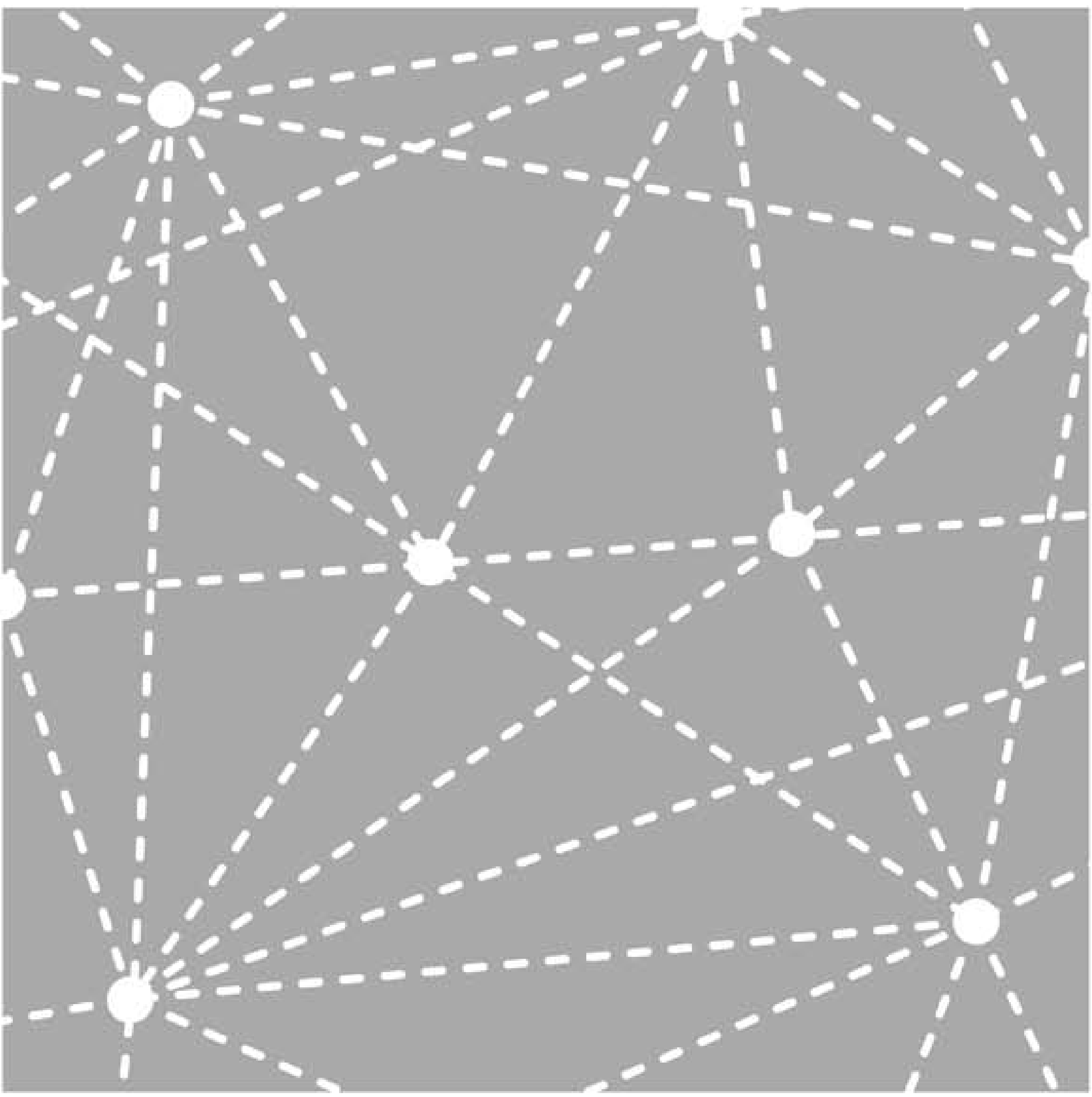
TESSCO

firetide™
instant mesh networks™

WHITE PAPER

A Guide to Video Mesh Networking



800.472.7373
www.tessco.com

A Guide to Video Mesh Networking

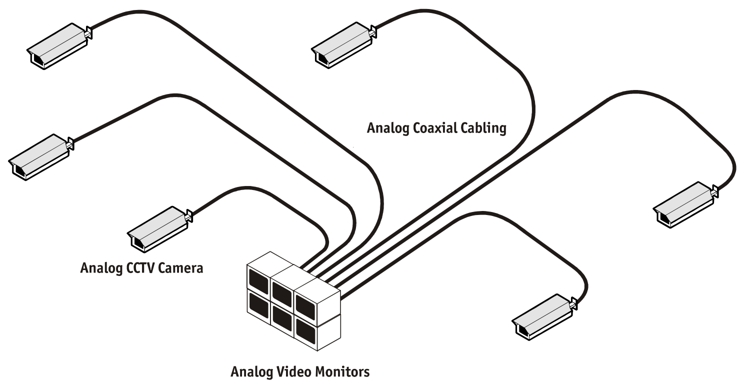
July 2005

Contents

WP-VSMN-0705

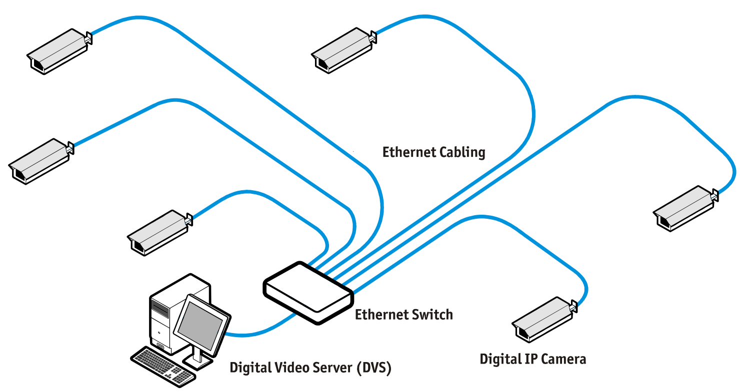
Introduction

Traditional video monitoring and surveillance applications employed analog CCTV (closed-circuit television) cameras that were hard-wired via coaxial cabling to a centralized monitoring and recording facility. This arrangement, dating back to the 1960's, works well enough today within and around a building, and even in some campus environments—despite the high cost of cabling.



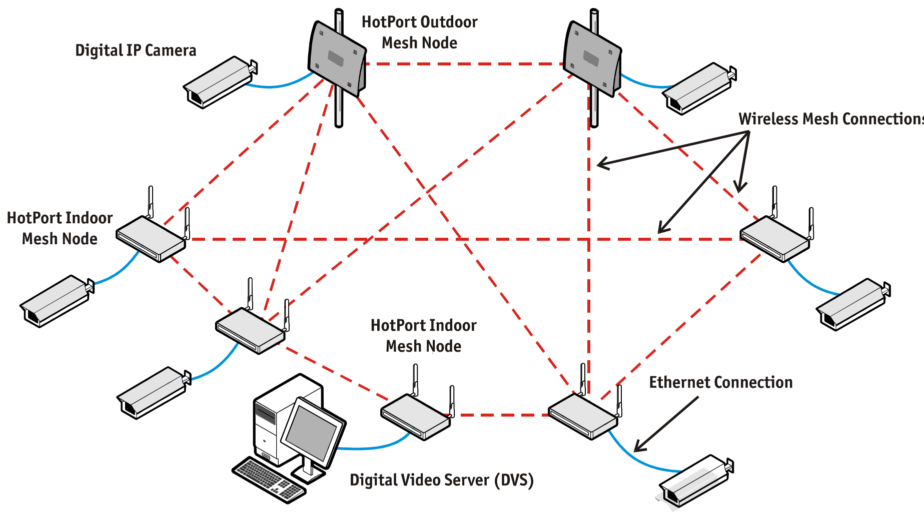
Analog CCTV (closed-circuit television) System with Coaxial Cabling

The advent of digital CCD (charge-coupled device) cameras and companion digital video server (DVS) represented a breakthrough advance. The primary advantage over analog systems, of course, is that digital technology has made video surveillance feasible with less bandwidth and with much more flexible and widespread distribution. It allowed video surveillance applications to take advantage of low bandwidth data networking infrastructures, carrier services like T1/E1, DSL (digital subscriber line), metropolitan Ethernet, and even worldwide coverage via the Internet. These digital cameras are compact and feature-rich with a wide range of configuration options. Most also come equipped with an Ethernet interface and support for the Internet Protocol (IP) built-in, and some even sport an integral Web server.



