2007/10/22/howto-port-forwarding-101/)
  - the following items which need to be considered when preparing your camera:
    - Set up our camera with a static local IP address
    - Input the correct subnet mask and default gateway addresses
    - Set up your DNS server addresses
    - Configure the port number: Remember also that when changing to a custom port number the URL for your camera will change both internally and externally. For example if we changed our camera on http://192.168.0.90 from port 80 to port 4440 we would have to use http://192.168.0.90:4440 to connect to the camera, specifying the port number explicitly at the end of the IP address. This is the same for accessing the camera externally.

Protocols Used

(http://www.camera-sdk.com/p_34-codecs-and-protocols-supported-by-ozeki-ip-camera-sdk-onvif.html)

Protocols needed for video streaming

- **SIP**: Session Initialization Protocol: Session Initiation Protocol (SIP) is IETF signaling protocol used for multimedia communication sessions such as voice and video calls over Internet Protocol (IP). SIP can be used for creating, modifying and terminating two-party (unicast) or multiparty (multicast) sessions. For example internet telephone calls, multimedia distribution, multimedia conferences, instant messaging etc.
- **UDP**: User Datagram Protocol: The User Datagram Protocol (UDP) belongs to the Internet Protocol Suite that is a set of network protocols for the Internet. UDP makes it possible for the computers to send messages. UDP supposes that error checking and correction is not necessary. Time-sensitive applications often employ UDP as real-time system that prefers dropping packets instead of waiting for delayed ones.
- **SDP**: Session Description Protocol: The Session Description Protocol (SDP) conveys information on media streams in multimedia sessions in order to allow recipients of a session description to participate in the session. It is mainly used in inter-network but it can also describe conferences in other network environments. SDP is often used together with RTP, SIP or as a standalone format.
- **RTSP**: Real Time Streaming Protocol: The Real Time Streaming Protocol (RTSP) is an application-level protocol that is used/can be used for controlling the delivery of data with real-time properties. RTSP provides an extensible framework to enable controlled, on-demand delivery of real-time data, such as audio and video. Sources of data can include both live data feeds and stored clips.
- **RTP**: Real-time Transport Protocol: Real-time Transport Protocol specifies a standardized packet format that is applied for the transmission of multimedia data such as audio and video over the Internet. RTP ensures end-to-end multimedia data delivery with real-time characteristics. Practically it means that with the implementation of RTP it is possible to deliver interactive video or audio data.
- **RTCP**: Real-Time Control Protocol: The Real-Time Transport Control Protocol (RTCP) is a companion protocol of the Real-time Transport Protocol (RTP) the one used to send and receive most media over IP these days. RTCP gathers statistics for a media connection and information. RTCP gives information on transmitted octet and packet counts, lost packet counts, jitter, and round-trip delay time.
- **H323** Protocol: H.323 is an ITU VOIP protocol. It provides a foundation for audio, video, and data communications across IP-based networks, including the Internet. It is implemented by voice and video conferencing equipment manufacturers, real-time applications and is deployed worldwide by service providers and enterprises for both voice and video services over IP networks.