Wireless Mesh Networks for Distributed Video Surveillance

Today’s IP networked video surveillance systems are capable of providing a far greater resolution, flexibility, reliability and increased cost savings in comparison to conventional analog video solutions. In the past, wireless IP video surveillance has been viewed as an “adhoc” solution with limited reliability. Wireless mesh networks are changing that perception as more customers implement video surveillance over Strix wireless mesh networks. Robust high performance, low latency and multi-hop scalability enable range and coverage that wasn’t possible only a few years ago.

The video surveillance market is a billion dollar international industry. According to a special 2007 report by iSuppli Corporation, the equipment market for surveillance cameras, embedded Digital Video Recorders (DVRs), and IP video servers will grow to nearly $12B by 2011 and Frost and Sullivan state in their recent 2007 report, "Network-based systems are expected to completely replace analog and hybrid (analog video capture devices with digital storage devices) systems by 2015-2016." At the same time IMS Research indicates that by 2009 "analog recording systems are forecast to account for less than 5% of the market."

This growth in the IP surveillance market is occurring as a result of the expansion of existing network-based deployments and the architecting of new completely networked digital surveillance systems both in the public and private sector. The IP segments of the surveillance equipment market is experiencing the fastest growth, as cameras integrate IP and digital video recorders (DVRs) transition to networked video recorders (NVRs). Additionally, growth in IP video surveillance will also broaden the surveillance market, with new applications and new market segments.

The most significant enabler for the video surveillance market is the deployment of wireless mesh networks. Strix wireless mesh networks are the catalyst for large-scale distributed video surveillance deployments by delivering the industry’s highest throughput, lowest latency, unmatched flexibility, scalability and resilience for IP video cameras, servers and video storage.
Strix wireless mesh networks are deployed worldwide where robust "wireless like wired" performance is a requirement and the delivering of mission critical video surveillance, the highest quality voice and data applications are essential. Strix Access/One® is the only wireless architecture qualified by independent testing and real-life worldwide installations where the result is the industry's highest throughput, lowest latency, the greatest range and coverage, unmatched scalability and carrier class resilience.

Old-school deployments utilize coax, expensive fiber multiplexers and distribution amplifiers coexist with encoders and even category 5/6 Ethernet-like, but proprietary, wiring. This method of directly cabling surveillance devices is changing rapidly. Eliminating any dependence on wires, removes a significant number of obstacles and the excessive costs associated with deploying video cameras where it was previously impractical or impossible. Cameras and video servers can now be placed virtually anywhere within range of the wireless mesh network infrastructure and is used to supplement existing analog CCTV systems. And an increasing number of organizations are finding the advantages of networked video so compelling, they are replacing their legacy analog CCTV infrastructure entirely.

The Distributed Video Surveillance Network

Strix Systems wireless mesh networks are making large-scale and strategic IP-based video surveillance possible. Whether used for government, municipal, public safety or enterprise security, video surveillance is a critical application which, until now, has been restricted to wires, cable, fiber and unreliable wireless solutions and expensive to deploy.

Distributed video surveillance provides the ability to view, share and ‘distribute’ video, statistical

---

Strix Systems, Inc., www.strixsystems.com, info@strixsystems.com 1.877.STRIXSYS
All trademarks, logos and service marks are the property of Strix Systems.
Copyright © 2000-2008 Strix Systems, Inc. All rights reserved.
and integrate information with other application and systems such as the access control and intrusion detection systems without the need for centralized servers and removes the risk of single point of failure. Strix Systems makes a fully distributed IP surveillance system possible for cameras, video servers, storage clusters, custom applications and remote viewing to be located in any location, even geographically.

Additionally, networked video surveillance integrated with other security applications such as alarm systems in geographically remote areas enables an increase in effectiveness of security operations personnel and cuts the expense of responding to false alarms. This unification helps to reduce the false alarm rates, which exceeds 90 percent in most organizations.

**Benefits of IP Surveillance Systems**

- Scalable installations that can scale with your requirements
- Integrate with other security systems at geographically separate locations.
- Optimization of video streams resulting in less storage space compared to previous solutions.
- Video streams distributed to multiple locations.
- Wider distribution and remote access anywhere, anytime.
- Easy viewing of live and multiple video images on multiple computer and handheld devices.
- Quick and simple searching from any location.
- Cheaper and faster installation with easy upgrades.
- Takes full advantage of wireless and other infrastructures.
- Interoperable with other network appliances.
- Can utilize existing IP infrastructure.
- Standard video compression techniques.
- Leverage emerging wireless transmission technologies.
- Save time, money and human resources.
- Improve security coverage and realize a fast return on your investment.
- Inherent cost advantage due to open systems components and architectures.

