A ZK Research Whitepaper

June 2014

IP Video Surveillance

The Network Is Critical

Introduction: The Time for IP Video Surveillance Is Now

The need for IP video surveillance has been rising for well over a decade. Many organizations that historically focused on securing the IT infrastructure have shifted their focus to physical security. When deployed correctly, video surveillance can be an effective tool in protecting organizations of all sizes. In fact, there have been many instances, including the Boston Marathon bombings, where IP video surveillance played a significant role in solving a crime quickly. For this reason, ZK Research predicts that the market for IP-based video surveillance cameras will grow from $4 billion in 2012 to well over $19 billion in 2017 (Exhibit 1).

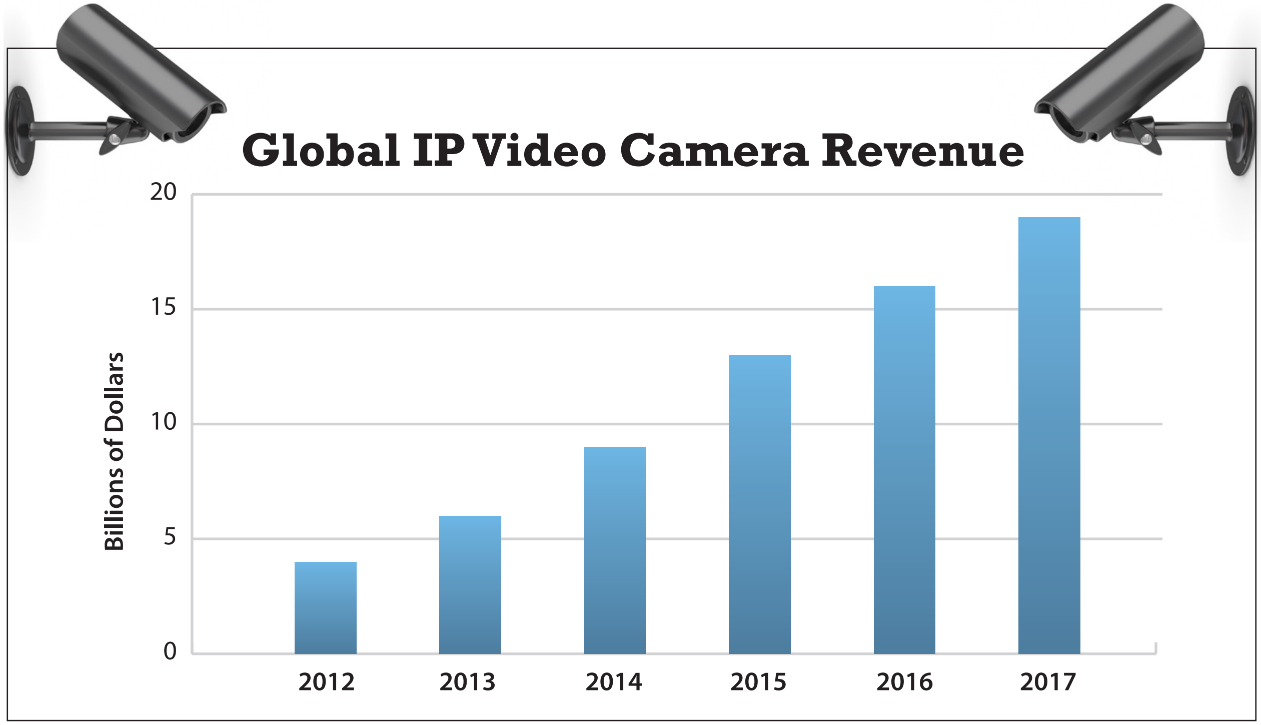
Physical security often falls under the purview of the CIO, which has been a significant driver for IP video surveillance. This has led to significant evolution in the technology over the past five years. Historically, the industry was plagued with low-quality analog cameras that were built on dedicated networks and consequently were expensive to deploy and maintain.

Today, video surveillance cameras are built on IP, which is the same protocol that drives the Internet. This shift to IP enables better quality at a lower cost because an organization can deploy video surveillance on the same IP network that it leverages for other IT services and applications. This is one reason why almost 50% of companies participating in the ZK Research 2014 IP Video Surveillance Survey have turned IP video surveillance over to the network operations team.

