Combining Security and Networking Technologies for

UNIFIED SOLUTIONS

securityinformed.com
Making The World A Safer Place

Alcatel·Lucent Enterprise

convergint

About the author

An experienced journalist and longtime presence in the U.S. technology marketplace, Larry Anderson is the Editor of leading digital publications SecurityInformed.com and SourceSecurity.com. Mr. Anderson is the websites' eyes and ears in the fast-changing security sector, attending industry and corporate events, interviewing leaders and contributing original editorial content to the two sites. He leads a team of dedicated editorial and content professionals, guiding the editorial roadmap to ensure that SecurityInformed.com and SourceSecurity.com provide the most relevant content for industry professionals. From 1996 to 2008, Mr. Anderson was editor of Access Control & Security Systems magazine and its affiliated websites. He has written numerous articles for and about some of the largest companies in the security industry and has received numerous awards for editorial excellence. He earned a Bachelor of Arts in journalism from Georgia State University with a minor in marketing.

Table of Content

Alcatel-Lucent Enterprise and Convergint commissioned SecurityInformed.com to produce this document.

Combining Security and Networking Technologies for Unified Solutions

By Larry Anderson

It is impossible to overstate the importance of the network to any physical security system. Because it is the backbone of the system, the quality of networking equipment is paramount.

The network is the foundational layer of the system. It is also the orchestration layer, the management layer, and the data sharing layer. "It's the layer that drives a lot of the foundational rules and components that everything needs to connect and sit on, and it also drives a lot of the standards on how things are going to be managed, communicated and orchestrated," says Amir Shechter, Convergint's Executive Director of Solutions.

Investment in networking equipment that is dependable, supported, and provides advanced features ensures a system that performs as promised. Managed switches are a requirement of today's physical security systems; low-cost unmanaged switches just will not get the job done. Customers should not be tempted by the lower costs. Rather, they should consider the return-on-investment, in terms of better dependability and resiliency, of buying more expensive equipment. Today's more sophisticated security systems require more sophisticated networks.

Physical security and networking technologies evolved separately in the days before physical security systems depended on networking. The historical needs of physical security remain, even as the technologies to meet those needs have migrated to the network environment. The two separate worlds must today operate seamlessly to deliver the benefits of the latest networked physical security systems.

This Technology Report, produced with the help of Alcatel-Lucent Enterprise (ALE), will describe how physical security and networking technologies are converging, how they are adapting to address their common needs, and how together they deliver the best unified physical security systems ever. Additional commentary is provided by Convergint, a global service-based systems integrator supplying comprehensive security solutions.

Network layer is the layer that drives a lot of the foundational rules and components that everything needs to connect and sit on, and it also drives a lot of the standards on how things are going to be managed, communicated and orchestrated

- **Amir Shechter**

Executive Director of Solution

Convergint

Confer With Networking Providers Early and Often

Consulting with a system's networking equipment manufacturer early in the facility planning process ensures that the physical infrastructure is designed to accommodate the technology needs of the system. The design of the physical infrastructure – where copper and/or fiber cabling are installed, for example – can help to enable the best use of the latest technology. In general, multimode fiber technology should not be used when deploying the infrastructure; the older technology has significant limitations. Instead, single-mode fiber should be installed throughout to ensure the best customer deployment and a future-proof system. In general, early input in the facility planning process from the network equipment manufacturer can ensure a fully optimized system.

Like many network providers, ALE interfaces with physical security integrators on a regular basis, going to their events, training with them, attending their shows, etc. Maintaining regular touch points with valued customers enables manufacturers to listen to the needs of integrators. "When they talk about their workflow, we are making notes," says Scott Howard, ALE's Director of Americas Sales Technology and Business Strategy. "If they have a complaint, or request a new feature, we actually listen, and then create the tools and develop the software."

"Regular communications and a continuous improvement process over several years have led us to develop purpose-built tools, hardware and software, and to improve their workflow," says Howard. "If you're a physical security integrator, we put together all the things that make you better, faster, at less expense, and easier to work with."

Integrator customers also benefit from networking equipment that is easy to install, even for technicians that might not be IT specialists. Ease of installation is another contributing factor to ROI.

"We have to be continuously aware of the evolving specifications and building toward them years before they become common in an RFP," says Charles Matthews, ALE's Senior Vice President of Strategy.

The overall trend in physical security systems is toward more integration, more interoperability, and more efficient use of data. The network is key to achieving those goals because it provides the "orchestration layer" that manages all the various factors effectively.

