

WIRELESS SECURITY SURVEILLANCE:  
LEVERAGING IP NETWORKS FOR  
ENHANCED SAFETY AND  
SECURITY



Implementing an Affordable,  
Highly-functional Security System

www.proxim.com



## Contents

Wireless and IP-Surveillance: What's Next in Monitoring and Surveillance	1
What is Wireless IP-Surveillance?	2
Wireless IP-Surveillance Advantages	3
The Market Opportunity	6
Wireless IP-Surveillance In Action	7
Common Misconceptions Related to Wireless IP-Surveillance	10
Image Formats Used for IP-Surveillance	12
Negotiating the Trade-Offs: Image Quality, Frame Rate and Compression	15
The Companies Behind Wireless IP-Surveillance	16
Conclusion	18

## Wireless and IP-Surveillance: What's Next in Monitoring and Surveillance

More than ever, 9/11 and its aftermath have made security for organizations and enterprises worldwide a major priority. World events and organizational demands have hastened our search for better, more cost-effective security applications. In many instances, rapid deployment of security systems has become essential.

As critical as improved security has become, budgets to accomplish this goal are by no means unlimited. In fact, while many organizations have placed greater emphasis on security management, budgets have not always kept apace. When installing security and surveillance systems, equipment represents only one of the cost components. System installation represents a whole additional cost consideration. For installations that cover expansive territory and/or require that all data be transferred to a distant, central monitoring station, the feasibility of running wire is often limited. Fiber optics is always an alternative, but for many enterprises it can be cost-prohibitive. What then?

Against this backdrop, we are experiencing many fast-moving developments in security and related technology areas. For example, security applications are increasingly migrating from analog to digital technology; meanwhile, the IT and security markets are rapidly converging. These two developments have led to increased interest and viability for IP network-based solutions and use of the Internet. All told, these developments have fundamentally shaken up the security and IT markets in the last year or two, creating new markets, expanding markets, and unveiling tremendous opportunities for innovating, selling, and installing new solutions.

Whether it's establishing video monitoring for a highly visible bridge or creating an affordable surveillance system for your company's far-flung parking lots, a fast-emerging solution is the integration of the established IP-Surveillance technology with wireless networking technology. Some readers are probably asking, "IP and networks?" "Wireless?" "How do they fit together, and how reliable and effective are such solutions?"

In this white paper, we'll explore these and several other questions to clearly define what Wireless IP-Surveillance is, how it functions, where it is being used, and why it is a powerful monitoring and surveillance solution whose time has come. We'll also introduce and debunk several myths, which have given end users pause in implementing such technology.

Wireless IP-Surveillance is a surprisingly easy technology to understand. It is highly affordable and easily deployed. For any enterprise or organization that has been challenged by outdoor conditions, distance, lack of network connectivity, or simple fear of “new” technology when implementing a monitoring and surveillance system—Wireless IP-Surveillance is in your future.

## What is Wireless IP-Surveillance?

Wireless IP-Surveillance takes two proven technologies—outdoor wireless transmission and networked video surveillance—and combines them to create a powerful solution that overcomes many of the challenges that up to now prevented end users from installing surveillance and monitoring systems: distance, lack of network infrastructure, inclement conditions, price, and others. Wireless IP-Surveillance represents an innovative breakthrough, but what is it exactly?

IP is an abbreviation for Internet Protocol, the most common protocol for communication over computer networks and the Internet. An IP-Surveillance application creates digitized video streams that are transferred via a computer network, enabling remote monitoring as far away as the network reaches as well as viewing and monitoring from any remote location over the Internet.

Because of its scalability, among other advantages, IP-Surveillance is an established, attractive technology not only for enhancing or revitalizing existing surveillance and remote monitoring applications, but for a vast number of new applications as well. And when we add the power of wireless transmission to IP-Surveillance, we create an even more robust, flexible solution: an Ethernet cable (network connection) that can easily connect network cameras to a wireless point-to-multipoint connectivity solution, instantly creating a wireless WAN capable of transmitting high-resolution video back to a base station in real time. The combination of IP-Surveillance with wireless technology creates a security application that goes beyond anything currently available and offers these highly compelling features:

- Easy to deploy
- High degree of functionality
- Cost-effective in installation and operation
- Completely scalable

For most, this may seem a bit too good to be true. Below, we'll examine these features and the advantages of Wireless IP-Surveillance more closely.