**Assessing the Components**

To make the most accurate assessment for the network, it's critical to consider the video compression algorithms, number of cameras, and location of video servers and where remote viewing will take place. Not to be confused with analog standards defined by NTSC and PAL, VGA standard defines resolution for IP-based video surveillance cameras. Video compression algorithms which determine resolution quality, image size, frame rate and image updating techniques used ultimately impacts the bandwidth requirement. This bandwidth can vary from a few hundred Kilobits per second to multiple Megabits per second transmitted in streams at frame rates up to 30 frames per second.

In order to reduce bandwidth consumption, built-in camera intelligence and bandwidth optimization features can reduce the size and speed of images transmitted over the network. Bandwidth and latency requirements for remote client viewing and PTZ (Pan/Tilt/Zoom) capabilities should be considered. While the latency ceiling and tolerance for each PTZ should be evaluated, the ceiling set for analog PTZ's combined with video encoders is set by pan/tilt/zoom control to <250ms (depending on the camera used). Additionally in this analog configuration, encoding/decoding process could add 150-
200ms. Remote viewing client applications typically consume a fraction of video cameras transmission bandwidth as monitoring optionally connects to the surveillance server; however it is possible for personnel to connect directly to the cameras. In this case, monitoring can consume equal bandwidth as cameras and each manufacturer’s remote viewing technology enables the user to select the number of cameras being viewed as well as the cameras themselves, camera groups, resolution, frame rate and PTZ control.

To adequately address the challenges of bandwidth requirements, a discussion on video compression, IP video cameras and the network video surveillance server components is required.

### Video Compression Methods

An ordinary, uncompressed analog video stream can consume as much as 165 Mbps of bandwidth while Megapixel IP video cameras can consume multiple Gigabits per second. Video compression techniques have been developed to reduce size of video images to conserve bandwidth.

Increasing the compression level causes degradation of the image which can manifest into visual inaccuracies, or digital artifacts. A balance needs to be drawn between reducing image size and keeping the image clear. Typically, the defaults used by IP video camera and video server manufacturers have achieved this balance, and standards have been established for manufactures to follow.

While there are many different types of compression—some of the more familiar being H.264, MPEG4 and MJPEG there are basically two types: frame-by-frame (still image encoding) and Temporal (motion encoding).

When considering video compression methods, MJPEG is the most widely deployed frame-by-frame compression technique which compresses each image in its entirety. This technique enables you to predictably determine bandwidth requirements, but by the same token it’s not bandwidth efficient, especially in cases with inconsequential events such as movement of tree leaves.

H.263, H.264 and MPEG4 techniques are gaining popularity and widely deployed where bandwidth is a premium commodity and lesser image quality is acceptable. To accomplish this, the “Temporal” method compresses the “key frame,” in its entirety, subsequent, but not all, frames with changes are compressed and transmitted. The advantage of this technique is that by sending only changes to the key frame, you can save 50-80% of the network bandwidth. The added performance benefits of Strix Access/One performance translates directly to increased network scalability.
IP Video Cameras

Today’s IP Video cameras not only improve on previous technologies and add a network interface, but take a tremendous leap forward employing new analog conversion technologies. The balance of image quality and bandwidth is of primary concern, but it’s important to consider these improvements. Over the last few years CMOS (Complementary Metal Oxide Semiconductor) technology has enabled low cost analog-digital conversion for IP transport of video. “Progressive scan” better depicts moving objects in contrast to Analog cameras, which at high resolution (4CIF), have significant problems with interlacing - causing moving objects to blur. Since analog video images are made up of lines, and each image is formed from two interlaced fields, when an image contains a lot of movement, it will become blurry because the object moves between the two interlaced fields.

Advancements in digital pixel image sampling, used in today’s IP video cameras, surpass previous analog CCD (charge-coupled device) technology. With digital pixel image sampling an entire image is captured at one time, providing crystal clear images even with a high degree of motion. The latest pixel image sampling methods now support low light and special lighting conditions, which was the only remaining benefit of CCD technology. With the integration of imbedded intelligent algorithms, such capabilities as built-in motion detection, automatic compression selection, bandwidth and network optimization controls and decision processes to determine when an operator should be informed. This new generation of cameras includes programmable APIs (application programming interfaces) and DSP (digital signal processors) accessed directly or through programming interfaces built-in to the NVR. This makes it possible to program, for example, pan-tilt-zoom (PTZ) cameras to identify an object, zoom in for a high-resolution picture and trigger an alarm, phone call and email to security personnel. Moreover, with the introduction of megapixel imaging technology, IP video cameras now surpasses the industry’s previous highest resolutions defined by NTSC/PAL. In comparison with today’s digital/analog cameras which in terms of megapixels equates to a maximum of 0.4 megapixels (640 x 408 VGA or 704 x 480 (NTSC 4CIF) or 704 x 576 (PAL 4CIF), megapixel cameras are capable of achieving variations of 1.0 to 5.0 megapixels and greater in the future.
New bandwidth optimizing capabilities such as “frame rate control” are built-in, in contrast to analog video where “all video is sent from the camera all the time”. Frame rate control in network video systems means that the IP video camera/video server only sends images at the specified frame rate – no unnecessary frames are transferred over the network. The IP video camera/video server or video management software can be configured to raise this frame rate if, for example, activity is detected. It is also possible to send video with different frame rates to different recipients – a benefit especially when using low bandwidth links to remote locations.