- **Early collaboration with networking providers** ensures infrastructure compatibility with modern security technologies.
- **Single-mode fiber** is preferred over multimode for scalability and future-proofing.
- **ALE maintains constant communication with integrators** via events, training, and direct feedback loops.
- **Feedback-driven innovation** results in tools tailored to improve integrators' workflows.
- **Ease of installation**, even for non-IT technicians, adds value and enhances ROI.
- **Unified infrastructure** replaces legacy interconnectivity methods like coaxial or serial connections.

Combining systems and ensuring interoperability has historically been the job of the systems integrator, which puts the partnership between the integrator and the network manufacturer at the center of creating today's systems. Integrators guide their customers to achieve interconnectedness using the network.

As networking specialists, ALE is focused on understanding how all the equipment connects, whether it is video management systems (VMS), door locks or access control badges. While a network manufacturer understands networking, they must work closely with the integrators to share information on the needs of the individual system components and how they work with the network. "We expect the integrators to be experts in the things that we are not experts in," says Matthews.

Before the advent of networked systems, interconnectivity was via a variety of coaxial cables, serial communications, and other devices. Networking has eliminated the diverse methods of connectivity and replaced them with a single underlying infrastructure that operates across a variety of product types.

Providing both power and data through a single connection, networks have simplified many of the traditional elements used in physical security. In effect, networks have transitioned silos into integrated, interoperable systems, both within security systems and between security systems and the broader enterprise.

> *We have to be continuously aware of the evolving specifications and build toward them years in advance.*
>
> - **Charles Matthews**
>
> Senior Vice President of Strategy
>
> Alcatel-Lucent Enterprise

Understanding the Needs of Physical Security

Network manufacturers need to understand how physical security has evolved, how it works, and the impact of expectations on how networked devices operate. Systems integrators must translate the expected behavior of security devices, as they have evolved over time, to the network environment. Networking equipment manufacturers need a thorough understanding of the needs of security systems and how to accommodate those needs in the networking climate.

“Understanding how security works and the little nuances is absolutely critical to be successful, especially if you are building a large and complex system,” says Mark Schweitzer, Convergint Portfolio Manager. A mutual evolution of networking and physical security technologies is required to address the needs of today’s systems.

“We work very closely with manufacturers to make sure that we optimize the way solutions are deployed on the network, and we understand the needs of each solution to work in an optimized way in the network environment,” says Shechter.

Integrators aggregate information from the various security product teams to communicate that information to the network manufacturer, highlighting needed network features and opportunities that can make a better overall system. Hearing feedback from 10 customers in a month about a needed additional feature provides a resource for network manufacturers to respond to the needs of the market.

Integrators communicate with networking manufacturers about the exact needs of security systems, providing an opportunity to tweak networking systems to address the specific requirements of security. “Part of the integrator’s role is to orchestrate the communication to make sure everybody knows what needs to be done,” says Schechter.

Often there is an education process involved when communicating with integrators and end users about the available benefits and advanced features in a new networking system. Communicating these features empowers customers to ask for them and to include them in RFPs. Can I test my cable? Can I power-cycle my camera? Requesting these capabilities ensures selection of the right manufacturer.

- **Networking manufacturers** must understand the operational behaviors and expectations of modern security systems.
- **Integrators serve as a bridge** between security device manufacturers and network providers, translating device needs into network requirements.
- **Aggregated customer feedback** helps network providers identify trends and prioritize feature development.
- **Education of end users** and integrators about networking features improves RFP accuracy and purchasing decisions.
- **Effective communication** enables faster integration of advanced networking tools into physical security environments.

Accommodating the Requirements of IT

Convergint works closely with enterprise IT departments to ensure that security equipment and software adheres to established IT standards and certifications, whether related to encryption, application access, authentication, device management, data governance, compliance (ISO 27001) or other requirements.

Enterprise IT departments have strong processes to evaluate anything that will sit on its networks, ensuring that each device is known, stable and secure. "Most of our large customers will dictate the IT standards they have, and we meet those standards with the solution we are providing for security," says Schechter. Smaller customers may not have the same level of resources, and thus more flexibility, and they rely more on the security integrator to provide needed IT resources and guidance.

When installing a system, the integrator also works to incorporate any legacy security devices deployed at the site onto the network, emphasizing automation, flexibility, and expansion.

Furthermore, security today is becoming more integrated into the broader enterprise, no longer treated as a silo that is separate from other enterprise operations. Being integral to the enterprise also requires security systems that are in accordance with the broader standards of the enterprise "We're coming into the IT world, so we need to really adhere to the IT standards and the other enterprise requirements," says Schechter.

