



MRV Communications

Video Surveillance Application Note

Zdraer@mrv.com





Table of Contents

| | |
|--|----------|
| INTRODUCTION | 3 |
| SURVEILLANCE BACKGROUND | 3 |
| VIDEO SURVEILLANCE AND IP..... | 4 |
| NETWORK PLANNING | 5 |
| MRV'S SOLUTION | 7 |
| MRV'S SOLUTION ADVANTAGES | 8 |
| SUMMARY | 9 |



Introduction

One of the major market drivers for lawful authorized surveillance and infrastructure protection was the 9/11 terrorist attack. In light of this tragic event, homeland security accelerated and endorsed privacy measures standardization/regulations.

The critical locations that were placed in the spotlight of surveillance were:

- Airports
- Train stations
- Military compounds and airbases
- Public "hotspots"

Each of the above-mentioned locations can be a potential to threats and requires situational awareness to the possible effective response of the relevant enforcement agencies.

Digital technology emerged as the ultimate facilitator for surveillance needs, which enables flexible, real-time, highly manageable and tunable solution. The purpose for IP/Digital surveillance is to provide constant real-time operational information, such as high-quality digital images, in order to maintain security and intrusion detection at the monitored locations. Digital surveillance covers numerous areas, including computer surveillance, telephone tapping and many more...

In this application note, we will focus mainly on video surveillance and its effects on network infrastructure and application planning as they are synthesized by MRV's networking solutions.

Surveillance background

Monitoring and "seeing through the walls" appear as an aided method for enforcement agencies to get remote technological eyes. In fact, the word surveillance in French means, "watch from above". This is exactly the outlook that is required for a distributed monitoring of remote locations, to get visual information from a central or any geographical place.

Video monitoring started as a simple method of black and white video feeds from remote cameras to a central monitoring location. The central location was attended by people and the analog recording was performed by cumbersome analog technologies. This was the basic start of what is known as closed-circuit television (CCTV).

Over the decade, CCTV became very popular and started offering collection surveillance by analog cameras connected in closed network via coaxial cables to multiplexing controllers, monitor TVs and video recorders. Traditional video surveillance had several technological limitations that were critical, and required adapting to new technologies in order to match the growing demand for video control, collection and processing of monitored information.

Historically, video quality was in low resolution, reflecting unrecognized objects that were transported over coaxial cables that were limited in bandwidth and distance reach. Video was stored as an analog signal on magnetic tape. Magnetic tapes had many operational problems, like constant tape changing, cumbersome information retrieval and very limited remote access. Around the time when the well-known hard drives entered the market as a digital-format replacement for analog video, it became feasible to also begin storing and using video in digital form, and its integration with IP technologies began to emerge.

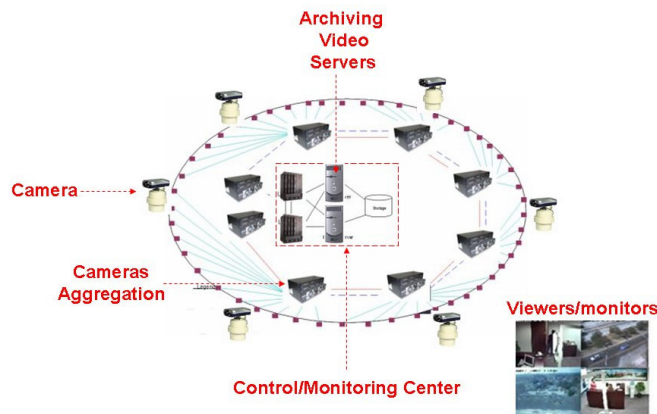
Video Surveillance and IP

IP technology over Ethernet infrastructure, combined with digital video, resolved the operational and technological limitations faced in traditional analog CCTV systems. In addition, it is affordable and cost-effective for mass and customized deployments.

The concept of video collection and monitoring remained the same, but it made possible the use of IP and Ethernet transport to carry excellent video quality and to be securely extended to any distance and managed from anywhere.

A Video over IP application consists of the following five main building blocks:

1. Remote digital IP cameras or analog cameras with an attached digital encoder
2. Archive video servers for digital recording
3. Monitor stations (viewers)
4. IP/Ethernet infrastructure



IP as a dominant widely applicable protocol used across all network building blocks and that offers an interconnection protocol, which can be used on all interfaces and at the application level.

