

# IP Surveillance

## The Next Generation Security Camera Application

White Paper  
July, 2005

### Abstract

This White Paper provides a short introduction to Internet Protocol (IP) surveillance systems that use digital cameras networked via standard Ethernet networks. The paper explains basic technology concepts, provides a benefit overview, describes advantages for specific security applications in selected vertical markets, and details the necessary requirements and considerations for implementation of the technology.

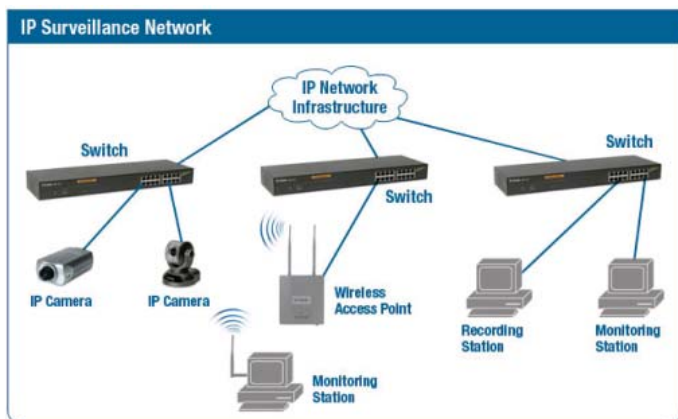
## IP Surveillance Technology

The growth in IP Surveillance systems is quickly gaining significant ground on conventional analog closed circuit television (CCTV) security camera installations for reasons of both performance and cost-benefits.

IP Surveillance systems digitize video streams at each camera on the network, this digital stream is then transferred over a standard wired or wireless Internet Protocol (IP) network. Unlike traditional analog closed circuit television systems that transport analog signals back to a centralized video recording device, IP surveillance systems digitize and compress the video at each camera and send a digital signal across a common IP or Ethernet network. IP Surveillance employs a decentralized data encoding system that sends binary data across a shared, standards-based IP network – the same one used for email, Web pages, file transfers, and other data network applications.

Since digital networked surveillance is IP-based, users can monitor, store, and archive video, audio and associated application data over the Internet or across private data networks. Compressed video can be carried anywhere that the IP network extends as opposed to CCTV systems that are built on and require dedicated coaxial cabling. Anyone with the proper access credentials and a standard browser can monitor video as well as control and configure the camera from any location that has Internet or private network connectivity.

Since networking equipment and IP protocols adhere to open standards, the IP Surveillance system itself is low cost, and new integration opportunities and applications are continually coming into focus. Event-driven alert and alarm software for IP systems already far exceed the capabilities of old CCTV systems. Digital IP cameras can be used to monitor on a 24x7 basis and be configured to trigger on events while immediately alerting administrators when certain conditions arise or specific thresholds are reached.



*IP Surveillance networks run over a standard Ethernet Infrastructure*

## Benefits of IP Surveillance

A growing number of security organizations, small and medium sized businesses, and home users throughout the world use networked IP Surveillance equipment, and industry analysts expect that number to rise dramatically as organizations of all sizes continue to understand the benefits of the technology. The advantages that IP Surveillance has over traditional analog systems are numerous, and the benefits usually fall into one of the four following categories:

### Cost Effectiveness

When compared to analog CCTV systems, networked IP camera systems have several cost advantages. First, the wiring required is less expensive. Most buildings contain installed Cat-5 data networking cable, and if additional wiring is necessary, Cat-5 costs less per foot than single purpose analog coaxial cable. Thus, IP Surveillance can often use the existing wired infrastructure and not require the installation of a second and parallel cabling infrastructure.

A digital, packet-switched network enables centralized, cost-effective management. IP networks carry all kinds of data, including video, audio and standard document files like email and web pages. Any existing infrastructure and personnel used to manage the data network can easily absorb a new IP Surveillance application. Infrastructure maintenance, monitoring and management of IP Surveillance applications are easily learned without the need for specialized components, cabling, or training required for a separate analog CCTV alternative. The elimination of a separately installed and managed infrastructure will save time and resources.

Since IP networks employ well documented, understood, and heavily deployed standards for cabling and transmission protocols, the costs for equipment and service have diminished as application adoption increases. Technology advancements and adoption have already had a profound effect on the price of networking equipment and digital cameras. Expect that trend to continue as competition naturally flourishes in a standards-based deployment environment.

### Advanced Functionality and Performance

#### Event Driven Intelligence

One of the most compelling reasons to adopt IP network surveillance is event-driven intelligence. A regular digital video recorder (DVR) based surveillance system is only as smart as the person monitoring it at the moment it is being monitored. With IP networks there is access to a wide range of automated software settings and alert systems that make security management more efficient, less costly, more intelligent and less error prone.