Another significant development is VariableMotion Detection (VMD). VMD is an integrated function of IP video cameras and NVR’s which offers substantial advantages over DVRs - the most significant being that the VMD is processed in the IP video camera or video server itself. This alleviates the workload for any recording devices in the system and makes “event-driven surveillance” possible. In that case, no video (or only video with low frame rate) is sent to the operator or recording system unless activity is detected in the scene. VMD data with information about the activity can also be included in the video stream to simplify activity searches in recorded material. VMD can also reside in the video management software, thus providing VMD functionality to IP video cameras that do not originally equipped with this feature.

Advantages of local VMD in the “endpoint” (IP video camera and video server compared with systems using central analyzing such as DVRs) include: conserving bandwidth, reducing CPU load on recording servers, saving storage space and cameras can interact with others systems using I/O Ports (for example triggering alarms).

It’s important to acknowledge those bandwidth features mentioned above, however, it would be a difficult task to estimate bandwidth requirements based on the dynamics of these features,
so the table to the right is provided as a guideline to make some general throughput calculations in relation to a selected resolution. Determining bandwidth is accomplished by simply calculating the size of each image and keeping the compression for all cameras the same. Once you have the image size, you multiply that by the images per second to get your bandwidth requirements.

**Network Video Recorders (NVRs)**

The Network Video Recorder is a major component of the distributed video surveillance systems and can be located anywhere on the network. It inherits the best capabilities from today's DVRs with the essential difference being that the NVRs is a completely digital systems with no analog components and designed specifically for IP transport of video from the ground-floor up. NVR’s enable users to access, view and control surveillance cameras from anywhere on the LAN, WAN, intranet or Internet.

An NVR is essentially software solutions, making the hardware like servers, storage, encoders and decoders and cameras choices for the end-user. NVRs can support traditional analog and IP video cameras from a variety of manufacturers, including advanced imaging mega-pixel cameras and many now offer advanced API’s for greater control and customized functionality.
The systems are fully-digital IP-based video surveillance systems that bring together a CCTV matrix of multiplexers, switches, control panels and a DVR with unlimited storage capacity into one unified system. As a software-based enterprise-level video, audio and data management system, it offers in a single graphical user interface (GUI), monitoring, recording and analysis functionality for providing timely, accurate information to the operator.

The NVR is the best choice for multi-site surveillance as it enables the distribution of the surveillance components while also enabling centralized control of unlimited remote installations and offline storage of recording — with full redundancy — to secure locations as needed. In a network video system, the NVR records and manages the video.

The NVR can be selected according to the performance needed. Performance is often specified as number of frames per second, total for the system. If 30 fps (frames per second) is needed for each camera, one server may only record 25 cameras. If 2 fps is sufficient, 300 cameras can be managed by one server. This means that the performance of the system is used efficiently and can be optimized.

For larger installations, an IP network video system is easy to scale. When higher recording frame rates or longer recording times are needed, more processing and/or memory capacity can be added to the server managing the video. Even more simply, another NVR can be added, located either at a central location, or at remote locations.

Now that IP video cameras perform the video encoding function, or analog cameras can be coupled with a separate IP encoder/decoder, the NVR can be located anywhere on the network - at an organization's headquarters, for example, or using servers in two data centers - to simplify management and increase availability. Physically separating the encoding device from the server has another advantage as well - the server no longer needs to devote compute cycles to managing video cards and compression.

NVRs offer both video stream management and video stream storage management. Not to be overlooked, storage management can be an important factor for users with high 24-hour “record everything” storage requirements. NVRs that can prune stored video based on motion or other criteria (i.e. first-in first-out) can further minimize regular maintenance tasks and potentially reduce the amount of storage needed to meet long-term retention requirements.

Today, organizations, institutions and agencies have resorted to maintaining a separate database for each remote DVR. However, when using NVRs, which be deployed anywhere on the network, it is possible to centralize the video collection into fewer distinct geographic database environments that can be replicated back to the organization's central safety and security operations center.
Partitioning of the surveillance systems functions also helps improve operational efficiency. An organization's IT group can be tasked with the responsibility of maintaining the video surveillance servers and storage, as well as protecting them along with other mission-critical servers. This ensures that edge devices are properly connected to the network and servers are properly maintained, and provides constant monitoring of these networked assets.

Moreover, the IT group can work with the appropriate security policies that are in place to provide appropriate access to restricted resources. This allows security personnel to focus on security issues, not maintenance of storage devices. As a result, it is possible to reduce not only redundant capital infrastructure investment by using the network for transport and access of the video, but also optimize operational roles and responsibilities.

