Will Network Camera Continue to Shape the Future Security?

The future of wireless is an exciting prospect from the camera surveillance area

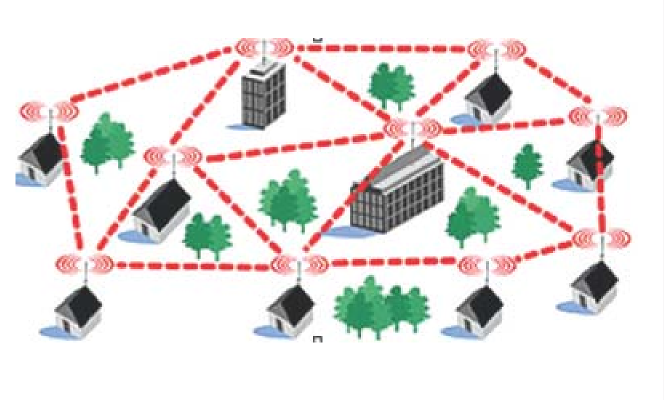
Tomorrows cameras will have RF devices built in with high gain antennas capable of 5km distances, compression techniques will improve to see high resolution images compressed to 1 KB. No hardware will be required at the control room apart from a dedicated Video server capable of processing hundreds of cameras simultaneously and displaying them on numerous large flat LCD screens. They are all happening very soon thanks to video over wireless IP.

By Douglas Grant MCSF, President, Advanced Networking Solutions

2004 will bring with it fascinating new technologies in the area of IP video surveillance, along with these new concepts will follow a greater acceptance of IP surveillance networks. The acceptance of transmitting video images over IP using RF (Radio Frequency) will definitely lead to the greater expansion of camera systems. In the past, RF gained a poor name in the CCTV industry with the use of 900 Meg Hz. This low frequency had the advantage of what some termed, “could bent around corners” or more correctly, NLOS (near line of sight). The energy pattern was able to follow the lay of the landscape and reflect some of its energy back into NLOS locations. The disadvantages were many unfortunately, poor bandwidth which caused the unacceptable delay in pictures being transmitted from camera locations. Of course the never ending problems associated with interference cause by other users in the area using the same frequency. We will not see these systems being implemented anymore thanks to the work done by the IEEE in the area of 802.11. Vendors have pioneered these new protocols into reliable transmission devices or nodes, which transmit the entire suite of TCP. Designing systems onto IP Networks has taken the guess work out of RF installations. In order to design and guarantee a deployment of multiple nodes and various cameras onto an existing network there are certain steps one must take to implement a high bandwidth link with reliable transmission of all IP packets. Lets take a look at a hypothetical situation with the obvious requirement to use RF rather than cable. The base station or the clients network access point is in Building A, the areas which require surveillance are 25 - 30 kms away in another building we’ll call B. There’s more, within 1 - 2 kms of Building B there are five other buildings all requiring the same level of surveillance as the rest. What do you do first? You might be asking yourself. The first thing you must do in a situation like this is to carry out a precise site survey. The Site survey will be the kernel of the design and every bit of work you will do from the time the survey is completed will be based on these findings. “So take care, and do it right the first time”

The Site Survey

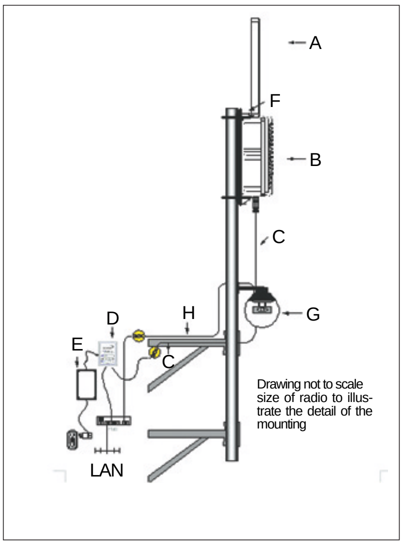
Armed with a good set of binoculars, a hand held GPS, a mirror, flashing light, a spectrum analyzer, good quality digital camera and a (15 meter lift



A hypothetical situation with the obvious requirement to use RF rather than cable (Photo by Advanced Networking Solutions) truck), we're off. I would possibly start at the base station and determine the height of mast required to achieve LOS (line of sight) directly to Building B or find a water tower or hill I could use to retransmit the signal if I could not see Building B. At each location a GPS reading is taken along with elevation, this information is recorded for publication of the survey report after all the data has been logged. The spectrum analyzer prints out a report of each frequency that could possibly be used in the licensed or unlicensed frequency channels. The next stop may be the water tower or hill if the Building B cannot be seen from the lift truck. If sighting is difficult I have someone at the distant site using a mirror or flashing light to get my attention. Before leaving the second location we should be able to determine LOS from the Base Station to the repeater site and Building B, if it is visible. Again all the data is recorded and once this is done we move on to Building B. At Building B we quickly find the highest point on the building and use a mast if required to gain the best possible LOS with either the repeater site or the Base Station using directional antennas. At this point we theoretically have connectivity with the Base Station over a 25 - 30 kms. The other buildings within 1 -2 kms require the same attention and all data must be recorded at this locations as well. If you got this far in one day you have done well, back at the office a site survey must be documented and published. This is the part of the exercise which takes the experience and Know-How to complete. The RF specialist knows that each link has the potential to transmit the maximum signal in regard to the EIRP (effective isotropic radiated power). It is a mistake to go over this power margin for any reason.

