Alternate Approaches to Implementing Closed Circuit Television Traditional surveillance (CCTV) cameras are usually connected to a monitor by means of dedicated coaxial cabling. If a multiplexer is added, it?s then possible to display images from several cameras on a single monitor. It is also relatively easy to add one or two more monitors within a building. But viewing images from additional outside locations becomes progressively more complicated, because dedicated cable is required to add a new monitor or camera to any existing system. What?s more, CCTV users must always consider how to store the large quantities of magnetic tape that result.

In contrast, network cameras are designed with built-in video servers and Ethernet connectivity, enabling their images to be viewed from any computer connected to a local area network, over a private intranet, or even the Internet. A network video camera can be configured to provide the entire Internet community with access to its images via a web site, or conversely to provide restricted viewing access to a limited number of authorized people.

Why use networked video over IP technology? Because it makes it possible to access up-to-the-second images at any time from any computer anywhere. The images can be stored at remote locations for convenience and/or security, and the Internet can be used as carrier for the information. A camera can be placed almost anywhere. There are no limitations tied to physical inputs or frame grabbers; the product can be connected to a LAN, xDSL, modem, wireless adapter, or mobile phone. Network video images can be received from any location that calls can be received on a mobile phone. And network video technology is highly cost-effective, since it doesn?t even require a new PC to make the camera usable. Any existing computer can be used for viewing video images; there is no need to buy dedicated video monitors. With an existing network infrastructure capable of video transmission, no separate coaxial video cables are required.

Example Applications *Remote monitoring* Network video is useful for thousands of applications. Simply attach a camera to an existing IP network and view live video on a PC with an Internet browser. Use network cameras in schools to see who is in the hall, computer room, lab, or cafeteria. Install it at manufacturing plants to see that production is running smoothly, and that the machinery is performing as it should. Or remotely monitor and record images from

multiple retail outlets to protect staff and assets

Security surveillance False alarms present a big problem to security systems. Network cameras enable alarms to be checked and confirmed from anywhere before action is taken. They are as equally well suited to taking snapshots of people passing through a door, as they are to being used in sophisticated biometric systems with dedicated application software. For example, a security guard who has been alerted to a break-in can get a view of the room where the break in has occurred by checking video images sent to his wireless PDA. Then he knows whether or not it is safe to enter. With network video products there is no longer any need to worry about changing (or forgetting to change) tapes in time-lapse recorders. And because images are stored on hard disks instead of VHS tapes, any old unwanted images can be erased automatically. The ability to deliver live high-quality images and sound also makes network video ideal for improving school and campus security. In combination with a security firewall, network cameras can be quickly configured for securely monitoring hallways, classrooms, and parking lots.

Broadcasting images over the Internet is a great way for companies to promote their services, and to provide customers with upto- the minute information. For example, cameras transmitting video of a ski station show the weather conditions on the slopes. People can check these by browsing the Internet before leaving home. Live video? whether it shows images and sounds of a bustling city, a busy university, or the beauty of a mountain, beach, or forest?can make a web site attractive, dynamic, interesting and worth a return visit. With HTML (Hyper-Text Mark-up Language) it?s easy to create web pages, web sites, or home pages that display images from network cameras

Network Video Use in Market Sectors ***Education*** Educational establishments are increasingly using network cameras to monitor and protect staff, students, and property. Surveillance and remote monitoring of playground areas, corridors, halls, and classrooms are easy to achieve. It?s even possible to give parents limited, controlled access to let them monitor their child in the school environment.

Banking Bank branch offices are often small and geographically dispersed. A network video system offers the major advantage of enabling security personnel to view from a central location images from every local office. The administration of a network video system is simpler and less labor intensive than CCTV. Images are stored on computer hard disks? employees do not have to change and take care of video tapes. Using a network video system also makes it possible to quickly provide emergency services agencies with photos that can help them identity and apprehend suspected criminals.

Industrial Manufacturing lines, industrial and pharmaceutical processes, automation, warehouse, and stock control systems are just a few of the many industrial applications that network video can monitor effectively. This ?virtual set of eyes? can greatly improve efficiency at a production plant.

Retailing The use of network video for security and remote monitoring purposes can help keep store owners better informed, prevent theft, and improve store management efficiency. Images from stores from various locations can be accessed from a chain?s headquarters at any time over the IP network. Cameras can also be deployed quickly in stores to monitor consumer behavior and to improve the impact of merchandising efforts.