## Wireless IP-Surveillance Advantages

### The Wireless Advantage

When it comes to providing security protection outdoors, organizations are often faced with major cost and installation nightmares. For a growing number of the most security-sensitive organizations, fixed wireless networks offer reliable, affordable surveillance networks that can secure the toughest outdoor environments. There are a number of reasons why more organizations are choosing wireless for their security networks:

- **Fast, easy to deploy.** Depending on the outdoor location, fiber is not always available. Wireless, on the other hand, can be deployed virtually anywhere, including bodies of water, rugged terrain, and remote locations. Wireless networks install in hours, eliminating long waiting periods and right-of-way issues associated with trenching for fiber.
- **Affordable.** Fiber often costs significantly more to deploy than a wireless system. Just a few miles of trenching can cost hundreds of thousands of dollars.
- **Flexible.** Wireless solutions provide unparalleled flexibility. Because the security network is wireless, cameras are not permanently fixed in one location. If necessary, cameras and subscriber units can be moved to a new location with minimal hassle and can usually be reconnected within minutes.
- **High capacity.** Wireless networks are available in a wide range of bandwidth capacities from 11 to 860 Mbps. The systems ensure the transmission of high-resolution video in real-time that is required of surveillance systems.
- **Reliable.** High-end wireless systems ensure up to 99.999% carrier-class reliability, enabling virtually non-stop security.
- **Tiered wireless solutions.** A wide range of solutions means almost any organization can consider implementing a security network for a variety of applications. Carrier-class solutions are available for tough all weather, large scale deployments, while more economical solutions are ideal for smaller, more budget-conscious deployments.
- **Outdoor design.** Outdoor wireless networks are sometimes confused with wireless LAN technology that is not appropriate for outdoor use. Based on a special protocol (Proxim calls it WORP) that enables system scalability and the management required for outdoor deployments, outdoor wireless networks (or “wireless WANs”) are versatile and powerful when used in security and surveillance applications. It’s important end users distinguish between indoor technology and those technologies designed for outdoor system demands.

## Advanced Network-Ready Camera Technology

IP-Surveillance, with network camera technology at its core, is a major advance over analog CCTV systems. The fast-paced growth in the network video market has been fueled by the highly impressive and comprehensive benefits an IP-Surveillance system offers:

- **Utilization of a more cost-efficient infrastructure.** Most facilities are already wired with twisted pair infrastructure, so no additional wiring—an expensive part of the CCTV install—is required. In cases where there is no infrastructure, installation of twisted pair is still a fraction of the cost of coax wiring. In addition, wireless networking can be used where cabling is non-existent, impractical or too expensive.
- **Remote accessibility cuts costs.** Any video stream, live or recorded, can be accessed from any location in the world over wired or wireless networks. Improved access over an intranet (e.g. LAN) or the Internet provides quicker and more immediate access to images, while substantially reducing travel costs and time to and from monitored site locations. Images can also be automatically stored at off-site locations for convenience or to enhance security.
- **Scalability.** IP-Surveillance scales from one to thousands of cameras in increments of a single camera based on the same networking principles of operation. There are no 16-channel jumps like we see in the DVR world. Increase frame rate and storage by adding hard drives and application servers to the network. Any frame rate for any camera at any time is available—no limitations.
- **Wide application.** While this white paper mainly focuses on connecting network cameras via a wireless network, there are a whole host of other powerful applications. For example, police cars with wireless access can view any network camera in a facility under observation.
- **Network convergence.** Only one type of network (IP) manages the enterprise for data, video, voice, etc.—making management more effective and cost efficient.
- **Lower system cost.** In many installations, the IP-Surveillance system has proven to be a lower cost alternative. Open and standard network, server and storage equipment enables cost-effective choices versus the “black box,” single-vendor approach of standard digital video recorders (DVR). And that’s just looking at the hardware. Add in lower installation costs and all the other benefits, and the end user can save a substantial amount of money.
- **Increased reliability.** IP-based data transport enables off-site storage and the ability to use redundant infrastructure, server and storage architecture. Management software provides real-time system health status and information on preventive measures to keep the system operating at peak performance.

- **Open and interoperable.** Unlike the DVR “black box,” closed solution approach, IP-Surveillance is based on open standards allowing use of products from different manufacturers, such as switches, routers, servers and application software. Thus, substantially lowering cost and increasing performance choices.

## Wireless IP-Surveillance: An Easy, Affordable Security Solution

Previously, outdoor wireless security and surveillance deployments were considered to be an option only for customers where budget was no object. In fact, there are premium wireless solutions that represent a significant investment—but the true beauty of Wireless IP-Surveillance is a flexibility and scalability that allows end users to create a system to fit most any budget requirement. With wireless technology and a network-ready camera, it is quick and easy to set up a simple security network. Whether you’re concerned with providing security to students on a university campus or safeguarding a national waterway, the challenge is the same: how to connect surveillance cameras in locations where running wire is either cost-prohibitive or impossible.

Wireless Ethernet systems provide a simple, elegant solution. Modern security and surveillance video cameras can convert images into Internet protocol (IP) packets that can be easily transmitted using wireless point-to-point and multipoint systems. Cameras at multiple locations are simply connected to wireless bridges (Subscriber Units), which send the data back to a wireless Base Station Unit located at an organization’s security command and control center. If needed, high-performance point-to-point solutions can be used to connect to a remote site under surveillance up to 40 miles away from the command center. The high-resolution video collected from all locations can then be downloaded to a large viewing screen at the command and control center.

