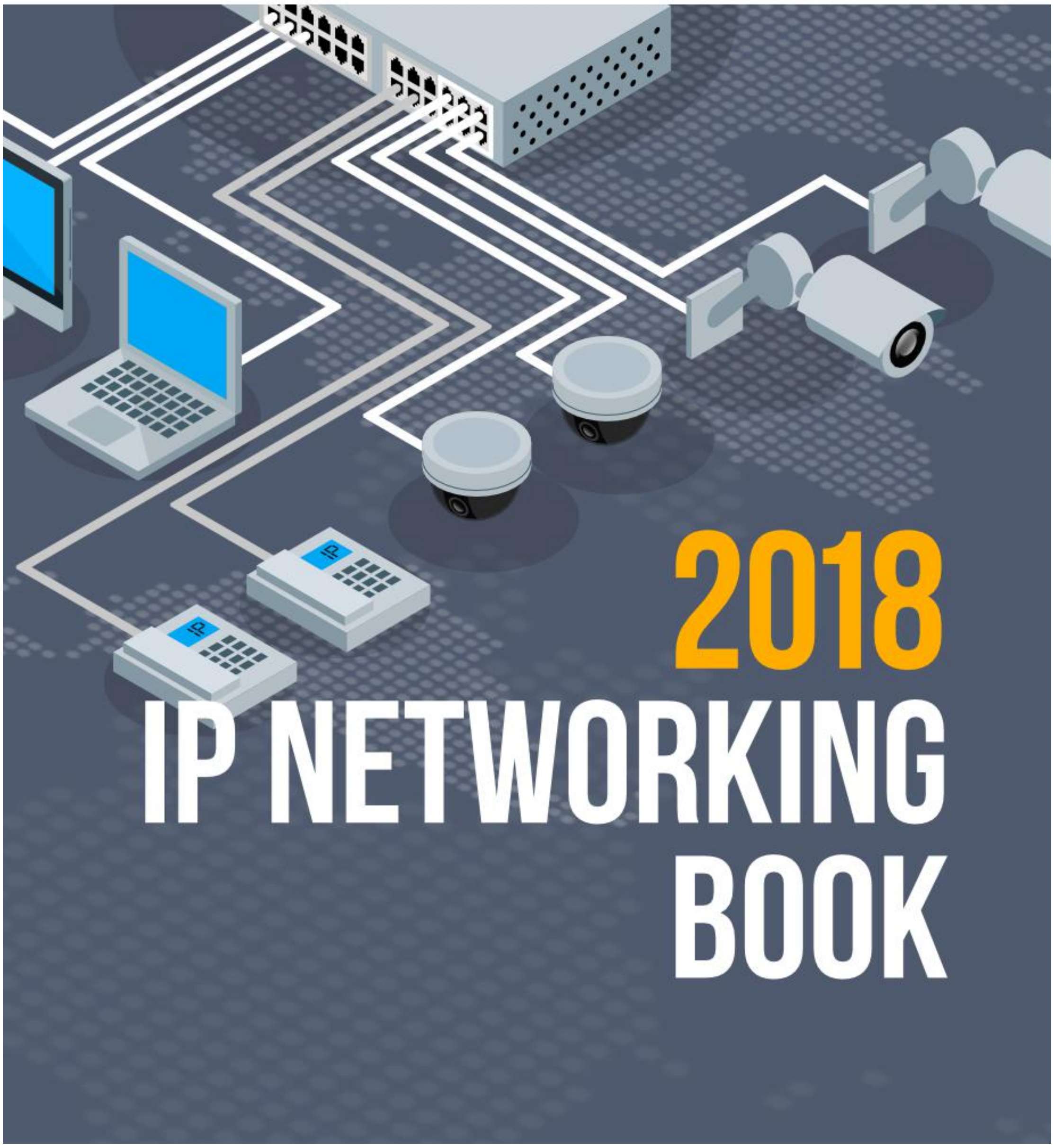
IPVM



2018 IP NETWORKING BOOK

TABLE OF CONTENTS

PREFACE

This book will give you the knowledge and confidence to make the right decisions when designing and deploying video surveillance systems on IP networks and working with IT departments.

IPVM has spent thousands of hours testing video surveillance on IT networks in the past year to measure and document real world performance issues.

If you have questions, please ask any questions in our discussions group and we will be happy to answer them.

If you would like to take a class in IP networking for video surveillance to get certified and learn more, IPVM offers this. Learn more about IPVM courses.

Finally, this book is only authorized for the use of IPVM members with IPVM logins.

Networking Fundamentals

Bandwidth

Bandwidth is the most fundamental element of computer networking for video surveillance systems. Because video surveillance can consume an immense amount of bandwidth and because variations in bandwidth load of surveillance cameras can be so significant, understanding bandwidth for video surveillance is critical.

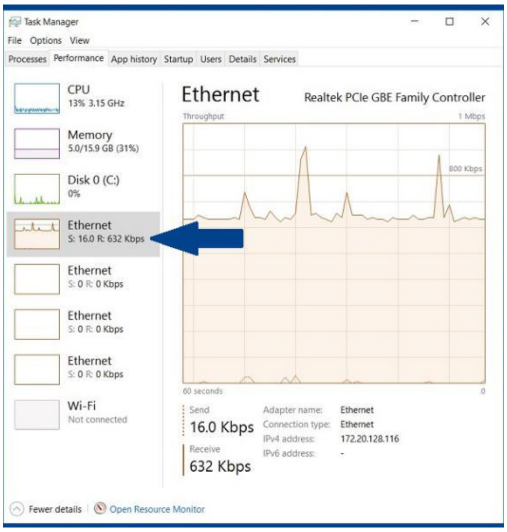
We break down each of the following:

- Measuring Bandwidth
- Bits vs Bytes
- Kilo vs Mega vs Giga
- Bit Rates
- Compression and Bandwidth
- Bandwidth Per Camera
- Constant vs Variable Bit Rates (CBR vs VBR vs MBR)
- Drivers of Camera Bandwidth Consumption
- Practical Examples of Camera Bandwidth
- LAN vs WAN
- Network Bandwidth Capacities
- Symmetric vs Asymmetric Networks
- Sizing Networks for Video Surveillance

Measuring Bandwidth

Bandwidth is typically measured in bits (e.g., 100Kb/s, 1Mb/s, 1000Mb/s, etc.). A bit is the most fundamental unit of bandwidth and storage.

You should be comfortable measuring the bandwidth, in bits, on your computer. On a PC, this can be done by opening up the task manager as shown below:



Send
16.0 Kbps

Receive
632 Kbps

Adapter name: Ethernet
Connection type: Ethernet
IPv4 address: 172.20.128.116
IPv6 address: -

On your computer, it typically shows bandwidth being received by and bandwidth being sent out from your computer (i.e., when you watch a YouTube video you are receiving bandwidth, when you send an email you are transmitting bandwidth). These are also known as download and upload speeds respectively.

Bits vs Bytes

In video surveillance, bandwidth is typically measured in bits but sometimes measured in bytes, causing confusion. 8 bits equals 1 byte, so someone saying 40 Megabits per second and another person saying 5

Megabytes per second mean the same thing but is easy to misunderstand or mishear.

Bits and bytes both use the same letter for shorthand reference. The only difference is that bits uses a lower case ‘b’ and bytes uses an upper case ‘B’. You can remember this by recalling that bytes are ‘bigger’ than bits. We see people confuse this often because at a glance they look similar. For example, 100Kb/s and 100KB/s, the latter is 8x greater than the former.

We recommend you use bits when describing video surveillance bandwidth but beware that some people, often from the server / storage side, will use bytes. Because of this, be alert and ask for confirmation if there is any unclarity (i.e., “Sorry did you say X bits or bytes”).

Kilo vs Mega vs Giga

It takes a lot of bits (or bytes) to send video. In practice, you will never have a video stream of 500b/s or even 500B/s. Video generally needs at least thousands or millions of bits. Aggregated video streams often need billions of bits.

The common expression / prefixes for expressing large amount of bandwidth are:

- Kilobits, is thousands, e.g., 500Kb/s is equal to 500,000b/s. An individual video stream in the kilobits tends to be either low resolution or low frame or high compression (or all of the above).
- Megabits is millions, e.g., 5Mb/s is equal to 5,000,000b/s. An individual HD / MP video stream tends to be in the single digit megabits (e.g., 2Mb/s or 4Mb/s or 8Mb/s are fairly common ranges). More than 10Mb/s for an individual video stream is less common

(the most typical case is from using the less bandwidth efficient MJPEG codec). However, a 100 cameras being streamed at the same time can routinely require 200Mb/s or 400Mb/s, etc.

- Gigabits is billions, e.g., 5Gb/s is equal to 5,000,000,000b/s. One rarely needs more than a gigabit of bandwidth for video surveillance unless one has a very large-scale surveillance system backhauling all video to a central site.

Bit Rates

Bandwidth is like vehicle speed. It is a rate over time. So just like you might say you were driving 60mph (or 96kph), you could say the bandwidth of a camera is 600Kb/s, i.e., that 600 kilobits were transmitted in a second. If you say the bandwidth of your camera is 600Kb or 600KB, not only will you be wrong, you will look incompetent.

Bit rates are always expressed as data (bits or bytes) over a second. Per minute or hour are not applicable, primarily because networking equipment is rated as what the device can handle per second.

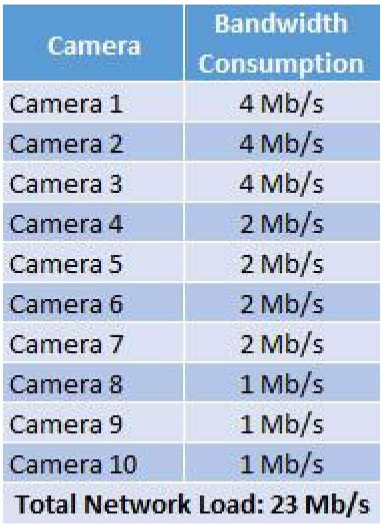
Compression and Bandwidth

Essentially all video surveillance that is sent on an IP network is compressed. Surveillance cameras can produce uncompressed video (e.g., analog) but that is almost always compressed before sending over a network. It is theoretically possible to send uncompressed surveillance video over a network but the immense bit rate of even a single stream (1,000Mb/s+) makes it impractical and unjustifiable for almost all.

Bandwidth Per Camera

Bandwidth is typically measured per camera and the amount of bandwidth each camera needs can vary significantly.

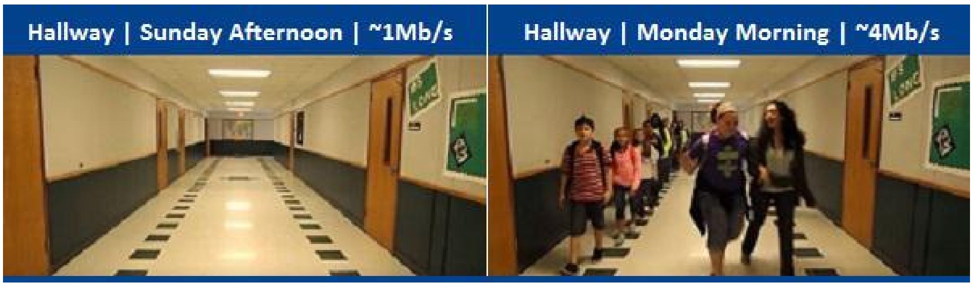
One can and should sum / add up the bandwidth needs of each camera on a network to determine total load. For example, if you have 10 cameras on a network and 3 of them use 4Mb/s, 4 of them use 2Mb/s and 3 of them use 1Mb/s, the total load on the network for those 10 cameras would be 23Mb/s.



Camera	Bandwidth Consumption
Camera 1	4 Mb/s
Camera 2	4 Mb/s
Camera 3	4 Mb/s
Camera 4	2 Mb/s
Camera 5	2 Mb/s
Camera 6	2 Mb/s
Camera 7	2 Mb/s
Camera 8	1 Mb/s
Camera 9	1 Mb/s
Camera 10	1 Mb/s
Total Network Load: 23 Mb/s	

Constant vs Variable Bit Rate (CBR vs VBR vs MBR)

The amount of bandwidth a camera needs at any given time to maintain a specific quality level varies over time, sometimes substantially. For example, a camera might need 1Mb/s for an empty school hallway on a Sunday afternoon but might need 4Mb/s for that same spot come Monday morning.


Hallway | Sunday Afternoon | ~1Mb/s
Hallway | Monday Morning | ~4Mb/s

There are three ways to deal with this:

- Constant bit rates (CBR) , where the bit rate of the camera does not change even if the scene does.
- Variable bit rate (VBR), where the bit rate does change.
- Maximum bit rate (MBR), where the bit rate changes but no more than a user defined maximum

For more, see: CBR vs VBR vs MBR: Surveillance Streaming.

