White Paper

Five Reasons to Converge Video Surveillance onto the Corporate IP Network

Introduction

With the evolution of CCTV technology, the emphasis has moved from simple monitoring of video footage to intelligent systems that are capable of identifying abnormal events or behavior. As intelligence increases in these systems, so too do the applications for this technology.

Several factors have led to the growth in digital video surveillance:

- **IP networking**

  IP is becoming a universal communication medium. It is used for telephony, video conferencing and TV distribution.
- **Technical improvements in surveillance cameras**

  As the reliability, image resolution and video analysis capabilities of surveillance systems improve, the demand for these high-end features is growing.
- **Crime prevention**

  There is increasing deployment of intelligent video surveillance systems for crime prevention, using 'analytics' that can create virtual boundaries and count people in and out of specified areas.
- **Use of surveillance information for marketing**

  Advanced surveillance systems with video analysis capabilities can provide data on how people move around a store, and where they spend most of their time.
- **Increasing expectations of disaster prevention systems**

  Enterprises and local governments are devoting more energy and investment into minimizing the damage and disruption caused by natural disasters.

The transition from analog to IP-based digital technology has opened the door for numerous enhancements to the operation of video surveillance:

- Simplified storage of native digital video streams.
- Mixed-vendor interoperability due to standardization of signalling and connectivity technology.
- Simplified deployment, with Power over Ethernet (PoE).
- Multi-location viewing and storing of the same video feed, using multicast.
- Intelligent, real-time software analysis of video.
- In-service upgrade of camera firmware, via remote connection.
- Flexible network scalability–new cameras are easily added to the system, and bandwidth is the only limiting factor on the number of cameras that can be supported.

These improvements have increased the value of video surveillance-based security, whilst reducing its total cost (equipment, installation and operational costs). This has facilitated the enormous increase in the rate of uptake of video surveillance in recent years.

Another advantage—convergence

Another major advantage of the move to IP-based video surveillance is the ability to converge video surveillance onto the existing corporate IP network.

IP cameras no longer need special cabling, special receiving equipment or special recording equipment. They just use Internet Protocol over Ethernet (IPoE), like all the other equipment in the corporate LAN. There is no need for dedicated switching, cabling or recording infrastructure for the video surveillance system.

Cameras can simply be peripherals on the data network, much like printers, scanners and workstations. Video recorders are just another server in the data center rack. Monitoring and camera-control stations are now no different to any other PC or workstation on the network.

Provisioning the bandwidth and Quality of Service (QoS) for video streams is not difficult. Video cameras send data at quite predictable and steady rates. It is straightforward to calculate the total bandwidth that a set of cameras require.

It is necessary to give video data a high QoS priority, as good quality IP video is achieved by ensuring low packet loss and low jitter. However, giving high priority to video data does not incur a risk of unpredictable impact on other network data, due to the inherently steady nature of video data transmission rates.

So, there are no technical barriers against converging the video surveillance system onto the main data network, and the bandwidth provisioning requirements are predictable. Importantly, there are clear advantages to be gained from doing so.

5 reasons to take advantage of the opportunity to converge

1) Cost saving

Buying, installing and maintaining a separate network infrastructure purely for video surveillance adds unnecessary financial overheads to an organization. Converging the video surveillance system onto the existing data network, and adding only as much equipment as needed to provision the extra ports required for video connectivity, greatly decreases the incremental cost of introducing video surveillance.

Moreover, convergence reduces ongoing operational expenditure. Monitoring, troubleshooting, upgrading and repairing the video surveillance infrastructure are simply subsumed into the overall operation of the data systems.

Thanks to protocol and technology standardization, there is little extra training required for existing IT staff to be able to manage the video surveillance network along with their other responsibilities. Long gone are the days when the proprietary video equipment, signalling and transport technology required a whole separate set of expertise.

Reducing equipment duplication also saves in electricity consumption, both in running and cooling the equipment.

2) Consistency

Consolidating all of an organization's IP networking onto a single infrastructure allows consistent policies to be applied across all data systems. Achieving consistent standards of security, reliability and manageability across all networking equipment is important, to avoid costly security breaches and lengthy periods of downtime.

Consistent security policies are of particular importance. An organization's data security protection is only as strong as its weakest link. Having robust security fully implemented throughout one portion of the networking infrastructure is of little value if another portion is significantly less secure.