To summarize, IP-Surveillance, combined with versatile, affordable wireless transmission capabilities offers a host of practical advantages for every end user regardless of size, application, or budget:

- For outdoor applications, there’s no disruptive, time-consuming digging and no expensive cabling
- Fast, easy deployment
- No analog to digital, back to analog conversion—this is a totally digital system
- Put cameras virtually anywhere and move them easily when required
- Add or subtract cameras with ease
- A wide array of hardware combinations coupled with system flexibility and scalability make it a solution for any enterprise or organization

In the expanding arena of IP networks, cameras, coax and fiber, and all the other hardware and software choices, it's sometimes easy to get lost in all the complexity. Wireless IP-Surveillance cuts through this clutter to reveal two simple pieces that fit together—network cameras and wireless transmission—to enable monitoring and surveillance at unprecedented levels of performance and affordability.

## The Market Opportunity

According to industry analyst, J.P. Freeman and Co., Inc. there are more than 20 million analog cameras installed in the U.S. alone. Of this 20 million, 1.5 million analog cameras were sold in 2002. Despite these rather impressive numbers for analog cameras, network cameras have emerged as the fastest growing product category and are forecast to comprise more than half of the security camera market by 2007, with revenues of \$500 million in the United States alone.

Whether it's analog cameras, network cameras, or a combination of the two, Wireless IP-Surveillance is proving to be attractive in a vast array of wide-ranging applications. In numerous applications this revolutionary technology is replacing traditional systems to reduce costs. While in other applications it is being used for the first time to create and stimulate new, exciting markets. Wireless security and surveillance solutions are ideal for many standard markets as well as the critical and fast-growing Homeland Security markets:

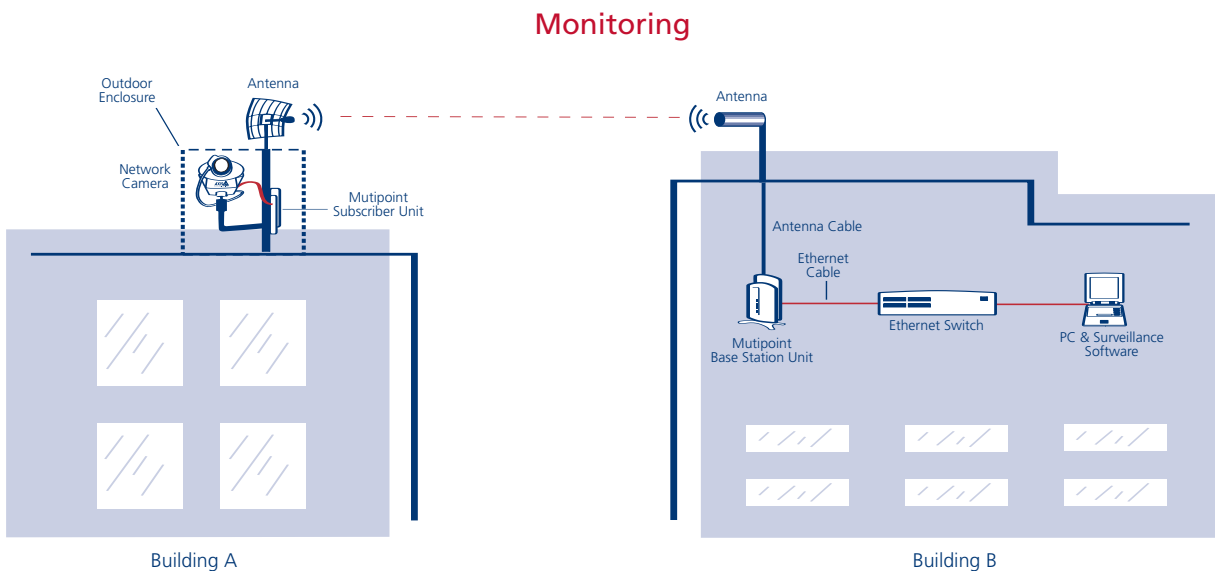
- **Enterprises.** Perimeter security for buildings; monitoring warehouse loading docks
- **Shopping Malls.** Customer security in parking lots
- **Banks/Financial Institutions.** Increasing security at ATM/bank machines
- **Municipalities.** Monitoring traffic intersections; securing city parks and municipal buildings
- **University Campuses.** Monitoring walkways for student protection
- **K-12 Schools.** Acting as virtual hall monitors or parking lot attendants; protecting students from intruders
- **Government.** Anti-terrorist surveillance systems for national security
- **Transportation.** Securing dams, bridges, highways and tunnels
- **Military.** Security in and around military installations
- **Law Enforcement.** Reducing crime and violence in troubled areas

It's clear to see that IP-Surveillance and wireless transmission technology combined in a single, powerful security system can serve practically any market challenge at present—from retail and banks, all the way to the most sophisticated and challenging homeland security installations.