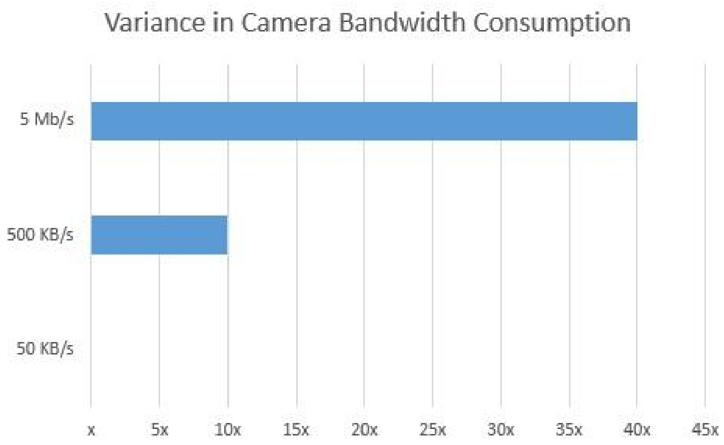
Knowing what type of bit rate control a camera uses is critical, because it impacts bandwidth load significantly.

Statistically, most surveillance networks use variable bit rate today. However, some IT organizations prefer constant bit rate because they can more easily plan around it (i.e., “Ok, I know if I allocate 3Mb/s per camera, using CBR, I will never have to worry about the surveillance cameras using more than Xb/s total (where X is equal to CBR times the number of cameras.”)

Drivers of Camera Bandwidth Consumption

There is no set standard or even typical camera bandwidth consumption. Using a vehicle example, on a US highway, you can reasonably estimate that almost all cars will drive between 55mph and 85mph.

For video surveillance, some video feeds are as low as 50Kb/s (.05Mb/s) and others are routinely 300 times higher at (15000Kb/s) 15Mb/s.



Here are a few common drivers of camera bandwidth consumption:

- Resolution: everything else equal, the greater the resolution, the greater the bandwidth
- Frame rate: everything else equal, the greater the frame rate, the greater the bandwidth
- Scene complexity: The more activity in the scene (lots of cars and people moving vs no on in the scene), the greater the bandwidth needed.
- Night: night time often, but not always, requires more bandwidth due to noise from cameras. See: Testing Bandwidth vs Low Light.
- Model variations: Some models depending on imager or processing can consume far more or less bandwidth.
- Smart Codecs: This is relatively new (developed over the past couple of years), but some cameras even using the same H.264 codec, can intelligently adapt compression for great bandwidth reduction. See: Smart CODEC Guide

Practical Examples of Camera Bandwidth

The following list is an excerpt from IPVM tests of actual bandwidth recording for a variety of cameras:

- Cif 5FPS Office: 50 KB/s
- 720P 10FPS Conference Room: 0.5 Mb/s
- 720P 30FPS Intersection: 4 Mb/s
- 1080P 10FPS Conference Room: 2 Mb/s
- 1080P 30FPS IR On Intersection: 8 Mb/s
- 5MP 15FPs Panoramic Office: 4.5 Mb/s
- 4K 30FPS Intersection: 7 Mb/s
- 4K (super low light) 10 FPS Night Outdoors: 32 Mb/s

Bandwidth and Recorder Placement

Video surveillance consumes network bandwidth in one of the following 2 typical scenarios:

- Camera / encoder to recorder: Video is generally generated in different devices than they are recorded (e.g., a camera generates the video, a DVR / NVR / VMS server records it). In between, the video needs to be transmitted. If it goes over an IP network (e.g., IP cameras to NVR / VMS), bandwidth is required.
- Recorder to client: Statistically, a very low percentage of video is watched by humans. Often, where the person is watching is on a different device on an IP network than the recorder. For example, the recorder might be in a rack in an IT closet but the viewer (i.e., client) is on a laptop, mobile phone or a monitoring station.

Because of this design, the overwhelming majority of bandwidth needed in surveillance systems is dictated by (1) camera type and (2) the relative placement of cameras and recorders.

In terms of camera type, non IP cameras (NTSC / PAL analog, Analog HD, HD SDI) typically do not consume network bandwidth unless video is being sent to clients as each camera has a cable directly connected to a recorder.

For all camera types, the relative physical placement of the recorder near the camera significantly impacts bandwidth needs. For example, imagine 1000 cameras, with 100 cameras each at 10 buildings on a campus. If each building has a recorder, the peak bandwidth requirements will be ~90% lower than if there is only a single site for recording (i.e., each building recording its own might only need ~200Mb/s network connection compared to ~2Gb/s if they are all being sent back to one building). There are pros and cons to each approach but knowing where you will place recorders has a major impact.

LAN vs WAN

The local area network (LAN) and the wide area network (WAN) are two common acronyms in networking. LAN, as the name implies, refers to networks that are local to a building or campus. By contrast, the WAN, are networks that connect 'widely' across cities, states, countries, etc.

Relatively speaking, bandwidth is cheaper and easier on LANs than WANs.

Network Bandwidth Capacities

In LANs, the three most common network bandwidth capacities are:

- 100Mb/s

- 1,000Mb/s (1 Gig)
- 10,000Mb/s (10 Gig)

In particular, 100Mb/s and 1,000Mb/s connections are quite ordinary for modern networks. For more, see the IP Network Hardware for Surveillance Guide.

Lower than 100Mb/s networks in LANs are relics of the past. They may exist from networks installed many years ago but no one installs LAN networks under 100Mb/s today.

WANs can deliver the same or more bandwidth as the LAN but the costs tend to be significantly higher (in the order of 10 or 100x more expensive per bit) because these networks need to run great distances and across many obstacles. While one certainly could secure a 1 Gig WAN connection, the likelihood that one would do this for surveillance is very low, given the cost this would typically incur.

Symmetric vs Asymmetric Bandwidth

Many WAN networks / connections have asymmetric bandwidth, a problem for remote monitoring or recording of video.

Symmetric bandwidth means the bandwidth is the same ‘up’ and ‘down’, i.e., a link can send the same amount of bandwidth as it can receive (100Mb/s up and 100Mb/s down is a classic example).

Asymmetric bandwidth means the bandwidth up and down are not the same. Specifically, the bandwidth ‘up’ is frequently much lower than the bandwidth ‘down’. This is common in homes and remote offices. These asymmetric connections provide sufficient downstream speeds while only providing ~10% of those speeds for upload. The downstream bandwidth might be 10Mb/s or 25Mb/s but the upstream might only be 500 Kb/s or 2Mb/s. In this example, if someone at home wanted to stream a movie (send it downstream from the cloud / Internet), it would not be a problem but if they wanted to upload a movie (or HD surveillance feed), it would be a problem.

The most common asymmetric bandwidth WAN networks are:

- Cable Modem
- DSL
- Satellite

The main exceptions, those that offer symmetrical bandwidth commonplace, are:

- Telecommunication / telephony networks (e.g., T1s, T3s) but these are fairly expensive and relatively low bit rate (e.g., respectively 1.5Mb/s and 45Mb/s)
- Fiber to the Home (FTTH) / Business (FTTB) are much less expensive than telephony networks and routinely offer 100Mb/s connections. The main limitation is access to such networks. While increasing over the past decade, they tend to be limited to densely populated urban areas.

Sizing Networks for Video Surveillance

Putting this information together, to size a network for video surveillance, you will need to know:

- How much bandwidth each camera consumes, recognizing that wide variations can exist
- How close (or far) the recorder is going to be placed to the cameras connected to it, presuming they need an IP network
- What the bandwidth of those network connections are and what pre-existing load those networks must also support.

For more, see: How to Calculate Surveillance Storage / Bandwidth

Video Surveillance Bandwidth

Bandwidth is one of the most fundamental, complex and overlooked aspects of video surveillance.

Many simply assume it is a linear function of resolution and frame rate. Not only is that wrong, it misses a number of other critical elements and failing to consider these issues could result in overloaded networks or shorter storage duration than expected.

Fundamental Issues

- Resolution: Does doubling pixels double bandwidth?
- Framerate: Is 30 FPS triple the bandwidth of 10 FPS?
- Compression: How do compression levels impact bandwidth?
- CODEC: How does CODEC choice impact bandwidth?
- Smart CODECs: How do these new technologies impact bandwidth?

Practical Performance/Field Issues

- Scene complexity: How much do objects in the FOV impact bitrate?
- Field of view: Do wider views mean more bandwidth?
- Low light: How do low lux levels impact bandwidth?
- WDR: Is bitrate higher with WDR on or off?
- Sharpness: How does this oft-forgotten setting impact bitrate?
- Color: How much does color impact bandwidth?
- Manufacturer model performance: Same manufacturer, same resolution, same FPS. Same bitrate?

Scene Complexity

The most basic commonly missed element is scene complexity. Contrast the 'simple' indoor room to the 'complex' parking lot:

Even if everything else is equal (same camera, same settings), the 'complex' parking lot routinely requires 300%+ more bandwidth than the 'simple' indoor room because there is more activity and more details. Additionally, scene complexity may change by time of day, season of the year, weather, and other factors, making it even more difficult to fairly assess.

We look at this issue in our Advanced Camera Bandwidth Test.

Resolution

On average, a linear relationship exists between pixel count (1MP, 2MP, etc.) and bandwidth. So for example, if a 1MP camera uses 1 Mb/s of bandwidth, a 2MP camera on average might use ~2Mb/s.

However, variations across manufacturers and models are significant. In IPVM testing, some cameras increase at a far less than linear level (e.g., just 60% more bandwidth for 100% more pixels) while others rose at far greater than linear (e.g., over 200% more bandwidth for 100% more pixels). There were no obvious drivers / factors that distinguished why models differed in their rate of increase.

As a rule of thumb, a 1x ratio may be used when estimating bandwidth difference across resolution. However, we strongly recommend measurements of actual cameras as such a rule of thumb may be off by a lot.

Frame Rate

Frame rate impacts bandwidth, but for inter-frame CODECs such as H.264, it is less than linear. So if you increase frame rate by 10x, the increase in bandwidth is likely to be far less, often only 3 to 5 times more bandwidth. Illustrating this, we took 30, 10, and 1 fps measurements to demonstrate the change in bit rate in a controlled setting in our conference room. The average bitrates were as follows:

- 1 fps: 0.179 Mb/s
- 10 fps: 0.693 Mb/s (10x the frames of 1 fps, but only 4x bandwidth)
- 30 fps: 1.299 Mb/s (3x the frames of 10 fps, but only double bandwidth. 30x frames of 1 fps, but only 7x bandwidth)

(These measurements were done at 1 I frame per second with quantization standardized ~28.)

For more detail on frame rate's impact on bitrate, see our Frame Rate Guide for Video Surveillance.

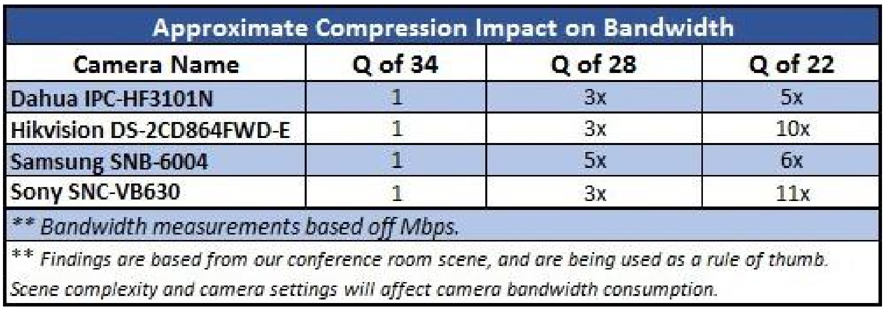
Compression

Compression, also known as quantization, has an inverse relationship to bandwidth: the higher the compression, the lower bandwidth will be.

CRITICAL: Compression and resolution are two different things. In IPVM courses, we routinely see professionals mix the two. Resolution, in our industry, is the number of pixels in an image / video. Compression is how heavily compressed those pixels are.

For example, the chart below shows the impact of compression across four different cameras (note: with H.264, quantization / compression is measured on a standard scale of 0 to 51, higher meaning more compression, lower quality).

Lowering quantization from 34 (high compression) to 28 (average) resulted in at least a 3x increase in bandwidth, while further lowering it to 22 (very low compression) resulted increases of 5-11x depending on the camera.