Advantages of Video over IP Solutions In comparison to legacy video monitoring systems, IP-based video cameras can dramatically impact the total cost of ownership while delivering enhanced features and flexibility. They offer the following advantages:

- Lower infrastructure costs?converged networks use a single cable infrastructure and

component equipment, typically less expensive than legacy CCTV systems; separate support and maintenance contracts for dedicated coax CCTV network can also be eliminated

- Scalability?changing camera placement or adding new cameras can be accomplished with relative ease.
- Integration with other applications?many related technologies, such as building access control systems and biometrics, can be supported by the same network infrastructure

- Digital storage?digitally recorded images are not prone to degradation, are easily stored on computer hard drives, and take up less space than traditional and less reliable VCR analogue magnetic tape cassettes. Digital images are easier to index, archive, search, and retrieve for fast access
- Remote accessibility?camera access can be made available to any authorized user at any place within an organization?s IP network; in the case of a special event, a wider community can be given access via the Internet

Installation Considerations There are several key factors that should be considered before implementing a video over IP solution for surveillance cameras:

- power delivery
- IP addressing
- bandwidth

Power Delivery The majority of networked video cameras utilize an external power supply to provide the low voltage (typically between 12 and 24V DC) from the AC main supply. Given that the majority of cameras will be physically installed in hard-to-reach places such as ceiling corners, supplying easily accessed power can be a significant problem.

There are innovative technologies that can address this issue. Of particular benefit is IEEE 802.3af Power over Ethernet (PoE), which enables a single UTP cable to supply both DC power and Ethernet connectivity to the camera. If the networked camera does not support this type of power delivery, then small external ?splitters? can be used to channel the PoE-enabled connection to separate traditional data and DC power connections.

There are two methods for providing Power over Ethernet.

1. Use a PoE-enabled switch such as the 3Com Switch 5500 to provide LAN switching and power over the same connection.
2. Use a ?mid-span? PoE device that sits inbetween an existing data-only switch and combines the data with the provision of DC power. For new installations, a PoE switch provides a lower cost of acquisition and requires less space in the wiring closet.

If PoE is the chosen power delivery method, then a single network cable is the only connection required from the network camera back to the switch / mid-span PoE device. If there is a nearby Ethernet cable already in place, it is possible to use small in-wall mountable devices such as the 3Com Intellijack? switch to increase the density of ports and provide PoE forwarding. These switches are powered via the PoE feed. If PoE is not selected, then a suitable local source of main AC power will need to be provided for the networked camera?s power supply.

When the networked video camera is to be connected directly to a wireless local area network (WLAN), but does not have an inbuilt WLAN capability, an external ?client bridge? can be used. WLAN and IP cameras are ideal for quick installation of a temporary or ad-hoc video system.

IP Addressing Network video cameras are IP devices and as such require defined IP address properties to participate in the IP network. It is common practice for client PCs and devices to have dynamically allocated IP addresses using a network service such as Dynamic Host Configuration Protocol (DHCP). A DHCP server (or software service running on a device within the network) allocates IP address properties from a pool of free addresses when requested by network devices wishing to join the IP network. DCHP servers typically supply IP addresses for a single IP Subnet.

While DHCP is a very useful network feature that reduces IP administrative overheads, it is recommended that cameras use fixed IP addresses for fast and consistent address accessibility. This fixed IP address can be manually configured within the camera, It must be removed from the pool of addresses available to any DHCP server to eliminate the chance of duplicate IP addresses appearing in the network. Where the DHCP server supports mapping of the camera?s Ethernet MAC address to a fixed IP address, the DHCP server can handle the IP address assignment.

The majority of networked cameras can be managed remotely, typically with a webbased or a command line interface, using a telnet session or SNMP (Simple Network Management Protocol). To prevent unwanted configuration changes within the device, it is highly recommended that the default administrator password be replaced. To further boost security, the web-based management can be reconfigured with a nonstandard TCP port (HTTP Default Port is 80), preventing the loading of a web browser session and even an administrative management login. For still further safety, the cameras can be placed on a separate virtual LAN (VLAN). A ?Camera? VLAN can be completely isolated from the regular users of the network or made visible only to defined devices within the main network by using intra-VLAN routing and Access Control Lists (ACLs) on a Layer 3 switch or router (See Figure 1). And when the camera is connected to a managed PoE switch, it?s possible to remotely re-set the camera or turn its power on and off?greatly enhancing management and control.

Bandwidth Though the amount of bandwidth utilized by a network camera is dynamic, it is closely influenced by the image frame size, rate, and amount of image motion, as well as by the video compression algorithm used (e.g. MPEG or Motion JPG). The more detailed the image and rapid the refresh rat, the greater the bandwidth requirement.

Transmission speeds are measured in bits per second, 8 bits making up one byte. To transmit one byte, approximately two extra bits are needed for control. This means that approximately 10 bits are required to transmit one byte. Table 1 on the following page illustrates some possible transmission rates.

In single-site local area network installations, technologies such as wire-speed 10/100/1000 switched Ethernet can deliver the raw bandwidth demanded by high-resolution, full-motion video. However, where other critical applications co-exist on the same network infrastructure, consideration should be given to identifying and controlling the differing applications and classes of service to ensure application performance is not impacted by network loading.

