

Wireless Video Security with Tropos MetroMesh[™] Networks

A TROPOS NETWORKS WHITE PAPER

Introduction

Conventional CCTV video surveillance has converged with PC and networking technology to create dramatic improvement in features and functionality. Digital security solutions can now deliver unprecedented price/performance on a scale that was previously impossible. Wireless technology accelerates this trend by almost totally removing the need for expensive cabling, which can account for over 80% of the cost of a surveillance installation in an outdoor environment. This promise is being delivered today by the expansion of high throughput Wi-Fi wireless networking from its in-building roots to outdoor deployments, now available on a city-wide scale.



Metro-scale Wi-Fi broadband data access, as pioneered and deployed by Tropos Networks using its patented metro-scale mesh technology, is now enabling many applications that were previously impossible. In the public safety sector, for example, applications such as virtual lineups, fingerprint analysis and access to detailed mug-shots or floor plans are now being brought out of the station house and into the field where they are needed.

Video and access control data streams are now routinely transported digitally using standard Internet Protocol (IP). When this happens over a metro-scale

Co-ax Video Cable Video Cable Analog Monitors

Figure 1: Conventional Analog Video Surveillance

IP Network

石

IP Hub

Huk

IP Router

IP Cameras

Wi-Fi network such as Tropos', the result is affordable metro-scale video security.

The use of standard IP technology allows customers and integrators to assemble complex video security solutions from readily available COTS (commercial, off-the-shelf), best-ofbreed components. This paper describes the convergence of video, computer and networking technologies, identifies the component pieces, and discusses how they can be assembled to deliver complete city-wide video security applications at a price/performance level and speed-of-deployment never before attainable.

The Evolution of Video Surveillance Technology

Traditional video surveillance solutions rely on analog technology to transfer images from conventional CCTV cameras to banks of video recorders. Systems are characterized by long cable runs, and banks of analog switching, recording and monitoring equipment. They have been in use for many years and are proven to be effective, especially when the expense of dedicated cabling is acceptable, and where monitoring and recording is only required at a central location.

The convergence of video and computer networking technology is revolutionizing the video security industry. Second generation solutions are entirely computer-based and can readily capitalize on existing IP infrastructure instead of requiring dedicated video cabling.

• IP cameras with self-contained video server appliances internally generate MPEG, MJPEG, or H.264 images. These images are made available to other devices on the network through a standard IP network interface.



IP Hub

Analog

Cameras

Co-ax

IP Video

Server

Figure 2: IP-Based Video Surveillance



- Conventional analog cameras can be connected to the network through small, adjacent video server appliances to digitize the analog images.
- Monitoring and recording can be performed by entirely software-based network video recorders (NVRs) running on standard PC hardware.
- Advanced video analytics software can be used to automatically detect suspicious events or behavior without having to continuously monitor dozens or hundreds of screens
- Images viewed and recorded using this software can simultaneously be made available to browser-equipped PCs or PDAs on the IP network, and securely over the Internet.

IP-based security systems can dramatically reduce installation and operating costs, particularly if existing IP networks and their attendant security and routing solutions can be used.

Up to now, deploying a wired IP network on a metro-scale has not been feasible due to the cost of installing and maintaining network cable runs measured in miles instead of feet. However, high performance MetroMesh technology has now become available to deploy scalable, reliable and economical IP wireless networks over entire cities and counties. By providing true broadband connectivity over extremely large areas, such wireless IP infrastructure enables the next generation of video surveillance solutions: metro-scale video security.

Metro-Scale IP Video Surveillance

IP video security solutions deliver enhanced functionality and improved price/ performance for all sizes of installation. However, the availability of high capacity, metro-scale wireless networks now enables video systems to be deployed on an unprecedented scale. Deployments from campuses, to shopping malls, to public



Figure 3: Metro-Scale Surveillance

safety and traffic systems across entire cities are all now economically feasible using this latest wireless technology.