Digital IP Cameras and Digital Video Server (DVS) on Wired Ethernet Network

Another new networking technology offers an equally promising breakthrough advance in video monitoring and surveillance applications: the wireless mesh network. The HotPort™ High Performance Mesh network is the third generation of mesh networking products from Firetide, a leading developer of wireless mesh network solutions. The HotPort system is a multi-service mesh network that enables standard Ethernet devices, including IP video cameras and DVSs, to connect securely via the wireless mesh network as if connected to a virtual Ethernet switch. Designed for maximum performance, scalability, and ease-of-use, the HotPort mesh network operates seamlessly between indoor and outdoor environments in either the 2.4 GHz or 5 GHz spectrum for optimal performance and minimal radio interference. With its self-healing capabilities and high sustained throughput, a HotPort mesh network is very reliable and readily satisfies the security and performance demands of video monitoring and surveillance applications.



Digital IP Cameras and Digital Video Server (DVS) on Wireless Mesh Network

By eliminating any dependence on wires, cameras can be placed—easily and cost-effectively—virtually anywhere with a mesh network infrastructure. The compromises of the past (especially neglecting those locations that were impractical or impossible to wire before) can finally be remedied. The combination of digital cameras and a wireless mesh network is now regularly used to supplement existing analog CCTV systems. And an increasing number of companies are finding the advantages of digital video so compelling, they are starting to replace their legacy analog CCTV infrastructure entirely.

The remaining content is organized into three sections followed by a brief conclusion. The first section on *Understanding Digital Video Network Requirements* establishes a set of seven criteria that must be satisfied when deploying wireless technology in a digital video monitoring and surveillance application. The section on *Calculating Digital Video Network Performance Requirements* provides the details necessary to assess the video packet throughput required by the network. The third section, *Implementing a HotPort High Performance Wireless Mesh*, applies these considerations to a typical deployment and supplies specific guidance on designing a network for optimal performance.

Understanding Digital Video Network Requirements

Connecting digital cameras via wired Ethernet LANs is now common practice. A switched Ethernet network readily meets and exceeds any and all requirements for video monitoring and surveillance. The same cannot be said for all wireless networks, however. For this reason, it is important to understand what is required of a wireless network to adequately support video traffic.

In digital video monitoring and surveillance applications, each camera generates a stream of sequential digital images typically at a rate of 2-20 every second. The destination for all this traffic is normally a centralized monitoring facility, which includes one or more real-time displays (normally on a PC) and a digital video server (DVS) for storing and retrieving the many individual streams. A single DVS system is typically capable of supporting up to 32 cameras, and multiple DVSs can be deployed in either a centralized or distributed fashion. Depending on the application, the DVS's contents may be archived to disk or a more cost-effective high volume medium, such as tape. Analog video from CCTV cameras can optionally be converted to digital video format for real-time and/or archival storage via the DVS.

In a video application, the data network must be capable of sustaining the aggregate throughput required to deliver the packetized video streams being generated by all of the cameras. Assuring adequate packet throughput performance can require a substantial amount of bandwidth to accommodate the total, end-to-end traffic load. Bandwidth, of course, is just one measure of Quality of Service (QoS), and QoS often encompasses latency (the delay between transmitting and receiving packets) and jitter (the variations in that delay from packet to packet).

Traffic is generally considered uni-directional in a video monitoring or surveillance application; that is, the vast majority of traffic results from the video streams that flow *from* the camera(s) *to* the DVS(s). There is some traffic that must flow in the other direction, of course, which is why the network must provide robust bi-directional capabilities. There are three reasons for this requirement. The first is the need for traffic control mechanisms that regulate flow, enforce priority settings, guarantee packet receipt and satisfy other network needs. Secondly, the network itself is likely to be managed "in band," which requires communications by a centralized network management system (NMS) to and from all distributed nodes. Third and finally, some cameras offer similar centralized in-band control, whether to simply adjust settings from time-to-time or to pan/tilt/zoom (PTZ) the cameras in real-time.

The discussion above focused on the performance (and implicitly the scalability) of the network. While performance is critical, video monitoring and surveillance applications demand much more from the network. Given the nature of these applications, the network must offer mission-critical dependability and ironclad security. Fortunately, most systems (cameras, DVSs, networking equipment, etc.) all provide adequate reliability. And most wireless networking technologies also now offer a variety of robust security provisions. These same standard security provisions (proven in billions of e-commerce and other financial transactions daily on the Internet) can make a wireless network infrastructure virtually tamper-proof. Nevertheless, satisfying these three requirements (for performance, dependability and security) often means creating a dedicated network for the video surveillance application.