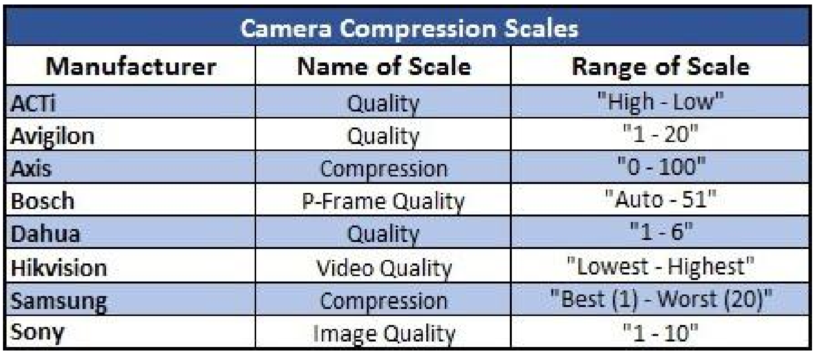
Approximate Compression Impact on Bandwidth

Camera Name	Q of 34	Q of 28	Q of 22
Dahua IPC-HF3101N	1	3x	5x
Hikvision DS-2CD864FWD-E	1	3x	10x
Samsung SNB-6004	1	5x	6x
Sony SNC-VB630	1	3x	11x

*** Bandwidth measurements based off Mbps.*

*** Findings are based from our conference room scene, and are being used as a rule of thumb. Scene complexity and camera settings will affect camera bandwidth consumption.*

Additionally, manufacturers use different scales and terminology for their compression levels with most giving little indication of what actual quantization level is used. Some may use a numeric scale from 1-100, while others use labels such as "low, high, best", and others use the actual 0-51 quantization scale. This chart shows just some of the options in use:



Camera Compression Scales

Manufacturer	Name of Scale	Range of Scale
ACTi	Quality	"High - Low"
Avigilon	Quality	"1 - 20"
Axis	Compression	"0 - 100"
Bosch	P-Frame Quality	"Auto - 51"
Dahua	Quality	"1 - 6"
Hikvision	Video Quality	"Lowest - Highest"
Samsung	Compression	"Best (1) - Worst (20)"
Sony	Image Quality	"1 - 10"

See our IP Camera Manufacturer Compression Comparison for more detail on understanding manufacturer differences and how to standardize Q levels across different lines.

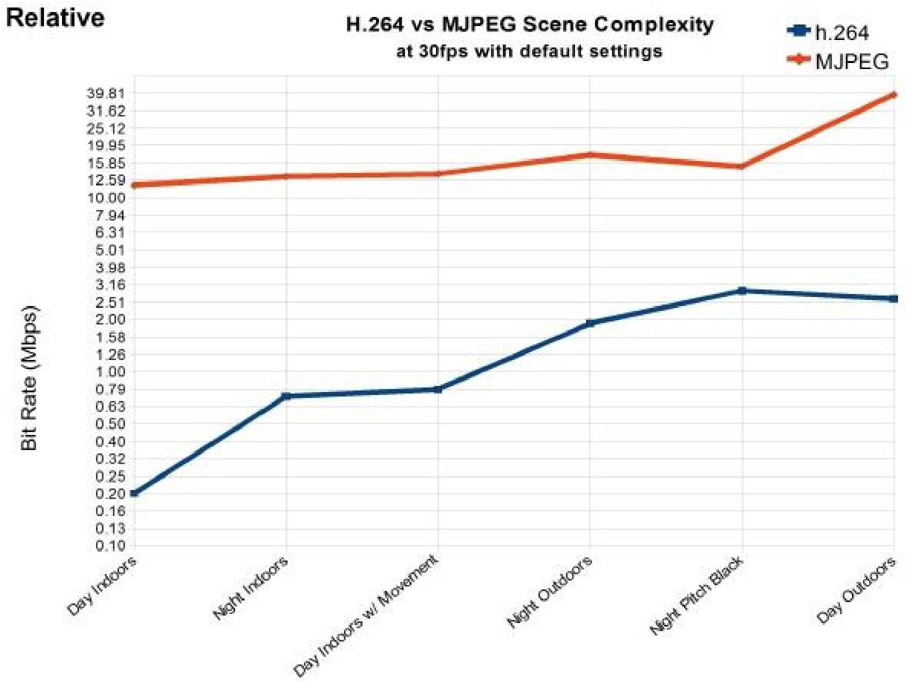
CODECs

A key differentiation across CODECs is supporting inter-frames (e.g., H.264, H.265) vs intra-frame only (e.g., MJPEG, JPEG2000).

- Inter-frame CODECs such as H.264/265 not only compress similar pixels in an image, they reference previous frames and transmit only the changes in the scene from frame to frame, potentially a large bandwidth savings. For example, if a subject moves through an empty hallway, only the pixels displaying him change between frames and are transmitted, while the static background is not.
- Intra-frame only CODECs encode each individual frame as an image, compressing similar pixels to reduce bitrate. This results in higher bandwidth as each frame must be re-encoded fully, regardless of any activity in the scene.

For more on inter and intra frame compression, see our CODEC tutorial.

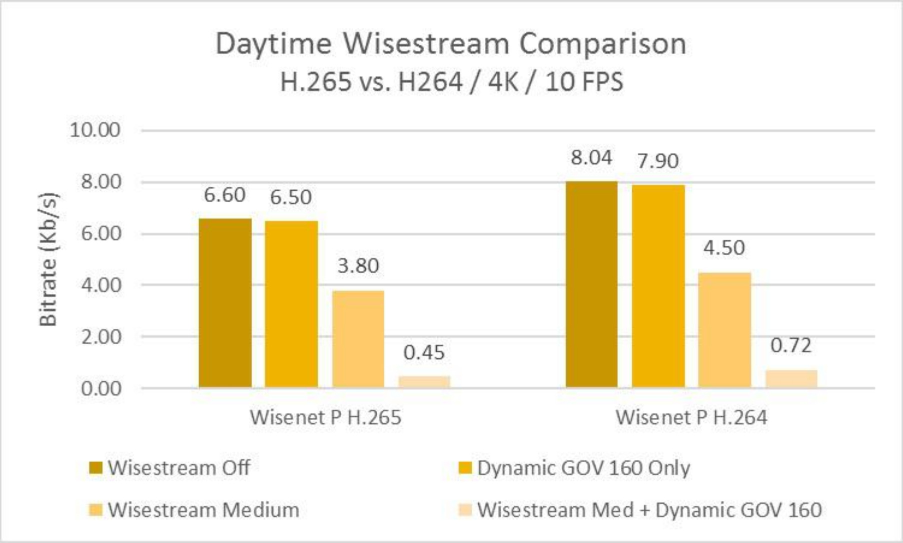
The vast majority of cameras in use today, and for the past several years, use H.264, due to its bandwidth advantages over MPEG-4 and Motion JPEG. In our H.264 vs MJPEG - Quality and Bandwidth Tested shootout, H.264 consumed far less bandwidth in all scenes than MJPEG, seen in the chart below:



What About H.265?

H.265 has been the "next big thing" in CODECs for several years, claiming 50% savings over H.264, but camera and VMS support for it remain relatively rare. Additionally, in our tests, H.265 has had limited benefit over H.264 in similar scenes, about 10-15% on average, with H.264 Smart CODEC cameras (see section below) generally providing bigger bandwidth savings than H.265.

For example, in our Smart H.265 Samsung Test, H.265 produced ~15-20% lower bitrates than H.264 (with smart CODECs off on both), shown in the chart below. However, using smart CODECs with H.264, bitrates dropped by at least ~40% (daytime still scene) and as much as 90%+.



Note that H.265 is still developing, and will likely become more efficient over time, as H.264 has.

Readers should see our H.265 / HEVC Codec Tutorial for more details on H.265 issues, including bitrates, camera support, and VMS integration.

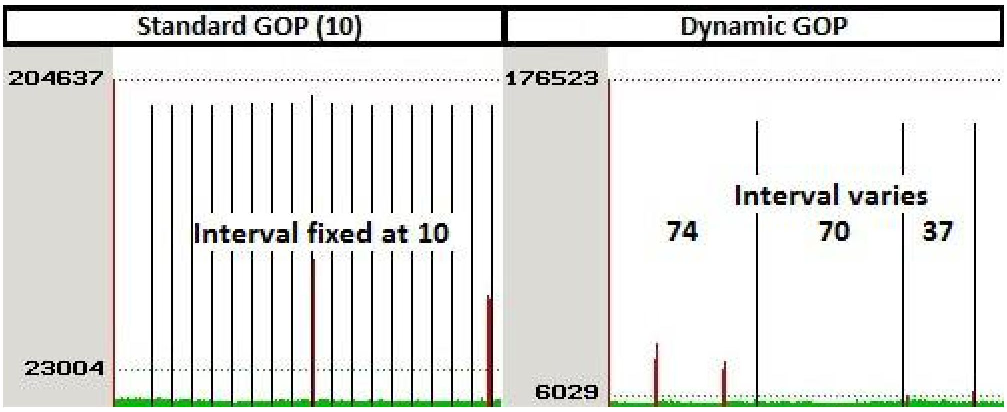
I-Frames vs. P-Frames

In inter-frame CODECs, frames which capture the full field of view are called I-frames, while those sending only changes are P-frames. Because they capture a full image, the more I-frames in a stream, the higher the bandwidth.

For years, cameras were typically only able to use a fixed I-frame interval, measured either in seconds or frames. Sending too few I-frames could negatively impact imaging, with long "trails" of encoding artifacts, while too many I-frames provides little to no visible benefit, seen in this video from our Test: H.264 I vs P Frame Impact.

Note: ***Click here to watch the video on IPVM***

However, with the introduction of Smart CODECs in the past 1-2 years, cameras are now able to dynamically adjust I-frame interval, instead of using a fixed value. So where a typical 10 FPS camera might be set to send an I-frame every second, a smart CODEC enabled model would extend this when there is no motion in the scene, shown in this example:

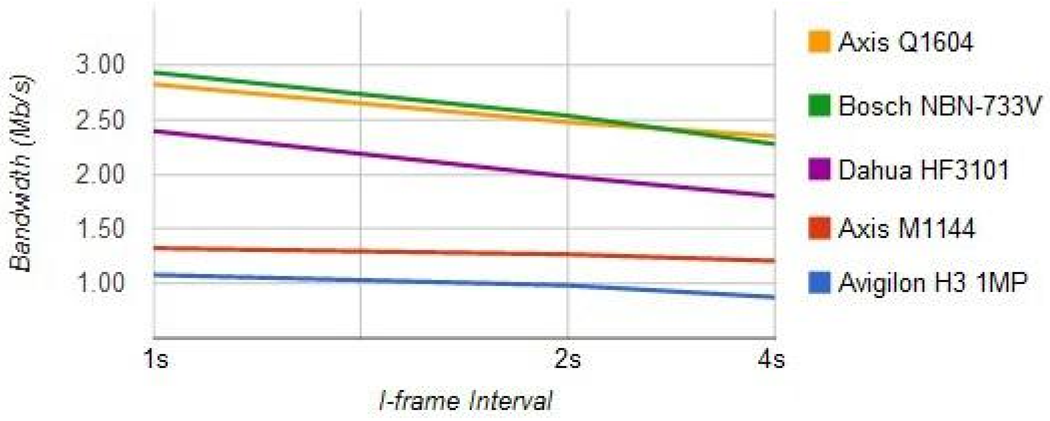


Smart CODECs are a complex topic, covered in more detail below and in our Smart CODEC Guide.

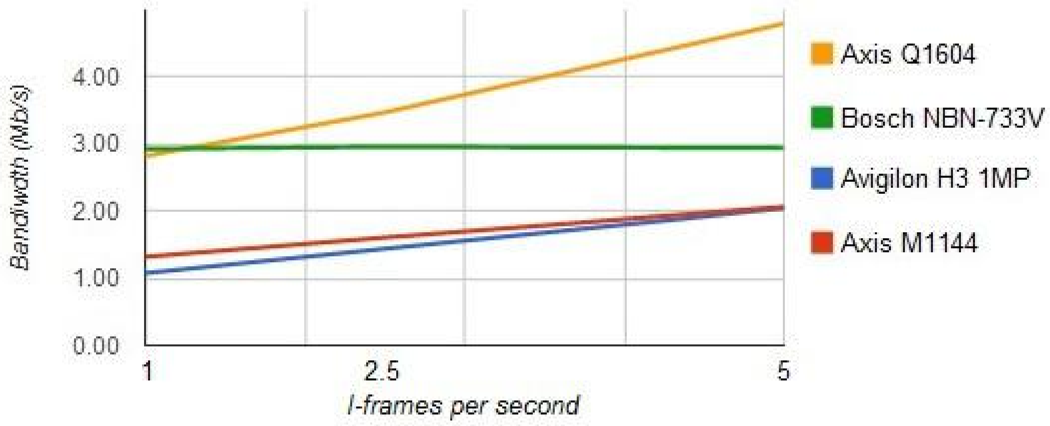
Fixed I-frame Interval Effects

Though many cameras are smart CODEC enabled and do not use fixed I-frame intervals, many (especially older models) do not and users may simply choose not to use them, so it is important to understand the impact of I-frame interval on bandwidth.

