Video Surveillance

Best practices: Management of video surveillance streaming

Billy Short

3/30/2017

Abstract

Video surveillance is becoming more and more prevalent in today's enterprise environments. Business factors that include security, accountability and monitoring needs drive the implementation of video surveillance systems. Video surveillance systems help keep company assets safe, monitors organizational processes and ensures accountability throughout the entire facility. Because many video surveillance systems today are primarily network (IP) based, Information technology management teams must ensure that local area network infrastructures will be able to support the ever growing need of resources that video surveillance devices require. The purpose of this writing is to discuss and survey the best practices of managing and implementing video surveillance streaming and devices within a local area network.

Introduction

Security is one of the most common aspects of any commercial or consumer application. One of the best practices that businesses utilize is the implementation of security and video surveillance[1]. Video surveillance is one of the biggest precautions that a business can take in order to keep assets protected, ensure company processes are being correctly used and monitor customers, employees and vital facility components without having the need of having to be there physically. In recent years, more and more companies are turning to network-based video surveillance. As an information technology professional, one must ensure that current network infrastructures are able to support the addition of numerous network cameras streaming to various endpoints. Some of these endpoints may include network video recorders, mobile devices, workstations and other storage devices. These are all dependent on current and possible future needs of the business.

As more and more network devices are added to an infrastructure, information technology professionals must make necessary adjustments to accommodate these network devices. In regards to video surveillance, many different protocols must be taken into account in order to stream video across the network. While implementing video surveillance devices, network management must decide whether it is best for their organization to utilize User Datagram Protocol (UDP) [2][3] or Transmission Control Protocol (TCP)[4]. Unicast or multicast streaming are choices in which IT administrators must decide that best suits the desired needs of the company's network infrastructure. At this point, a network professional must determine whether it is best to use unicast [6] or multicast [7] video transmission for network cameras within the local area network. At the next level, protocols such as Real-Time Transport Protocol (RTP) and Hypertext Transfer Protocol (HTTP) create the ability to stream video across networks. Video may possibly use File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP) to transmit this streamed data to centralized server locations in order to access, view and manage at a later date [8]. The implementation of surveillance cameras and the protocols in which video is moved from source to destination is a lengthy process. A network professional must make decisions and changes in order to implement surveillance cameras. In regards to the local area network, surveillance cameras affect other devices and network utilization. There are advantages, disadvantages, differences and requirements of using unicast routing and multicast routing. This paper weighs the options of these differences to ensure effective and efficient video delivery from source to destination.

The purpose of this writing is to inform network professionals the best practices of implementing video surveillance devices within a network. This includes tamper resistant devices, alarm input/outputs, Virtual Local Area Network (VLAN) implementation, standard device configuration and firewall port configuration. Video surveillance and video streaming command a large amount of bandwidth within a local area network will also be discussed. With more and more devices being added to a network, information technology management must make the necessary adjustments in order to ensure networks are stable and can handle the additional bandwidth requirements of these additional network devices [9]. Some network professionals have declared that choosing the correct type of streaming protocol can actually save a company [10]. More information and studies will be detailed in a later section of this writing.

Not only will this writing focus on fixed camera streaming assets to set storage and network video recorders, but also streaming over a network to mobile devices has become a much more common practice[11]. Also noted will be the changing needs of network and streaming protocols differing from a fixed environment to a more mobile environment A published journal states that mobility may actually lower the distinction between unicast and multicast streaming in video surveillance [2].

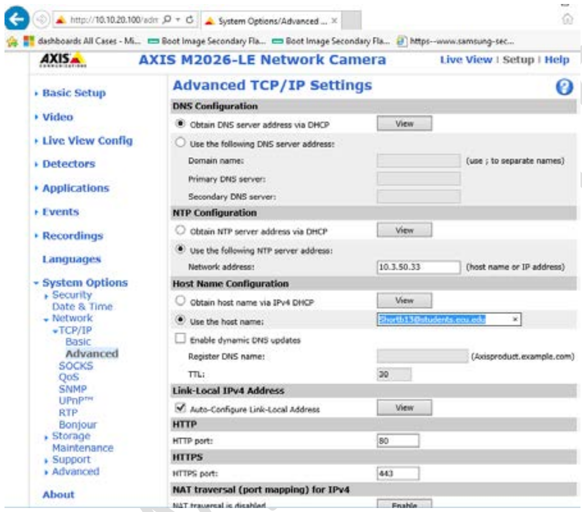
This paper will present a glimpse for the use of multicast and unicast when implementing video surveillance [12]. Best practices when implementing these network devices will be discussed in detail, as well as the advantages and disadvantage of each in various situations within a network.