ABOUT THE AUTHOR

Zeus Kerravala is the founder and principal analyst with ZK Research. Kerravala provides a mix of tactical advice to help his clients in the current business climate and long-term strategic advice. He delivers research and advice to the following constituents: end-user IT and network managers; vendors of IT hardware, software and services; and members of the financial community looking to invest in the companies that he covers.

Exhibit 1: IP Video Surveillance Is on the Rise



Source: ZK Research, 2014

However, now that the cameras and other infrastructure have evolved, a new challenge has emerged for companies interested in IP video surveillance. Although the cameras may be state-of-the-art, high-definition endpoints, the networks that act as the foundation for video surveillance rely on IP protocols that were developed well over 15 years ago. In order for companies to deploy IP video surveillance successfully, it is time for the network to evolve. This is especially true for IP multicast technology, which is increasingly being used in video surveillance networks due to its bandwidth efficiencies.

Section II: The Network Challenges in Deploying IP Video Surveillance

Deploying IP video surveillance successfully requires more than just new, high-definition IP-based cameras. Although these are important, the quality of the video will only be as good as the quality of the network. A poor network can impact video quality in several ways (Exhibit 2), which limits the company's return on investment and creates additional risk.

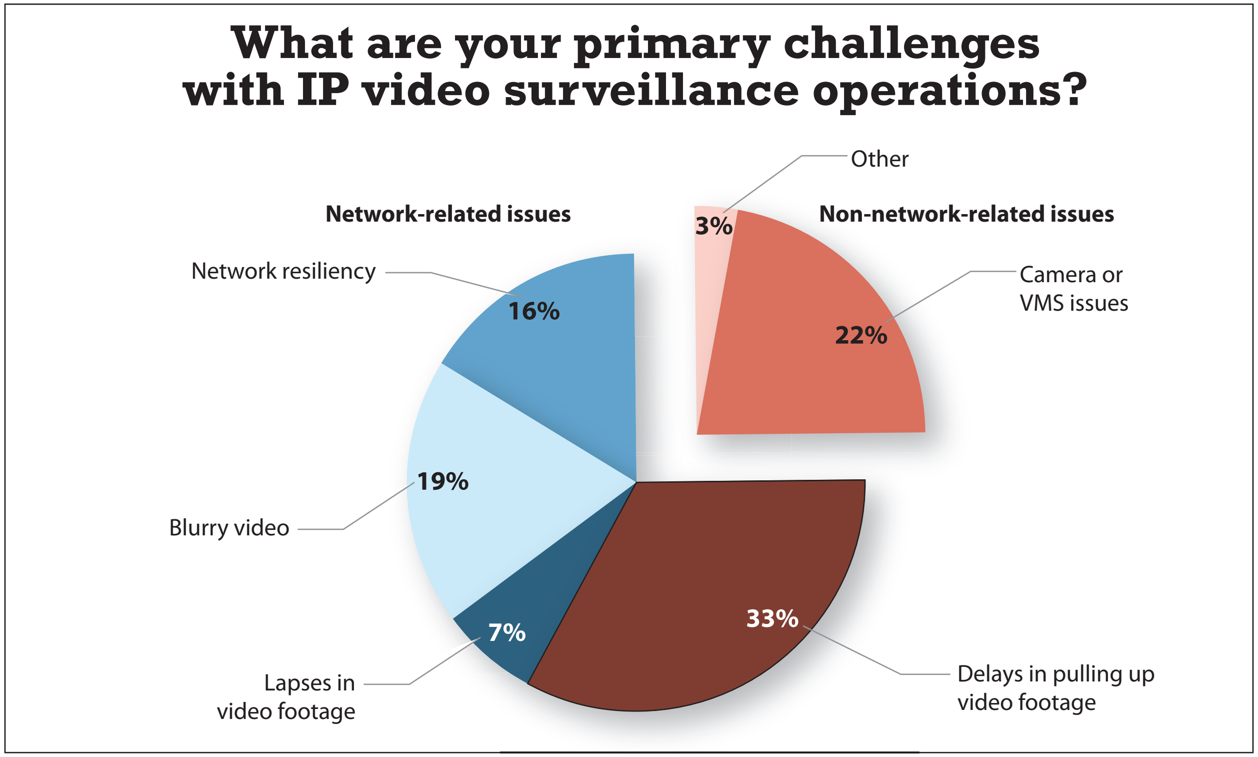
Improving network performance is the top network priority related to IP video surveillance.