IP systems handle motion detection, event triggers, and alert automation and have a multitude of options for changing frame rates, resolution and timed record cycles.

For example, certain cameras might only send data to the recording servers when a specific threshold of motion is detected. Sensitivity settings can be adjusted so insignificant movements will not trigger a recording. This saves recording space and human analysis time by keeping only what is relevant to the particular security situation at hand. With digital images, integration is possible with available third party applications for license plate recognition, people counting, Geographic Information Systems (GIS), and face recognition.

Alerts can also be configured and emailed to any email address or group and retrieved with any IP-connected communication system containing an email client. This includes notifications to handheld PDAs, cell phones, or other IP connected devices.

With an analog camera system, none of these applications can be performed without some digital conversion. The multiple analog/digital conversions required, however, reduces image quality. With IP Surveillance systems, the digitization process occurs once at the camera and is carried across the digital IP network. The video data starts digital and stays digital throughout the infrastructure.

#### Superior Image Quality

Network IP Surveillance equipment also provides better image quality than analog systems. Analog coax cables can compromise image clarity, since signals can degrade over long cabling distances. Analog cameras adhere to NTSC/PAL standards, effectively limiting resolution to 0.4 megapixels. Network cameras, on the other hand, use progressive scan technology and high resolutions that depict moving objects more clearly and cover larger areas with sharper images. These technological advantages enable digital pan, tilt and zoom features that analog systems can only perform with additional, dedicated cabling.

#### Securing the Security Camera

IP Surveillance systems can encrypt data across the network, so only the cameras and servers know what kind of packets to expect across the system. Without the proper authentication keys, outsiders cannot break into the network to steal video data or feed false video into the system.

With analog systems, access is needed to the cabling to tap into the electrical circuit. Video can be fed into the wire or recorded off of it at will without raising any intrusion alarms. The analog system sees electricity coming across the wires. IP systems are much more difficult to compromise because encryption requires two nodes that agree on exactly what is being sent and received (and have the algorithms or keys that decode the data). Any interruption to the data stream can automatically trigger alarms and alerts.

#### One-Way or Two-Way Audio

Since IP Surveillance systems are merely passing around information packets, any kind of additional data (sound, graphics, applications, event triggers, etc) can accompany the data stream. Thus, one-way or two-way audio requires only microphones and speakers at the end points when used with appropriate IP cameras that support audio capabilities. Analog systems, on the other hand, can't handle single channel audio or two-way sound channels without added cabling and expense. Deploying audio with the video images becomes very simple in IP Surveillance applications.

#### Back-Up and Storage

Storage systems are easier to configure and more reliable with IP systems as well. All the redundant components found in standard computer based systems like RAID disks, uninterruptible power supplies and secure off-site storage can be leveraged in IP Surveillance applications. In many cases, the infrastructure may already exist and available staff will not have to learn new storage systems. Analog systems, however, require proprietary recording and back-up systems that add significant component, maintenance, and training costs as the system grows. In addition analog tape based recording systems require ongoing replacement tapes. After a period of use the tapes become stretched, can no longer be effectively used, and must be replaced.

#### Flexibility of Deployment Standards Based

The Internet Protocol itself offers a wide range of flexibility because it is a global standard that runs on a wide range of open, standardized, low-cost equipment. "Best of breed" products and services can be combined from an assortment of vendors. Price competition and vendor choices truly make it a buyer's market.

Of course, IP Surveillance data can be securely viewed anytime, anywhere from a standard Web browser like Internet Explorer. This simply cannot be done with analog systems that are relegated to the local redundant cabling infrastructure that has been established. Remote site monitoring becomes difficult with analog CCTV systems.

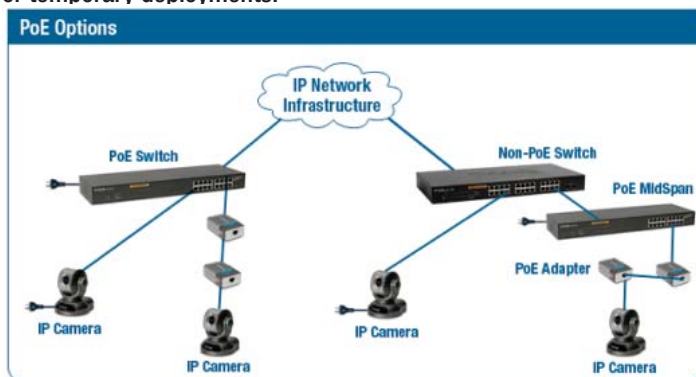


*Remote viewing through standard web browser*

### PoE and 802.11 Wireless LAN

There are a couple of other features or standards that make IP Surveillance even more attractive: Power over Ethernet (PoE) and 802.11 wireless LAN connectivity.

