IP Networking

Options and Considerations

SYNECTICS

Migrating to IP and Maximizing Infrastructure

Migration to IP, and introducing new technologies such as high-definition cameras, is the dominant surveillance trend across most sectors where security and mission-critical decision-making are a priority.

What many organizations might not realize is that existing IT infrastructure may not be fit for purpose without modification. Another consideration is when a poorly designed network infrastructure that does not reflect surveillance objectives can negate any quality and performance benefits afforded by investing in new IP-based cameras and software solutions.

Issues caused by poor network design can include: network failure/unreliability, image quality and latency/drop out, therefore negatively impacting other mission-critical systems. To avoid falling into this trap there are several key areas to consider that are discussed in this technical paper.

What is an IP-based Surveillance System?

With an IP-based surveillance solution, video is captured and converted to digital data (by the camera itself or via video encoders) and transmitted through an IP network. Any IP device can transmit data on the network as long as it has access. This access is typically achieved using a wired connection. However, wireless is popular in small-scale/domestic applications and fiber or wireless backhaul links are also often used in high-distance/high-speed applications.

IP-based surveillance offers several important benefits including:

IMAGE QUALITY
HD/megapixel IP cameras offer far superior resolution levels for detailed image capture. For example, a 2.1 MP IP camera – considered a basic level IP camera – has resolution four times higher than a standard analog camera.

A white paper detailing camera trends and capabilities can be found at https://bit.ly/46mFU9B.

COST EFFICIENCY
Using an existing IT network to operate a video surveillance system is more cost- and resource-efficient than running a separate standalone network in tandem with existing IT infrastructure.

SCALABILITY
With analog systems, video is transmitted from the analog camera to a DVR using a coax cable, at which point the data is converted into digital information that can be stored and reviewed. The problem with this is that each DVR only has a finite capacity in terms of the number of cameras that can be 'plugged in'. Scaling up to accommodate changing needs by adding more cameras will therefore necessitate disruptive and expensive investment in physical infrastructure. With an IP-based solution, any number of cameras can be added easily to the network, in line with enterprise requirements without the need for cameras to be physically cabled to DVRs (as they only need to be connected to the closest network switch).

REMOTE/MULTI-LOCATION VIEWING
Linked to scalability, IP-based surveillance solutions also offer greater flexibility in terms of where footage is viewed. This is because information can be transmitted over a WAN or a secure VPN via the internet to/from any connected site.

DATA MINING
An IP-based surveillance solution provides the opportunity for more sophisticated data integrations and analytics. Using an open-protocol video management system or command and control platform, data from any device on the network (visual, audio, numerical) can be collated, interrogated, and used to proactively identify a wide range of threats relating to security, safety, or efficiency.

Can any Legacy Analog Equipment be Used?

Having an IP surveillance network does not preclude the use of legacy technology such as analog camera solutions. This is an important point as it allows existing system assets that remain of operational use to be retained.

Network-based encoders, ideally suited for centralized or edge encoding of analog video data, can be used to convert analog data to a digital video signal. This data can be viewed using an integrated, open-architecture video management system, and recorded on a variety of network-attached storage solutions such as primary and hot standby storage.

Key Considerations for Network Infrastructure

In order to achieve these benefits it is important to be aware of several key elements relating to network design. Failure to do so can result in poor performance and ROI.

Connecting cameras with storage

With an IP-based surveillance solution, video is transmitted to an NVR which processes the information and often distributes data for monitoring (viewing client station) and potentially deeper storage such as an SAN. How this data is transmitted between points is hugely important as some options may not be suitable for the surveillance objectives.

There are three main transmission modes – TCP IP, UDP unicast, and UDP multicast.