The network should operate seamlessly indoors and outdoors. Although some outdoor cameras could be considered to be "indoors" from the network perspective (e.g. attached with a short cable through the wall of a building), the network should be able to accommodate the inevitable real-world outdoor installation without a major upgrade or other disruptive change. Naturally, the network should also be easy to install and operate. And last but certainly not least, the network must be affordable. The total cost of ownership (TCO) should include both the initial capital expenditure (CapEx) and the ongoing annual operation expenditure (OpEx).

Video Monitoring and Surveillance with a Firetide Wireless Mesh Network

This summary shows how a Firetide HotPort High Performance Mesh network readily satisfies the seven basic network requirements for video monitoring and surveillance applications.

Performance/Scalability—Mesh topologies are renowned for their high aggregate throughput (based on multiple concurrent traffic flows) and virtually unlimited scalability. A HotPort mesh can extend to cover significantly large areas in excess of 25 square miles (36 square kilometers). Traffic can be categorized and prioritized for maximum throughput with minimal latency. Other features that enhance performance and scalability include dual-spectrum radios with Transmit Power Control, use of multiple Network Gateway Interfaces and support for Virtual LANs.

Dependability—A HotPort mesh can be designed to eliminate all network-wide single points of failure. The innovative self-healing nature of the Firetide Mesh Routing Protocol (FMRP) automatically routes traffic around any node that becomes congested, experiences intermittent interference or obstructions, or fails to operate. For example, installing two HotPort nodes at the “center” of the mesh (where the DVS is located) provides automatic failover without a separate (and costly) load-balancing switch. The result is a remarkably resilient and reliable network that also readily overcomes any line of sight obstacles.

Security—Robust security is assured in a HotPort mesh through a number of complementary provisions. Only HotPort nodes are permitted to participate directly within the mesh network, to prevent outside tampering. Traffic filtering and Virtual LAN provisions block any and all unauthorized traffic from ever entering the mesh. And strong encryption—up to 256 bit keys for Advanced Encryption Standard (AES)—protects the integrity and privacy of all traffic from end-to-end.

Indoors and Outdoors—Seamless operation within, through and beyond walls has been designed into the HotPort system. All HotPort equipment is appropriately ruggedized, with the indoor unit being plenum-rated and the outdoor unit being fully weatherized in a cast aluminum enclosure. Indoor units can be securely mounted to a wall, ceiling or countertop using an optional mounting bracket. Each outdoor unit features weatherproof Ethernet connectors, high gain antennas for extended range, a removable sun shield and a choice of secure mounting options. Outdoor HotPort units offer industry standard Power over Ethernet (IEEE 802.3af) to power attached cameras. HotPort units are available with an optional external battery and solar-power panel to accommodate a fully untethered application.

Ease of Installation/Use—A HotPort mesh is fully self-configuring, which makes its installation truly plug-and-play. Simply connect each camera and DVS to an indoor or outdoor HotPort unit, add a few more to fill in the voids, and apply power. The mesh will then automatically configure itself for optimal operation. The mesh will also automatically reconfigure itself in real-time, which enables cameras to become portable or even mobile. HotView™ mesh management software provides highly intuitive command and control of the entire mesh and individual mesh nodes from both centralized and remote locations.

Affordability—A HotPort mesh affords both a low CapEx and very low OpEx, together yielding the lowest overall TCO of any viable alternatives—either wired or wireless. The mesh also easily and quickly adapts to changing needs, providing solid investment protection and a continual return on that investment.

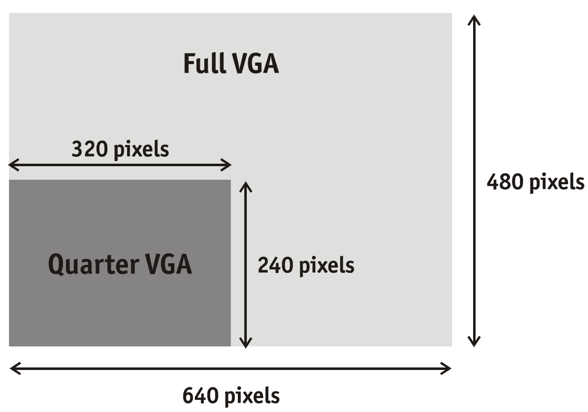
Mobility – A HotPort video mesh network facilitates the real-time redeployment of assets, which is particularly valuable for police and fire departments, and in other tactical situations. The self-healing mesh automatically adds new nodes as they move within and throughout the range of other nodes. In addition, the ability to power an outdoor HotPort node with 12 or 24 VDC batteries can make any vehicle or vessel a fully mobile member of the mesh. These mobile nodes can be equipped with either cameras or PC monitors—or both, if desired.