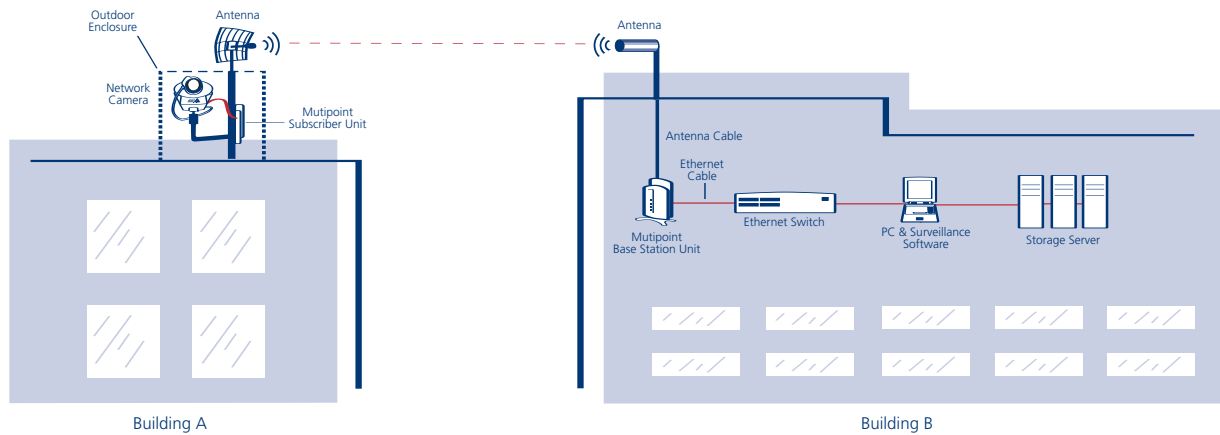
## Wireless IP-Surveillance in Action

Wireless IP-Surveillance can be broken down into two functions—monitoring and surveillance. The simpler of the two, monitoring, is implemented when the end user wants to view action in areas covered by the cameras, but no storage of data is required. Examples of this type of monitoring include verifying identity for door entrance approval.

The surveillance function is utilized when post-event investigation or other requirements demand storage of video data. The diagrams below illustrate configuration examples for both of these applications.



## Surveillance



Following is an examination of the core components of these systems to provide a better understanding of how a Wireless IP-Surveillance system functions and the many end user benefits it delivers.

### Network Camera

Network camera technology makes it possible to have a camera at one location and view live video at another location over the network/Internet. If a building is equipped with an IP network, then the necessary infrastructure already exists to add network cameras. A network camera performs many of the same functions as a standard analog CCTV camera, but it does so with greater functionality at a substantial cost saving. Because network cameras plug directly into the existing network via an Ethernet port, companies can save thousands of dollars by avoiding wiring their facilities with coaxial cabling as required for analog cameras.

When computers are already in place, no additional equipment is needed to view network camera output. The output can be viewed in its simplest form in a Web browser at the computer monitor and in more complex security solutions with the aid of dedicated software. In cases where analog cameras are already installed, video servers can be employed to digitize the analog signal, thus incorporating such a camera into the high-functioning Wireless IP-Surveillance system and making those images available in any location required.

A modern network camera will typically include a lens, optical filter, image sensor, image digitizer, image compressor and web server with network and phone modem interfaces. More advanced network cameras can also include many other attractive functions such as, motion detection, alarm inputs/outputs and email support.

## Wireless Networking Technology

Wireless networks offer higher capacities at significantly lower costs than wired data networks. Reliable and easy to deploy, they primarily come in two varieties: point-to-multipoint and point-to-point systems. For security and surveillance applications, point-to-multipoint systems are the most relevant, but point-to-point can also be used for longer distances and higher bandwidth requirements.

### Point-to-multipoint Wireless Systems

Using IP packet radio transmitters, standard Ethernet interfaces, and an easy-to-deploy design, these systems enable high-speed network connections to multiple Ethernet switches, routers, or PCs from a single location. The system consists of multiple wireless bridges, called Subscriber Units (SU), that communicate with a wireless Base Station Unit (BSU). Network cameras can be connected to a SU, which can be conveniently located wherever necessary. The Subscriber Units transmit the digital data back to a centrally located BSU. Transmission capacities vary from 11 Mbps to 60 Mbps and transmission distances can be from three to as far away as 12 miles.

### Point-to-point Wireless Ethernet Bridges

While point-to-multipoint systems provide connectivity from one location to multiple locations, point-to-point bridges connect two locations. These systems offer higher capacities and greater distances than the point-to-multipoint systems. When used for security and surveillance, they are ideal for backhauling video data from the local central site where a Base Station is located to a central command and control center that's located farther away. They are also ideal for connecting to a remote site under surveillance up to 40 miles away from the center. Point-to-point systems are available in capacities ranging from 11 to 430 Mbps data rate.