With external PoE adapters, power is delivered to the IP Surveillance cameras via Cat-5 Ethernet cabling. This eliminates the need for costly electrical wiring and opens up more opportunities for effective camera placement. Equipment can be placed based on the needs of the application versus where power outlets may be available. More effective camera placement will lend itself to a more effective surveillance system. PoE enables flexible, more efficient network designs, simplifies and speeds installation, and generally reduces costs across the board. PoE also facilitates changing environments or temporary deployments.



*PoE reduces costs associated with running AC power to difficult to reach locations*

PoE technology allows for centralized power management. With centralized power management, the IP network is protected by uninterruptible power supplies with battery back-up (UPS). If power goes down, the critical network and surveillance infrastructure can stay online. Centrally managed power enables remote shutdown or remote reset capabilities, saving the time and expense of dispatching a technician to a camera location. With analog CCTV systems all distributed devices need UPS power supplies adding complexity and costs to the overall system.

Wireless installations offer similar kinds of benefits. If running Ethernet cable is undesirable, installing low cost 802.11 wireless access points and placing wireless cameras anywhere within the cell of coverage is an option. The 54 Mbps 802.11g standard is sufficient for many video surveillance applications. Current wireless security standards, like WiFi Protected Access (WPA) offer robust authentication and encryption for the wireless signal to prevent snooping and interception of the video signal.

### Ease of Expansion and Scalability

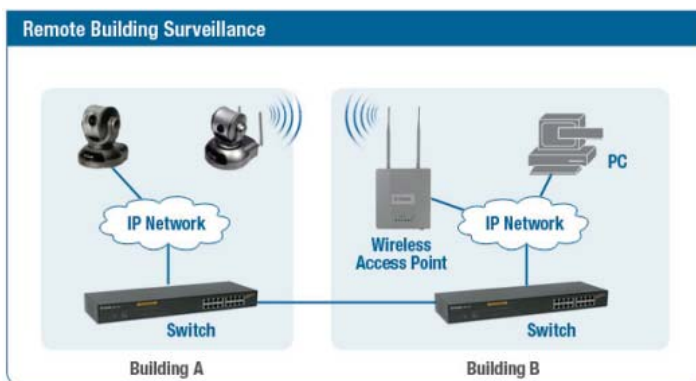
IP Surveillance applications are also highly scalable. Cameras can be added one at a time, whereas DVR analog systems may require increments of 8, 16 or 24 additional cameras. As a company grows, the digital system keeps costs in check.

With Gigabit and 10 Gigabit Ethernet readily available, the IP network is scalable as well. Several cameras can be supported on the same IP infrastructure. Typical switches and routers available today simply segregate traffic for larger scale video applications. With proper network design, installations with 200-300 cameras are common, and some organizations are easily using more than 1000 cameras at a time.

Storage and server systems scale easily and cheaply, with no need for specialized recording equipment or training. The IP protocol is familiar to network administrators therefore they have the knowledge needed to deploy IP Surveillance applications.

## IP Surveillance Examples

IP Surveillance solutions cover a wide range of possible applications, including security/safety, observation, and quality control monitoring. A typical example is remote building surveillance where the interior or exterior of a building may be monitored safely from a second secure building.



*IP Cameras can be monitored from anywhere on a Local or Wide Area Network*

Examples of and requirements for IP Surveillance solutions can be identified across a wide mix of vertical industries. All types of organizations, from government agencies and educational institutions to research labs and retailers, can benefit from IP Surveillance systems. Consider some of these possible uses:

**Government** – A large opportunity exists in the government sector. Homeland security, installation protection (military, energy, infrastructure), and transportation security measures require continuous, intelligent surveillance in large scales.

**Education** - Institutions need to protect both their assets and populations from crime, theft, and vandalism.

**Retail** - Businesses need to protect employees, customers, premises, and inventory from internal and external theft as well as from other criminal activity. Retailers want to provide a safe environment for their patrons while also protecting themselves.

**Financial** - Banks need surveillance at branch offices, teller windows, and ATMs.

**Transportation** - Agencies need to monitor rapid transit stations, railways, highways and airports.

A wide variety of businesses, research organizations and manufacturing facilities require monitoring for productivity measures, workplace safety, and the protection of intellectual property, logistics systems, and warehouse supply chain systems.

## Implementing IP Surveillance

Several considerations come into play when implementing an IP Surveillance system. The following points or options should be



*Captured at 2:00 pm*



*Captured at 10:00 pm in near total darkness with a D-Link DCS-6620 camera featuring ultra low light sensitivity.*

considered when implementing an IP Surveillance application.