NVR's due to their fully distributed capabilities are an exceptional match when coupled with a wireless mesh network and reduces the initial and ongoing equipment and operations costs.

**Delivering Multi-Radio Performance**

A critical factor for bandwidth calculations of IP video cameras, NVR and subsequent remote viewing locations, is throughput requirements at the intermediate wireless mesh nodes. These nodes commonly handle access and backhaul receive and transmit simultaneously. In large mesh networks, there may also be multiple “hops” between the source (the IP camera) and the ultimate destination (the NVR).

To ensure the highest performance for the network it’s important to first consider that a multi-radio broadband wireless architecture is the only solution that can support the high throughput and low latency required for IP video surveillance. A single radio solution (or dual-radio solutions with single radio backhauls) can not scale. Multi-radio systems (specifically with dual-radio backhauls) make it possible to focus on the additional benefits of optimal path selection, quality of service, client security, and high-speed mobile roaming.

But let’s take one step back as there are some critical factors that should be considered for a video surveillance over broadband wireless networks. WiFi radios must listen before it transmits to avoid the “collisions” that can occur if two or more nodes transmit at the same time. This collision avoidance protocol is a factor for all nodes within radio range, whether these nodes are along the data path (upstream and downstream) or...
elsewhere in the mesh. It is also important to note that this analysis does not take into account radio interference that might be caused by other systems (e.g. wireless phones or wireless access points) in the vicinity.

Not all wireless mesh products are equal. Multi-radio products (having three or more radios) commonly outperform single and dual-radio solutions proven to exhibit fifty percent degradation after the first node and even greater over subsequent hops. A poorly designed mesh network utilizing generic multi-radio products can also suffer. Total system capacity is often overstated and the overall effectiveness of an IP-based video surveillance network suffers due to inefficiencies in packet handling and increasing TCP congestion.

There are two characteristics of 802.11 multi-hop wireless networks that affect TCP performance and IP video transport: First, contention for the shared wireless channel on a given radio; consistent link-layer contention caused by large numbers of wireless client devices, given a particular node's limited overall capacity, will cause packets to drop. Second, while improving channel availability through spatial reuse (simultaneous scheduling of non-interfering transmissions), TCP's windowing mechanism will limit its effectiveness. Traffic load has significant impact on link contention and spatial channel reuse. TCP increases its average window size to cope with buffer overflow. When the buffer gets full—which occurs quickly, and especially if latency is already high, then more packets are dropped causing potentially significant retransmissions. The problem becomes self-perpetuating until there is nothing but a trickle of throughput due to degraded spatial reuse and increased packet loss.

To ensure the highest overall performance of the network it's important to consider that the right multi-radio architecture is not only capable of high throughput and low latency, but offers the total capacity to achieve maximum performance to every radio. Equally important is the dynamic mesh algorithm that enables fully distributed localized node intelligence (DLNI), placing sub-millisecond mesh decisions at each node, while having full mesh knowledge and using less than one percent of the networks resources for mesh management.

In a Strix Access/One solution, at a minimum, one radio is used for wireless client traffic while a pair of radios are dedicated for the 802.11a wireless backhaul traffic: one for ingress backhaul and one for egress backhaul. This approach to wireless mesh with Strix Dynamic Mesh Architecture (Strix DMA™) offers the industry’s highest performance.
Strix Metro-Scale Mesh Architecture

Strix Access/One® multi-radio products are purpose built for maximum performance and flexibility. Strix patent pending multi-radio designs incorporate standards-based 2.4GHz, 802.11b/g, 5GHz 802.11a, high-power 4.9GHz DSRC-C for public safety networks and provide support for industry-first “any radio”, “any service”, “any configuration” flexibility.

Strix Access/One is powered by Strix Dynamic Mesh Architecture (Strix DMA™) which enables Strix High Performance Mesh Algorithm (HPMA) and Scalable Mesh Fast Re-route (SMFR). Strix DMA solves the problems associated with other mesh algorithms. SMFR enables automatic, self-forming and self-healing, topology-independent fast re-routing that supports high-speed mobile roaming, near-zero throughput loss, and near-zero latency over multiple hops.

Strix Access/One is the industry’s most cost effective wireless mesh platform delivering up to 3x more radios per square mile at a lower overall cost (TCO) than any other system.

The platform is deployed in mesh sectors of up to 100 nodes (up to 600 radios) covering 4 or more square miles from a single Internet backhaul location. This materially reduces site acquisition time, cost and complexity, substantially reduces time to market and results in the industries lowest TCO. No other platform can match this capability.

The industries only modular (chassis-based) system: delivering the largest capacity, highest throughput and lowest latency to support voice, data and video applications.