IP Cameras - Physical

Surveillance devices, such as network cameras, are used my many organizations to monitor and protect company assets. Unlike older traditional analog cameras, Network cameras utilize Internet Protocol (IP), which transmits data over networks using various protocols, all of which are UDP and/or TCP. Although these devices are used for security purposes, the devices themselves must be secure as well. Many network cameras are equipped with unique vandal-resistant and tamper-resistant mechanisms to prevent damage and physical loss of devices. Network cameras are powered by power-over-ethernet (PoE), which utilizes pins within the cat6 network cable to supply power to electronic devices, in this case, network cameras. Because these devices are powered via PoE, camera positions can be installed anywhere within 100 meters of a PoE enabled switch, making installations of network cameras possible in virtually any location required.

IP Cameras - Software

IP cameras typically run a Linux kernel based operating system within the camera. This is the central brains of the device. All software configurations may be administered from the designated web page. This web page may be accessed from the IP address that is assigned to this camera, which can be assigned via DHCP or it can be assigned statically.



AXIS M2026-LE Network Camera

Advanced TCP/IP Settings

DNS Configuration

● Obtain DNS server address via DHCP

○ Use the following DNS server address:

Domain name: (use ; to separate names)

Primary DNS server:

Secondary DNS server:

NTP Configuration

○ Obtain NTP server address via DHCP

● Use the following NTP server address:

Network address: 10.3.50.33 (host name or IP address)

Host Name Configuration

○ Obtain host name via IPv4 DHCP

● Use the host name: Shorttb13@students.ecu.edu

□ Enable dynamic DNS updates

Register DNS name: (Axisproduct.example.com)

TTL: 30

Link-Local IPv4 Address

☑ Auto-Configure Link-Local Address

HTTP

HTTP port: 80

HTTPS

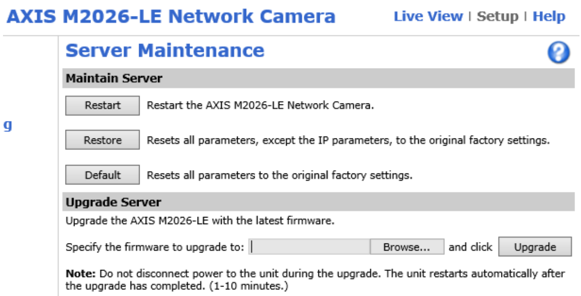
HTTPS port: 443

NAT traversal (port mapping) for IPv4

NAT traversal is disabled

Figure 1-1

Axis is one of the leading brands of enterprise-level network cameras. In Figure 1-1, TCP/IP settings are shown for the Axis M2026-LE network camera. Various settings may be adjusted here by accessing the web interface. Some of the protocols shown in Figure 1-1 will be discussed in a later section.



AXIS M2026-LE Network Camera

Server Maintenance

Maintain Server

Restart the AXIS M2026-LE Network Camera.

Resets all parameters, except the IP parameters, to the original factory settings.

Resets all parameters to the original factory settings.

Upgrade Server

Upgrade the AXIS M2026-LE with the latest firmware.

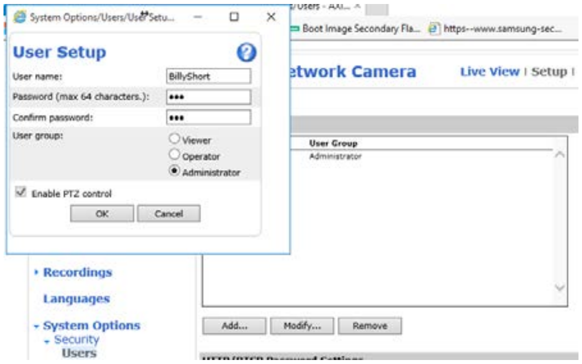
Specify the firmware to upgrade to: and click

Note: Do not disconnect power to the unit during the upgrade. The unit restarts automatically after the upgrade has completed. (1-10 minutes.)