Additionally, video traffic can drive a significant amount of network bandwidth, which ultimately can impact the performance of other mission-critical business applications. Solving these network challenges requires an understanding of the current network's limitations, which include the following:

> **Poor network performance:** Improving network performance is overwhelmingly the top network priority related to IP video surveillance (Exhibit 3). Processing hundreds of simultaneous network feeds is very network intensive and impairs its performance, causing the video feed to drop packets or become blurry.

> **Complexity of multiple protocols:** The current multicast architecture can be very difficult to deploy using Protocol-Independent Multicast (PIM). Network architects must design a network with multiple protocols to handle the video including Spanning Tree Protocol (STP), Layer 3 routing protocols, and PIM. Making changes to the architecture also requires

Exhibit 2: Many IP Video Surveillance Problems Are Related to the Network

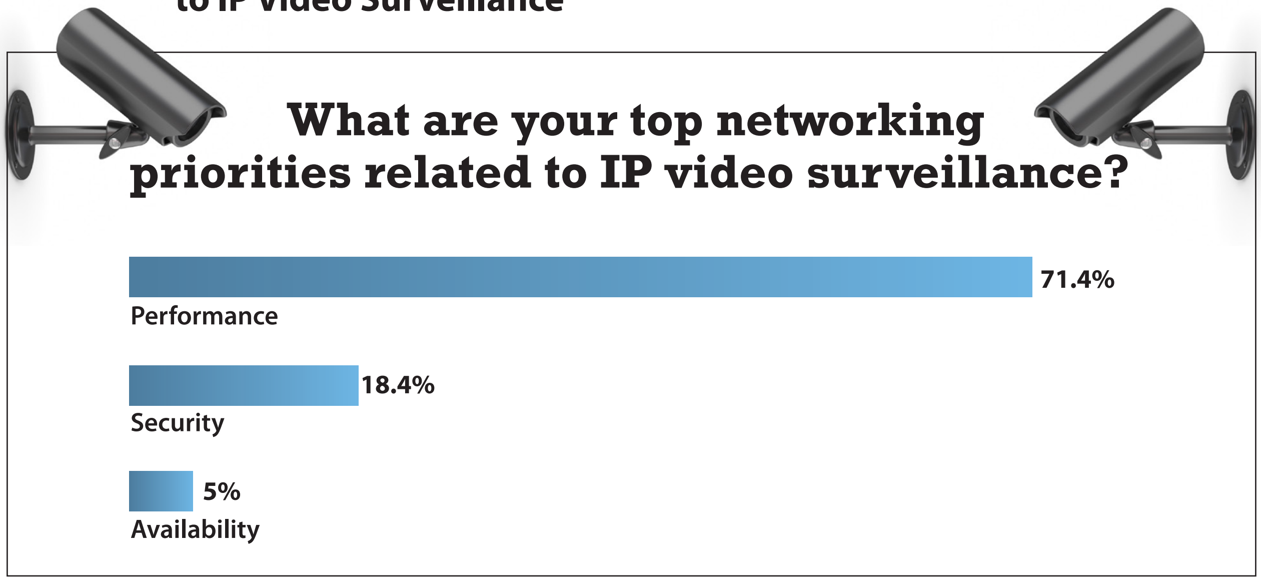


Source: ZK Research 2014 IP Video Surveillance Survey

changing each protocol and its dependence on other protocols, further compounding the complexity.

> **Slow recovery time:** When multiple protocols are being used and a network outage occurs, each protocol must go through a sequence to return to normal operations. This is known as network re-convergence, and the time this takes gets exponentially longer as more indepen-

Exhibit 3: Performance Is the Top Network Priority Related to IP Video Surveillance



Source: ZK Research 2014 IP Video Surveillance Survey

dent protocols are layered on top of each other. Large networks with thousands of video feeds can be down for several minutes when a network change, such as adding a network device or making configuration changes, is made. These minutes of downtime correlate directly to gaps in recording times, which may be less than ideal in many environments, and may be problematic in others.

> **Security challenges:** Today's networks require manual provisioning of each switch or box if a new secured partition (VLAN) needs to be added to the network. Misconfigurations can

cause outages and result in a loss of video.