TCP/IP

This is the most reliable method that requires a point-to-point connection. It orders data packets in sequences and uses a retry mechanism to ensure the receiving storage devices 'know' if any information is missing (and will resend accordingly until the sequence is complete). A negative for this method is that the point-to-point aspect makes it unsuitable for solutions that require multiple clients to view data from a large volume of cameras. Image latency can also be an issue. However, for small networks with no requirement for real-time viewing, this remains a valid option to achieve reliability over potentially unreliable links.

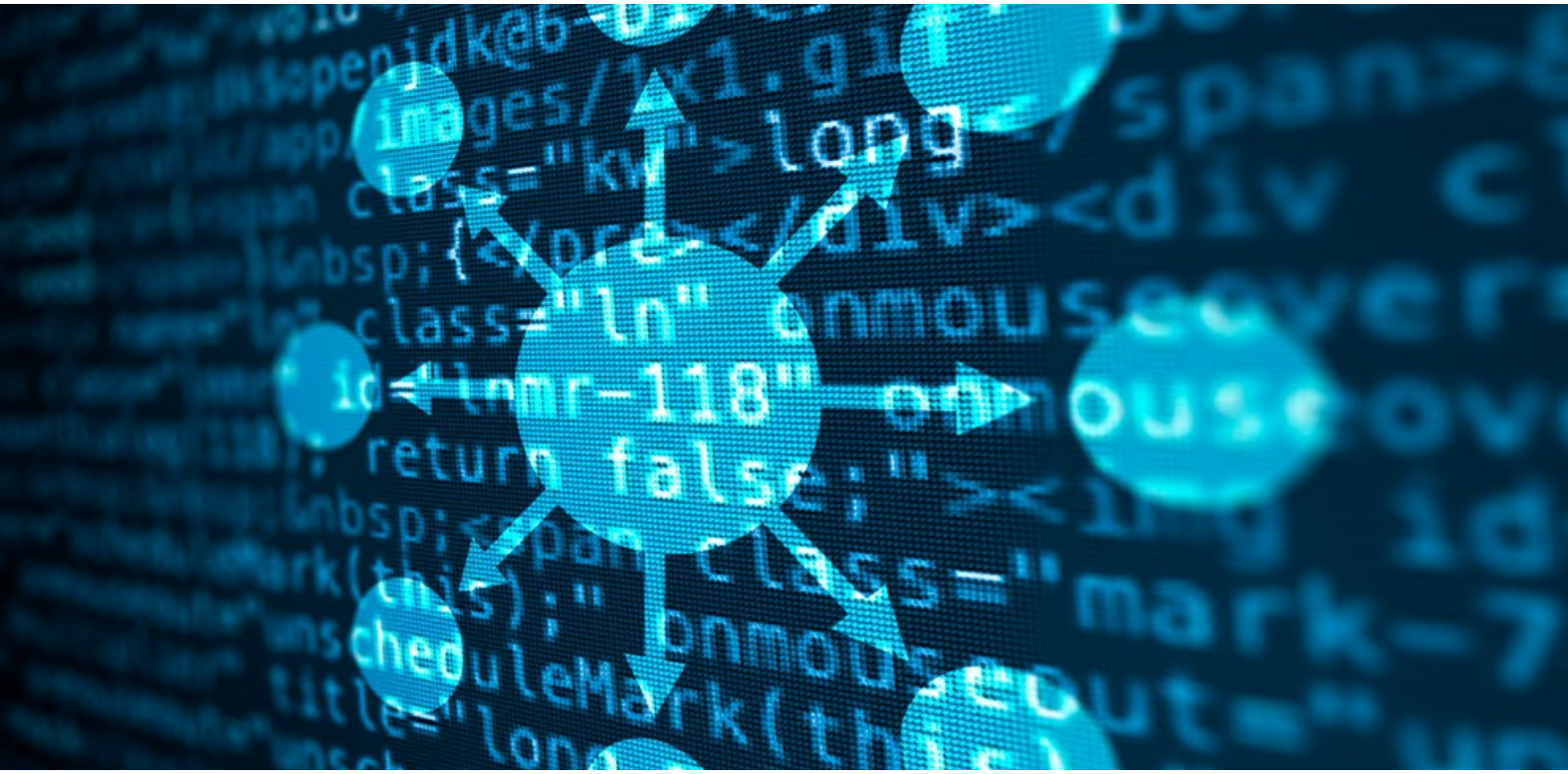
UDP unicast

This method is virtually identical to TCP/IP in that it operates on a one-to-one basis, the key difference being that there is no retry mechanism. Again, for systems involving a large volume of cameras, this may result in a significant drain on bandwidth capacity and/or result in 'dropped packets' and negative effects on the video image.