## PC Server and Software

Although the Motion JPEG images generated by an IP-Surveillance system are native to most standard Web browsers, the true value of IP-Surveillance products is best realized when utilizing professional monitoring and recording software, which turns a PC server into a network video recorder (NVR).

While IP-Surveillance video can be viewed directly from a normal web browser without the need for dedicated software, it is strongly recommended to use a software application in combination with the cameras. This software provides the user with more flexible viewing options and, more importantly, the ability to store and manage the video, with an NVR. Dedicated software is installed onto a PC for monitoring, storing, replaying and conveniently managing video images, to create a synergy

that offers a level of system functionality vastly superior to any contemporary analog system on the market today. The software can be a stand-alone solution for a single PC or a more advanced client/server-based application providing support for multiple simultaneous users. Any system from one to thousands of cameras can be deployed, and scaled in steps of one.

In some cases, the end user can select software to implement support for multiple systems such as video and access control. Selecting a suitable software package to match the application and system goals is one of the keys to designing an effective and successful system.

## Common Misconceptions Related to Wireless IP-Surveillance

We've seen that Wireless IP-Surveillance technology offers an impressive array of end user benefits in addition to a very attractive total cost of ownership (TCO). However, as with any relatively new technology, there may be a number of misconceptions regarding technology performance that may give potential users pause in implementing Wireless IP-Surveillance. Below are important clarifications addressed to several common misperceptions regarding this technology.

### Security

**IP-Surveillance:** Although primarily used as a domain for public information, the Internet can also be used to transfer all types of sensitive information—provided the correct security measures, such as firewalls and password protection are implemented. With an increasing number of banks and financial institutions regularly using the Internet as a medium for global money transactions, it has emerged as a proven medium for other secure applications like surveillance and security monitoring. In combination with an organization's firewall, Axis' IP-Surveillance technology allows product security to be tightly maintained using available internal password-protected security settings. In stark contrast to this new digital technology, analog surveillance systems have no encryption of information whatsoever, making it extremely easy for anyone to tap into the cables and illicitly view "secure" video transmissions.

**Wireless:** Security can be an area of concern for those considering the use of fixed wireless devices to transmit data. Because fixed wireless bridges transmit signals into the "air," there is a perception that anyone could possibly "steal" the user's data. Top of the line wireless providers will incorporate a variety of counter-measures to ensure rigorous security of data. These include: Password protection—protection at two levels, one for the monitor and one to provide monitor/modify privileges. Transmission protection/ encryption—unique transmission signals that require the same maker's equipment at both ends for decoding. In addition, "line of site" transmission, as opposed to omni-directional transmission ensures that only antennas firmly in the radio frequency target area can receive the data. Data coding—potential intruders would have to obtain a unique transmission code set by the administrator to decode the data. Most potential data thieves don't have the several million years needed to run

through all the codes so as to get to the data. Should someone try to capture the data, but not provide the proper codes at regular intervals, transmission is immediately terminated. If further proof of the secure nature of wireless transmission is required, look to the many high-level military installations that use it—they cannot afford to use a risky technology.

## Bandwidth

**IP-Surveillance:** Today, most computer networks are 100 Mbps Ethernet networks. In practice this means that the maximum usable bandwidth is around 50 Mbps. Consequently, one network camera, transmitting the highest resolution image at the maximum frame rate (30 frames per second) can potentially consume 5 Mbps. This means running an IP-Surveillance system on an office network simultaneously with other data applications could prove problematic. However, these potential difficulties can be easily overcome by employing the following techniques:

- **Switched networks:** By using network switching—a common networking technique today—the same physical computer and IP-Surveillance network can be separated into two autonomous networks. Even though these networks remain physically connected, the network switch logically divides them into two virtual and independent networks.
- **Faster networks:** As the price of hubs, switches, and routers continues to fall, the affordability of Gigabyte networks increases. Reducing the effect of limited bandwidth, the trend towards faster networks increases the potential value of remote monitoring over networks.
- **Event driven frame rate:** 30 frames per seconds (fps) on all cameras at all times is more than what is required for most applications. With the configuration capabilities and built-in intelligence of the network camera/video server, frame rates under normal conditions can be set lower, e.g. 1-3 fps, to dramatically decrease bandwidth consumption. In the event of an alarm, if motion detection is triggered, the recording frame rate speed can be automatically increased to a higher frame level.

**Wireless:** Bandwidth is a natural concern when it comes to wireless transmission. Proxim's outdoor wireless networking solutions offer capacities ranging from 11 Mbps to 860 Mbps, by using different radio technologies. Basically, there are two major radio technologies employed for transmission—Frequency Division Duplex (FDD) and Time Division Duplex (TDD). TDD is typically used in multipoint environments, while FDD technology is used for high-speed point-to-point connectivity. By employing the right technology, end users can ensure sufficient bandwidth over required distances to support the number of cameras needed in any given deployment.