Strix OWS is field upgradeable to 6 radios in a compact chassis with a variety of antenna options. Up to four radios can be dedicated to subscriber access: thus enabling a substantial increase in in-building penetration (with sector antennas) and supporting a 3x increase in subscriber density. In addition, introduction of new technology, such as WiMAX, is easily accomplished, without a fork-lift upgrade.

Strix IWVS, based on Strix Systems patented high performance hardware and software, is a vandal-tough weatherized enclosure supporting the hottest and coldest climate conditions. Supporting industry-leading IP-enabled Intelligent Pan-Tilt-Zoom (PTZ) cameras, the IWVS achieves robust, continuous high throughput and low latency via Strix intelligent radio algorithms that dynamically adjust to the environment. Maximum power enables the greatest signal strength, receive sensitivity and optimal channel selection for the most robust wireless connectivity and highest achievable throughput.
Strix Systems Mobile Wireless System is the industry’s highest performance mobile extension for in-vehicle wired or wireless client connectivity for public safety, security, municipal, government and tactical wireless broadband mesh networks. The MWS 100 offers the industry’s fastest mobile roaming hand-off between mesh access points, the lowest latency, the highest throughput, superior multi-megabit, multi-RF and multi-channel sequencing for the best performance for mobile video, voice and data applications.

The Strix Access/One products have are proven independent test labs and in live installations worldwide in public safety, strategic and large-scale deployments covering hundreds of square. Strix Systems Access/One is the industry’s best performing wireless mesh network platform utilizing a 100 Mbps switching engine between radios enabling the highest media-rate capable over 802.11a/b/g and 4.9 GHz radios. Strix Access/One is the highest performance wireless mesh network system enabled with carrier-grade quality of service for video surveillance, optimizations for VoIP enabling the highest VoIP call volumes achieving the highest quality ratings of (MOS=5 (Mean Operating Score 5 = the highest)) in the presence of high-bandwidth data and high-speed mobility handoff well below 50ms stipulated by telecom operators enabling seamless mobile networking at speeds exceeding 200 mph.

Strix EWS platform based on is designed for zero-configuration and scaling for country-wide deployments. Easily managed, Strix graphical and command-line interfaces (CLI) enable quick visual management and detailed statistics to provide complete network awareness. Strix products provide hardware-accelerated automatic AES encryption between wireless nodes, WiFi Protected Access security for client access.

Technology Leadership

Strix Systems delivers the industry’s highest performance: based on Strix DMA™.

Strix wireless mesh networks and distributed wireless mesh networks are easier and less expensive to install, can be leveraged for multiple applications such as voice and data, and once in place doesn’t easily accepts new devices on to the network. For scalability, radios can be added to nodes or nodes added to the mesh to increase coverage and range.
Strix Outdoor Wireless System (OWS) can be mounted in minutes while secured user and backhaul connectivity are automatic. Strix nodes require only power to operate and photocell adapters make the connection simple. For geographically challenging networks, Strix offers a proven solar-cell solution that is effective in high-speed railway applications.

Distributed IP video surveillance systems are a critical step in the future of nation-wide security and personal safety. Strix Systems is an asset to deployment of distributed surveillance networks and the integration of surveillance technologies into wireless products.

Strix wireless mesh networks provide wired-like performance and resilience for mission critical applications including public safety, Department of Homeland Security. Industrial and transportation systems surveillance as well as integration with hundreds of alarm, access control, RFID and other network capable sensor and integrated security technologies.
“Wireless Mesh Ready” Certification

Strix Systems has developed its “Wireless Mesh Ready” Certified Technology Partner program to verify voice, video and applications. While Strix Systems maintains a large list of interoperable technology partners, in this program each manufacture is tested and certified with Strix Systems award winning and industry-leading Access/One® Outdoor Wireless Systems (OWS), Indoor Wireless System (IWS), Edge Wireless System (EWS) and Mobile Wireless System (MWS) products in live configurations. Certification involves three levels of validation to verify the hardware and software components: Interoperability, bandwidth optimization, future-proof technologies. The interoperability of the solution over Strix multi-radio mesh network test-bed and the monitoring and success of deployment. Performance levels and application stability over the industry’s strongest wireless mesh network infrastructure gives manufactures the data they need to enhance their applications, while Strix Partners gain a new set of application options. Strix existing technology partnerships are further enhanced by this certification which provides customers implementing wireless networks the confidence to deploy “any scale” wireless mesh network.

Manufactures desiring certification as “Wireless Mesh Ready” should contact Strix Systems at 1-818-251-1058 or sending an email to solutionmktg@strixsystems.com

”Wireless Mesh Ready” Video Surveillance Partners

There are a large number of products (servers, cameras, etc.) available in the video surveillance market. Of those, only a few have proven the ability to provide a scalable architecture capable of being deployed in a fully distributed fashion while also offering a solid set of features and industry-leading versatility. Milestone Systems is one such manufacture that offers a proven product capable of large-scale distributed deployments.