The application level enables flexibilities like remotely control cameras, easy export of images, connecting to archived information for reviewing based on a simple date/time entry and integration with other intelligent/pattern recognition systems.

The evolution in video monitoring and IP technologies created possibilities of high quality pictures with lower bandwidth consumption. High quality for surveillance means that transported pictures that are monitored by viewers display sharp crystal clear visualization of what is going on at any given location. In fact, the fundamentals of such concept is the well known MPEG digital standard.

MPEG is an international standard that defines the compression technique of analog video signals with very high-resolution quality. MPEG performs the streaming feeds from remote cameras into digital streams. The use of MPEG video codecs permits the usage of a compression that reduces the bandwidth required to transport the video and control signals, and thus offers a more cost-effective solution of bandwidth transport. The MPEG digital streams interface with the IP network and transmit the streams to the archiving servers at the monitoring/control center for logging and database manipulation. At the control center, the monitoring stations (viewers) can select any camera remotely and control its monitoring attributes, or access archived data for inspection of historical recorded events.

Network Planning

Advances in networking technologies and video codecs have made it possible to extend deployments on existing shared or private LANs. However, an IP enabled network should be planned keeping the following characteristics in mind:

1. Secure network
2. Predictable and controllable QoS
3. Elastic bandwidth for future growth
4. Reliable and redundant

Security

Network planning in terms of security implies management and the transmission of data to all the network elements that should be secure and protected for access of authorized staff only. This includes the centralized management of user authentications based on the RADIUS protocol and protection against malicious attempts to manipulate configurations on the network. Each network element, whether it is a camera, a server, a monitoring station or any other Ethernet electronic device, can be provisioned with a Media Access Control (MAC) security restriction. This method offers the possibility to configure the permitted MAC addresses of relevant allowed surveillance devices and to block any other spoof attempt at the switching port level. This option takes extensive administration resources, but is considered proven against hostile attempts to connect with portable Ethernet sniffing equipment.

A surveillance network should be isolated from other networks by logical and physical means. A logical separation can be based on technologies like Virtual LAN (VLAN), or by assignment of private IP addresses that can't be routed to external networks or public Internet. If a connection to the remote network is required, management traffic should be encrypted to avoid sniffing management packets. Physical isolation can be based on wavelength separation that implies using a completely different wavelength on the same physical fiber that serves on the surveillance network and enterprise networks. Such physical layer segregation is considered very secure against attempts of eavesdropping.

Assignment of IP addresses to cameras can be based on dynamic IP allocation (DHCP) or static allocation; the latter method is preferable because it allows for aliases necessary for tracing and logically control of network sites.

Quality of Service

Video streams and control traffic should be delivered in real-time and cannot suffer bandwidth spikes and any other unpredictable network behavior. Minimizing surveillance service interruption means that we have to configure certain rules on the network flows so they will get the highest/strict treatment with low-latency from all cameras towards the monitoring stations and archiving/logging video servers. Video traffic consumes bandwidth and we should take into consideration what video codecs are used, and how many cameras we have in our network. The highest the resolution required, the higher the bandwidth that will be consumed by each camera. The different resolution levels of digital video are usually expressed in terms of CIF (Common Intermediate Format) and correspond to certain levels of bandwidth consumption. The bandwidth can vary from a few hundreds Kbps to 3-4 Mbps and is noted by camera's/codec vendor. This size of bandwidth should be multiplied for each camera and be calculated for the overall number of cameras in the network. Network bandwidth should have 20-30% bandwidth margin to enjoy optimized resources and network overhead that includes all concurrent video streams.

Note: Along video traffic, we should calculate the management and video control traffic that generally consumes very low bandwidth, but should have its ensured end-to-end path with its relevant QoS policies.