Reducing the number of I-frames (moving from 1 to 2 to 4 second interval) produces minimal bandwidth reductions, as seen below, despite the severe negative image quality impact.



Inversely, increasing the number of I-frames to more than one per second significantly increased bandwidth, despite the minimal increase in image quality.



For full details on I and P frame impact on bandwidth and image quality see our H.264 I vs P Frame Test.

Smart CODECs

One recent development with huge impact on bandwidth is the introduction of smart CODECs. These technologies typically reduce bitrate in two ways:

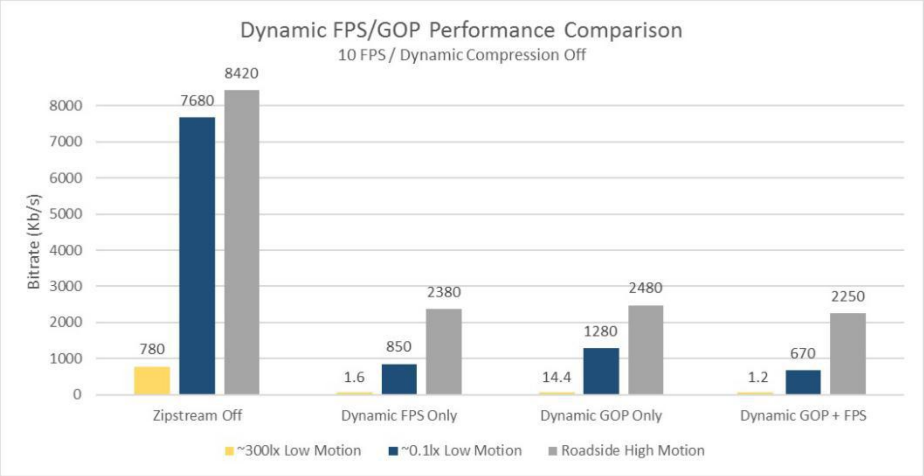
- Dynamic compression: First, instead of using a single compression level for the whole scene, the camera may apply little compression to moving objects, with higher compression/lower quality on static background areas, since we most often do not need detailed images of still areas of the scene.

- Dynamic I-frame interval: Second, instead of using a steady I-frame interval, cameras may increase the distance between I-frames when the scene is still, with some extending to very long intervals in our tests, over a minute in some cases. Then, when motion begins, the camera immediately generates an I-frame and reduces interval to previous levels.

Some smart CODECs may use other methods as well, such as dynamic framerates (used by Axis/Avigilon), increased/improved digital noise reduction (Panasonic Smart Coding), and others.

Exact methods used by each smart CODEC and their effectiveness vary. However, in general, bitrates in still scenes were reduced by 50-75% in our tests, with over 95% possible.

As an example, in our test of Zipstream 2, bitrates dropped by ~99% in still scenes using dynamic compression, I-frame interval, and FPS:

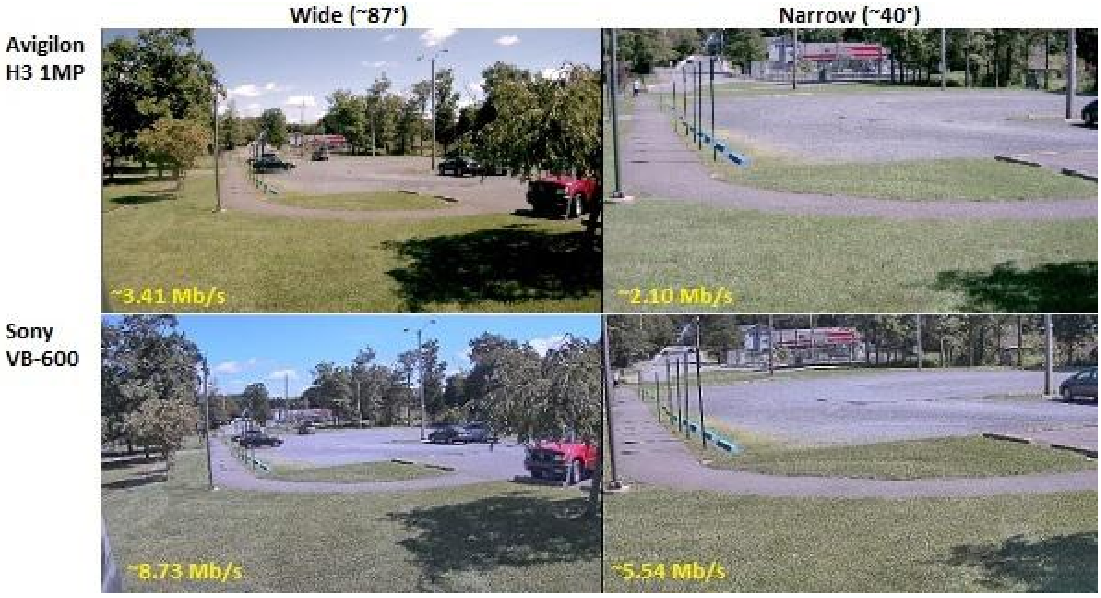


For more details, see our Smart CODEC Guide.

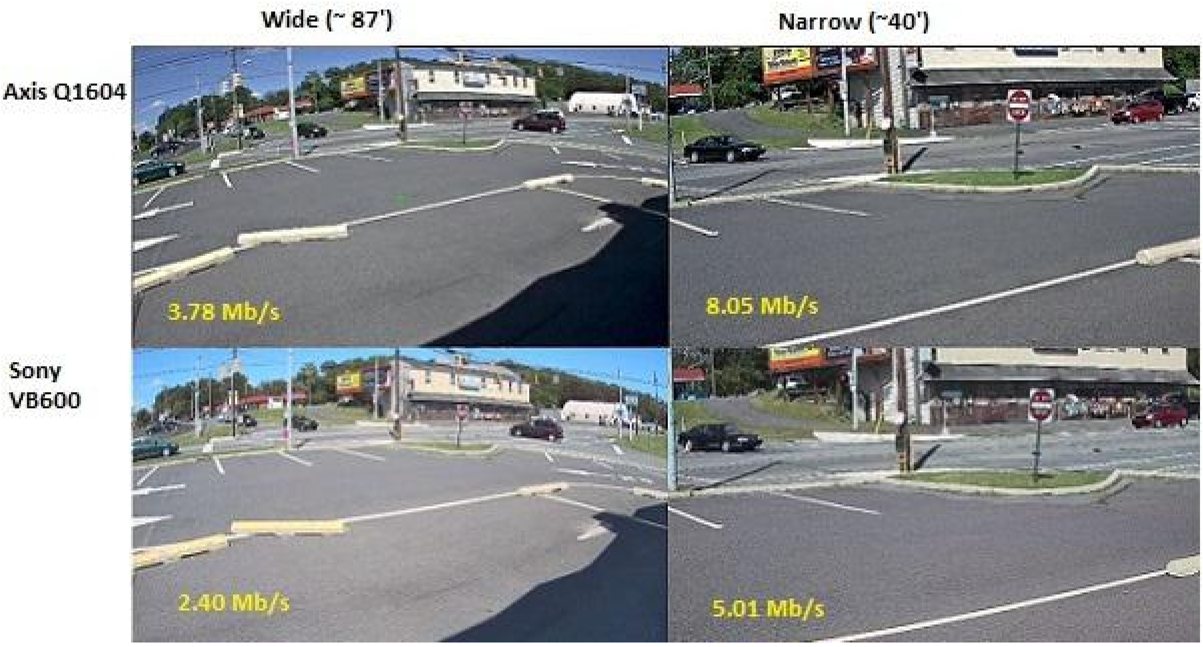
Camera Field of View

Field of view's impact on bandwidth varies depending on which width reveals more complex details of the scene. In scenes with large areas of moving objects, such as trees or other blowing vegetation, widening the field of view will likely increase bandwidth. In scenes with relatively low movement but repetitive backgrounds, such as parking lots, roofing, patterned carpet or walls, etc., narrowing the field of view will increase bandwidth due to more of these fine details being discernible.

For example, in the park shown below, increasing the field of view results in a ~60% increase in bandwidth due to more moving foliage and shadows in the scene compared to the narrower field of view.



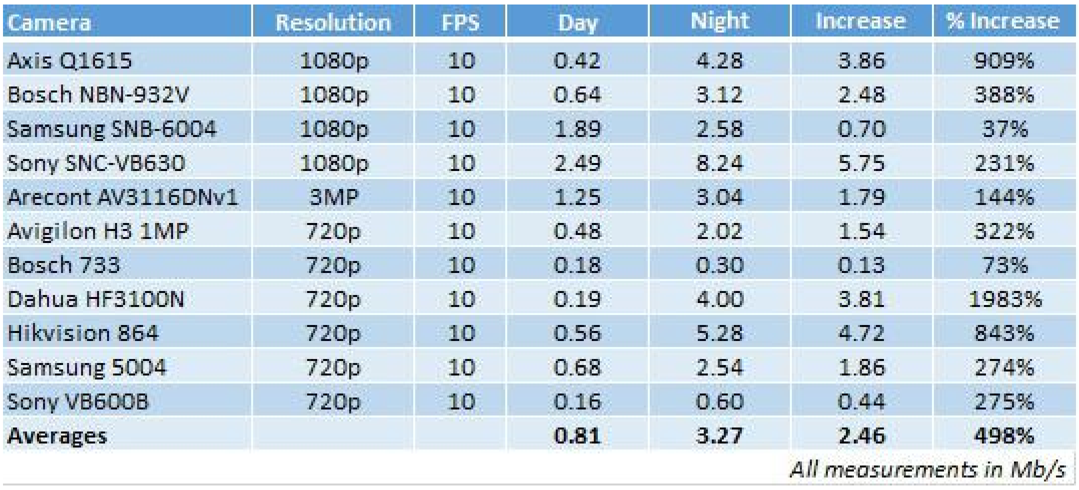
However, in a busy intersection/parking lot, bandwidth decreases by over 50% in the cameras below when widening the field of view. In the narrower FOV, more details of buildings are visible, and the repetitive pattern of the asphalt parking lot may be seen as well, making the scene more difficult to encode.



For further details of field of view's impact on bandwidth, see our Advanced Camera Bandwidth Test.

Low Light

Compared to day time, low light bitrates were an average of nearly 500% higher (seen below). This is mainly caused by increased digital noise caused by high levels of gain.

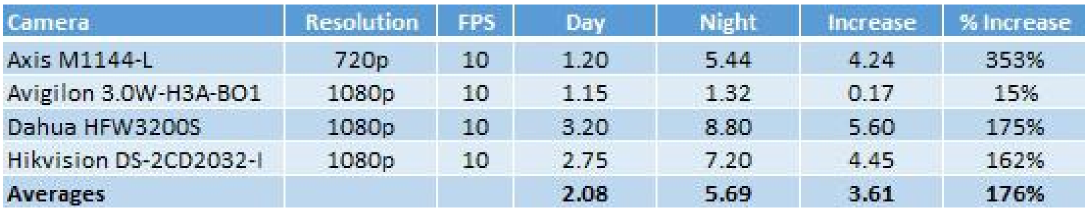


Camera	Resolution	FPS	Day	Night	Increase	% Increase
Axis Q1615	1080p	10	0.42	4.28	3.86	909%
Bosch NBN-932V	1080p	10	0.64	3.12	2.48	388%
Samsung SNB-6004	1080p	10	1.89	2.58	0.70	37%
Sony SNC-VB630	1080p	10	2.49	8.24	5.75	231%
Arecont AV3116DNv1	3MP	10	1.25	3.04	1.79	144%
Avigilon H3 1MP	720p	10	0.48	2.02	1.54	322%
Bosch 733	720p	10	0.18	0.30	0.13	73%
Dahua HF3100N	720p	10	0.19	4.00	3.81	1983%
Hikvision 864	720p	10	0.56	5.28	4.72	843%
Samsung 5004	720p	10	0.68	2.54	1.86	274%
Sony VB600B	720p	10	0.16	0.60	0.44	275%
Averages			**0.81**	**3.27**	**2.46**	**498%**

All measurements in Mb/s

However, two key improvements are increasingly used to reduce this:

- Digital noise reduction techniques have improved in recent years, greatly reducing these spikes on many cameras.
- Increased use of integrated IR cameras results in smaller spikes at night. Compared to nearly 500% in day/night models, integrated IR cameras increased by an average of 176% due to IR illumination (seen below).