## Interference

**Wireless:** As ISPs and enterprises increase deployments of wireless connections, the potential for interference among systems operating at or near the same frequency in an unlicensed band grows. Choosing the right wireless solution with the frequency and design features best suited for a particular application will ensure the end-user remains protected from interference. A 2.4 GHz wireless system that has been designed for outdoor use, such as Proxim's Tsunami MP.11, will mitigate interference and ensure enhanced communication. If 5.8 GHz is required, Proxim's Tsunami Multipoint offers the right solution. Tsunami Multipoint has been designed to counteract interference using a variety of measures including the use of directional antennas and multiple frequency channel plans. To further safeguard against interference, Proxim has introduced Tsunami Multipoint A.I.R. This solution combines Tsunami Multipoint's integrated defensive countermeasures with Proxim's patented Active Interference Rejection (A.I.R.) technology. The A.I.R. technology safeguards wireless access networks against interference in real time, enabling stable, consistent service deployment.

## Reliability

**Wireless:** The overall performance or reliability of a communications system is predicted and verified in terms of its "availability." Availability is defined as the total amount of time, within a one-year period, the system transports (in both directions) voice, data or video information, with normal path interference. The most available systems are designed for 99.999 percent uptime. This translates into just over five minutes of downtime during a one-year period. Proxim offers a wide range of reliable solutions to meet an equally wide range of budgets. Tsunami point-to-point systems offer 99.999% carrier-class reliability, while Tsunami Multipoint systems offer 99.995% reliability. With this high level of availability, Tsunami ensures the continuous transmission of real-time images without the dropped packets that could interrupt surveillance. In addition, all Tsunami systems are designed to perform in outdoor environments: Tsunami Multipoint is ideal for tough all-weather environments, while Tsunami MP.11 does require outdoor protective enclosures.

## Image Formats Used for IP-Surveillance

Digital images and video are often compressed in order to save space on hard drives and make transmission faster. Out of the many different types of digital camera and video products currently available on the market, all will employ one or more of the following compression techniques:

### **Motion JPEG**

The imaging standard employed by Axis video products, this standard generally refers to JPEG images shown at a high frame rate (up to 30 frames per second). It gives high-quality video, but the comparatively large file sizes of each individual image do put demands on the transmission bandwidth.

<b>Wavelet</b>	Optimized for images containing low amounts of data. The relatively inferior image quality is offset by the low bandwidth demands on the transmission medium. There is currently no formal standard for Wavelet available.
<b>JPEG 2000</b>	Based on Wavelet technology, this relatively new standard is optimized for images containing low amounts of data. The relatively inferior image quality is offset by the low bandwidth demands on the transmission medium.
<b>H-compression: H.261, H.263, H.321, &amp; H.324</b>	Offering a high frame rate, low image quality, these compression techniques are popular for video conferencing applications. The low image quality is particularly acute when the image contains moving objects.
<b>MPEG-1</b>	The video standard that typically delivers 30/25 (NTSC/PAL) frames per second. With many variations, this format provides low-resolution images but places low demand on the transmission medium.
<b>MPEG-2</b>	Offers higher resolution images and the same frame rates as MPEG-1. Only modern computers can decode this format, as it generally demands high computing capacity.
<b>MPEG-4</b>	A video standard that offers high performance video with good resolution and moderate demand on transmission bandwidth. Therefore suitable for low bandwidth applications, for example mobile phones.

Now that we've completed an overview of the many compression methodologies that are being used, what does this mean for implementing a Wireless IP-Surveillance system? What factors must the user and installer consider?

- How high a frame rate is needed?
- Are different frame rates needed during certain events or at specific times?
- What image quality is needed?
- What image resolution is needed?
- What is the available bandwidth for network transmission?

The following table provides a comparison of some of the most common compression methods:

	MJPEG	MPEG-1	MPEG-2	H.263
Target bit rate	N/A*	About 1.5 Mbit/sec	2 – 15 Mbit/sec	64, 128, 192 kbit/sec up to approx 2 Mbit/sec
Supported frame rates (fps=frames per second)	Camera / Video Server dependent	25/30 fps	25/30 fps	Any, up to 30 fps
Resolution	Any	320 x 288 320 x 240	320 x 288 320 x 240 720 x 576	352 x 288
Image quality	Low to Very good	Good	Very good	Low
Target application	Still images	Digital video on CD (VCD)	DVD, HDTV	Tele-conference
Basic algorithm	Digital Cosine Transform (DCT)	DCT with motion vectors	DCT with motion vectors	DCT with motion vectors
Standard	ISO/IEC 10918	ISO/IEC 11172	ISO/IEC 13818	ITU-T H.263

\* Since the JPEG and JPEG 2000 standards are primarily for still image compression techniques, they do not have set limits on frame rate, image resolution, image quality or target bit rates. MJPEG bit rate is dependent on available bandwidth and transfer capacity of the camera or video server.