Legacy networks simply were not designed for the demands of IP video surveillance. Many protocols used today were developed when a "best effort" network was the norm for most organizations. In order for organizations to leverage the benefits of IP video surveillance, the network must be built with different requirements in mind.

Companies should seek out a network solution that eliminates complexity, but still offers predictable traffic performance.

Section III: Network Requirements for IP Video Surveillance

IP video surveillance is on the rise as organizations look to better protect themselves by strengthening the physical security infrastructure. In addition to robust, high-definition video endpoints, companies need to focus on building a rock-solid network that is designed to meet the demands of IP video. The following are the primary network requirements IT leaders should look for when deploying a network today:

> **Network simplicity:** Using IP multicast to support IP video increases complexity because the various protocols that are overlaid must be kept in sync with the enterprise network. Companies should seek out a network solution that eliminates complexity but still offers predictable traffic performance. This will lower hardware costs as well as the level of operational support required for day-to-day maintenance.

> **A minimal number of provisioning points:** Eliminate as many provisioning points as possible in the network. Adding new services to a network can take several months because

legacy networks require provisioning across multiple devices and multiple places in the network including the edge, campus core, branch and data center. To simplify operations, the network should have a minimal number of provisioning points.

> **Support for both unicast and multicast:** The network should handle both types of traffic the same way without the need for additional protocols, such as PIM.

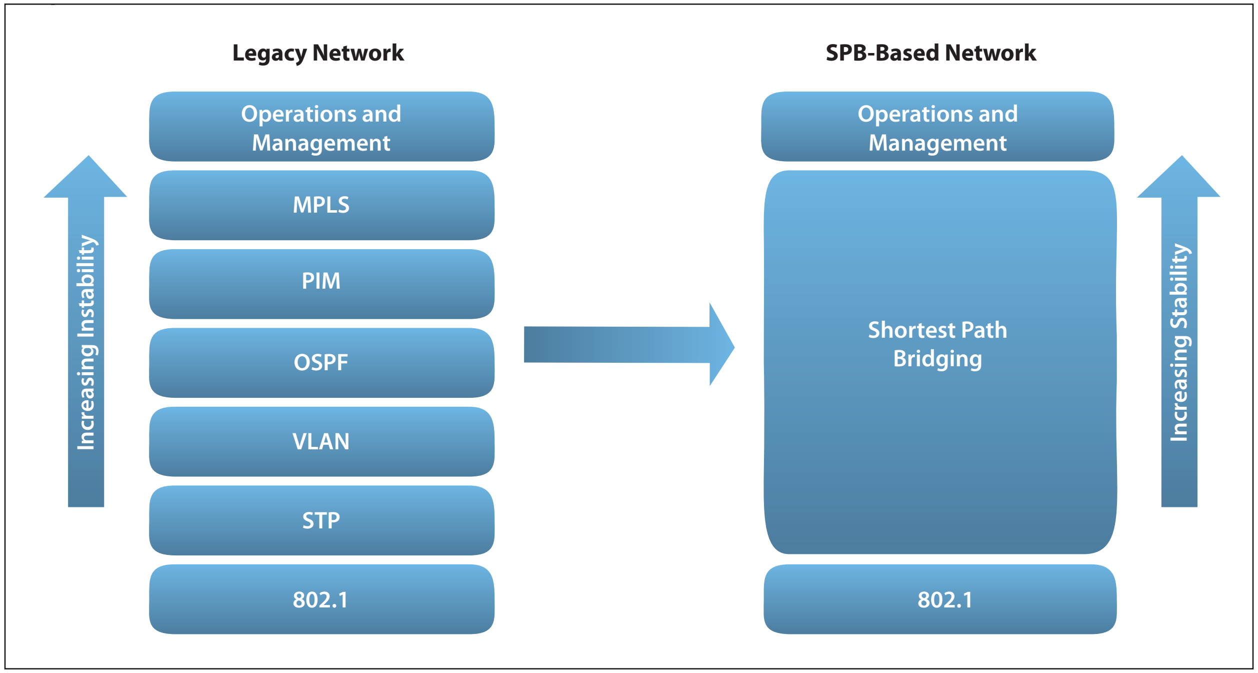
> **A minimal number of protocols:** Legacy networks often require numerous protocols to operate, including but not limited to Multi-Protocol Label Switching (MPLS), PIM, STP, Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF). Finding a way to eliminate as many of these as possible will ensure quick network recovery and efficient bandwidth use.