Adherence to IT Standards:

Security systems must align with enterprise IT standards including encryption, authentication, device management, and ISO 27001 compliance.

Integration with Enterprise Networks:

Every security device must be evaluated for stability and security before deployment on enterprise networks.

Convergence of IT and Security:

Security is now considered an integrated part of the broader enterprise operations rather than a siloed function.

Cloud and Modernization Readiness:

Security systems must be future-ready and aligned with broader IT transformations such as cloud adoption.

Security also must adapt to the enterprise IT changes and should not be left behind in modernization efforts or, for example, shocked by a corporate edict to move all their systems to the cloud. Some enterprises employ IT consultant companies, such as Capgemini and Deloitte, to guide their overall IT strategy, which can impact networked physical security systems.

However, if the security department turns decision-making completely over to the enterprise IT group, they may lose control over the success or failure of the project. The IT department might not fully understand the system requirements from a video or bandwidth perspective. Outsourcing a project to an internal IT department introduces a new level of risk that could put the project in jeopardy. The economic picture changes, too, with security facing additional costs outside their own department. Better that the security department remain involved in the process, working together with IT to maximize the system from both the IT and the security perspectives.

How well the security department works with IT varies greatly among various end user customers. There are obviously potential conflicts, but the ideal is a collaborative relationship in which both parties understand the roles and responsibilities in play.

> *Most of our large customers will dictate the IT standards they have, and we meet those standards with the solution we are providing for security.*
>
> - **Amir Shechter**
>
> **Executive Director of Solution**
>
> **Convergint**

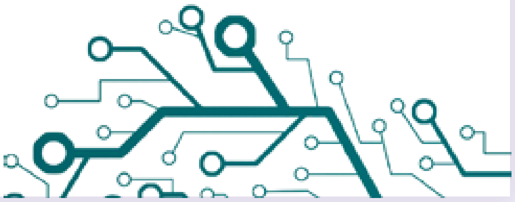
More Devices Than Ever on the Network

More demand for video in physical security is one of the reasons that networks are growing faster than ever. There are more devices than ever on the network, and changing architectures – whether cloud, on-premises, or hybrid – are impacting how networks are configured. Therefore, it is important for networks to be able to scale easily, especially given the growth of AI that will likely increase the demand substantially.

Air-gapping a network involves physically or logically isolating a computer system or network from other unsecured networks, particularly the public internet. The idea is to create a "gap" that cyber threats cannot bridge, thereby preventing remote access and protecting highly sensitive data. However, in today's connected world, air-gapping is usually not a useful alternative. Video and related analytics are increasingly seen as valuable "data" in the enterprise with usefulness that extends beyond the security department. The need to leverage that data rules out an "air-gapping" approach.

The two biggest needs of today's networks are power and bandwidth. As physical security equipment changes, the power and bandwidth requirements shift, so networking manufacturers must work closely to understand the market and adapt equipment as

- Increasing demand for video and AI in physical security is rapidly expanding the number of connected devices.
- Transitioning between cloud, on-premises, and hybrid systems affects how networks must be configured and scaled.
- While previously air-gapping considered a security tactic, It is no longer feasible due to the enterprise-wide value of video data.
- Modern networks must accommodate growing power demands (PoE++, 90W) and bandwidth needs (uplink speeds from 10G to 100G).
- Systems must support a wide range of PoE standards (PoE, PoE+, PoE++, and higher) to power evolving camera technologies.
- Edge-based AI applications and high-resolution video drive up data transfer rates, impacting network switch design.
- Networking hardware must function reliably in harsh environments like outdoor installations or elevator shafts.



needed. “We’re listening to the market, and we are aware of physical security and what the needs are,” says Matthews.

In the area of power, requirements are changing related to Power-over-Ethernet (PoE), power budgets and higher power requirements of newer equipment. Today’s PoE requirements are 60 watts per port (PoE++), and the trend is moving quickly toward 90 watts per port, required by newer, more robust cameras. However, a lot of cameras still use 30 watts (PoE+). Systems must support PoE, PoE+, PoE++, and higher-power PoE.

On the bandwidth side, uplink speeds on edge ports today are increasing from 10 to 25 to even 100 gigs. Per-camera bit rates are also increasing, and AI is increasing network requirements on the edge. The new requirements are showing up on RPFs, so switches must adapt to the expanding needs.

There are also requirements for switches that operate in harsh environments. Not all applications are nestled in an air-conditioned wiring closet. Some are outside or in another harsher environment such as an elevator shaft. There may be high heat, lower temperatures, and/or dust in harsh environments.