Calculating Digital Video Network Performance Requirements

Before configuring a HotPort wireless mesh network in a video monitoring or surveillance application, some additional and *quantitative* understanding of digital video communications is necessary.

Digital video cameras create compressed images utilizing standardized techniques from the Joint Photographic Experts Group (Motion JPEG or M-JPEG) or the Moving Picture Experts Group (MPEG). Both techniques are capable of producing a sequence or stream of images to create a full-motion video. The images vary in color saturation from none (grayscale) to full RGB (Red/Green/Blue) color. These images also vary in resolution, or frame size, from 160x120 pixels (19.2 KB) to the maximum VGA (Video Graphics Array) resolution of 640x480 pixels (307.2 KB). Full VGA has four times the image size and quality of traditional CCTV cameras operating at an equivalent CIF resolution of 320x240 pixels (76.8 KB). This helps explain why the Common Intermediate Format (CIF)-equivalent "Quarter-VGA" resolution is quite popular in video monitoring and surveillance applications. The Quarter-VGA designation derives from the fact that there are half as many pixels in both the horizontal (320) and vertical (240) directions yielding an image size that is one fourth (½ x ½) the size of a full VGA image.

Note that for the purposes of this document, we have chosen cameras with an image width to height ratio of 4:3. Image ratios vary by manufacturer. Some cameras use sensors producing images with ratios of 3:2, 5:4, or even odd pixel counts to approximate legacy analog CCTV formats.



Comparison of Full VGA and Quarter VGA Image Sizes

The frames are then transmitted in sequence at a specified rate, typically from 2-20 frames per second (FPS). Although a frame rate of 30 FPS is often dubbed "full motion" quality, far lower frame rates are more than adequate in video monitoring and surveillance applications. Normally a frame rate in the range of 5-15 FPS affords an optimal balance between image quality, storage capacity and bandwidth utilization.

The amount of bandwidth required for each data stream depends on a combination of the image resolution and its frame rate. Because most images will be viewed from a PC, the common VGA resolution of 640x480 pixels (0.3 MP) is generally considered the maximum frame size. Any higher resolution is generally considered a waste of precious resources. Because most organizations utilize the CIF-equivalent Quarter-VGA resolution at 320x240 pixels, this frame size will be used for the calculations in this document.

A relatively low frame rate, such as 5 FPS, is adequate in most video monitoring and surveillance applications. Many situations can even tolerate a lower frame rate with little or no practical degradation in the content quality. A higher frame rate is necessary only in those rare situations where fast-moving action must be captured, and even here, 15 FPS is generally considered to be "full motion" for all practical purposes. A mid-point rate of 10 FPS will be used for the calculations in this document.

Most digital monitoring systems offer a means of compressing the data stream. The M-JPEG and MPEG standards permit various levels of compression, and some vendors may offer extensions to these standards. Higher levels of compression consume less bandwidth, but also produce images with diminished quality. Compression ratios can range from 1/5, where image degradation is barely perceptible, to 1/60 which has higher image degradation but is still adequate for many video monitoring and surveillance needs. Typical levels of compression range from 1/15 to 1/30. This analysis will be based on a 1/30 compression ratio.

The following equation is used to determine bandwidth requirements (in Megabits per second or Mbps) for a single camera: Bandwidth (Mbps) = Depth x Width x Height x Compression Factor x FPS

Where...
Mbps = Megabits per second (1 Mbps = 1,048,576 bits per second)
Depth = color depth in bits (8-bit grayscale to 32-bit color)
Width = frame width in pixels
Height = frame height in pixels
Compression Factor = the ratio of the compressed version to the original image
FPS = frames rate in frames per second

Note that the depth, width, height and compression factor together determine the *Frame Size* of the image. Depth (or color depth) is the number of colors available in the palette. Computer displays utilize anywhere from eight digital bits to define 256 colors or grayscale levels (2^8) to 32 bits to define "True Color" images. It is common with many CCD cameras, however, to utilize a traditional Red/Green/Blue scheme with eight bits for each of the three primary colors. This results in a total of 24 bits for each image (3 colors x 8 bits/color), which is capable of producing a total of 16 million colors (2^{24}). Either approach is quite adequate for most video monitoring and surveillance needs; this document adopts the latter approach.