Tropos Networks has provided wireless mesh networks to over 500 customers world-wide, with deployments of up to 600 sq. miles (1,000 sq. km.) of contiguous wireless coverage, and for video applications as diverse as a drug dealing surveillance to "virtual life guards" on California beaches, to security for the GCC Summit in Abu Dhabi.

Tropos' unique technology allows standard 802.11 networks to be deployed across very large areas, including entire cities. Tropos Predictive Wireless Routing Protocol (PWRP[™]) is patented mesh routing technology that enables economical, secure, and reliable networks on a metro scale, minimizing the need for expensive IP cabling.



Real Metro-Scale Video Security Applications

Virtual Crime Watch

The City of Savannah, Georgia is leveraging video surveillance to increase public safety and offset a shortage of officers. Video cameras provide 24/7 monitoring of key areas of the city including 22 historic squares and the city's popular riverfront area.

http://www.tropos.com/pdf/success_stories/ tropos_success_story_savannah.pdf

Virtual Lifeguards and Fire Watch

In Laguna Beach, California, IP video cameras are used to extend the protective reach of lifeguards and fire watch personnel.

http://www.tropos.com/pdf/success_stories/ tropos_success_story_laguna_beach.pdf

Emergency Medical Services

In Tucson, Arizona, the nation's first videobased Emergency Medical Services (EMS) telemedicine system delivers live video and patient vital information to emergency room doctors while patients are en route, enabling doctors to gain advance knowledge about a patient's condition.

http://www.tropos.com/pdf/success_stories/ tropos_success_story_tucson.pdf Of course, by eliminating wiring, metro-scale wireless networks further dramatically reduce installation costs. The automatic configuration feature of Tropos PWRP also enables such networks to be deployed extremely rapidly, with entire city deployments measured in days instead of months, and temporary networks for high profile events installed in hours.

A Tropos network is totally IP-based, and performs as an extension of a standard IP network. It therefore serves as an excellent transport mechanism for IP video. The city-wide coverage delivered by the Tropos metro-scale wireless network enhances a metro-scale video security solution in two ways. First, with appropriate bandwidth planning and network configuration, a wireless network can provide some or all of the IP backbone needed to transmit camera images to central or distributed command and control stations. Metro-scale, ubiquitous wireless coverage allows these cameras to be mounted at locations city-wide, or in vehicles or other wirelessly connected temporary or mobile assets. Second, the network can be used to distribute live and recorded images to mobile units anywhere in the coverage area, providing on-scene "eyes" simultaneously for responders in the field and their commanders at headquarters.

Using the advanced capabilities of the latest generation of PC-based DVR (Digital Video Recorder) or multi-server NVR (Network Video Recorder) software, it is now even possible to "push" live video images to those mobile units. A silent alarm triggered in a bank, for example, can cause a live video feed from the bank's internal security system to be transmitted to the police

department's command and control center. From there, live video can be relayed along with the dispatch message to the laptop in the mobile unit attending the robbery. The ability of a responding officer to see in real time what is actually going on at the scene of an incident has been described as life saving technology.

Tropos MetroMesh Wi-Fi Networks

A Tropos MetroMesh Wi-Fi network uses standard wireless (802.11g, 802.11a, or 4.9GHz) as the communications medium to wireless clients (cameras, laptops or PDAs). For example, there are over 500 million Wi-Fi devices deployed worldwide, and Wi-Fi connectivity is now built in as standard to most new laptops. Many devices such as PDAs and video cameras have been enabled for its use.



Figure 4: Tropos Metro-Mesh Router



Tropos MetroMesh routers utilize PWRP[™], a patented mesh routing architecture to minimize the number of wired backhaul connections required when deploying Wi-Fi across an entire city. Tropos 5210, 5320 and 9532 outdoor MetroMesh Routers typically require only power, and can often be mounted in minutes using an adapter for the photocell sensor found on many lampposts.

802.11g is also used for inter-mesh communications along with 5GHz 802.11a or 4.9GHz (public safety only) radios. Tropos' deployments are unique in that the selection of the 802.11g, 802.11a or 4.9GHz bands is automatically determined by measured real time radio performance and constantly optimized along with the channel selection within the bands, radio transmission power, and data routing paths through the mesh.