Milestone System’s line of surveillance products are based on an open platform architecture and are successfully integrated with other systems and devices. Milestone solutions include XProtect™ Central, XProtect™ Matrix, XProtect™ Transact and XProtect™ Retail. All of these offerings operate together with the main XProtect Corporate and XProtect Enterprise surveillance systems, adding extra value and return-on-investment to your IP video platform.

Because Milestone XProtect™ is designed with an open platform, it allows integration with other systems and
devices by enterprising partners, as well. The Milestone SDK (Solutions Development Kit) offers partners the tools for creating integrations themselves, using Milestones product family and other third-party systems and devices, or with their own developed applications.

Milestone XProtect is the best open platform IP video management system you can get. It acts as the core of your surveillance system, connecting all the hardware of your choice for an optimal, integrated solution. The software is offered in tiers as packaged solutions scaled to different business needs in the marketplace: XProtect™ Basis, XProtect™ Basis+, XProtect™ Professional with 4-channel Remote Client, XProtect™ Enterprise with the XProtect™ Smart Client, 16-channel XProtect™ Remote Client, XProtect™ PDA Client, and XProtect™ Matrix plug-in, and XProtect™ Corporate with the XProtect™ Smart Client. Other solutions include XProtect™ Transact for integration of video images with POS or ATM transactions, XProtect™ Matrix for distribution of live video streams from any camera to any monitor on the network, XProtect™ Central for centralized video alarm control of multiple locations, and XProtect™ Retail for centrally managed shrinkage and fraud reduction with POS time-linked video evidence.

**Best of Breed IP Surveillance Camera Manufactures**

Strix Systems supports the widest range of IP Video Cameras. Below is a list of manufactures already used in customer deployments and/or have met “Wireless Mesh Ready” certification criteria.

**Panasonic**

- Progressive output with motion adaptive interlace/progressive conversion
- Built-in MPEG-4 and JPEG digital signal output (VGA) at up to 30 ips
- PoE (without optional heater)
- MPEG-4/JPEG dual stream output for simultaneous live monitoring and high resolution recording
- High sensitivity with D/N function: 0.08lx (Color), 0.08lx (B/W) with clear dome cover
- Vandal Auto-Back Focus
- Day/Night switching for optimal clarity in any lighting condition
- Video motion detection with 4 programmable detection areas and 3 sensitivity levels
- SD Memory card slot for alarm recording and backup upon network failure
- Multi-screen supports images from 8 cameras
- IP66 rated, resistant against water and dust
- Dehumidification device for use in various weather conditions

**ACTi cameras**

**Advantech I/O devices**

**Agilemesh cameras**

**Appro cameras**

**Arecont Vision cameras**

**Axis Communications cameras and video servers**

**Baxall cameras**

**Bosch cameras and video servers**

**Canon cameras**

**Convision video servers**

**D-Link cameras**

**DotWorks Cameras, Enclosures etc.**

**FLIR thermal cameras**

**ICOP in-vehicle public safety surveillance**

**Infinova cameras**

**Intellinet cameras**

**IQinetix cameras**

**JVC Professional cameras**

**Linudix video servers**

**Lumenera cameras**

**Mobotix cameras**

**Panasonic consumer products**

**Paxton Access**

**Pelco cameras**

**Pentax cameras**

**Pixord cameras**

**Polar Industries cameras**

**Samsung cameras**

**Sanvo cameras**

**Sony cameras**

**Toshiba cameras**

**Troy connectivity box**

**Vantage cameras**

**Verint video servers**

**Vivotek cameras**

**Webgate cameras**

**XView video servers**
Federal Signal Corp.

The Neighborhood Watch Video Surveillance system combines wireless backhaul, access and video surveillance in a weatherized enclosure. Law enforcement and first responders gain secured access to the video surveillance from their emergency vehicle. The same video feeds can be backhauled to the Emergency Operation Center or 911 centers for behind the scene monitoring, tracking and responding.

ICOP Digital, Inc

ICOP Model 20/20-W® is the leading digital in-car video recorder system for law enforcement, recording high quality video in the vehicle, capable of live streaming video to other first responder vehicles and headquarters, in addition to viewing live video from inside of buildings in the community. The ICOP Model 20/20-W is loaded with features that can be found in no other in-car video system. Download ICOP MODEL 20/20W specifications for complete product details.

If you are a manufacturer, consultant or provide services in the interest of public safety and related efforts go to http://www.strixsystems.com/certification and request certification as a Strix Certified Partner.

Now that we’ve discussed the technologies, architecture and design considerations we have summarized a guideline to assist in developing your solution.