When deploying networked video cameras across a network supporting multiple applications, it is important that the camera traffic can be identified by the network infrastructure and given priority to ensure good performance even under high network loads. This concept of building an intelligent network infrastructure to differentiate between applications can be achieved in two steps:

1. Identify each packet from the network cameras as it enters the network? configure the cameras to use a TCP port other than the typical default?TCP 80 (HTTP/web). A packet analysis tool can be used to identify which TCP port numbers are currently in use.
2. Mark the packet with a priority tag. Using edge switches that support Layer 4 features, insert a Quality of Service (Q0S) tag?the IEEE 802.1P standard defines eight levels of priority. To select an appropriate level of priority, take a holistic view of all key applications using the network, then allocate them into definitions as shown in Figure 2. It is suggested that the priority for network camera applications be set above that of any critical data applications, but below very time-sensitive application such as Voice over IP. This type of telephony requires predictable, rapid network response, though not particularly much bandwidth.

Once these two steps have been completed, the network infrastructure can recognize and differentiate the video camera traffic and ensure great application response. 3Com simplifies the defining of Class of Service policies with tools such as the Prioritize Network Traffic Wizard within its network management platforms. Such tools guide the network administrator through five steps to define and mark applications to be prioritized. The tool then ?rolls out? the quality

of service policy to the Layer 4 aware edge switches across the network.

Wireless LANs Radio-based WLANs are broadcast based and do not currently have the ability to enforce QoS. As at the time of writing the proposed IEEE 802.11e standard for WLAN QoS is not expected to be ratified before September 2005, other methods can be used to isolate the video traffic within a WLAN. Figure 3 provides some reference data to help select an alternative.

In cases where there is an existing IEEE 802.11b or 802.11g WLAN deployed for mobile access to data applications, a separate 802.11a based WLAN can be built to carry the video camera traffic. While IEEE 802.11a WLANs are typically more expensive than their 802.11b/g counterparts that operate in the 2.4 GHz frequency range, they use a 5 GHz frequency range that is normally less ?crowded? with other signals and often capable delivering better performance (see Figure 3). When the IEEE 802.11e WLAN QoS standard is implemented, it will become viable to deploy video cameras on 802.11g WLANs for lower implementation costs and co-existence with existing data applications and mobile user clients.

Wide Area Networks For installations that span multiple locations connected through a WAN, it is suggested that the WAN routers also be configured to prioritize the video camera traffic. Many modern routers have the ability to understand the IEEE 802.1P priority tag from within the Ethernet frame and map/translate it to a Layer 3 prioritization scheme such as IPTos or DiffServ. Such a configureation will ensure a high WAN priority level for video streams from remote located cameras? particularly important since WANs typically run at high levels of utilization and are comparatively slower than LANs. Due to the relatively smaller bandwidth available across WAN links, multisite implementations may require a choice between optimized image quality or bandwidth usage. By enabling cameras to send only images when motion is detected in a user-defined area of the video frame, the amount of network bandwidth required?as well as the image storage requirements of the video camera management application?can be dramatically reduced.

Internet and Virtual Private Networks When cameras are located at remote sites connected by the Internet, it is common for the Internet router/gateway/firewall device to provide a Network Translation Service (NAT). NAT enables a private IP addressing scheme in the remote LAN while presenting a single public IP address to the Internet (see Figure 4). This service disallows direct connection to the private IP address of the remote site camera(s). To address this limitation, an organization can have its ISP allocate a Static Public IP address and configure the NAT service so that different port numbers of the public IP address are ?mapped? (assigned) to the respective IP addresses of the cameras. For example, 10.10.10.243:8080 will access the LAN Private IP address 192.168.1.101.

To restrict direct Internet access to the cameras, a Virtual Private Network (VPN) should be established between the broadband router/gateway and the main site Internet router. The VPN forms an encrypted link between the two locations on the same network. When using VPNs to connect/remove sites via the Internet, there is no requirement to configure NAT mapping of public/private IP addresses and TCP ports. The one caveat to VPN use in this situation is that, if networked cameras utilize IP Multicast to broadcast video streams, the majority of VPN protocols do not natively support multicast applications.

For customers with switched without layer 4 classification features, an alternate technique to segment and control video camera traffic is to attach cameras to a dedicated VLAN. VLANs can be defined on the edge-switch ports where the cameras are directly connected. The video camera management application can either be directly connected to this ?video VLAN? in the case of an autonomous system, or it can be connected to the default VLAN. In the latter situation, a Layer 3 switch or router that handles the day-to-day application traffic and routing between the video VLAN can be used. If this last option is employed, consideration should be given to prioritizing the video VLAN within the main network infrastructure.