Using PWRP, MetroMesh Routers self-organize when deployed, and continually monitor the quality of wireless transmissions to provide a performance-optimized, self-healing network.

The result is, for the first time, metro-scale Wi-Fi coverage that is reliable, has the highest throughput of any mesh technology on the market today, is scalable for deployments from campuses to entire cities, and is economical to deploy and manage.

Metro-Scale Wireless Video Surveillance Components

Open software architecture and standard IP data infrastructure allows the selection of best-of-breed, state-of-the-art video components for specific video surveillance applications. The following list is illustrative of commercially available products that have been compatibility tested with Tropos networks. The video security industry is moving rapidly, however, with new IP-based components being introduced regularly, and high quality alternatives exist in most of the categories. Because IP networking and its 802.11 wireless extension is universal, new products based on these standards will be readily integrated as they become available.



IP Cameras

The latest IP pan/tilt/zoom (PTZ) cameras, for example, provide the ability to read license plates or identify faces from hundreds of meters. Even specialist analog infrared imaging systems can be added to the system for zero-light, nighttime applications using easily interfaced, off the shelf digital converters. Specifications of some commonly used IP cameras are shown below:

| Camera | PTZ | Encoding/ Resolution | Interface | Sensitivity |
|---|---|---|---|--|
| Sony ¹ SNC-RX550N Outdoor Pressurized Dome Housing | 360° pan/90° tilt 312:1 zoom (26:1 optical) 2-way audio | MJPEG/MPEG-4 /H.264 up to 30fps @ 640x480 | Built-in Ethernet, Compact Flash Wireless option | Auto iris, auto focus, auto day/night modes (0.15 lux @ F1.6) |
| Sony SNC-RZ50N Outdoor Pressurized Dome Housing | 340° pan/115° tilt 312:1 zoom (26:1 optical) 2-way audio | MJPEG/MPEG-4 /H.264 up to 30fps @ 640x480 | Built-in Ethernet CF Wireless option | Auto iris, auto focus, auto day/night modes (0.3 lux @ F1.6) |
| Sony SNC-RZ20N Outdoor Housing | Fixed 216:1 zoom (18:1 optical) | MJPEG /H.264 up to 30fps @ 640x480 | Built-in Ethernet PCMCIA ports for Wireless 802.11b | Auto iris, auto focus, auto day/night modes (0.01 lux @ F1.4) |
| Axis ² 221 w/PoE Outdoor Housing | Fixed | MJPEG/MPEG-4 up to 45fps @ 640x480 | Built-in Ethernet External 802.11b/g Wireless adapter | Auto iris, auto focus, auto day/night modes (0.08 lux) |
| Axis 223D Outdoor Housing | 360° pan/90° tilt 420:1 zoom (35:1 optical) 2-way audio | MJPEG/MPEG-4 up to 30fps @ 640x480 | Built-in Ethernet External 802.11b/g Wireless adapter | Auto iris, auto focus, auto day/night modes (0.008 lux) |
| Axis 241 Outdoor Housing | 340° pan/120° tilt 216:1 zoom (18:1 optical) 2-way audio | MJPEG/MPEG-4 up to 30fps @ 640x480 | Built-in Ethernet External 802.11b/g Wireless adapter | Auto iris, auto focus, auto day/night modes (0.005 lux @ F1.4) |

Command and Control Centers

Today's state of the art Command and Control (C2) centers are entirely digital, leveraging the power and cost-effectiveness of off-the-shelf servers and workstations with the latest digital, high resolution display technology. Software-based video recorders and video wall controllers can be readily integrated with the latest video analytics software that dramatically reduces manual camera monitoring.



Going far beyond basic motion detection, the current crop of video analytics systems can automatically identify behavior patterns such as illegal parking in sensitive areas, loitering, and tailgating. The latest systems can zoom in and track targets automatically.