UDP multicast

This method relies on an intelligent Layer 3 network. With this method, instead of having to resend the same information multiple times on a one-to-one basis, the camera or NVR publishes video data from specific IP addresses to clients that have 'opted in' to receive the information. Client lists are grouped and controlled using the Internet Group Management Protocol (IGMP). The key benefit of multicasting is that it enables data to be transmitted once, but received by numerous recipients, therefore reducing strain on network infrastructure and bandwidth.

A separate tech note specifically on multicasting can be found at **https://bit.ly/3yxnXUk**.



What to do with WiFi and Mobile Devices

For many public space, transport, and critical infrastructure organizations that require remote-site monitoring, or where mobile/in-field camera deployment is a priority, greater thought regarding wireless network (WLAN) design is required.

Wholly wireless networks are actually uncommon. Instead, it is more likely that a specific number of users on a system will require wireless viewing/control capability. Therefore, a hybrid approach can be adopted that identifies those users (or specific workstations) that require information to be sent in a different way to the methods already discussed.

Another common network feature for wireless IP surveillance solutions is something called 'meshing'. A wireless mesh network can be used to bridge long distances that would otherwise prove too problematic (in terms of latency/drop off). It works by using mesh nodes (such as radio transmitters) to break up the distance that data needs to travel, instead facilitating smaller data 'hops'. As well as helping in long-distance applications, this particular solution also helps with cases where there is a poor line of sight or none at all, which would make standard wireless transmission difficult.

Increasingly, organizations are adopting 3G and 4G cameras – including body-worn devices – that utilize mobile network transmission signals (mobile handsets can be used as mesh nodes in this instance). While this provides a useful work-around solution, it is important to remember that bandwidth capability, network speed, and coverage capability can be unpredictable.

Existing system assets that remain of operational value can be retained for a cost-effective upgrade path.

Considering Compression

The level of video compression required is also a key consideration – particularly as adoption of ultra-high-definition and megapixel cameras becomes more widespread. IP and hybrid networks facilitate use of multiple compression methods so it is important to understand pros and cons for effective network design.

The compression process involves applying a specific algorithm to the source video in order to compress it for transmission and storage (to best accommodate image quality requirements and bandwidth availability). The data captured then has to be 'decompressed' in order to be viewed. The time it takes to complete this process is referred to as latency.

There are three main compression standards used – MJPEG, MPEG4, and H.264.

MJPEG is the oldest technique of the three and works by removing unnecessary information from individual image frames – information that would not be visible to the human eye – in order to compress the footage. **MPEG4** and **H.264** work slightly differently by identifying and coding only changes in frames in order to reduce the size of data for transmission/storage.

MJPEG compression delivers high image quality with lower relative latency (making it ideally suited to live viewing and PTZ control). Also, as there is no dependency between frames transmitted, MJPEG compression is also very robust. However, as the technique requires multiple coded JPEG standard images to be sent, bandwidth/storage requirements are significant.

The technique utilized with MPEG4 and H.264 requires much lower bandwidth/storage, with H.264 having the best overall performance in this respect (reducing file size by up to 80%). The fact that image quality has also improved significantly with H.264 has meant this standard has become the most commonly used method for HD video compression.

Camera capacity

The benefits of compression can be further maximized with the right video management solution, so that a lower-resolution stream is transmitted for live monitoring in a split screen format such as 3x3, 4x4 etc., while a high-resolution version is recorded for evidentiary review if required.