The Report

After the survey is completed the published version will document the topology of the network and explain the various methods used to transmit the IP packets back to Base. In some cases, a PTP (Point to Point) link will be used with mesh or a star configuration. File sizes have been taken into consideration with numbers of cameras used at each location. The specified design would accomplish real time viewing of each camera at any time. When multiple camera sites are used with large numbers of cameras a reduction in frame rate will have to be tolerated unless the budget for the project has taken this into consideration. The report will also list the antenna selection of each node location along with mast heights and adequate mast rigging. I have seen design reports that include two antennas from a single node, my response to this practice is very simple to remember, "Don't do it". When you attach two antennas to a node using a passive splitter you create a 3db loss to start with, which effectively halves your distance calculation. If one of the antennas energy pattern crosses the other you will experience more problems. Point is, when you are designing a network with wireless radios devices, design the system to function at the highest level possible, you will be pleased you did. Back to the report, as the client flips through the report they will be able to easily identify the links between buildings and see for themselves the antenna design and mast elevations. The radio frequencies are clearly listed with and channel noted that read interference from any other source. Another good practice in RF is to stay at least four channels away from any interference. This rule of thumb will keep your system from overlapping the other radio frequency and losing bandwidth from the interference. Once the document has been read and understood the deployment of radios can begin with the sound knowledge that it will achieve the maximum bandwidth if good trade practices are upheld and no additional losses are added to the system by using too much antenna cable or a poor quality cable with additional adapters.


A
F
B
C
G
H
D
E
C
LAN
Drawing not to scale size of radio to illustrate the detail of the mounting

Good trade practices are upheld and no additional losses are added to the system by using too much antenna cable or a poor quality cable with additional adapters (Source: by Advanced Networking Solutions)

I mentioned earlier the work the IEEE standards committee have done with 802.11 in regards to all the 802.xx protocols. It would be remiss of me not to mention that security is a huge issue with these RF systems. There are many radio devices to chose from within the industry and there are just as many using 802.11 compliant encryption techniques. This to me is a problem waiting to happen. The encryption used by 802.11 compliant devices is easily hacked these days and for this reason alone I would stay away from any radio that uses the 802.11 method of encryption. I am not suggesting you use an IP device that does not comply to 802.3 which is the physical ethernet interface side of the radio. I believe you should absolutely use anything but 802.11 compliant devices if you want security on your network. To date the most sophisticated encryption available is 128 bit AES (advanced encryption standard) below are a few questions and answers I have copied for your edification on this standard.

Once you do your research into the security of encryption you will possibly agree with my previous statement of how non-secure 802.11 devices really are. With these points in mind one can see how RF transmission of video images over IP will be readily accepted with little hesitation. Cost is not an issue here if the larger bandwidth is a requirement. The tele-communication companies of the world are demanding a huge cost for little BW (bandwidth) and are quickly being seen as not an option. Cabling over 20 kms is going to cost more so there are not many options left at this time leaving RF a practical means of deploying a surveillance system with the added advantage of linking other buildings up with the same radio system and creating a larger LAN (local area network) for the office. In Australia, we are noticing the upsurge of radio usage in the 2.4 Ghz range for longer distances and where 2.4 Ghz has reached saturation in CBD areas 5.8 Ghz is becoming a popular option. Local governments are using RF for traffic intersection diagnostics, City Councils are using the technology to expand existing or deploy new camera surveillance systems within the CBD and outlying areas. These systems are used to manage vandalism and problems associated with the upturn in crime. Other applications include ISP (internet service providers) using these devices as access points for clients requiring remote services to the internet. Police and military are using radios to set up instant networks for personnel communications on the ground. Similar tactics for camera surveillance by the Police in undercover situations are quick and easy to install and take down. These systems only take minutes to set up and are secure if high level encryption is used. The choice of monitoring and recording these IP wireless networks is yours to make. If the specification demands seamless connectivity into the existing switchers using video monitors, then IP converters are used to restore the analogue composite signal. New surveillance systems are designed with desktop management using the LAN to monitor the cameras at any workstation. No need to purchase DVR's anymore either, IP software will enable storage and management of all the cameras from a GUI (graphic user interface) on your desktop. The future of wireless is an exciting prospect from the camera surveillance area. Tomorrows cameras will have RF devices built in with high gain antennas capable of 5km distances, compression techniques will improve to see high resolution images compressed to 1 KB. No hardware will be required at the control room apart from a dedicated Video server capable of processing hundreds of cameras simultaneously and displaying them on numerous large flat LCD screens. I can see it all happening very soon thanks to Video over Wireless IP.

What is the Advanced Encryption Standard (AES)?

The Advanced Encryption Standard (AES) will be a new Federal Information Processing Standard (FIPS) Publication that will specify a cryptographic algorithm for use by U.S. Government organizations to protect sensitive (unclassified) information. NIST also anticipates that the AES will be widely used on a voluntary basis by organizations, institutions, and individuals outside of the U.S. Government - and outside of the United States - in some cases.

Who Submitted the Algorithm, and Where are they from?

The two researchers who developed and submitted Rijndael for the AES are both cryptographers from Belgium: Dr. Joan Daemen (Yo'-ahn Dah'-mun) of Proton World International and Dr. Vincent Rijmen (Rye'-mun), a post-doctoral researcher in the Electrical Engineering Department (ESAT) of Katholieke Universiteit Leuven.

Is there a Document that Provides Details on NIST's Selection for the AES?

NIST's ad hoc AES selection "team" has written Report on the Development of the Advanced Encryption Standard (AES). It is a comprehensive report that discusses various issues related to the AES, presents analysis and comments received during the public comment period, summarizes characteristics of the five finalist AES algorithms, compares and contrasts the finalists, and presents NIST's selection of Rijndael. Complete AES-related information is available on the AES home page, www.nist.gov/aes. The site includes NIST's Report on the Development of the Advanced Encryption Standard (AES); Rijndael specifications, test values, and code; all public comments, including analysis papers from the various AES conferences; and other "historical" AES information.