The same software provides sophisticated alarm management, and the ability to securely transmit live and recorded video images to any location on the network. Open interfaces allow ready integration with access control and other external devices and systems. The main C2 components include:



- Network Video Recording (NVR) software
- Video wall monitors
- Video wall switching software
- Video analytics software
- PC-based servers and workstations

Network Video Recording and Management

Although also used in single-server versions for single site operation, NVR software is now available that supports unlimited numbers of cameras, with an unlimited number of servers distributed among many network-connected sites. This feature allows, for example, a city-wide video command and control infrastructure to be set up in parallel with an existing logical C2 infrastructure.



Camera deployments for a particular district can be monitored by agencies responsible for that district, while aggregated "views" can be created for regional and central commanders for real time monitoring and recording access.

Each authorized user in the system can, depending on their security level, have access to any camera or group of cameras and can send or receive alerts based on a large number of parameters. They also have access to comprehensive, built-in investigation tools such as multi-camera synchronized playback, advanced searching, and secure video export for evidence presentation. Of course, using a metro-scale wireless network, these users may also be totally mobile.

On-Net Surveillance Systems (ONSSI)³ provides a next generation NVMS (Network Video Management System) system that incorporates a full function, distributable NVR, integrated with video wall switching, alarm management, and video analytics components. ONSSI supports hundreds of different camera models from dozens of manufacturers.

Next Generation Video Analytics

Large scale video deployments, consisting of hundreds or thousands of cameras, are impractical to monitor in real time with human assets. Video analytics is the ability to automatically identify objects and behaviors in real time, and to issue alarms when those behaviors are identified. This dramatically reduces the number of C2 personnel required, and is, in fact, the only practical way to monitor metro-scale deployments which are otherwise reduced to after-the-fact incident recording.

Agent VI⁴ is a next generation video analytics solution that works well with Tropos networks and other suggested recommended such as OnSSI's C2 software. The analytics capability is totally integrated with the NVR and video wall control









components, enabling analytic events to trigger C2 alarms, automatically display events on video walls, and "push" video streams to designated fixed or mobile users.

Agent VI uses a new "Image Processing over IP" (IPoIP) architecture which dramatically reduces network bandwidth and equipment costs. Conventional analytic systems are based on central or distributed servers which, because of the intense processing load required from the application, generally can only handle 1-4 cameras per server. The IPoIP architecture distributes much of the image processing to an agent running on the camera or local video encoder, allowing the central server to be used for object identification, vectoring and rule and event processing. Data rates from agent-equipped cameras are reduced to 20-60kbps during non-event monitoring, and the analytics server can handle over 100 cameras simultaneously.

Behaviors detectable using this system currently include:

- Person or vehicle moving into/out of an area
- Loitering
- Illegal parking
- Tailgating
- Leaving objects behind
- Removing (stealing) objects
- People counting (queues, crowds)
- Vehicle counting
- Camera/network tampering

Multiple rules can be sequentially processed, and multiple events generated. For example, a fixed camera can be used to monitor a defined security area.

A person entering that area (identified by size, shape and speed as a person), can generate an alarm which will cause a nearby PTZ camera to automatically zoom in on and track the person, while simultaneously switching the video wall to display the output from both cameras.

Deploying Metro-Scale Video Security Systems

Video applications can place significant additional bandwidth demands on any network for the following of reasons:

- The amount of data transmitted by a video camera is greater than with virtually any other device
- That data is normally transmitted continuously, unlike in an average Internet session where data is uploaded and downloaded in bursts with relatively long periods of low bandwidth usage between.

When delivering city-wide broadband Internet access, MetroMesh networks are typically designed to deliver client access data rates of 1-5 Mbps across the entire coverage area. Networks must be designed carefully if they are to be used for wireless data transmissions from cameras to the NVR server.



Video Data Bandwidth Requirements

Video security applications have fundamentally different requirements to the streaming video used to download video clips. For example, video surveillance images are rarely monitored live. Most video control rooms are used to monitor and record from multiple cameras, where viewing of each individual camera feed is impossible. The primary requirement of such systems is to record time-stamped, high quality individual images and, to do so, they rely on sophisticated event detection from on-screen movement, door alarms, infrared sensors, or intelligent video analytics.