Example

A 24-bit color Quarter VGA video stream with 1/30 compression transmitted at 10 FPS requires 614 Kbps (or 0.6 Mbps) of bandwidth (24 bits x 320 pixels x 240 pixels x 1/30 compression x 10 frames per second)

The following table shows the bandwidth requirements in Mbps for Quarter and Full VGA frame sizes at four different frame rates. The examples in this document utilize a Quarter VGA frame at 10 FPS, which is typical of video monitoring and surveillance applications.

Frame Rate	5 FPS	10 FPS	15 FPS	30 FPS
Quarter VGA (320 x 240)	0.3 Mbps	0.6 Mbps	0.9 Mbps	1.8 Mbps
Full VGA (640 x 480)	1.2 Mbps	2.5 Mbps	3.7 Mbps	7.4 Mbps

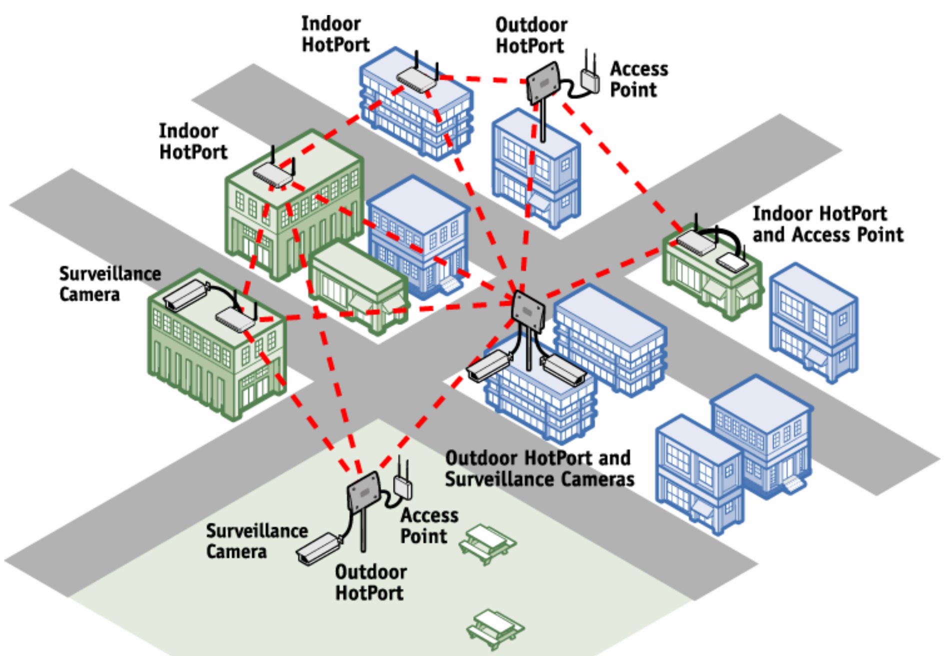
Bandwidth requirements (Mbps) for digital video surveillance

Implementing a HotPort High Performance Wireless Mesh

Firetide's HotPort High Performance Mesh network was designed for maximum performance and reliability in a variety of applications. The HotPort mesh is highly scalable and operates seamlessly between indoor and outdoor environments in either the 2.4 GHz or 5 GHz spectrum. And unlike other wireless networks, a HotPort mesh is remarkably easy to install and operate. With its self-healing capabilities, intuitive traffic management, and throughput up to 25 Mbps, a HotPort mesh readily satisfies the demands of most high-bandwidth/low latency applications, including video monitoring and surveillance.

The major advantage of a Firetide wireless mesh network is its ability to provide Ethernet connectivity virtually anywhere—indoors and outdoors—without a wired backbone. This distinguishing characteristic makes the mesh ideal for any location where network cabling is too difficult or expensive to install, such as historic buildings, outdoor locations, temporary venues, office spaces that change frequently and so on. Even in locations where wiring may be abundant, wireless mesh technology often affords greater flexibility, less disruption and a superior return on investment.