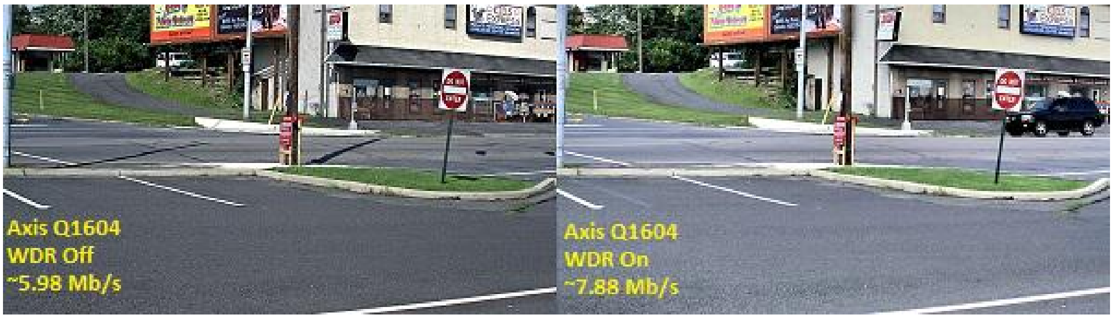


Camera	Resolution	FPS	Day	Night	Increase	% Increase
Axis M1144-L	720p	10	1.20	5.44	4.24	353%
Avigilon 3.0W-H3A-BO1	1080p	10	1.15	1.32	0.17	15%
Dahua HFW3200S	1080p	10	3.20	8.80	5.60	175%
Hikvision DS-2CD2032-I	1080p	10	2.75	7.20	4.45	162%
Averages			**2.08**	**5.69**	**3.61**	**176%**

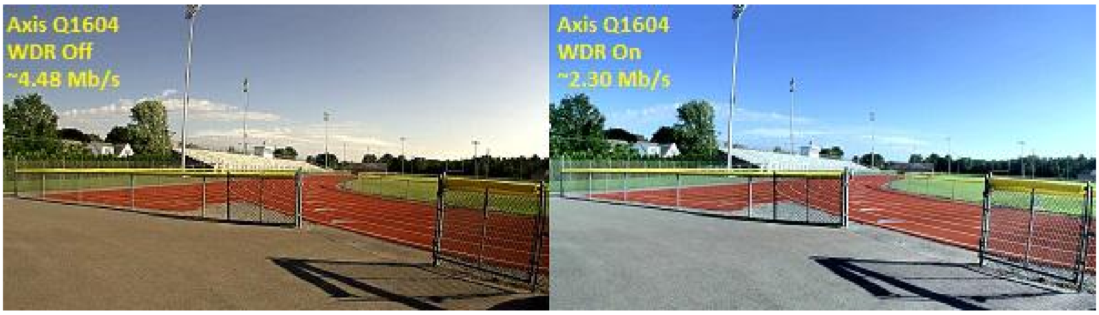
For full details of low light's impact on bandwidth, see our Bandwidth vs Low Light test report.

Wide Dynamic Performance

WDR's impact on bitrate varies depending on the camera and the scene. Again taking examples from our Advanced Camera Bandwidth Test, when switching WDR on in an Axis WDR in an outdoor intersection scene, bandwidth increases, as more details are visible (beneath the eaves of buildings, in the treeline, etc.).



However, looking at an outdoor track and sports field, bandwidth decreases. In this case, the Q1604 increases contrast slightly on some areas of the image, such as the trees and bleachers in the center/left of the FOV. Because of this, these areas are more similarly colored and easier to compress, lowering bitrate.

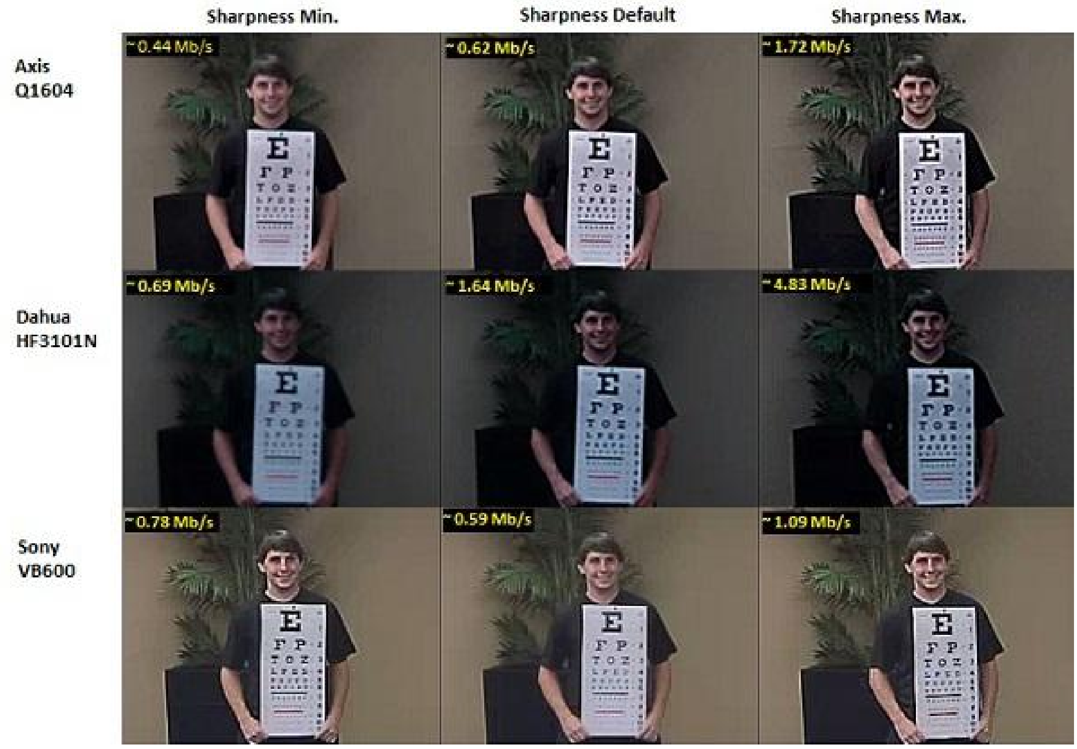


Note that for other cameras, these results may vary, depending on how well they handle light and dark areas, how they handle contrast when WDR is turned on, and more.

Sharpness

Sharpness has a huge impact on bandwidth consumption, yet it is rarely considered during configuration, even by experienced technicians. Oversharpening reveals more fine (though rarely practically useful) details of the scene, such as carpet and fabric patterns, edges of leaves and blades of grass, etc. Because more detail is shown, bandwidth increases.

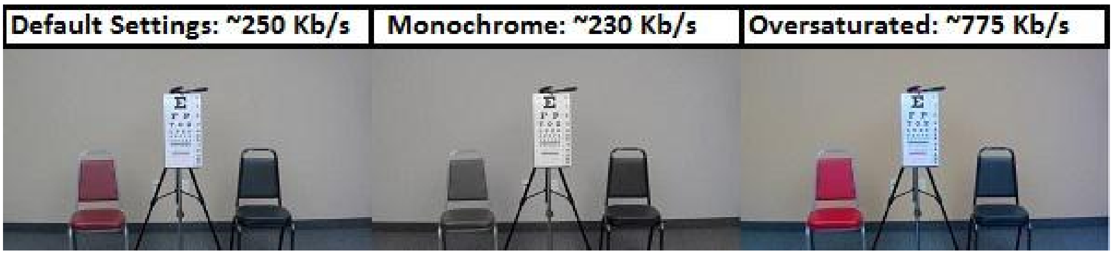
For example, in the FOV below (from our Advanced Camera Bandwidth Test), bitrate increases by nearly 600% from minimum to maximum sharpness in the Dahua camera, and almost 300% in the Axis Q1604.



Color vs. Monochrome

At practical levels (without desaturation or oversaturation effects), color has minimal impact on bandwidth. In the examples below, moving from default color settings to monochrome decreases bandwidth by 20 Kb/s, about an 8% decrease.

However, oversaturation may result in abnormally high bandwidth. In this example, bandwidth increases by over 200% when changing color settings from default to their highest level, which also creates oversaturation effects such as color bleeding (seen in the red chair).

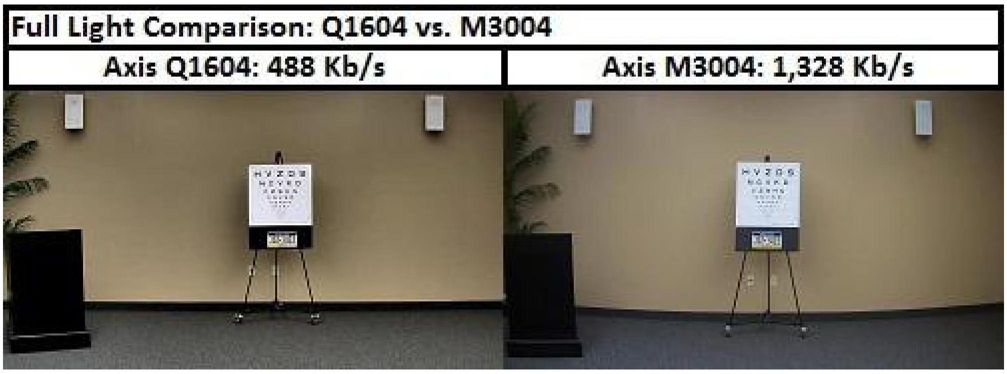


One practical example of a manufacture desaturating their video to 'save' bandwidth is Arecont Bandwidth Savings Mode (which we tested here).

Manufacturer Model Differences

Across specific models in a given manufacturer's line, significant differences in bitrate may occur, despite the cameras using the same resolution and framerate. This may be due to different image sensors or processors being used, different default settings in each model, better or worse low light performance, or any number of other factors.

For example, the following image shows two cameras, an Axis Q1604 and Axis M3004, both 720p, 10 fps, set to a ~20' horizontal FOV, at compression of ~Q28. Despite these factors being standardized, in this well lit indoor scene, the Q1604's bitrate was 488 Kb/s while the M3004 consumed 1.32 Mb/s, nearly 3x the bandwidth.



Beware: model differences have become more extreme in some cases, as some cameras support Smart CODECs while others in the same line may not.

Measure Your Own Cameras

As this guide shows, there are few easy, safe rules for estimating bandwidth (and therefore) storage, abstractly. Too many factors impact it, and some of them are driven by impossible to know factors within the camera.

Though it is important to understand which factors impact bandwidth, use this knowledge with your own measurements of the cameras you plan to deploy. This will ensure the most accurate estimates and planning for deployments.

Network Addressing

We explain addressing devices on IP networks, focusing on how IP cameras and recorders are used in those networks.

- MAC Addresses
- Multiple NICs Possible
- Manufacturer OUIs
- IP Addresses
- Address Conflicts
- IPv4 vs IPv6 Formats
- Video and IP Addresses
- Dynamic vs. Static Addresses
- Public vs Private Addresses
- Network Classes

MAC Addresses

All network devices (PCs, servers, cameras, switches, etc.) are hardcoded with a permanent address, called a MAC address (Media Access Control), a unique 12 character identifier, such as:

AC:CC:8E:0C:B5:F4

Since MAC addresses are issued at the factory and do not change, they are generally useful for identifying devices on a network even if the IP address is unknown.

Multiple MACs Possible but Unlikely

If a device has multiple network interfaces, it may have more than one single MAC address. The MAC is associated with a device's network interfaces, but not the general device. In the case of cameras with multiple network connections, like a camera with both a wired ethernet port and an integrated wireless radio, the device would have more than a single MAC address.

However, since the vast majority of cameras include only a single ethernet port, the MAC address could be/is often indirectly used to describe the entire camera.

Organizationally Unique Identifier

The first six digits of a MAC are called the OUI, and each manufacturer is assigned one or more unique identifiers. For example, these are the OUIs of some common cameras manufacturers:

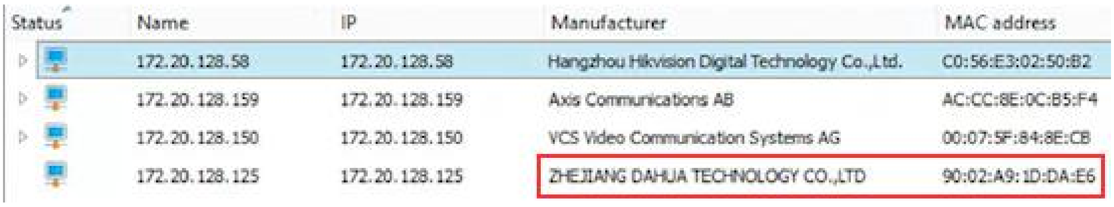
- Avigilon: 00:18:85
- Axis: 00:40:8C, AC:CC:8E
- Bosch: 00:01:31, 00:04:63, 00:10:17, 00:1B:86, 00:1C:44, 00:07:5F
- Dahua: 4C:11:BF, 90:02:A9
- Hikvision: 44:19:B6, C0:56:E3
- Samsung (Techwin): 00:09:18
- Sony: 00:01:4A, 00:13:A9, 00:1A:80, 00:1D:BA, 00:24:BE, 08:00:46, 30:F9:ED, 3C:07:71, 54:42:49, 54:53:ED, 78:84:3C, D8:D4:3C, F0:BF:97, FC:F1:52

In the case of manufacturers such as Sony, which are part of a larger conglomerate, it is difficult to know which of these OUIs is used specifically for security without scanning devices, as they are listed simply as "Sony Corporation" in OUI lookups.