How Network Technology Can Make Security Technology Better

Working with networking specialists, and communicating system needs, can yield systems that work better together. Here is an example: The integrator needs an easy way to toggle a switch quickly right from the VMS. If a camera is not operating, the first step in correcting the problem is to toggle the switch – that is, turn the port on and off correctly. Restarting equipment sometimes solves the problem. Previously, a technician would have to physically travel to the camera location and climb a ladder to restart the camera. Based on customer feedback, the networking equipment company now offers the ability to restart the switch remotely, using a "plug-in" to the VMS system, thus saving time and expense when troubleshooting a problem.

> *Remote tools and automation are solving problems before the customer even notices them.*
>
> - **Mark Schweitzer**
>
> Manager Solutions Strategy
>
> Convergint

“Integrators know what it’s like to work on the ground with equipment and completely understand how video cameras work,” says Matthews. “In this case, we were able to do a rather quick software development to help those customers and make their life easier. We would not have dreamed up this plug-in on our own without the help of our integrators.”

Network switches provide an application programming interface (API) that enables creation of such additional functionality in partnership with software engineers throughout the industry. For example, new applications can automate factors related to cybersecurity, health monitoring, or lifecycle management of assets.

The emergence of network platforms that provide APIs is boosting interconnections so that the physical security system can be managed as a whole. Software systems are helping integrators improve overall performance as well as leverage visualization of the networking traffic to help them understand any roadblocks or issues, says Schweitzer.

There are also tools to make the actual configuration of the switch during the onboarding process easier for installers. To achieve the goal, ALE developed the Lightning Configuration tool, software that activates a switch, optimizes for video surveillance needs, and adds it live to the network faster.

In addition to automatic configuration, today’s networks provide device management and transparency into operation of the network. From a troubleshooting perspective, networks can trigger certain activities that can provide information on any problems remotely without having to visit the site.

If the network detects a camera that is down, it can automatically alarm and implement a workflow process to address the problem. The remote services team can log into the system, do advanced troubleshooting, and only then roll a technician to the site, all before the customer even knows there is an issue.

- Networking companies are now building VMS plug-ins that allow remote power toggling, saving technician time and cost.
- APIs from network switches are enabling developers to add customized cybersecurity and device management features.
- Visualization tools now let integrators understand bottlenecks, performance issues, and optimize system behavior.
- ALE’s Lightning Configuration enables quick, optimized deployment of switches tailored for surveillance.
- Remote troubleshooting now includes advanced workflows that often resolve issues before on-site techs are needed.
- Smart alerts detect downed cameras and initiate troubleshooting protocols automatically.

More Networking Tools for Integrators

Another tool for integrators is the OmniVista Smart Tool, which automates the process of documenting a system. Creating the required documentation before handing a system over to a customer is a time-consuming process for integrators. OmniVista automates the process, requiring only three minutes per switch. OST provides information on each camera, where it is connected, how much power it consumes, how fast it runs, and whether it is operating correctly.

All the information is supplied in a document, a file that the integrator or end user can import, change, or print out. It is easy for them to import the information into their existing processes. The tool can also deliver any documentation updates as needed on demand throughout the life of the system.

Device fingerprinting can simplify connections, shorten the onboarding process, and make regular maintenance easier. The process recognizes information about a device based on its MAC address, packet flows and other information. The network recognizes an IoT device from its "fingerprint" and then makes Quality-of-Service (QoS) policy decisions based on the type of device, whether it's a camera, a door lock, or an irrigation sprinkler. Policies can be applied to various products, and like devices can be operated within a particular VLAN on the network. Quality of Service (QoS) refers to the use of network resources to manage and prioritize different types of network traffic, ensuring a certain level of performance for critical applications and services.

Device fingerprinting also prevents someone from unplugging one device and using the connection to plug in some other device for nefarious purposes. If the original device has been fingerprinted, the system can flag an alert that a non-compliant device has been connected to the network before cybersecurity is compromised.

Shortest path bridging provides a tool to create redundancy and resiliency in a complex network. The tool enables data to travel the fastest route from one point to another,

Dual-core switches can provide the uptime needed in high-stakes security deployments, failure is not an option.

without having to be specifically configured to travel a certain route. In terms of redundancy, if a previous route fails, the data automatically seeks an alternative shortest route to ensure continued system operation.

Shortest path bridging (SPB) also offers significant contributions to cybersecurity. SPB excels at creating logical network segments (VPNs or "communities") on a shared physical infrastructure. SPB inherently supports multi-tenancy by creating separate virtual networks that are completely isolated from each other. This is invaluable in environments where different departments, customers, or types of devices need to be segmented for security. For example, IoT devices can be isolated in their own segment to prevent them from impacting critical business systems if compromised.