The table demonstrates that the H.261/263 method requires less bandwidth capacity, but this is achieved at the expense of a lower image quality. The MPEG standards, on the other hand, are focused on video at different resolutions and at good or very good image quality.

## Negotiating the Trade-offs: Image Quality, Frame Rate and Compression

Although consistent image quality is important to the vast majority of security application users, it does come at a price—high bandwidth demands on the network and related costs. High bandwidth usage is prohibitive in many applications and perceived as a distinct disadvantage by users who want high quality, full-motion video and audio combined, but at comparatively low bandwidth consumption. Is there a way to minimize the apparent required trade-off so as to achieve a sufficiently high frame rate at good to excellent image quality, but without overloading the network?

The most appropriate compression technique depends on the trade-off the user is willing to accept between recording frame rate, video image quality and bandwidth consumption. Wireless networks come in a range of capacities. The network, as well as the compression chosen by the user, will dictate the quality of image transmitted. The frame rate a wireless network can support also depends on the type of compression chosen.

Because our chosen application is professional monitoring and surveillance, it is important to select a compression methodology that places a high priority on high image quality. It is also important to make sure to use a standard so that any video can be easily viewed from any location, if necessary. These priorities and requirements leave us with two formats: JPEG (or motion JPEG) and MPEG.

### JPEG

JPEG's advantages include full frame rate; very high image quality; a format supported in all web browsers; a highly scalable frame rate from 1 image per year to 30 frames per second; and a very low latency (discussed below).

JPEG's major disadvantage is that it consumes a high amount of bandwidth at the high frame rates often required.

### MPEG

MPEG has the distinct advantage of a lower bandwidth requirement at high frame rates (above 10 fps). However MPEG does have the disadvantages of a complex compression method, higher latency, and the consumption of a lot of PC power to decompress images. In addition, MPEG uses differential compression, where only one out of 15 frames is a full image. In certain applications where all frames are required to be full images, MPEG cannot be used.

For a video surveillance system based on MPEG-compressed video, viewing the MPEG stream requires that users have a computer capacity and system memory at least four times higher than that required for MJPEG images. For users who want to view video real-time, latency (the amount of time required for compression) becomes an important factor. Latency increases

with the complexity of the compression technique, as well as the complexity of the installed system. Latency can be upwards to one second. Applications such as live monitoring, including control of PTZ (pan-tilt-zoom) cameras, will require as little latency as possible; hence, MPEG is not a good choice.

When transmitting a complete image every time, as with MJPEG, image quality is never compromised. To achieve this level of image quality, while keeping bandwidth (storage) demands manageable, the frame rate needs to be reduced. This method is most suitable for applications that stress the importance of details—for example, monitoring product quality on an assembly line. When a reference image and continuous updates are used, as with MPEG, a compromise is made between image quality and a higher frame rate. This method particularly suits applications where we want to see an ongoing flow of events at a site, at a relatively high frame rate, but we need not view the minute details of the observed events.

For Wireless IP-Surveillance, the choice of compression method is between JPEG and MPEG. As we've seen, both have advantages and disadvantages and both require a trade-off between image quality and frame rate. The appropriate compression depends on each end user's application and needs and the manner in which they choose to negotiate the image quality vs. frame rate trade-off.

## **The Companies Behind Wireless IP-Surveillance**

### **Axis Communications, Inc.**

With 90% of today's networks now IP-enabled, Axis IP-Surveillance technology is founded on a well-proven, yet future-proof, communications technology.

While several manufacturers have identified the market opportunity for IP-Surveillance, market pioneer Axis remains the clear leader according to recent market studies conducted by Frost and Sullivan. Axis Communications has more than 16 years experience in making network products that work in multiple environments using multiple protocols. Axis' first IP-based product was released in 1992 and the first IP-Surveillance product (the AXIS NetEye 200) started to ship in 1996.

Axis' product portfolio includes market-leading network cameras and video servers. Some surveillance software and accessories are also available from Axis. Depending on the kind of application being developed, there are several software applications from other companies that can be integrated with the Axis products. Axis has signed these companies into the Axis ADP (Application Developer Partner) program: a technology partner program that aims to promote the availability of complementary application software for Axis video products, and ensure a 100% compatibility with the new product releases.