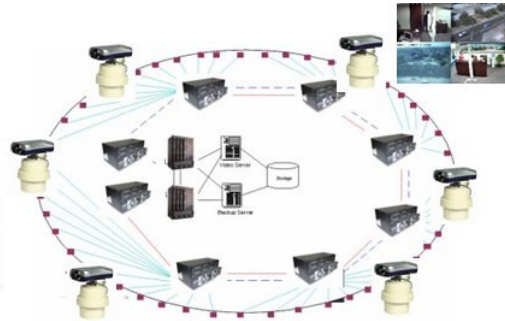
Bandwidth - future growth

Today's application status is that on one hand the optical technology has tremendous future-proof transport and on the other, video technology evolves towards lower bandwidth consumption over IP, along high resolution pictures with compression ratios that can be easily optimized upon demand. However, a preferable network environment should be one that is scalable, non-blocking and will fit various enhancements and flexibility for internal applications like database backups/replications or any other transfers that can consume enormous bandwidth loads. Accordingly, in an IP/Ethernet design, all the network ports can be shifted from 10 Mbps to 100/1000/10000 Mbps upon demand. This can literally satisfy any large size surveillance network.

Reliability and redundancy

A proper network design determines the level of network survivability. The infrastructure should be treated as real-time critical and, as so, this will imply enabling redundancy of the central monitoring facility and networking devices at device and link level. Recovery time in case of network failures should be minimal at less than 1 second and in several topologies less than 50 msec.

- **Security**
- **QoS**
- **Bandwidth - future growth**
- **Reliability and redundancy**



MRV's Solution

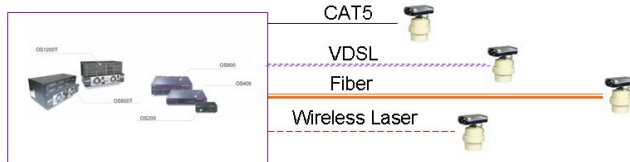
As the industry completely migrated towards IP/Ethernet infrastructures, an end-to-end digital network solution means a simple, cost-effective and versatile solution. MRV's solution offers scalable and intelligent architecture with hardware expansion capabilities to support the transmission, switching and distribution of digital video, control and alarm signals for surveillance applications.

MRV offers superior security, QoS and manageability over optical, copper, wireless connectivity and aggregation layer from remote cameras as well as other various sensors that can be deployed for control and alarm, based on IP/Ethernet.

The infrastructure can be based on several variants or a mix of them:

1. Optical fiber
2. Copper CAT5/CAT6 cables
3. Copper CAT3 old telephone cables
4. Wireless Optical Laser broadband (Free Space Optics)
5. Power over Ethernet for IP cameras and sensors within 100 m distance

Ethernet Aggregation for video pictures from IP cameras or any other signals from sensors



Each method has its own characteristics that can be convincing, based on field and application requirements.

Copper cables in existing infrastructure can be used either as CAT5/CAT6 cables for 10/100/1000 Gbps transmission and distances of up to 100 meters.

Telephony CAT3 cables can be used as transport for VDSL technology over Ethernet with bandwidth up to 15 Mbps and distance extension up to 1500 m. The VDSL technology has the advantage of preserving existing telephony transmission in parallel to video surveillance, thus saving rollout of new cables. In addition, this method can be used for fast and "silent" assignment of remote cameras at required monitored sites.

The optical fiber advantages include distances up to 100 km from the control site; the bandwidth grows up to 10 Gbps; it is highly secure against tapping and immune to lightning. In fact, the optical technology protects the surveillance infrastructure over the years against obsolescence, and ensures a lesser cost for system extension and maintenance. For example, the fiber can be used with wavelength separation services for security or higher utilization of bandwidth on one same dual or single optical strand.

The wireless laser technology has the same characteristics as the optical fiber transmission, but with distance limitation and line of sight requirements. Distances vary between a few hundred meters to 2-3 km, depending on weather conditions.



Power-over-Ethernet (PoE) eliminates the need to run 110/220 VAC power to video cameras or any other surveillance devices on wired CAT5/CAT6 cables. The use of Power-over-Ethernet switch requires running only a single CAT5/CAT6 Ethernet cable that carries both power and data to each device. This allows for greater flexibility in the locating of the surveillance devices and significantly decreases installation costs.

For outdoor installations in harsh environments, MRV offers a special solution to address temperatures between -25°C/-13°F to +65°C/149°F. Our solution can be based on outdoor cabinets that can control environmental status, or equipments specifically designed to handle extreme environmental requirements.