One way to meet the challenges listed above is to leverage Shortest Path Bridging (SPB). Traditional networks are built on a concept of "stacked protocols" (Exhibit 4). Each layer in the stack was developed to add new functionality to the existing Ethernet standards. However, each of these protocols runs independently and must be managed separately, causing network instability. SPB is an industry-standard protocol that can consolidate all of these functions and create a more efficient, simpler network. Also, SPB-based networks can recover in less than 200 ms due to the efficiency of a single protocol.

Other requirements for a network to support IP video surveillance are as follows:

> **Built on a network fabric:** Legacy networks are built on a multi-tier architecture optimized for best-effort traffic. IP video puts significantly higher demands on the network and

Exhibit 4: SPB-Based Networks Offer Simplicity and Greater Stability



Source: ZK Research, 2014

requires the performance and resiliency of a network fabric. A network fabric should be considered the underlying foundation for multicast traffic or any other high-performance application. The fabric should be extended to the edge of the network. This enables zero-touch provisioning for end devices such as IP phones and IP video cameras.

> **Massively scalable:** As IP video surveillance becomes more common, organizations will deploy cameras across the entire company instead of select locations. This means the network

must support tens of thousands of streams, which is orders of magnitude higher than what's available today.

> **Highest levels of security:** MPLS and VLANs do an adequate job of separating traffic for performance purposes. However, IP video surveillance requires the highest level of security, which equates to totally private and closed virtual networks.

> **Predictable performance:** Multicast sessions are very CPU intensive. The rapid initiation of video streams can create CPU spikes and cause erratic performance on the network. Networks that support IP video surveillance must eliminate these spikes to ensure all corporate applications perform consistently.

Exhibit 5 summarizes the benefits of a multicast network that uses a fabric as the foundation versus a legacy network.

IP video surveillance needs to be a top priority for any company looking to develop stronger physical security practices.

Section IV: Conclusion and Recommendations

Due to better camera technology combined with a greater awareness of IP video surveillance's value, the technology has grown at an unprecedented rate over the past few years. This growth is expected to continue for at least the next five years.

More and more CIOs have added facilities management and physical security to their mandate, which means IT will be responsible for deploying and managing IP video surveillance in many organizations. However, because most networks are built on protocols that were de-

Exhibit 5: Fabric-Based Multicast Has Many Advantages over Legacy Multicast

	Legacy Multicast	Fabric-Based Multicast
Architecture	Complex—multiple protocols	Simple—single protocol
Recovery Time	Slow—seconds to minutes	Fast—sub-second recovery time
Multicast Streams Supported	Hundreds	Tens of thousands
Security	Limited end-to-end	Totally private and closed
Configurability	Difficult due to multidevice configuration and protocol overlays	Simple due to network edge provisioning
Performance	Erratic due to CPU spikes	Predictable

Source: ZK Research, 2014

signed in an era of best-effort traffic, most networks are not equipped to meet the demands of today's IP video surveillance solutions. In many cases, the network will be the primary issue that holds organizations back from being more aggressive with IP video surveillance. For CIOs and other IT leaders to implement IP video surveillance, the network must evolve.

However, building a roadmap for network evolution can be challenging. ZK Research offers the following recommendations to help IT leaders start the process:

> **Make IP video surveillance a priority.** The new IP-based solutions are far superior to anything from even a few years ago. IP video surveillance needs to be a top priority for any company looking to develop stronger physical security practices.

> **Choose an SPB-based network solution.** Shortest Path Bridging is supported by many

vendors now, and it can offer superior performance with lower overhead. Organizations that choose to deploy SPB will have 10 times greater network scalability, 3 times the performance of a legacy network and at least 50 times better network re-convergence. SPB is the right protocol for today's networks. It enables network managers to deploy a network without having to compromise.

> Be willing to change vendors and deploy the best solution. When evaluating network infrastructure, it's often easy to stay with the brand leader or incumbent vendor. However, IP video surveillance's demands on the network are far greater than ever expected. This is one reason why 37% of businesses are willing to change network vendors if doing so could improve the performance, reliability or security of IP video surveillance, according to the ZK Research 2014 IP Video Surveillance Survey. Conduct the proper due diligence and evaluate at least two alternatives to the incumbent vendor.

RESEARCH