Figure 1-2

Firmware updates are vital in ensuring network devices connected to a local area network are secure. Firmware updates must be applied, typically following maintenance schedules in place by security policies of an organization. Once updates are released from the manufacturer, they may be applied directly to the device, as shown in Figure 1-2. Firmware updates may include various security patches and updates, vulnerability notices, and last but not least, more features that are available or innovated for the device. Just like any other device within a network, it is very important to keep firmware updated in order to keep networks as safe and secure as possible.

Lastly, general setup must include storage devices, password setups or web logins, and user accounts for streaming video. Cameras can be configured on a per user basis. Certain users may have the ability to view different parts and settings of the network camera based on its security rights and privileges.



User Setup

User name: BillyShort

Password (max 64 characters.): •••

Confirm password: •••

User group: ○ Viewer ○ Operator ● Administrator

☑ Enable PTZ control

Figure 1-3

Figure 1-3 shows the user "BillyShort" being added as an administrator to the network camera device. This allows that user to adjust all settings and other advanced settings that is on the camera. Most users typically only need operator or viewer rights because settings can only be adjusted by administrator users, which should not need to be adjusted once they are set. Passwords are encrypted within the network camera using an advanced algorithm. After passwords are created, storage devices must be configured in order to receive data from cameras across the network. Network Video Recorders (NVR's) are storage devices that have a local interface. These devices are able to record large amounts of data and provide an easy to use interface for users to play back video and other information that the cameras may have. Storage is a huge must because it allows organizations to have the ability to review video instead of a more traditional approach of having security guards manning video camera stations at all times. Because devices such as NVR's receive transmitted data from network cameras on the LAN, it is important that cameras are configured to optimally perform.

Problem Statement

As discussed in an earlier section, more and more devices are connecting to local area networks. This requires information technology teams and network administrators make changes to network infrastructure to keep up with the new demands of these network devices. In order to keep up with this demand, IT teams must decide on multiple aspects of the implementation of surveillance systems and network camera devices. Based on the information in this writing, IT teams will be able to choose what standards are best in regards to surveillance systems for their network needs from demands within their organization.

Protocol Selection

The proposal in this writing will compare various video streaming protocols. These protocols will focus on UDP and TCP protocols, including multicast video streaming and TCP video streaming. Advantages and disadvantages will be compared in regards to both UDP and TCP, and how unicast and multicast should be used in certain situations, as well as why unicast should still be implemented.

Video Streaming - UDP and TCP

Network devices are growing at an exponential rate on local area networks. Information technology management teams must realize Internet of Things (IoT) devices are becoming more and more prevalent in today's networks. Because of the massive growth in the utilization of these devices, networks must be able to accommodate these devices with appropriate speeds and bandwidth needed. Network cameras and network surveillance devices transmit and stream video from one location to another, and in some cases, multiple destinations. Because of this, there is a high demand of bandwidth to transmit this high definition video across networks. All video is transmitted via User Datagram Protocol (UDP) or Transmission Control Protocol (TCP). TCP streaming is connection-oriented streaming. TCP uses acknowledgements in order to transmit data from source to destination, meaning that one bit is transferred, the source receives an acknowledgement from the destination confirming the bit made it to destination. Once the destination reply has made it back to the source, more bits will be sent. UDP does not use acknowledgements. This protocol essentially floods the destination with the bits almost in real time because it does not require replies from the destination. High Definition video can be a large amount of bits per second, so UDP is the preferred means of streaming live video. UDP is much more efficient and overall faster in comparison to TCP. UDP is not only preferred in video streaming, but it is also preferred in other time sensitive applications such as VoIP applications and other sources of live video or streaming services such as Netflix and Hulu. Instead of awaiting replies from a bad bit sent from source to destination, UDP continues to send packets, providing an uninterrupted video stream.