OEM Devices

In cases where manufacturers OEM their devices from another, which OUI is used depends on manufacturing agreements. For example, checking the MAC address of a Q-See camera (90:02:A9:1D:DA:E6), it is listed as Dahua, seen in the results from an IP scanning tool below. Others, however, show the OUI of the manufacturer relabeling the

camera.



Status	Name	IP	Manufacturer	MAC address
▷	172.20.128.58	172.20.128.58	Hangzhou Hikvision Digital Technology Co.,Ltd.	C0:56:E3:02:50:B2
▷	172.20.128.159	172.20.128.159	Axis Communications AB	AC:CC:8E:0C:B5:F4
▷	172.20.128.150	172.20.128.150	VCS Video Communication Systems AG	00:07:5F:84:8E:CB
	172.20.128.125	172.20.128.125	ZHEJIANG DAHUA TECHNOLOGY CO.,LTD	90:02:A9:1D:DA:E6

Looking up Other Manufacturer OUIs

Here is a OUI to manufacturer lookup engine that lets you put in any manufacturer (IP cameras, DVRs, PCs, etc.) and find their OUIs.

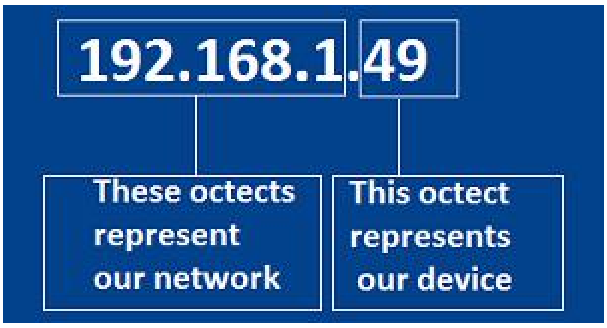
IP Addresses Defined

In security, many components are IP addressed, including cameras, recorders, access control panels, and more. The IP address of a camera is used to add it to a VMS or NVR, while client software connects to the VMS via its IP address.

An IP address (IPv4 specifically) consists of four parts (called octets because they contain 8 bits of data) ranging in value from 0-255, separated by periods, such as:

192.168.1.49

The IP address is divided into a network address (192.168.1 in the example above) and a host address (.49 in this case). On a single LAN, the network address is typically the same for all devices, while the host address differs. So 192.168.1.49, 192.168.1.50, and 192.168.1.51 all reflect different devices. The illustration below is using a 255.255.255.0 subnet mask


192.168.1.49
These octects represent our network
This octect represents our device

IP Addresses Must Be Unique

If more than one device attempts to use the same IP address, generally neither will be able to connect to the network. On PCs, the user is typically notified that a device has connected and is causing an IP address conflict. However, if two cameras share the same address, errors will generally not be generated, leading to wasted troubleshooting time.

Note that some manufacturers ship their cameras with a hardcoded default IP address. Plugging more than one into the network at a time will cause address conflicts, so these cameras must be connected one at a time and re-addressed. Installers should check if their chosen manufacturer(s) use default IP addresses and plan initial setup accordingly. An IP Scanner may save you time and frustration.

IPv4 vs. IPv6

Because the use of the internet has expanded over time, concerns about the number of addresses available using IPv4 format arose (called address exhaustion), lead to development of an expanded address format, IPv6.

Unlike IPv4, which uses 32 bits (8x4) for each address, IPv6 uses 16 octets (128 bits total), displayed in hexadecimal (0-9 + A-F). Each group separated by colons represents two octets. For example:

FA80:43220:0000:0000:0202:B3EF:FE1E:8329

This increase in address size results in approximately 34 undecillion addresses, a huge increase over the IPv4 limit of about 4.2 billion addresses.

Many networks support either and both formats, and most modern IP cameras can be configured to use either format. Note that the same format should be used throughout.

IPv4 for Surveillance

Despite IPv6's larger address pool, IPv4 continues to be the dominant format used. Especially for private networks, with a finite number of connected devices like a surveillance system, address exhaustion is not a practical problem. IPv4 remains easier to use and administer, and there is little or no reason to use the more complex IPv6 format.

Static vs. Dynamic Addressing

Devices may be set with either a static (does not change over time) or dynamic (changes periodically based on lease time) IP address. Because cameras and NVRs are typically fixed devices and configured to communicate via IP address, giving them dynamic address causes issues when the IP changes, forcing users to reconfigure devices. Therefore, all devices in security systems are typically manually assigned static addresses.   Using dynamic addresses for devices that need to be found via their IP address is comparable to trying to deliver postal to homes in a town where the houses are renumbered and the streets are renamed periodically.

However, there are some cases in which dynamic addresses may be used.

- When setting up a new surveillance network, a DHCP (dynamic host configuration protocol) server is often used to temporarily assign IP addresses to devices so they may be reached for configuration. for example, a new camera connected to the network receives an address from the server, which the installer users to perform initial configuration and assign a permanent address.
- Some less crucial devices, such as client PCs and tablets may be dynamically addressed. Since these devices are typically used only periodically, and generally do not need to be reached for configuration or connected to a VMS by IP address as cameras are, assigning them a dynamic address is often sufficient.

For more detail on why static addressing is a 'best practice' for IP Video systems, read our Dynamic vs. Static IP Addresses post.

Zero-Configuration

There is a subset of dynamic addresses available in use by zero-configuration, commonly called zeroconf, which allows devices to use a dynamic address without a DHCP server in place. In surveillance the most common example of this is initial setup of IP cameras. Connecting a laptop directly to a camera, with both devices set to use dynamic addressing, they will both be automatically addressed to an address beginning with 169.254. This allows initial configuration to be performed and the IP address changed without needing a DHCP server (note that many, but not all, current cameras support this).

Default Gateways

Generally, and typically in video surveillance, the term 'default gateway' is synonymous with routers. IP cameras and DVRs, like PCs, have fields to enter in the address of the default gateway. In practice, this means the address of the router - the gateway to the internet.

The default gateway is needed for computers on other networks to access the IP video surveillance equipment. For example, users at a remote site or on their phones would typically not be able to connect to an IP camera or recorder that does not have a default gateway set. Sometimes, in security applications, this is done on purpose, to block any access to the system.

Network Classes

In general, the relationship between potential unique addresses in a network, and total potential number of unique sub-networks supported is a decision well beyond a surveillance system. The three most common network classes are limited as follows:

- Class A: This type supports over 16 million IP addresses per network, but only supports 128 different subnets. (From 0.0.0.0 to 127.255.255.255)

- Class B: The type supports over 65,000 IP addresses per network, and about 16,000 different subnets. (From 128.0.0.0 to 191.255.255.255)
- Class C: This type supports only 256 IP addresses per network, but almost 3 million subnets.   (From 192.0.0.0 to 223.255.255.255)

Private/ Public Networks

Every device on the Internet has an IP address, but not every networked device is on the internet. The difference is the boundary between private vs. public networks. For example, a IP Video network might consist of hundreds or thousands of cameras without a single unit being directly connected to the internet.

Typically only a few tightly controlled devices like routers or firewalls are given a public IP address.   However, some recorders or IP cameras may be publicly available (example 1, 2) on the web. This is far more common in consumer/residential and small office use than midsize and enterprise systems, which typically demand tighter security, with organizations' IT department preferring not to open these devices to the internet.

Portions of the "172" and the "192" address ranges are designated for private networks. The remaining addresses are "public," and routable on the global Internet. Private networks can use IP addresses anywhere in the following ranges:

- 192.168.0.0 - 192.168.255.255 (65,536 IP addresses)
- 172.16.0.0 - 172.31.255.255 (1,048,576 IP addresses)
- 10.0.0.0 - 10.255.255.255 (16,777,216 IP addresses)

In modern systems, IP addresses are associated with subnet masking, which helps regulate traffic within a network at the expense of adding a trivial configuration step. Most surveillance systems are installed on a class C network, as evidenced in our Which Private IP Addresses Do You Use For IP Video? discussion, in which 50% of respondents said they use 192.168.X networks for their installations.

IP Network Hardware

Video surveillance systems depend on running over IP networking equipment.

The topics covered include:

- Fast / Gigabit / 10 Gigabit Ethernet
- Ethernet Switches
- PoE vs non-PoE Switches
- Managed vs. Unmanaged Switches
- Switches vs Hubs
- Routers
- Default Gateways
- Media Converters - Fiber and Coax
- Ethernet Network Distance
- Ethernet over UTP Extenders
- Network Interface Cards
- Multiple NICs
- Customer Premise Equipment

Network Speeds

The vast majority of network gear is rated for either 100 Mb/s (Fast Ethernet) or 1000 Mb/s (Gigabit Ethernet/GbE). These ratings describe throughput capacity, i.e., how much data each port may handle. Other variants, such as 10 or 40 Gigabit Ethernet, are available though generally not used in surveillance.

Fast Ethernet

Fast Ethernet (100 Mb/sec) is used for connections to field devices, such as cameras, encoders, and I/O modules. Rarely do these devices support gigabit speeds. Despite multi-megapixel and 4K cameras becoming common (with some including gigabit ports), camera streams are typically 15 Mb/s and below, simply not large enough to warrant the use of Gigabit Ethernet for the bulk of the network.

Gigabit Ethernet

By contrast, GbE devices are rated to handle 10X more data per second than Fast Ethernet devices.   GbE devices are generally moderately more expensive (20-30%) than their equivalent Fast Ethernet counterparts. In surveillance, GbE is typically used to connect switches together, as Fast Ethernet is typically not fast enough for these backbones. Additionally, it may be used to connect servers to storage devices (NAS/SAN).

10 Gigabit Ethernet

10 GbE is uncommon in surveillance. It is generally used in data center applications connecting large quantities of switches and servers which require more throughput than 1000 Mb/s links can provide. The only likely application for 10 GbE in surveillance is in connecting large quantities of servers to a storage network (SAN), typically only seen in very large systems, such as citywide surveillance.

Actual Throughput

Total actual throughput capacity of all of these options will be less than the category implies, as other network variables and the switch design itself deduct a portion of bandwidth as overhead. Typically, about 70-80% of rated speed can be expected for actual throughput, meaning 70-80 Mb/s in a Fast Ethernet link, 700-800 in GbE, etc.

Ethernet Switches

The switch is a central connecting device in IP surveillance networks. The primary function of a switch is to provide distribution for data within a network, with a typical role in a surveillance system of connecting cameras to recorders and recorders to viewing clients.

Both standalone and rackmount switches are common, usually ranging in size from 4 or 5 ports, to 96 ports or even more in a single box. At the high-end enterprise scale, multiple switches can be joined together into a single logical unit potentially comprised of thousands of ports.

Fast Ethernet models may be furnished with two or four GbE ports, which for surveillance applications is useful for connecting multiple switches together leading to a central recording server. Alternatively, a switch may come equipped with an SFP/+ port compatible for connecting the switch to fiber optic cables or another high bandwidth cabling format.

PoE vs Non-PoE Switches

Statistically, most IP camera deployments use PoE switches. These are Ethernet switches that also power IP cameras connected to them. The key issues for PoE switches is how much total power they provide (many do not provide enough if all ports are powering IP cameras) and how many ports are PoE powered. For more, see our PoE Guide for IP Video Surveillance.

Managed vs. Unmanaged Switches

Switches may be either managed (allowing users to connect and change settings) or unmanaged (plug and play, with no configuration possible).

Unmanaged Switches

Unmanaged switches offer no configuration or monitoring capabilities, simply connecting devices on a single physical LAN. These switches are typically the lowest-cost models available, but should be used only in very small systems, typically 8 cameras and under, where monitoring and advanced configuration are not required.

Managed Switches

Managed switches allow the user to connect, most commonly via web interface, to perform monitoring and setup tasks. Differing levels of management are available, normally referred to as "smart switches" versus "fully managed", though the features contained by each vary by manufacturer.

In surveillance, managed switches are more commonly used, as most PoE models (outside of very small, low cost 4-5 port options) include some sort of management capability. Surveillance users may use the management interface to reboot cameras by cycling PoE power, set up network monitoring via SNMP, port mirroring for troubleshooting, segment surveillance traffic via VLANs, or configure multicast, all functions not found in unmanaged models.

This survey shows that Cisco is most popular brand of switch in video surveillance infrastructure, being selected as a favorite by over a third of those surveyed.   Many integrators specifically mention the small business 300 series switches.