Digital imaging emulates or extends all of the traditional analog video standards from CIF resolution (320x240 pixel equivalent), to 4CIF (640x480 pixels-VGA) and beyond. The ultimate desired result of most video surveillance sessions is a single, high quality image containing recognizable content at the moment an event occurs. The quality and resolution of that image is usually more important than recording flicker-free movement.

Motion JPEG (MJPEG) was the first image compression protocol developed for this purpose and is still in wide use today. It provides a continuous stream of individually compressed images at frame rates varying from 1 frame every few seconds to 30 frames per second (fps). Most IP cameras use MJPEG, but also offer MPEG-4 and perhaps the newer H.264 as higher compression options. For the comparison below, the starting point is MJPEG as the bandwidth required does not vary with the content of the image.

The data rate required to support an IP camera is dependent on three variables: image resolution, degree of compression (image quality), and the frame rate.

| Compression vs. Frame Data Size: MJPEG (Sony ⁵) | | | | | | | | | |
|---|-----|------|------|------|------|--|--|--|--|
| Image Quality Level | 10 | 7 | 5 | 3 | 1 | | | | |
| Compression Factor | 1/5 | 1/20 | 1/30 | 1/40 | 1/60 | | | | |
| Data Size (KB/frame) | 180 | 45 | 30 | 22.5 | 15 | | | | |

Most surveillance applications operate with a normally acceptable image quality index of 5 (30KB/Frame). At this quality index:

| Data Bandwidth vs. Frame Rate: MJPEG on Sony SNC-RZ30N | | | | | | | | |
|--|------|------|------|------|------|--|--|--|
| Frame Rate (fps) | 1 | 4 | 8 | 15 | 30 | | | |
| Required Bandwidth (Mbps) | 0.24 | 0.96 | 1.92 | 3.60 | 7.20 | | | |

Note: KB/frame = Kilo Bytes/frame, fps = frames per second, Mbps = Mega bits per second

For many video surveillance situations 2-10 fps is an adequate frame rate and, at the higher VGA resolution, is preferable to 320x200 smooth motion streaming



video at 15-30fps. At an often acceptable viewing/recording rate of 4 fps, each MJPEG camera on the network will generate a continuous data stream of around 1 Mbps. The higher data rates available with MetroMesh networks can enable higher quality images, higher frame rates (up to full motion video at 30fps), or more cameras supported on the same network.

The use of MPEG-4 or H.264 compression codecs can further reduce bandwidth significantly. These codecs work by updating only the changed parts of the image. If the subject is rapidly changing, such as with monitoring traffic at a busy intersection, bandwidth improvement will be marginal and may actually degrade. At the other end of the spectrum, for security applications with little on screen activity, MPEG-4 can reduce the throughput requirement by 50-90%. For many security applications using the higher compression codecs, a 0.5 - 1Mbps per camera bandwidth "budget" will deliver a frame rate of 8-15 fps – fast enough for effective PTZ control and a quality video stream.

Using Tropos MetroMesh for IP Camera Data Infrastructure

Because of the high continuous data transmission rates of the cameras, it is important to plan the network topology of a metro-scale video security system carefully. The following factors affect network data throughput and should be calculated carefully. Specific design recommendations are highlighted in gray.

Number of Cameras

Obviously the number of cameras directly affects the overall network bandwidth required. Although somewhat more expensive than the fixed devices, strategically placed PTZ cameras are often more capital cost effective if each can replace at least two fixed cameras. At a road intersection, for example, a single camera can patrol all four road directions and, importantly, requires only one fourth the data bandwidth of four fixed cameras.

- Use PTZ rather than fixed mount cameras wherever possible to keep the total number of cameras to a minimum. This will reduce initial capital expenditure and minimize network bandwidth requirements.
- Be realistic when matching video camera resolution, image quality and frame rate with the surveillance application. Factors such as careful camera placement, so that movement is towards or away from the camera, will make lower frame rates more acceptable for most applications.