Ironically, a parallel infrastructure for video surveillance–created to enhance physical security–can easily be a source of data insecurity if it is not fully integrated into the organization's security policies. Converging the video surveillance system onto the main data network ensures that the equipment involved in video surveillance is automatically subject to the same security auditing, monitoring and upgrading as the rest of the organization's information systems.

3) Opportunities for new service deployment

The distributed nature of a video surveillance network will often necessitate the installation of switches in physical locations that are not traditionally occupied by network equipment. If the video surveillance network is integrated with the main data network, then installing remote switches for video surveillance has the effect of extending the whole data network to these locations.

Once the data network is physically extended in this manner, opportunities arise to take advantage of this situation. For example, remote environmental monitoring equipment could also be connected to these switches, or electronic signage, wireless hotspots, and so on.

Many data switches can supply Power over Ethernet (PoE) to power the video surveillance cameras, so a separate power feed is not required, which simplifies installation in remote or inaccessible areas. If PoE-capable switches are used to power video cameras, this can also be leveraged to power other network devices such as wireless APs.

In short, if video surveillance is converged with the rest of the data transport infrastructure, then the investment in installing network equipment for video surveillance can be leveraged to the advantage of other aspects of the organization.

4) Flexibility

Networks rarely stay fixed for long periods of time. Bandwidth requirements grow, resiliency features improve, and physical workspaces are rearranged.

When video surveillance equipment operates as peripherals on the main data network, it is possible to carry out major data system rearrangements like relocating the in-house data center, or installing a new campus-wide resilient core, without the extra overhead of having to rearrange a separate video surveillance network in addition to the main network. Video surveillance can be treated as just another service that is sending data over the main data network.

Furthermore, once video surveillance data is integrated with the main data network infrastructure, there is much greater flexibility in where the data can be fed to. Video monitoring can be carried out at any location that is connected to the network, so security personnel can be more flexibly located, and can be easily provided with mobile monitoring solutions.

Convergence means that adding new monitoring options becomes simply a matter of routing the video data to certain network nodes, rather than adding physical extensions to a dedicated video surveillance network.

5) Participation in a network management framework

The complexity of modern data networks, and the reliance that organizations put on them, mean that effective network management and maintenance is expensive. Network failures are expensive. Preventing or resolving them are tasks that require specialized skills.

Allied Telesis has recognized the need to reduce the cost and complexity of network management, and has created an intelligent network management framework that significantly reduces network operation overheads.

By embedding intelligence into the network itself, Allied Telesis Autonomous Management Framework™ (AMF) automates time-consuming tasks, and reduces the possibility of error in network configuration and maintenance activities.

A key benefit of AMF is that it enables the network to be managed as a single, coherent entity:

- commands can be issued to all network nodes simultaneously
- all network nodes have regular automated firmware and configuration backup
- newly connected or replacement switches are easily integrated into the framework, and automatically receive the correct firmware and configuration
- software upgrades can be automatically rolled out across the network with a single command

A unifying management framework like AMF further enhances the benefit of converging an organization's video surveillance network with the main data network. The more integrated networking services are, the more they can benefit from the efficiencies provided by intelligent management.

A data system that is fragmented into multiple, dedicated-purpose networks does not reap the benefits of features like unified configuration of ALL nodes, or automated software rollouts over the whole network.

Furthermore, the benefits of unified management increase significantly as the scale of the network increases. The benefit of applying this framework to a single large network is more than twice that of applying it separately to two smaller networks. The larger and more complex a network is, the more scope there is for process automation to save time, reduce errors, and reduce costs.

As a bonus, AMF provides plug-and-play addition of switches to the network, and replacement of faulty switches. For a video surveillance network, which is inherently spread out physically, this is particularly advantageous. The installation of new or replacement switches in remote parts of the network does not require sending out a skilled engineer, but can be performed by a non-specialist.

Summary

Converging video surveillance onto the corporate data network simplifies network administration and lower ICT running costs. Allied Telesis has a portfolio of advanced switching and routing products that have all of the features required to support businesses in moving to a converged data network, saving both time and money.

Visit www.alliedtelesis.com/about/technology/amf for more information about how AMF delivers convenience, simplicity and reliability in enterprise network management, today.

AlliedTelesis.com
Allied Telesis™
© 2020 Allied Telesis, Inc. All rights reserved.
C613-08020-00 RevB