Routers

While switches are used to connect devices together in a local network, routers are used to connect multiple networks. The router inspects network traffic, sending only packets addressed outside the local network through its WAN port to a modem (connected to the internet). Local traffic is kept internal.

While some routers are simply used to route network traffic, more commonly they include firewall features. This allows only specific traffic from specific devices through the router, based on rules set by users.

In surveillance, routers are most often used to connect the surveillance network to other networks, acting as a physical firewall. This allows the surveillance network to remain inaccessible except to those hosts which administrators choose.

Typically IP cameras are not connected directly to routers, they are connected to switches and then the switches are connected to the router.

Router/Switch 'Convergence'

Some routers may include switch ports, especially models intended for remote sites or consumer use. This eliminates the need for a separate switch in small networks. However, these ports are rarely PoE, so making direct camera connections requires a separate PoE midspan.

Also, some switches have begun to include routing functions. However, these devices are typically used in local area networks to more efficiently connect multiple VLANs than traditional routers, while routers are still used for higher security applications, such as connecting to the internet.

Media Converters - Fiber and Coax

Media converters adapt Ethernet from copper/UTP cables to fiber optics. Fiber optic cables support higher bandwidth, longer distances, and are immune to common types of interference which affect copper Ethernet cables.

In surveillance, fiber media converters are most commonly used to connect cameras more than 100m away from a switch to a standard network, such as pole-mounted cameras in parking lots. For more, see Daisy Chained Fiber Explained .

Another type of media converter common to surveillance is the Ethernet over Coax adapter. The specialized media converters allow users to reuse existing coaxial cables installed for analog camera systems to connect new IP cameras. We cover these in detail in our Reusing Existing Coax tutorial.

Ethernet Network Distances

Another key element that remains constant, regardless of speed, is distance between two devices. For Ethernet over most types of UTP cable, the distance should not exceed 100m (330') per the guidelines set in IEEE802.3. Trying to stretch the distance longer leads to data reliability problems, usually causing video quality and communication issues between cameras, switches, and servers.

Ethernet Over UTP

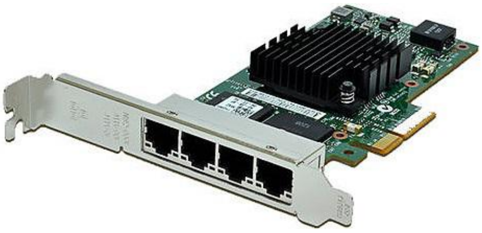
It is also possible to exceed distance limitations on typical UTP cabling far beyond the 100m max. In general, the farther an extender reaches, the lower data throughput it supports. Powered UTP Extenders (used on both ends of a long cabling run) can increase the maximum allowed 100m length by 8 or 9 times while still supporting 'Fast Ethernet'.

Costs for UTP Ethernet Extender range from ~$300 - $500 per link, with single port devices being most common in surveillance.

Network Interface Card

The Network Interface Card (NIC) performs the essential function of connecting a computer to a network. A "computer" might be a server or workstation, but could also describe an IP camera or NVR. In general, any device that accessible or managed on a network includes a NIC.

In modern use, NIC typically does not refer to a separate card installed onto a server's motherboard or camera's PCB. Instead, the NIC is often



physically integrated with the computer it is matched with, and true dedicated Network Interface Cards are typically only found in servers:

Multiple Server NICs Usage

Usually, devices like cameras have a single network interface, but a server may have two or more. A common 'best practice' in terms of recorder performance and security is to physically segregate network connections to a dedicated NIC. A server might have two NICs, where one is connected to the network of cameras and the other is connected to a common LAN composed of workstations accessing video.

Every device network requires it's own NIC. In mixed network environments including both wired and wireless networks, computers must have separate NICs for each. Each NIC has at least one IP address that declares its presence and location on a network.

Customer Premise Equipment

CPE, or customer premise equipment, generally refers to equipment the customer has already installed as part of their existing network. CPE equipment typically connects a building/office/home to a telecommunications network. Today, the most common types include cable and DSL modems that allow connecting on-site devices, like PCs and IP cameras to the public Internet.

For example, an IP video surveillance system typically needs telecom CPE equipment if the system is going to be remotely accessed. The most important differentiator of CPEs is the upstream bandwidth provided by the equipment / service. Since even a single video stream can require multiple Mb/s of bandwidth, users need to be sure the CPE can deliver that bandwidth. In particular, most telecommunication services support less upstream bandwidth (from the site to the Internet) than downstream, which can be a significant problem for IP video services.

PoE

We provide comprehensive explanations of the elements in selecting, using Power Over Ethernet with IP cameras, covering:

- PoE vs Low Voltage
- When to Use PoE, When Not
- PoE Classes
- 802.3af vs 802.3at vs 802.3bt
- Nonstandard PoE Implementations
- Spare Pairs
- Distance Limitations
- PoE Extenders
- Power Consumption vs Specification
- Calculating Power Budget
- PoE via Switch, MidSpan or NVR
- The Top 5 PoE Misunderstandings

PoE vs Low Voltage

All cameras need electrical power to operate.

'Power over Ethernet' (PoE) uses a single cable to connect a camera to both the data network and a power supply. In most cases, powering cameras before the advent of PoE meant using low voltage power using separate power supplies and dedicated power wiring. PoE eliminates the second cable / supply.

In addition, relative to low voltage power supplies, IPVM estimates PoE saves $10 to $30 in cost per camera for powering. See: PoE vs Low Voltage Power Supplies Cost Compared.

PoE Use Almost Always

PoE is supported and used, in practice, in almost all professional IP cameras and installations.

Exceptions Not To Use PoE

There are a few exceptions where PoE is not used with IP cameras. Most typically this is when locations are connected via fiber or wireless backhaul, with local high-voltage power used. Additionally, solar powered sites may prefer lower low voltage power when connecting directly to batteries.

Indeed, many budget cameras today only support PoE creating logistical issues in those edge cases where low voltage power is required. For example, see: Dealing with PoE Only Cameras.

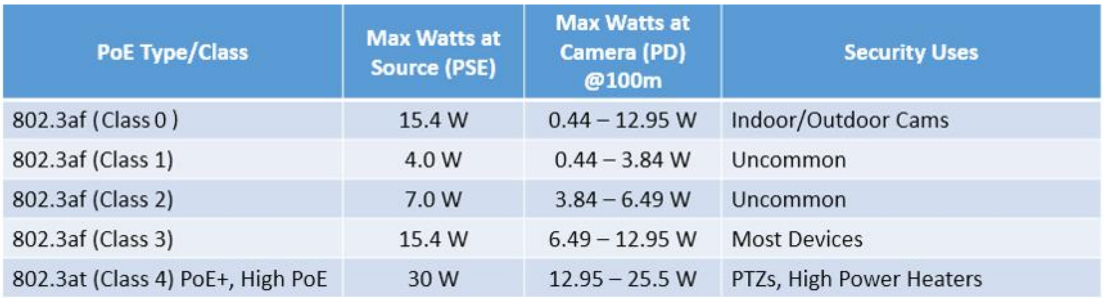
PoE Types

PoE is defined by IEEE standards. These include:

- 802.3af, which is the 'standard' PoE used by 90%+ of all IP cameras, supporting up to 15.4W
- 802.3at, which is 'high' PoE used only by a small fraction of IP cameras that need more than 15.4W and up to 30W. 802.3at support is most commonly found / needed when dealing with PTZs or cameras with integrated heaters / blowers.
- 802.3bt is a draft currently, with the potential for 100W PoE, that is beyond the needs of almost all IP cameras.

PoE Classes

PoE also offers classes that segment / specify more precisely how much power the device consumes. The chart below summarizes the types and classes used in surveillance:



PoE Type/Class	Max Watts at Source (PSE)	Max Watts at Camera (PD) @100m	Security Uses
802.3af (Class 0)	15.4 W	0.44 – 12.95 W	Indoor/Outdoor Cams
802.3af (Class 1)	4.0 W	0.44 – 3.84 W	Uncommon
802.3af (Class 2)	7.0 W	3.84 – 6.49 W	Uncommon
802.3af (Class 3)	15.4 W	6.49 – 12.95 W	Most Devices
802.3at (Class 4) PoE+, High PoE	30 W	12.95 – 25.5 W	PTZs, High Power Heaters

A formal PoE specification should include both a type and class, but that requirement is typically ignored. Most often, PoE is defined as '802.3af' only with no class modifier, meaning that anywhere between 0.44 to 15.4 W is available at the source.

However, when a class is given, it limits further the minimum and maximum power available. For example, if a supply is a 802.3af Class 2 rated, it can only deliver a max of 7.0 W.

While familiarity with the type/class nomenclature is important, most current PoE supplies and devices are classless, and that designation is becoming less common.

802.3bt on Horizon

While still in draft stages and early development, an even more substantial class of PoE (802.3bt) is expected to be ratified in 2017. That draft proposes a variant of PoE able to deliver 100 watts at the source by using all four pairs in a category cable, a point we cover in depth in the next section.

While the prospect of more than doubling 802.3at wattage is creating buzz, using it for surveillance gear may not be needed.

The most likely markets for 802.3bt appear to be lighting systems, electrical motor controllers, and high powered industrial sensors. However, most cameras operate successfully using less than 10 watts.

Nonstandard PoE Implementations

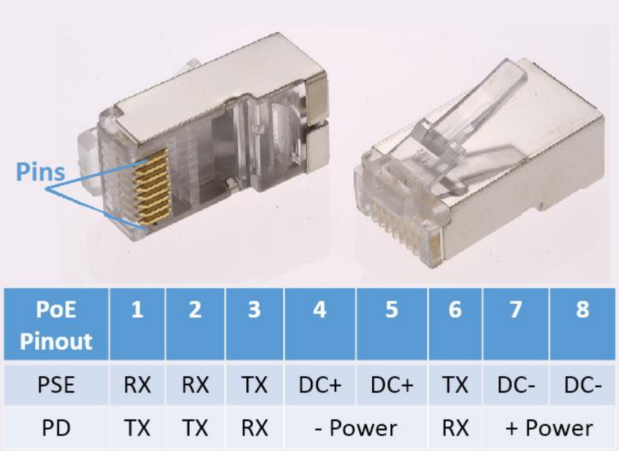
Not all devices claiming PoE use 802.3at/af as a standard. In the surveillance market, there are scattered proprietary implementations of the same basic idea but with different voltages or wattages. Unless a PoE product specifically claims to be 802.3af/at compliant, there could be incompatibility problems.

In some cases, proprietary PoE implementations will work according to standards, but will operate in a downrated capacity. 802.3af/at uses a passive format, where power is delivered on unused pairs, but it is possible to send more power using an active format that interlaces power with data on the data pairs.

One example: some versions of Ubiquiti products use a 24VDC base for PoE instead of the standards compliant 48VDC base. While power indeed is supplied over an ethernet cable, it must be provided by a non-standard PoE injector. Another example: Phihong's MegaPoE that claims to deliver up to 95 W using active PoE, but is backward compatible with the passive-only 802.3af/at standards as well.

Alternate A vs. B Operation

So how does PoE work? The answer is found by looking more closely at the typical RJ-45/8P8C connectors and UTP cable. The chart below shows that while eight strands of wire are in a Cat5/5e/6 bundle, only four of them are typically used. The remaining four are left unused. (Passive) 'Alternate A' PoE injects power on the data pairs, while 'Alternate B' implementations simply use the unused strands to deliver electricity to a connected device. The chart below shows a 'Alternate B' pinout:



PoE Pinout	1	2	3	4	5	6	7	8
PSE	RX	RX	TX	DC+	DC+	TX	DC-	DC-
PD	TX	TX	RX	- Power		RX	+ Power	

With Alternate B, two pins in the standard 8-pin connector are used to transmit data, two pins to receive, two push DC+ power, and the remaining two complete the circuit with DC- back to the supply.

However, most surveillance devices auto-sense which pairs are used to supply power. Many PoE devices are 'Alternate A or B agnostic', with only a minority of connectors (ie: Axis M12 connector) as Alternate Type specific. (The M12 is Type B PoE only.)

While the actual order of pins vary according to cabling standards (ie: TIA/EIA 568A or B), those standards affect the 2 data pairs, not the power pairs. Regardless of which wiring standard is used, if power sources and devices comply with the 802.3af/at spec, power connections will be made in the same way.

Distance Limitations

PoE is essentially limited to the same 100m distance limitation as general Ethernet network. Data being carried by the cable will drop and degrade before the power drops below what the standard guarantees.

A few manufacturers have adopted a variation of camera power that allows a string of cameras to be connected to each other in a 'Daisy Chain' style format. (see: New Daisy Chain IP Cameras (Vivotek) for one example).