Unicast and Multicast streaming

Unicast video can be described as information, in this case, video streaming, is sent from point A to point B. The source of video streaming can only send that data and video to one destination, which means there is only one sender and one receiver. Unicast was the initial form of data transmission in earlier local area networks, but most networks have migrated to multicast. TCP only supports unicast video streaming due to the acknowledgement requirement. TCP can only send from point A to point B because it cannot transmit data from one source to multiple destinations due to replies required.

Unlike unicast streaming, multicast streaming may allow source video streams to be sent to multiple destinations. For example, source A may send to destination B and C, while unicast would have only been able to send to destination B OR C. When many clients want to stream a live video from a single network, multicast should be employed or adopted. Multicast videos employ UDP at the transport layer. Encoded multicast videos have cameras that transmit only one part of the video into the network and this allows the client to get a video copy. Every client is required to be connected to the source camera in order to utilize Session Description Protocol (SDP) file. This allows any connected clients to get information required to have the video on the internet and to begin rendering and decoding. With the acquisition of the multicast video, CohuHD cameras listen to Real Time Streaming Protocol (RTSP), and hypertext transfer protocol (HTTP) as a way of making connections that are initial to SDP files (CohuHD, 2013).

Advantages of Multicast

As stated in a previous section, UDP is the preferred method of live video transmission. When sending and transmitting video streams to other network devices such as network video recorders, UDP is used in the majority of networks today. Older networks may have used unicast video streaming, but once more and more network devices are connected to the local area network, the migration to multicast is critical for proper network performance and function. Many larger companies send video streams to many different destinations, such as one to a NVR, and another to a security station within an organization. Unicast would not be able to support this due to using TCP protocol and only one source transmitting to one destination. Multicast will support sending video streams to both destinations (Gallagher, 2015).

Disadvantages of Multicast

Because multicast video streaming supports more than two destination links from one source, more network bandwidth is required. This may put more strain on network devices such as routers and switches because bandwidth utilization is much higher than with unicast. The sole advantage that unicast has over multicast in regards to streaming is the fact that unicast costs less to implement and is overall a much less amount of bandwidth required to send video from one source to one destination. Unicast will also ensure the ability to maintain lower latency in network bandwidth utilization due to only one source to one destination ratio (Tyco Security Products,2012).

Other ports and protocols

Network based surveillance systems have the ability to take advantage of other video streaming protocols. Many network cameras use port 80, which is HTTP. Other widely used ports are TCP 554 and RSTP. These ports must be configured in local area network firewalls in order to be utilized. Based on storage protocols, most cameras support H.264 codec, which is a compressed version of streaming video. This allows network video recording hardware to store much more data and information due to the video files stored in the system being compressed. With many network cameras being high definition, ultra high definition, and some even being 4k, network utilization is at all time highs with video surveillance transmission rates.

Conclusion

Larger companies may have much more video surveillance needs than smaller organizations. Because of this, larger organizations should opt for multicast video streaming for their video surveillance systems. Smaller companies may opt for unicast surveillance streaming to storage devices, only because most small companies will only need one source streaming video to one destination. Larger companies may have other requirements, making a multicast streaming environment mandatory. This would include having more than one source to destination video streaming requirement. Cost may play a factor in deciding whether to utilize multicast or unicast. Unicast video streaming tends to be a cheaper option since less destinations are required, meaning less infrastructure is required to support the much higher required bandwidths of implementing multicast. The factors surveyed in this writing must be taken into account in order for information technology team management to decide what network based surveillance system options that best suits enterprise mission objectives.

References

[1] "Workplace video surveillance,". [Online]. Available: http://search.proquest.com.jproxy.lib.ecu.edu/docview/235690328?pq-origsite=summon. Accessed: Mar. 1, 2017.

[2] T. A. Al-Radaei and Z. A. Zukarnain, "Comparison study of transmission control protocol and user Datagram protocol behavior over multi-protocol label switching networks in case of failures," *Journal of Computer Science*, vol. 5, no. 12, pp. 1042–1047, Dec. 2009.

[3] V. Markovski, F. Xue, and L. Trajković, "Simulation and Analysis of Packet Loss in User Datagram Protocol Transfers," *The Journal of Supercomputing*, vol. 20, no. 2, pp. 175–196, 2001.