To all connected systems and equipment, the entire HotPort mesh network functions as a virtual Ethernet switch. For this reason, any Ethernet device can operate over the wireless mesh backbone without any additional setup, drivers or other special software. Any device—IP camera, DVS, server, PC or whatever—simply connects to one of the Ethernet ports on a HotPort mesh node exactly as it would to a physical Ethernet switch. Operation at Layer 2 Ethernet not only makes the mesh easy to deploy, it also maintains compatibility with all higher-layer protocols, thereby preserving the integrity of all applications operating on the mesh network.



Firetide HotPort Wireless Mesh Network

Deploying a HotPort High Performance Mesh Network Step-by-Step

A Firetide HotPort High Performance Mesh network is *very* easy to install. In fact, because the mesh is self-configuring, installation is about as "plug-and-play" as any network could ever be. A detailed tutorial on planning an optimal mesh network implementation can be found in a publication titled *Designing a Firetide Instant Mesh Network* available on the Web at www.firetide.com. Presented here is the basic four-step process for deploying a HotPort High Performance Mesh network for video monitoring and surveillance applications.

Deploying a fully-functional HotPort mesh network requires following only four basic steps outlined below. *The Math Behind the Mesh* sidebar supplies the detailed calculations that may be warranted in Steps #2 and #3. In addition, some application-specific guidelines are also provided to help assure an optimal configuration.

Step 1—Begin by installing one HotPort node for each indoor and outdoor camera location. The camera will connect directly to an Ethernet port on the HotPort node. And, of course, both the HotPort node and camera require power. On outdoor units, the HotPort node can be battery-operated and is also capable of providing power to the camera via Power over Ethernet (PoE).

Step 2—Next provide a HotPort node for each "centralized" digital video server (DVS) system. In very large-scale applications, multiple HotPort/DVS pairs may be necessary based on either a limitation of the DVS (some support only 16-32 cameras) or the bandwidth requirement (determined by the frame size and rate). In situations requiring multiple DVSs, each HotPort node is configured as a special Network Gateway Interconnect (NGI) to optimize the flow of traffic for peak performance. The multiple DVSs can be optionally internetworked via the existing wired Ethernet infrastructure. To avoid creating a single point of failure in the mesh, take advantage of its automatic failover capability by installing two HotPort DVS nodes in primary/secondary fashion. This configuration provides the services of a separate load-balancing switch without the additional cost and complexity.

Step 3—Deploy "intermediate" nodes as required to link the camera nodes to the DVS node(s). This is the only "tricky" part of the deployment, and even this step is fairly straightforward. The goal here is to create a wireless "path" from each camera all the way to its assigned DVS. The required path may already exist, either directly (a single "hop") or via other HotPort mesh nodes (multiple "hops"). But where a "gap" exists in the mesh, one or more intermediate HotPort node(s) may be required to relay traffic. If no surveillance is required at their locations, these intermediate nodes will not require cameras. After the initial installation, it may be necessary to reorient or reposition these intermediate nodes or to change or adjust their antennas to optimize mesh traffic flow.

Step 4—Once power is applied to all nodes, the robust Firetide Mesh Routing Protocol (FMRP) will automatically form the mesh network using a set of default values. These default values specify the IP address, Extended Service Set Identifier (ESSID), radio mode/channel, encryption level and node names for the mesh network—all of which can be changed later if desired. The invisible wireless links among all nodes can now be "seen" using the HotView mesh management system, which also provides the tools needed to monitor the network's operation and "tweak" its configuration. Because the use of HotView is beyond the scope of this white paper, please consult the HotView documentation for a detailed explanation of how to get the most from this powerful mesh management tool.

The Math Behind the Mesh

This sidebar is for those who desire a more in-depth understanding of how to characterize wireless mesh performance. As mentioned previously, this analysis utilizes a 24-bit color Quarter VGA frame with a compression ratio of 1/30 and a transmission rate of 10 FPS. The types of calculations used here are equally valid for other scenarios using different values. Therefore, transmitting a single 61,000 bit frame via radio at a 54 Mbps half-duplex data rate takes approximately 1.1 milliseconds (1.1 ms or 0.0011 seconds). A frame rate of 10 frames per second leaves a window of 100 ms for sending each frame.

The limiting factor for throughput in a mesh network normally involves the "intermediate" nodes that must both receive and retransmit. In large mesh networks, there may be multiple "hops" between the source (in this case a camera) and the ultimate destination (in this case a DVS). It becomes important at this point to understand a little about IEEE standards-based radio communications. Much like Ethernet, a mesh node 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.