### Network

A number of network variables dictate optimal network speeds, storage capacity and server performance. Ideally, the network switches and routers should provide high performance and offer a range of speeds from 100 Mbps to 10 Gbps. For high quality feeds or large numbers of cameras, consider 100 Mbps attached cameras with backbone network speeds of 1 Gigabit or higher. 10/100 Mbps networks can be used for applications where high-resolution video quality is not as critical. To avoid choppy, delayed data transfers traffic calculations should be made with respect to network performance. Estimates of throughput and peak demand requirements that will be placed on the network and how those demands may impact other network applications should be considered. Examine how much other traffic is moving around the network at specific times of the day. Consider switching infrastructures that implement Quality of Service (QoS) mechanisms to provide the desired level of video quality to your IP Surveillance application.

The 802.11g wireless standard offers less throughput, but it's perfectly fine for certain applications. With a dedicated network of wireless cameras, capturing high-resolution images without taxing the network is possible. Performance depends on the resolutions and frame rates selected for each camera. Security is also an issue with wireless networks. WPA or WEP authentication and encryption are recommended.

### Cameras

With PoE technology, camera placement can be made in the best locations, untethered and independent from AC power outlets. This enables a centralized power management strategy with UPS battery back-up availability for all cameras. The same UPS system that delivers back-up power to servers and data center equipment backs up the cameras – it can be managed from the same console.

Digital IP camera vendors sell a wide variety of indoor and outdoor cameras that perform well in all kinds of environments. Enclosures with thermal barriers on certain models protect the equipment from extreme weather. Others contain heater blowers for cold temperature climates and waterproof seals to protect from water damage.

Camera capabilities will vary based on the application. The cameras come in video only, audio/video and two-way audio with speaker attachments and built in microphone options, as well. Some are stationary while other offer remote controlled pan, tilt and zoom (both digital and optical). Another camera consideration is the lighting conditions. Some cameras will be much better than others

in low light conditions. Whereas most cameras would provide no image at all in low light conditions, those with low light sensitivity can still produce a picture.

### Monitoring and Recording Stations

Monitoring stations provide multi-camera monitoring via either a hardware or software interface. Multiple monitors or a single screen split into multiple frames can be configured with IP camera management software.

Recording and playback options for setting sensitivity levels, motion trigger thresholds, and screen area triggers are available. Surveillance applications should be analyzed to determine the requirements for these types of advanced functionality.

Management and monitoring software solutions sold with digital IP systems include automated snapshot, event, alarm and motion detection features. Check with your vendor to determine whether these applications are available and if they come at additional costs. D-Link provides the management and surveillance software free with its IP cameras, unlike some other vendors.

For more information about IP Surveillance products from D-Link please visit the D-Link website at:

<http://www.dlink.com/securicam>

Or contact us directly:

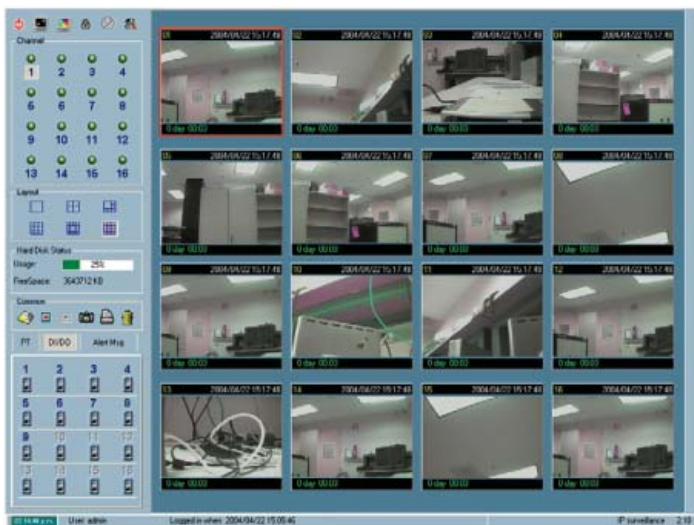
**ASK FOR THE SYSTEMS INTEGRATION TEAM!**

Send us an email to [SI@dlink.com](mailto:SI@dlink.com) [SI@dlink.com](mailto:SI@dlink.com)

call us at (888) DLINK-SI (888-354-6574)

Faxing: (866) 743-4664

We look forward to building networks with you!



*Monitor up to 16 cameras simultaneously*

Prices and specifications are subject to change without notice. D-Link, the D-Link logo, Securicam logo are trademarks or registered trademarks of D-Link Corporation. All other company or product names mentioned herein are trademarks or registered trademarks of their respective companies. Copyright © 2006 D-Link Corporation/D-Link Systems, Inc.