[4] "FMTCP: a fountain code-based multipath transmission control protocol,". [Online]. Available: http://dl.acm.org.jproxy.lib.ecu.edu/citation.cfm?id=2817007. Accessed: Mar. 1, 2017.

[5] A. Begen, T. Akgul and M. Baugher. Watching video over the web: Part 1: Streaming protocols. *IEEE Internet Comput. 15(2),* pp. 54-63. 2011. Available: http://search.proquest.com.jproxy.lib.ecu.edu/docview/856632509?accountid=10639. DOI: http://dx.doi.org.jproxy.lib.ecu.edu/10.1109/MIC.2010.155.

[6] B. Coetzer, "Video surveillance systems," 2011. [Online]. Available: http://www.intechopen.com/books/video-surveillance. Accessed: Mar. 1, 2017.

[7] B. Bing, "Next-Generation Video Coding and Streaming,". [Online]. Available: http://site.ebrary.com.jproxy.lib.ecu.edu/lib/eastcarolina/detail.action?docID=11156303. Accessed: Mar. 1, 2017.

[8] Plunkett, Lance,J.D., L.L.M. Surveillance cameras in the office. *N. Y. State Dent. J. 79(1),* pp. 8-10. 2013. Available: http://search.proquest.com.jproxy.lib.ecu.edu/docview/1317184444?accountid=10639.

[9] Y. Liu and Y. Morgan, "Rate region of unicast routing networks," *Electronics Letters*, vol. 52, no. 21, pp. 1765–1767, Oct. 2016.

[10] A. Mehdizadeh, F. Hashim, R. S. A. R. Abdullah, and B. M. Ali, "Performance evaluation of cost-effective Multicast–Unicast key management method," *Wireless Personal Communications*, vol. 77, no. 3, pp. 2195–2212, Feb. 2014.

[11] "Mobility weakens the distinction between multicast and unicast,". [Online]. Available: http://dl.acm.org.jproxy.lib.ecu.edu/citation.cfm?id=2992194. Accessed: Mar. 1, 2017.

[12] "MRTP: a multiflow real-time transport protocol for ad hoc networks,". [Online]. Available: http://ieeexplore.ieee.org.jproxy.lib.ecu.edu/document/1608115/. Accessed: Mar. 1, 2017.

[13] Tycho security products. (2012). Multicast video transmission vs. Unicast video transmission methods. Retrieved from https://blog.tycosp.com/index.php/2012/05/14/multicast-video-transmission-vs-unicast-video-transmission-methods/

[14] Tikilive. (2014). Unicast and multicast streaming. Retrieved from http://www.tikilive.com/tiki-blog/tutorials/unicast-and-multicast-streaming/

[15] Jespersen, R. (2016). Six Benefits of P2P Unicast Streaming. Retrieved from https://www.wowza.com/blog/six-benefits-of-p2p-unicast-streaming

[16] Cisco Networking Academy. (2014). Cisco networking academys introduction to scaling networks. Retrieved from http://www.ciscopress.com/articles/article.asp?p=2189637&seqNum=4

[17] Moxa. (2012), CCTV Surveillance System Network Design Guide. Retrieved from http://pins.moxa.com/Tech_note/CCTV%20Surveillance%20System%20Network%20Design%20Guide.pdf

[18] Statseeeker. (2015). Network monitoring best practices for the new networks. Retrieved from https://statseeker.com/blog/2015/08/20/network-monitoring-best-practices-for-the-new-networks/

[19] Griffin, J. (2015). 12 best practices for securing surveillance networks against cyber attacks. Retrieved from http://www.securityinfowatch.com/article/12070169/eagle-eye-networks-whitepaper-outlines-12-best-practices-for-securing-surveillance-networks-against-cyber-attacks

[20] CohuHD. (2013). Video streaming protocols. Retrieved from http://www.cohuhd.com/Files/white_papers/CohuHDVideoStreamingProtocolsWhitePaper.pdf

[21] Gallagher, B. (2015). The Components and Advantages of IPTV. Retrieved from http://leightronix.com/blog/the-components-and-advantages-of-iptv/