Because the video is transmitted in a stream, the receipt and retransmissions of each frame must occur within the 100 ms window determined by the frame rate. To "relay" a frame in this fashion, therefore, takes approximately 3.0 ms (allowing some time for the slight collision avoidance delay involved). A single intermediate node can, therefore, tolerate a maximum of 33 streams, (with 8-12 being the norm), *occurring within its radio range*. Because it is good practice in mesh design for every node to have at least two neighbors, intermediate nodes may have up to six or eight neighbors within radio range. Assuming that its adjacent neighbors to either side (and not along its data path) are also transmitting video streams, a single path through the mesh should be able to accommodate four or five video streams (33 ÷ number of neighbors). Note that this is the maximum for any single path. The mesh in its entirety can support multiple concurrent paths.

The limiting factor for an entire mesh with a single, centralized DVS can be determined in a similar fashion. The key difference is a node connected directly to the DVS need not retransmit video streams via its radios. In other words, it behaves primarily as a "receive only" node. Although all nodes must transmit some protocol handshaking and management information, this concept does prove useful in determining the maximum number of cameras the mesh can accommodate. Because a frame from each stream must be received within the 100 ms window, the mesh is more than able to support the maximum number of cameras typically supported by the DVS (typically in the 16-32 range). However if a large number of cameras are used, additional receive only nodes, connected to the DVS via a router, may be needed to feed the multiple video paths to the DVS. Staying within these guidelines ensures that the HotPort mesh will not be a bottleneck in the system.

Additional Deployment Guidelines

Here are some additional "Rule of Thumb" recommendations that are useful in designing a HotPort High Performance Mesh network in video monitoring and surveillance applications:

- Minimize radio interference by utilizing a spectrum and channel set not currently in use in the vicinity.
- If using Power over Ethernet, be sure that the camera selected supports the IEEE 802.3af industry standard. Some cameras utilize a proprietary power scheme requiring the vendor's own power source.
- Minimize hop count by placing the DVS as close to the "center" of the mesh as possible. Ideally, there would be no more than one primary intermediate node between each camera and the HotPort node connected to the DVS system(s).
- Enhance the resiliency of the network by adding more intermediate nodes as secondary or alternate paths to eliminate any mesh-wide single points of failure. But be careful not to add too many redundant nodes, because doing so could increase the amount of intra-mesh interference.
- Eliminate any potential bottlenecks and enhance overall mesh resiliency by employing multiple Network Gateway Interconnects (NGIs) on selected nodes to expand the "center" of the mesh outward toward the edges where the cameras are located. These NGI nodes can then be networked via the existing wired Ethernet infrastructure to reach the monitoring facility and DVS system(s).
- Fine-tune the traffic, as needed, by creating Virtual LANs (VLANs) to direct traffic along desired routes. Utilize the Traffic Prioritization feature to give a higher priority to the most critical cameras.
- If security is a special concern, utilize the HotPort packet encryption and filtering capabilities to prevent tampering as well as the introduction of any unwanted traffic.
- For very large-scale deployments, consider utilizing multiple mesh networks (with different spectrum and/or channel assignments) to segment traffic for broader coverage and enhanced performance.

Conclusion

Wireless works well for an increasing number of networking applications, and advances in digital cameras and wireless technologies now enable the use of wireless networks for video monitoring and surveillance. But only one wireless technology satisfies the seven key requirements fully: the multi-service mesh, particularly the industry-leading HotPort High Performance Mesh network from Firetide.

Mesh networks are not new. Indeed, both the Internet and the Public Switched Telephone Network (PSTN) utilize mesh topologies. The idea of uniting mesh and wireless technologies originated by the very same organization that led to the birth of the Internet: the U.S. Department of Defense. The DoD's goal involved creating an instantaneous, highly secure and mission-critical real-time network for data, voice *and video* communications on the battlefield. Firetide's unique approach to mesh networking allows virtually any IP surveillance camera to be used on a wireless mesh infrastructure, resulting in flexible, cost effective, high quality video surveillance and monitoring.

To learn more about how your organization can benefit from the many advantages of mesh networking today, visit Firetide on the Web at www.firetide.com. There you will find additional information on mesh networking in general, and greater detail about the many advanced features in a HotPort High Performance Mesh network.