Quick Guidelines

- Determine a Network Video Recorder (NVR) or Digital Video Recorder (DVR) system that provides the greatest current/future benefits and cost effectiveness for your implementation.
- Verify compatibility of primary components including, but not limited to: cameras, switches, NVR/DVR, local and remote storage.
- For dedicated video surveillance mesh, wired backhaul locations might also be the logical central location for NVRs/DVRs, video storage and other central applications.
- For shared video surveillance/public safety and/or municipal or public access networks, wired backhaul locations may not necessarily be the best location for the NVRs/DVRs. The most appropriate location for NVRs/DVRs may be the theoretical “center” between remote viewing stations and other surveillance applications.
- For cameras and resolution, consider that approximately 20 pixels per foot are required for general surveillance applications, to identify objects 40 pixels per foot is required and for high detail at least 80 pixels per foot.
- Define radios for wireless backhaul and access needed for the required performance and resilience of the network.
• Backhaul links are automatically encrypted. Use Virtual LANs (VLANs) to provide segmented paths to and from NVR’s/DVRs, cameras, remote viewing stations and remote storage.

• Optimize video stream flows for recording and high priority viewing utilizing multi-level QoS and prioritization techniques for high-priority paths to recording and viewing locations.

• Consider using different spectrum and/or channel assignments to secure/segment traffic. For public safety applications, use 4.9 GHz DSRC-A or optional DSRC-C high power mask.

• MJPEG is commonly used for recording while MPEG-4 is used for remote viewing initially. As there are improvements in compression technologies, traffic levels over the network will likely decrease and performance will increase.

• Where possible allow a 20-30% bandwidth margin to allow for codec differences, camera settings and network paths.

• RADIUS is a recommended method to manage/authenticate users and devices into the network

• Each network element can be provisioned with a Media Access Control (MAC) security restriction.

• Remote viewing, Management and remote viewing traffic should be evaluated for optimization.

Quick Deploy Methodology

1) Provide power to the nodes and cameras. Install a Strix Access/One node for each indoor and outdoor location. Each node may support single or multiple cameras connected to the node via Ethernet. On indoor units Power over Ethernet (PoE) may be used to supply power to cameras, plug the cameras into the nodes Ethernet module. On outdoor units, Strix Access/One nodes may be completely wireless and powered by a solar power grid if needed.

2) A minimum number of wired locations are required for Strix Access/One networks although more is always an option. Perform a bandwidth calculation for the desired number of cameras and determine their desired location. Once the central sites for the surveillance server components are in place, install a Strix nodes to maximize performance. In a large-scale deployment you will want to take maximum bandwidth (frame size and bit rate) criteria into consideration. For redundancy, an additional node may be configured in close proximity to a primary node.

3) VLANs can be implemented to define paths between cameras and the NVR/DVR. QoS may be implemented for high throughput, low latency paths to the central nodes. Where a “gap” may exist, an Access/One node with high-speed backhaul may be required to relay traffic.
4) Once power is applied to all nodes, the robust Strix Access/One nodes will automatically form the mesh. Default values specify the IP address, Service Set Identifier (SSID), radio mode/channel, encryption level and node names for the mesh network—all of which can be changed later if desired.

The Business Case for Video Surveillance over Wireless Mesh

The business case for video surveillance is generally understood in relation to the life saving benefits of safety and security. However, going one step further, the Total Cost of Ownership (TCO) in a wireless video surveillance network, and therefore ROI, is achieved by selecting Strix multi-radio mesh network nodes. Further, the best way to minimize costs is to select an architecture that offers maximum throughput, and that allows for the most cost-effective incremental growth over time - the best path to this end is a multi-radio mesh with the ability to provision and field-upgrade a given node with additional radios.

The key elements influencing total cost of ownership (TCO) of a wireless mesh network for video surveillance can leverage metropolitan and municipal mesh infrastructure by assessing (a) the surveillance system, (b) number and cost of mesh nodes, (c) backhaul to external networks, (d) network management and OSS, (e) non-recurring engineering and installation.

Surveillance System – Legacy surveillance systems are expensive to deploy due to proprietary equipment, coax, fiber and other wired cabling, lack of scalability, requirements for personnel experience and the expensive support and maintenance of CCTV equipment. In contrast to legacy systems, the distributed video system doesn’t require complicated proprietary hardware, complex cabling connectivity and dedicated monitors. Multiple cameras can be added to the Strix mesh easily without years of experience in the video surveillance market. Existing network personnel can easily configure the cameras, the server components and make changes to, if needed, to the mesh network from any location. These systems easily scale from one to thousands of cameras in increments of a single camera (no mandatory 16-channel jumps like in the DVR world) and can be accessed as needed by desktop computer, laptop, PDA and even cellular phone.

Changing camera placement is simple and monitoring can be distributed or centralized as live camera feeds can be accessed from anywhere on the mesh network and, if desired, the Internet. Management software enables you to control access to surveillance video to authorized personnel only.