Port-level authentication is a network security mechanism that controls access to a network at the individual port level of a network device, such as a switch or wireless access point. It ensures that only authorized devices and users can connect to the network infrastructure.

Dual-core switches can be used in mission-critical situations when, for example, a single switch failure could jeopardize the entire network. In some cases, triple redundancy might be required, but it comes with a cost.

Ensuring Cybersecurity of IoT Devices

In general, IoT devices are not designed with cybersecurity top-of-mind. There is an ongoing need for updates and patches, some of which are not well-supported and/or are not applied in a timely manner. In the absence of timely cybersecurity updates, administrators are stuck with "insecure" devices. Customers should choose only vendors that take cybersecurity seriously and issue the needed security patches.

Given the inherent risks of IoT devices, an approach to cybersecurity is to create separation among various parts of the network, in effect segregating out any questionable devices from the main network. As we have seen, shortest path bridging (SPB) enables creation of virtual networks within a shared infrastructure. Grouping any questionable devices within their own virtual network keeps their data separate from the mainstream data flow. If a camera were hacked, it would not impact the larger network if all the cameras are quarantined into the same virtual network.

Another approach is to use Universal Network Profiles, which can implement any cybersecurity policy to each individual port, enforcing security and Quality of Service (QoS) at the access port level.

Coordinating closely with the IT department ensures there are no issues with permissions and connectivity. “When there is a problem, we need the ability to identify the core of the problem, which is where some of the network equipment comes into play,” says Schechter. “Now we have visibility into the network and can isolate the problem and know really quickly what the root cause of the issue is.”

Simple Network Management Protocol (SNMP) or APIs provides information on device health and operation on the network and traffic flow, aiding with everything from lifecycle management to firmware updates. Also, changes in network operations and bandwidth usage can provide a centralized view and an early warning of a malicious attack, and identify which port was affected.

Tight control of network access privileges, including two-factor authentication, is critical in the age of connected networks. Managing connected devices, including patch management, password management, version management and other factors, provides assurance, and vulnerability assessments highlight any problems. Everything on the network must be vetted, properly configured, and properly managed.

- **OmniVista Smart Tool** automates system documentation in 3 minutes per switch.
- **Device fingerprinting** simplifies onboarding and blocks unauthorized devices.
- **Quality-of-Service (QoS)** enables policy-based network traffic prioritization.
- **Shortest Path Bridging (SPB)** provides redundancy, resiliency, and logical network segmentation.
- **Port-level authentication** ensures only authorized devices can access network ports.

Easier Installation Helps the Integrator

It is the integrator's ultimate responsibility to deliver a working solution, which means they must thoroughly understand the various components and how they work together. Easy installation of networking equipment enables integrators to get their jobs done on spec and on time.

Integrators do not get paid until the customer is satisfied, so anything that keeps them from making a quick and efficient installation becomes a real problem. The network should not be an obstacle to efficient installation. In fact, the network equipment should be designed for efficient installation, and ease-of-use is a result of understanding the integrator's needs.

Networking manufacturers mostly provide the same baseline, but some may provide specific advantages in one area or another. "What's key for us is a platform that is easy to use and easy to get our technicians up to speed so that we can deploy a system rapidly," says Schweitzer. For example, if a system requires 10 similarly configured switches, the ability to "cut-and-paste" the configuration from one switch to the next greatly simplifies installation, which drives the cost down.

On day-to-day installations, Convergint depends on systems that are as close to "point-and-click" as possible to enable them to get equipment up and running faster.

For systems integrators like Convergint, networking challenges translate into a steep learning curve when training their workforce to utilize and support the platforms. Features such as automatic configuration can help. Networking platforms that are easy to use allow technicians to deploy them rapidly. Convergint has also recruited and hired IT specialists that are available to augment the

What's key for us is a platform that is easy to use and easy to get our technicians up to speed so that we can deploy a system rapidly

- **Mark Schweitzer**

Manager Solutions Strategy

Convergint

skillsets of the day-to-day technicians. Meanwhile, additional training brings more and more of the technicians to a higher skill level.

“A lot of the industry’s networking challenges from five years ago have been worked out because companies like ALE have worked to understand the unique needs of security and built that into their platform,” says Schweitzer. When necessary, the security integrator can augment the IT resources available inside the customer’s organization, especially if the security department struggles to communicate their needs to the IT department.

Given the additional networking requirements on the horizon as AI and machine learning gain momentum, not to mention interfacing with the cloud, a close and productive working relationship between networking companies and security technology companies will become even more important in the future.