Design the Wireless Mesh for Maximum Throughput

The maximum data rate for 802.11g is 54Mbps, with a maximum throughput of 27Mbps (each link is symmetrically bi-directional). In a metro-scale outdoor environment expect to see inter-node real data rates up to 20Mbps if the node density is increased by 50% over a "normal" public safety deployment used just to deliver broadband to mobile units.



Figure 4 illustrates a deployment using a mixed node density to increase throughput from the part of the network used to transmit video from the cameras. By increasing the node density by about 50% for the clusters around each camera location, the network can be designed for a throughput budget of, say, 2-3Mbps per camera cluster instead of 1Mbps at the standard node spacing.



Figure 4: Variable Mesh Density Optimizes Camera Data Rates

Actual throughput rates will vary depending on wireless topography and conditions. Each high density cluster must also have its own backhaul connection.

Also note that in Figure 4, each camera has been co-located with a Tropos unit and connected through its RJ45 sub-interface port. This has two important effects: it optimizes throughput, making the camera part of the self-healing, self-optimizing mesh, and it also effectively gives the camera a 4W (36dBm EIRP) client for improved data transmission.

- Increase the node density of the parts of the mesh used to transmit video data from the cameras. An increase in node density from, say, 15 to 25 nodes per square mile could increase mesh throughput rates by as much as 100%. Parts of the mesh only used for broadband coverage can be left at a standard density.
- Use only 802.11g clients for mesh access. A mesh with a mixture of 802.11b and 802.11g clients has to cope with clients at the lower speeds, slowing down the entire system.
- Wherever possible, co-locate cameras with the high powered Tropos nodes and connect directly to them through the Tropos sub-interface RJ45 port. This maximizes video data transmission rates and minimizes the number of wireless hops throughout the mesh.
- Where it is impractical to connect cameras directly to the Tropos nodes, use high-powered CPE devices rather than built-in Wi-Fi cards to wirelessly connect the cameras to the network

With a single band (i.e. a Tropos 5210-only network), self-interference reduces throughput for each additional wireless hop. The throughput drops to ½ at two hops, 1/3 at three hops and ¼ at four hops. Thereafter, the throughput can be expected to stay constant as self-interference does not extend past four hops. PWRP is particularly effective at constraining this multi-hop effect to very near the theoretical 1/n values, producing twice the throughput of other mesh systems. Note that wireless IP cameras create additional hops, adding to the 1/n throughput reduction. This final hop to the camera can be eliminated by connecting the



camera to the sub-interface RJ45 port on the Tropos node. When connected in this way to a wired gateway, all data loading on the mesh network is eliminated.

However, a dual-band Tropos network, using Tropos 5320 or 9532 mobile routers, mitigates the effect of multi-hop by optimized use of the second, 802.11a or 4.9GHz band for inter-node data transmissions. If the dual band routers are used carefully in situations where the higher frequency bands can be effective, i.e. with clear or near line-of-sight links between nodes, you can expect to improve internode capacity by up to 30%.

• If the topography allows, consider upgrading key parts of the network using dual-band 5320 or 9532 Tropos mesh routers.



Figure 5: Single Backhaul Connection

• Where possible, do not deploy any camera with more than two hops to the wire (including any wireless camera link).

Manage the Aggregate Network Capacity

The data rate of each camera is calculated from the required picture size, quality index and frame rate as described above. The number of cameras multiplied by the data rate gives the aggregate capacity requirement for the total network.

- It is not usually an option to use T1-level back haul connections for metro-scale video systems. At 1.5 Mbps, the backhaul will al most certainly become a bandwidth choke point.
- Use high capacity (10-45+ Mbps) point-to-multipoint or fiber backhaul connections throughout the network to avoid wireline bandwidth bottlenecks.

Over-Engineer Backhaul Provisioning

In general, networks configured to handle video surveillance traffic should have more backhaul capacity and gateway points than networks configured for Internet access alone.