For remote out-of-band management in a surveillance network, MRV offers remote control, alarm and conditional activation of actions. This capability can be applied onto IP/Ethernet or secure out-of-band access in order the set the following:

1. Remote power control - restart video archiving servers or any other element that is plugged into an AC or DC outlet
2. Remote alarms from sensors/circuits and predefined alarm or actions - includes door opens, safe unlocks etc.
3. Remote Ethernet to RS-232 management - Control of Archiving servers and other RS232 elements

MRV's Solution Advantages

MRV offers an IP based infrastructure for surveillance equipment that tremendously facilitates operation and maintenance.

MRV offers a comprehensive solution for various infrastructure requirements and a modular design for maintainability. Our products offer small form factor design to save rack, cabinets or other hosting appliance space and can be installed in extreme environmental conditions.

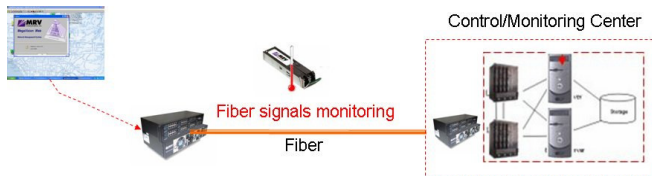
We offer unique infrastructure monitoring tools to assist in network stability and maintainability by point-and -click element management via MRV's NMS MegaVision software. A surveillance network can be logically monitored at the data layer and at the physical layer and can be equipped with physical layer infrastructure control offered by two unique feature components:

- Optical monitoring to predict fiber and transceiver aging
- Copper Time Domain Reflectometer (TDR)

Optical monitoring supports SFP digital diagnostics (SFF-8472), providing an optical monitoring tool for accessing a number of real-time SFP operating parameters. The information provided by the digital diagnostics, along with alarm and warning thresholds, enables the network administrator to identify potential problems in optical transmission and take preemptive action before any service outage actually occurs. A real life scenario can be an occurrence of a hostile attempt to tap optical fiber. This attempt is followed by the cutting of fiber strands and connecting a tapping device in the middle for sniffing purposes. In such a case, the system will detect optical disconnection and will send an alarm. Remotely, we can inspect optical signal reduction by optical monitoring due to a tapping connection and then activate the relevant procedures for other teams to trace the location and eliminate the tapping.

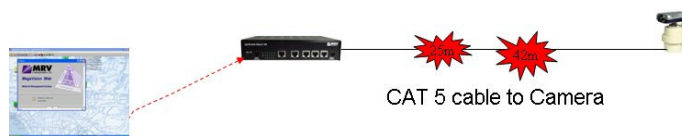


Video Surveillance Application Note



Copper TDR is a special tool that uses the time domain reflectometry (TDR) to diagnose cable and link problems on copper ports that are connected to cameras or other surveillance devices. Because the L1/L2 aspects of Ethernet are closely coupled together, it is often not possible with today's Ethernet equipment to isolate a layer at which a problem has occurred. In many cases, this results in an attempt to fix the problem without really knowing what/where it is and sending technical staff to remote locations. A good example of such a necessity is a scenario in which a remote camera that monitors an electronic fence is connected via a 100 meter copper cable to an aggregation switch in fiber distribution. The objective of this sophisticated tool is to better manage and troubleshoot Ethernet circuits of the last 100 m of the 100TX copper line and to offer a simple tool with which we can remotely analyze the copper lines and get a clear status of the following possible problems:

1. Report of cable shorts
2. Cut on a cable and its location
3. Impedance problems (connectors or bad quality cable)



Monitoring the network is an essential part of the MRV's overall solution that reflects a holistic approach of "watching from above" over all the layers with extensive capabilities to operate, manage and troubleshoot an Ethernet-based surveillance network.

MRV's flagship is to offer a modular concept solution to address network changes and maintainability. Such a concept offers a mix of technologies on the same platform with a richness of surveillance service delivery on isolated or converged networks. The product lines support superior QoS, security ACLs, bandwidth provisioning, remote traffic monitoring, alarm reporting and configuration intelligence.

Summary



Homeland security is getting its significant pace into IP networks infrastructure that can be either solely dedicated to surveillance, or consolidated with existing IP infrastructure and segregated for security. Planning and understanding surveillance components is critical groundwork for a successful and creative deployment.

MRV's solution facilitates the design and implementation of surveillance applications with comprehensive infrastructure intelligence. Our solution is offered with standard non-proprietary techniques, field-proven experience in surveillance deployment and transcended services.