Mesh nodes – This includes the cost of the nodes themselves, antennas, and associated hardware, which allows you to cost-effectively amortize additional capacity through the addition of multiple radios to existing nodes, providing the most cost-effective growth path over time. It is also important to select nodes that have excellent performance for a wide variety of traffic types; however, video surveillance is evolving as a primary application for wireless mesh networks. In fact, voice and data could be considered important secondary applications in this context with “triple play” as the eventual result. We
make the assumption here that over-provisioning capacity is the preferred deployment strategy, just as it is with wire, but tempered by the cost realities of deploying many nodes at once.

**Backhaul** – This is the other potentially large expense which can be mitigated by architectural choices. While many forms of both wired and wireless backhaul exist, all can add significant cost to a given installation. The good news here is that appropriate architectural choices can materially reduce the cost of backhaul by provisioning fewer (if higher-capacity) backhaul links. The cost of backhaul is offset by the ability to support the distributed nature of the video surveillance model presented here.

**Network Management** – Both wireless mesh and video surveillance management achieve significant cost benefits via the effective use of mesh network management and operational support system tools. While traffic flows through the mesh are self-managing to the greatest degree possible, it’s important to use automation wherever possible to hold operational expense down. Appropriate and effective automation in the management and OSS space can reduce personnel costs, improve customer-facing responsiveness, and increase overall customer satisfaction while holding maintenance costs to a minimum. An excellent example of the benefits possible here would be in a network management system that monitors throughput and latency, across the mesh, automatically identifying potential areas where more capacity should be deployed in the video surveillance network - providing advance warning of this condition.

**Engineering and Installation** – Designing, installing, testing and certifying metro-scale mesh and the distributed video surveillance network are engineering-based disciplines requiring expertise. The cost of engineering and installation is typically 25% to 30% of equipment cost. However, deployment circumstances can significantly increase this percentage. Examples of common situations leading to higher costs can include: installing or mounting the mesh network and surveillance components in locations other than initially planned, corrections to wire additional power to the mounting locations, and correcting installations for unexpected radio conditions such as lower-than-expected signal penetration due to interference or intervening structures (the latter known as shadow fading).

Other costs, which we group under the general heading of operational expense (OpEx), include administration, legal, maintenance, office expense, utilities, marketing, sales, support, and related customer-facing expenses, but these are irrespective of particular architectural choices.

It should be quite clear that multiple-radio nodes can have a profound impact not just on performance, but on the ultimate cost-effectiveness of a given metro-scale mesh. And, as gross margin is computed by subtracting cost from revenue, maximizing revenue via multiple classes of users each with sufficient capacity and performance to meet their specific requirements and minimizing costs via architectural innovations is the best path to a successful metro-scale WiFi mesh deployment.
Summary

It is very clear that metro-scale WiFi meshes are playing a critical role in the future of broadband communications, but also a significant role in video surveillance on a global basis. Issues such as bandwidth degradation, network latency, and application priority contention can easily arise in an improperly designed wireless mesh network. These phenomena are further exacerbated when covering large geographic areas. Lack of required network performance and resilience can wreak havoc on those network points where viewing and storage take place. The severity of the problems will also vary widely based on the particular wireless mesh architecture used.

Properly designed and implemented, mesh networks provide the capacity and convenience to serve as a primary communications mechanism for essentially everyone. We are also now seeing the beginnings of a trend towards the convergence of such WiFi networks and cellular broadband coupling the capacity of WiFi to the inherent coverage advantages of cellular. We know by experience that not all mesh networks are the same and if you start with low throughput, high latency and un-scalable technology, the results can be devastating. Implementing a wireless mesh network with Strix modular multi-radio, multi-RF, and multi-channel architecture and technology proven to deliver the highest throughput, lowest latency with the greatest scalability and resilience is the only way to build a scalable video surveillance network.

About Strix Systems

Strix Systems the a worldwide Leader in Wireless Mesh Networking, in market share (according to Heavy Reading, Infonetics and In-Stat) and technology (Iometrix) having thousands of customers in over 30 countries worldwide.

Strix’s Access/One products are the industry’s only modular (chassis-based) mesh systems, delivering the largest capacity, highest throughput and best scalability. This new generation of products provides the broadband mobility and reach to support voice, video, and data applications. Sold globally by a network of first-class distributors and integrators, Access/One solutions have been deployed in hundreds of networks worldwide, outdoor and indoor, for service providers, metros, public safety, government, energy, manufacturing, transportation, hospitality, education, enterprises, and residential markets. For Strix latest video case study on public safety, municipal networks and railway networks please go to: http://www.strixsystems.com/video/missioncritical.html.

Strix Systems products and services are available worldwide through a premium partner ecosystem of distributors, service providers, resellers and systems integrators. For more information about Strix Systems, please visit www.strixsystems.com.

For more information contact:
Strix Systems, Inc.
Telephone: 1-877-STRIXSYS or 1-818-251-1017