Properly distributed additional backhaul delivers three important benefits:

- It increases the aggregate backhaul capacity
- It reduces the number of hops from each camera in the system
- It increases the number of redundant data paths, improving over all system resilience and reliability



Figures 5 and 6 show how the addition of an extra backhaul connection, and the direct connection of one of the wireless cameras, ensures that none of cameras has more than one wireless hop to connect to the server.



Figure 6: Additional Backhaul Improves Data Throughput

In this example, the extra gateway also provides routing redundancy such that no link failure would create more than a 2-hop alternate route. A pointto-point or point-to-multipoint WiMax or pre-WiMax wireless backhaul system is often used to economically extend the wired backhaul in a metro-scale environment. These work well with MetroMesh, providing high bandwidth (up to 45Mbps) at long range (10+ miles, in clear line of sight).

- Plan on over-engineering the backhaul for a Tropos network designed to support video surveillance cameras. An optimum metroscale video surveillance network topology will often consist of a number of small clusters of three or four nodes each, supported by backhaul distributed throughout the network.
- Design a system for consistent throughput, balancing aggregate and individual backhaul requirements, mesh throughput and desired camera performance.
- Consider using a wireless point-to-multi-point system to distribute fixed backhaul to the gateways.
- Consider upgrading key parts of the network using 5320 Tropos mesh routers to take advantage of the increased data capacity delivered by a dual-band deployment.

Take Advantage of Advanced MetroMesh Multi-Use Features

Tropos MetroMesh can be configured to be securely accessible by multiple groups of users and optimized for specific applications. Even if the video system uses a dedicated IP mesh infrastructure, these features can be used to tune performance on both sides of the application: the transport of video data from the cameras to the servers, and the distribution of live and recorded images to mobile users.

On the camera side, the objective is usually to collect forensic-quality data for evidence, which should be of the highest possible quality. For mobile access, images are sent to mobile responders to improve situational awareness. In this case, image quality takes secondary priority over effective, real time image delivery to multiple users throughout the coverage area.



Tropos MetroMesh has several features that help meet these requirements:

- A single Tropos mesh infrastructure can support up to 16 virtual wireless networks with unique SSIDs, each configured with its own security and authentication policies. For video applications, Tropos recommends separating the network connecting the cameras to the servers from the network providing access to the servers by mobile users. In public safety deployments, for example, the second network is often the same as that supporting the other mobile applications, with the same officer access and security procedures. Isolation of the video collection network ensures that all camera access is through the video server, and prevents unauthorized access to the cameras themselves. Support for multiple VLANs and cross subnet roaming allows painless integration with existing systems.
- MetroMesh supports bandwidth control and data prioritization by network (SSID), user groups (IP addresses), and applications (ports). This enables video applications to be set up with high priority, but also with throughput restrictions so that the cameras can coexist with other applications without hogging all the bandwidth.
- Consider advanced MetroMesh multi-use, virtual wireless network features when designing secure, optimized video security solutions.

Match Server and Workstation Hardware to the System Requirements

Video recording is processor intensive, requiring simultaneous multiple image encoding and decoding and database access. It is important, therefore, to choose PC hardware platforms with sufficient processing power and data storage.

Several camera and NVR manufacturers publish tools to calculate the processor and storage requirements, based on the number and types of cameras, resolution and frame rate settings, data retention times, and other factors. ONSSI has two useful tools for this purpose: a data storage calculator⁶ and a processor calculator⁷, both available on their web site.

• Calculate the processing and storage requirements of the video system based on expected data throughputs, and make sure the server and workstation hardware exceed them (over-engineer to provide an operational buffer, since additional computer hardware costs are not usually a significant part to the overall project costs).