## Axis IP-Surveillance Products

PRODUCT	AXIS 2120 NETWORK CAMERA	AXIS 2420 NETWORK CAMERA	AXIS 2130R PTZ NETWORK CAMERA
Frames per second	up to 30	up to 30	up to 30
Motion Detection	yes	yes	no
Maximum video resolution	704 x 480	704 x 480	704 x 480
Outdoor Enclosure Required	Yes	Yes	Yes
Additional Features		Analog out	
Security applications	Government, Education, Retail, Transportation, Industry, Finance/Banking		
Market Differentiators	<ul style="list-style-type: none"> <li>• up to 30 frames/second</li> <li>• built-in motion detection</li> </ul>	<ul style="list-style-type: none"> <li>• simultaneous analog and digital video output</li> </ul>	<ul style="list-style-type: none"> <li>• customization utilizing API's</li> </ul>
Positioning within Family	High-end indoor & outdoor solutions	High end indoor & outdoor solutions, compatible with existing CCTV/analog networks	Ultimate functionality with pan, tilt, and zoom capabilities

## Proxim Corporation

Proxim Corporation is a leading manufacturer of high-performance wireless local area networking (WLAN) and wireless wide area networking (WWAN) products. The company is a leader in the fast-growing markets for 802.11b, 802.11a, and license-exempt fixed wireless networking systems. Proxim's systems securely connect networks within buildings as well as between locations up to 40 miles apart, providing enterprises, service providers, mobile operators and venue owners, with unprecedented networking capacity and mobility. Proxim's Tsunami high-performance outdoor wireless networking products are currently in use by military bases, transportation systems and office buildings for both military-grade and enterprise-class security and surveillance applications.

## Proxim Outdoor Wireless Networking Products

PRODUCT LINE	TSUNAMI MULTIPOINT A.I.R.		TSUNAMI MULTIPOINT				TSUNAMI MP.11		
Product	BSU* 20 Mbps	BSU 60 Mbps	BSU 20 Mbps	BSU 60 Mbps	SU* 20 Mbps	SU 60 Mbps	BSU	SU	Residential SU
Capacity	20 Mbps	60 Mbps	20 Mbps	60 Mbps	20 Mbps	60 Mbps	11 Mbps	11 Mbps	11 Mbps
Maximum Distance	6 miles	3 miles	6 miles	3 miles	6 miles	3 miles	5 miles	5 miles	5 miles
Frequencies	5.8 GHz	5.8 GHz	5.8 GHz	5.8 GHz	5.8 GHz	5.8 GHz	2.4 GHz	2.4 GHz	2.4 GHz
Outdoor Enclosure Required	No	No	No	No	No	No	Yes	Yes	Yes
Requires External Antenna	No	No	No	No	No	No	Yes	Yes	Yes
Number of subscribers supported	1023	1023	1023	1023	NA	NA	100	NA	NA
Security applications	Tough all-weather environments and large-scale deployments in urban areas where interference may be present		Tough all-weather environments and large-scale deployments				Smaller, more budget-conscious deployments		
Market Differentiators	<ul style="list-style-type: none"> <li>• patented Active Interference Rejection technology results in exceptional throughput, reliability and lower support costs</li> </ul>		<ul style="list-style-type: none"> <li>• industry's fastest unlicensed multipoint solution</li> <li>• audible alignment, self-installation and "over the air" upgrades reduce deployment and maintenance costs</li> </ul>				<ul style="list-style-type: none"> <li>• new Wireless Outdoor Router Protocol results in superior performance and scalability</li> <li>• self installation and remote monitoring capabilities</li> <li>• most economical point-to-multipoint solution on the market</li> </ul>		
Positioning within Family	For carrier-class security in RF congested markets		For carrier-class security in bandwidth-intensive environments				For economical outdoor security		

\* BSU is an abbreviation for Base Station Unit and SU is an abbreviation for Subscriber Unit

## Conclusion

IP-Surveillance is, indeed, the security and surveillance solution for the future. But, as powerful as this technology is, there are markets and applications where distance and an absence of network infrastructure can hamper IP-Surveillance implementation. For this reason, combining Proxim's leading wireless technology with the Axis IP-Surveillance solution has resulted in a combination that few, if any, providers can match in terms of performance, cost, and availability.

IP-Surveillance is quickly taking over the high-end range of the security monitoring and surveillance market, and has fast begun to penetrate low and mid-range market segments as awareness grows, costs come down, and users implement more sophisticated cost-benefit analyses. Bundling IP-Surveillance with Proxim wireless technology will further hasten and deepen this market penetration and ensure that IP-Surveillance remains the leading security application.

In this white paper, we've shown that Wireless IP-Surveillance is a relatively easy technology to understand. It represents an enormous market opportunity because of its cost and performance advantages. Wireless IP-Surveillance is a fast, easy, and reliable security application that can be deployed in any organization within hours and fits a wide array of budgets and organizational needs.

Wireless and IP-Surveillance: it's what's next in monitoring and surveillance



Tel: 800.229.1630  
Fax: 408.731.2700  
[www.proxim.com](http://www.proxim.com)



Tel: 800-444-AXIS (2947)  
Fax: 978-614-2100  
[www.axis.com](http://www.axis.com)