Taking this concept a step further, it is also now possible for video management systems to automatically switch lower live-viewing streams to HD if the operator selects a camera for full or quad screen viewing.

Selecting Storage

One of the most significant advantages of adopting an IP-based surveillance architecture is that it facilitates open storage solutions. This can be achieved by using NVRs but is increasingly achieved by also adopting either network-attached storage (NAS) or storage area networks (SAN).

The type of storage solution an organization should adopt is dictated by factors including the type of recording/viewing required (live vs. review), number/type of cameras and the level of detail required. However, large-scale, complex solutions will typically be best served by a SAN.

A detailed paper on the pros and cons of different storage solutions can be found by visiting **https://bit.ly/3SM9TSb**.

Remembering Redundancy and Resilience

The most effective IP-based surveillance solutions will always incorporate measures to guard against data loss and minimize – and ideally eliminate – any potential system downtime.

This is typically, and best, achieved by addressing redundancy and resiliency on two levels – through individual unit design (i.e. system components), and with system-wide measures such as server and database replication and network health monitoring.

You can find out more about system redundancy and resilience by downloading a free white paper from **https://bit.ly/42LSkGH**.

Pay Attention to Power Supply and Cabling Requirements

Finally, it is worth remembering that power supply is a crucial factor to consider (and one often overlooked).

With an analog surveillance system, camera cabling is achieved on a one function/one wire basis; separate cables are required to send video data, receive camera controls (e.g. for PTZs), and receive power. With IP cameras, PoE (Power over Ethernet) capability means that only one cable is required.

Further information about PoE is provided in our free-to-download tech note **https://bit.ly/3I5Zz2I**.

Power is also important in terms of system resiliency. Look out for devices with 'hot standby power' - or dual/redundant hot standby power – as this allows the device to draw power from an alternative source should the primary power supply fail, thus ensuring that data flow, storage, and retrieval are unaffected. In the event of a network power failure for example, digital recording/storage devices or networked cameras with this functionality – on detecting the outage – would immediately swap to a local power supply.

Compatibility is Crucial

There are many factors to consider in terms of network design when planning to adopt an IP-based solution, from surveillance objectives and camera specifications to bandwidth requirements/availability, power, and storage. This paper has touched on some of the key aspects for each of these areas.

However, one final consideration is to keep compatibility in mind.

Scalability, flexibility, and the ability to integrate a wealth of data sources with video surveillance are huge drivers in any organization's decision to adopt an IP-based solution. But many of these advantages will fail if system components are proprietary only and therefore dictate and restrict feasible integrations. Instead, organizations should look for open-protocol solutions that facilitate interoperability – only then can the true potential of IP network design be fully realized.

The ONVIF specification is important as it defines a common protocol for the exchange of information between IP network video devices including automatic device discovery, video streaming, and intelligence metadata. By selecting ONVIF-compliant solutions, organizations can be assured of interoperability irrespective of manufacturer.

Choosing the right compression format will ultimately depend on factors including camera resolution, frame rate, viewing requirements, and physical setting/environment.






Synectics designs integrated end-to-end surveillance control systems for the world's most demanding security environments. We excel at complex projects that require innovative, tailored solutions with high reliability and flexibility, specifically for casinos, oil and gas, marine, public space, banking, transport and critical infrastructure applications.

With over 30 years of high security systems experience, field proven products, and expert support personnel in the UK, US, Europe, UAE and Asia Pacific, Synectics offers its clients turnkey networked solutions for comprehensive protection and peace of mind.

Synectics' Systems division is part of Synectics plc, a global leader in advanced surveillance, security and integration technologies and services.

Synectics
synecticsglobal.com

Americas Asia Europe Middle East United Kingdom

Specifications subject to change. E & OE.
Literature Reference: IPNETWORKING-TP/0119/A4 Iss 3