Mobile Video Data Access

All current IP cameras have the capability to allow direct access of video images through a standard web browser from any PC on the network. In general, this is an undesirable way of distributing video around the network for several reasons:



Figure 7: Managing Mobile Data Access Bandwidth

- Each client accessing the network does so at the bandwidth defined in the camera, which should be optimized for high quality recording. In most cases this means at least an additional 1-4 Mbps data load for every client looking at the image. Since these clients are, by definition, mobile, planning the network loading (number of hops, backhaul throughput, etc.) becomes virtually impossible
- Normally the only way to record images is then on the client PCs themselves. This is undesirable from a data proliferation, and control viewpoint, particularly if the data is required to be formally collected, stored and backed up for evidence.
- It is difficult to apply standard, centralized data access control and security policies in such a distributed environment
- It is physically disruptive to allow key camera functionality such as PTZ controls to be available to many users at once.

PC-based video servers such as OnSSI's NetDVMS provide the functionality needed to centrally control data access and recorded assets. NetDVMS additionally has features that allow remote users access to live and recorded images through those same control mechanisms.

The remote access feature also manages bandwidth requirements by retransmitting the images in a lower resolution, compressed format such that the original 1-4 Mbps image now only occupies around 128Kbps, bandwidth equivalent to most standard Internet usage. This allows several mobile users to access the same video stream without overburdening the network.

Additionally, advanced functionality allows such images to be "pushed" to designated mobile PCs, allowing, for example, live video to be added to dispatch messages for officers attending an incident.

In general, mobile data access bandwidth requirements should be engineered to be similar to normal Internet usage. Be prepared, however for potential additional network loading created by mobile users congregating for specific events (at an emergency, for example).

Conclusions

The convergence of IP-based digital imaging recording and management, with Tropos' industry-standard wireless broadband infrastructure, has created a new class of video security applications on a scale that was previously impractical. It is now possible and economical to deploy video security solutions across entire cities and beyond.

A Tropos MetroMesh Wi-Fi network enables such solutions both in the provisioning of wireless backhaul for remote cameras, and in the distribution of live images and recordings to mobile units in the field. Mobile cameras, mounted in vehicles and other mobile mounting assets can also be incorporated into the surveillance system. With care, it is possible to design a MetroMesh network that meets aggregate data bandwidth requirements for high performance cameras and avoids data bottlenecks, while still delivering excellent service to other users of the network.

The availability of Tropos metro-scale Wi-Fi networks with the converging technologies of IP video and software-based video monitoring and recording has brought unprecedented economics to large-scale video security applications. Metro-scale video security is now an affordable reality.

About Tropos

Tropos Networks is the market leader in delivering metro-scale wireless mesh network systems with more than 800 customers in 30 countries around the world. The patented Tropos MetroMesh[™] architecture delivers the ultimate scalability, high capacity at low cost and great user experience demanded by enterpries and network users. Tropos Networks' unique expertise includes high reliability and performance mesh software development, mesh RF engineering, metro-scale network planning, deployment and optimization, and navigating the municipal approval process. Tropos Networks is headquartered in Sunnyvale, California.

For more information, please visit http://www.tropos.com, call 408-331-6800 or email info@tropos.com.

References

- ¹ http://bssc.sel.sony.com/BroadcastandBusiness/markets/10001/market_10001.shtml
- ² http://www.axis.com/
- ³ http://www.onssi.com/
- ⁴ http://www.agentvi.com/
- ⁵ "Sony Network Camera User Guide: SNC-RZ30N/RZ30P", 3-620-374-12 (1), p.24 http://bssc.sel.sony.com/Professional/docs/manuals/snc-rz30nuserguidev2.0.pdf
- ⁶ http://www.onssi.com/support/nvr.php
- ⁷ http://www.onssi.com/products/nvrs_recommended.php

©2003-2011 Tropos Networks, Inc. All rights reserved. Tropos and PWRP are registered trademarks of Tropos Networks, Inc. Tropos Networks, GridCom, and Metro-Mesh are trademarks of Tropos Networks, Inc. All other brand names, company names, product names, trademarks, and registered trademarks are the property of their respective holder(s). Information contained herein is subject to change without notice.



555 Del Rey Avenue Sunnyvale, Ca 94085 408.331.6800 tel 408.331.6801 fax www.tropos.com sales@tropos.com