PoE Extenders

For applications requiring more than 100m, PoE extenders are available. Typically, they are pairs of adapters for each camera, with power injected at the headend side. PoE extenders often provide 300m or even up to 600m total distance. Pricing is in the ~$200 range for the pair. For more, see: Long IP Camera Run Options: Fiber, PoE Extenders and EoC Examined.

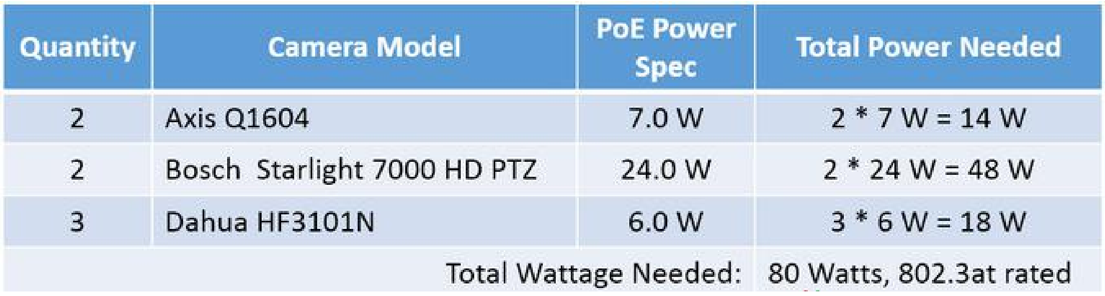
Typical PoE Consumption Vs Specification

Each IP camera manufacturers publishes specification of power draw in addition to whether or not the camera supports PoE. This is important to knowing how much total power you need as even if all cameras are 'regular' 802.3af PoE, power draw can range from as low as 2 watts to as high as 15. As a general rule of thumb, fixed IP cameras typically consume about 4 - 7 watts of power.

IP camera power specifications are typically higher than what is actually consumed by the camera, as verified in our IP Camera PoE Power Consumption Test.

Calculating Power Budget

Multiple IP cameras are typically powered from a single device. As such, one needs to check and add up the individual power requirements of cameras in one's system. Here is an example calculation for 7 total cameras, across 3 models:



Quantity	Camera Model	PoE Power Spec	Total Power Needed
2	Axis Q1604	7.0 W	2 * 7 W = 14 W
2	Bosch Starlight 7000 HD PTZ	24.0 W	2 * 24 W = 48 W
3	Dahua HF3101N	6.0 W	3 * 6 W = 18 W
		Total Wattage Needed:	80 Watts, 802.3at rated

The total wattage needed is 80 watts but they are not all the same PoE type. While the Axis and Dahua cameras use far less than 15.4 W furnished by 802.3af, the Bosch PTZs need 24 W, putting them in the PoE+/802.3at category. Therefore, our supply must be rated to provide PoE+ on at least two ports and 80 watts total.

PoE via Switch or Midspan or NVR

PoE is typically provided in one of three ways:

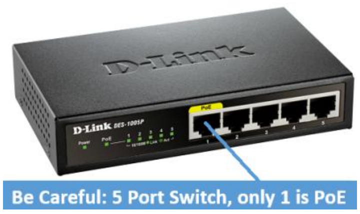
- From a network switch that supports PoE
- Via a box installed in series with the cable called a midspan injector
- From an NVR with an embedded PoE switch

The network switch is, by far, the most common approach for providing PoE power. The midspan is used much less often though is preferred by some as it allows separating switch selection and support from midspan / PoE power. See: PoE: Switch vs. Midspan Usage

Switch Issues

With the use of PoE growing in many areas, finding switches that offer PoE is not difficult.

However, care should be taken to confirm power is available on all switch ports. Especially in lower-end or consumer switch gear, it is common to enable PoE on one or half the available ports, but not them all:



Be Careful: 5 Port Switch, only 1 is PoE

Even with 'professional' switches, many only provide total power that is half of what is needed for full 802.3af support. For example, 12 port switches often supports 90 total watts of PoE power, which is equivalent to 7.5 W per port. If you use IP cameras on all 12 ports, you may use more than 90 watts total. In such cases, cameras can randomly go offline and be mistaken for a 'bad' camera when, in fact, is that the switch is turning off ports because it does not have sufficient power to support all cameras. For a modest premium, some switches offer 'full' PoE power to all ports. In our 12 port switch example, this would be 180 watts (i.e., 15 W x 12). See: PoE Power Problems for more details on this issue.

Midspans

The other option, Midspan Injectors, are less commonly used but may be the right choice in applications where PoE cameras are desired but where a non-PoE network already exists, or where special PoE requirements can be satisfied more inexpensively than buying more expensive gear.

For example, in our 7 camera system above, two of the cameras drove the more-expensive PoE+ requirement in our switch. Based on cost, it may prove to be less expensive to buy a regular (802.3af) PoE switch, and then buy two separate PoE+ midspan injectors just for the PTZs. Such a move could save hundreds, so considering both PoE supply options could be a big benefit. Below is an example of a single device midspan, also commonly referred to as a power injector.

NVRs

Some NVRs have PoE switches built in. This is the least commonly available and used of the three options. However, its main benefit is that it simplifies setup since buying / connecting to a separate PoE switch is eliminated. It shares the same concerns as regular network switches in that one still needs to check total power supplied and what types of power (PoE vs PoE+ etc.). Another issue can be that NVRs with built-in PoE switches may support more total cameras than the built-in switch has ports. For example, an NVR might have a built-in 9 port switch but support 16 cameras total. If one was to use all 16 cameras, then an additional switch / PoE power supply would be needed.

The main concern with NVRs with built-in PoE switches is reliability / maintenance of adding in the PoE switch to the NVR. These devices have not been in broad use long enough to make a definitive assessment of this.

Top 5 PoE Misunderstandings

In our guided IPVM IP Networking course, we include PoE as a core networking concept. Over the course of several sessions, certain questions are asked by students on a routine basis. Here they are:

1. Can I accidentally double PoE wattage by using midspans & switches together?
2. Does each port produce max rated wattage?
3. Can a cable plugged into a port, but not a camera electrocute me or be a safety hazard?
4. How far can PoE travel on cable?
5. Will cameras using power supplies be damaged by also plugging them into PoE ports?

In the sections below, we answer each question.

Question: "Can I accidentally double PoE wattage by using midspans & switches together?"

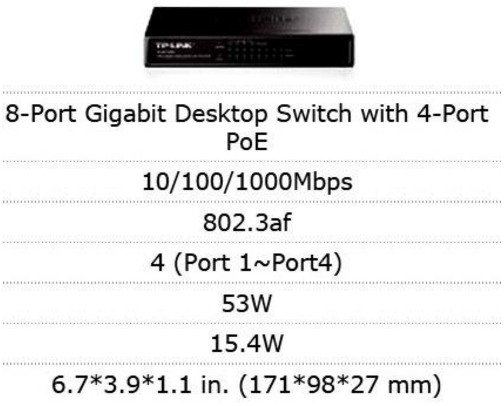
Answer: No. The process of devices using PoE generally involves a negotiation process where a device identifies and requests PoE power from a source like a switch or midspan injector. Because those source devices do not request power from potential sources, they do not themselves receive any PoE power. In this way, the 'only' PoE applied to the cable is done by the device nearest to the PoE powered camera or security device.

We tested this scenario in our PoE Midspan With Switch Tested report and describe the mechanics in full detail.

Question: "Does each port produce max rated wattage?

Answer: It is not guaranteed. While a port may be rated to deliver max wattage, (ie: 15.4W for 802.3af or 60W for 802.3at) the ability of the PSE to produce it depends on the total demand of PoE versus the maximum outputted power available. In many cases, demand outpaces supply, causing performance issues or brownout conditions for PoE devices.

For example, this consumer grade PoE switch (TPLink TL-SG1008P) has the following output specs:



8-Port Gigabit Desktop Switch with 4-Port PoE
10/100/1000Mbps
802.3af
4 (Port 1~Port4)
53W
15.4W
6.7*3.9*1.1 in. (171*98*27 mm)

The max PoE power available on the switch is 53W. With 4 PoE ports, this max power is divided between each, or: 53W / 4 ports = 13.25W per port. However, the max PoE power available per port is rated at 15.4W per 802.3af to 15.4 W * 4 = 61.6W. The difference between maximum port specifications and max output power available at the switch is a full 8.6W. This means if we had 4 cameras that required 15W each, the power budget would be overdrawn.

Question: "Can a cable plugged into a port, but not a camera electrocute me or be a safety hazard?"

Answer: No. Due to the initial negotiation process, PoE power is not actively issued unless a connected device requests it. This means that a cable connected to a PSE is not 'electrified' at all until plugged in to a PoE device and will not present a safety danger because of incidental contact.

Question: "How far can PoE travel on cable?"

Answer: The maximum 100m described by the ethernet IEE802.3 standard. By design, power will extend as far as any maximum length cable can be networked. In reality, this maximum length is much farther, per our IP Camera Long Distance Ethernet Test, where full PoE voltages were measured a full 1000' away from the source, beyond the point any data could travel on the same connected cable.

While PoE is rated for the max cable distance, any distance further than 100m does not meet ethernet standards, and additional lengths will not be supported and may void product warranties if used.

Question: "Will cameras using power supplies be damaged by also plugging them into PoE ports?"

Answer: Not likely, but beware. In most cases, cameras or other PoE devices will not request power even when available from a PSE if the device is already receiving power from a low-voltage power supply. However, especially with older PoE devices, instructions may warn against doing this at the risk of damaging the device.

In general, this is not an issue with newer cameras, but any disclaimers against this situation should be strictly heeded.

VLANs

Many people confidently say to 'use VLANs' as an answer to IP video networking problems and as a way to signal expertise.

But how should VLANs be used? What benefits do they really deliver or not?

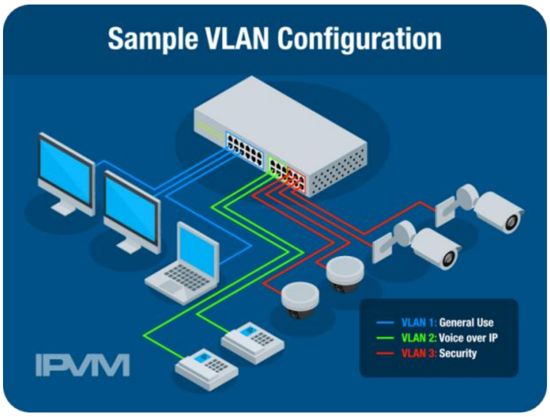
We examine:

- Segmentation of applications across VLANs
- Untagged vs tagged VLANs
- Static vs dynamic VLANs
- VLANs for uplinks
- Bandwidth and VLANs
- QoS and VLANs
- Common applications of VLANs

Overview

A VLAN (Virtual Local Area Network) logically divides a single physical switch or switches into multiple separate logical networks, making devices on one VLAN "invisible" to and unable to communicate with devices on another unless they are routed together.

The graphic is diagram shows VLANs on a typical shared / converged network. In this instance, surveillance traffic is separated from general office and VOIP traffic via three separate VLANs. The only devices that can communicate with each other in the illustration below are the camera and the NVR, as they are in the same VLAN.



Untagged vs. Tagged VLANs

There are two fundamental types of VLANs, tagged and untagged:

Untagged VLANs

By default, all ports of a switch are added to a default untagged VLAN (typically VLAN ID 1), meaning that all ports may "see" all others. Moving specific ports to another VLAN ID as untagged segregates this traffic.

The benefit untagged VLANs is reduced configuration, as no endpoint device configuration (cameras, servers, etc.) must be performed, as traffic is simply limited to the VLAN by the switch. However, ports (including uplinks) may only be assigned to a single untagged VLAN. So if a specific device must see multiple VLANs, such as office file transfer/printing, surveillance, and VOIP, users must either use tagging (below) or route the two VLAN segments together, both of which add complexity.

Tagged VLANs

Ports may also be tagged with specific VLAN IDs using 802.1Q tagging. Traffic entering and exiting the port is tagged with a specific ID which is inspected by the receiving device.

The benefit of tagged VLANs is that ports may be assigned to more than one VLAN, unlike untagged. However, end devices connected to these ports must also support 802.1Q, which is not supported by most IP cameras or other security devices, and requires additional Windows components to be installed/configured in PCs. Because of this, tagged VLANs are typically only used for uplink.

Static VLANs

Most video surveillance networks use static VLANs configured per port. For example, ports 1-12 on a switch may be part of the general LAN, while 13-24 are part of the camera VLAN.

Port based static VLANs are most common, and simplest to set up, but must be manually reconfigured if devices are moved or added, unlike dynamic VLANs. In the video below we provide a tutorial on configuring port based VLANs:

Note: ***Click here to watch the video on IPVM***

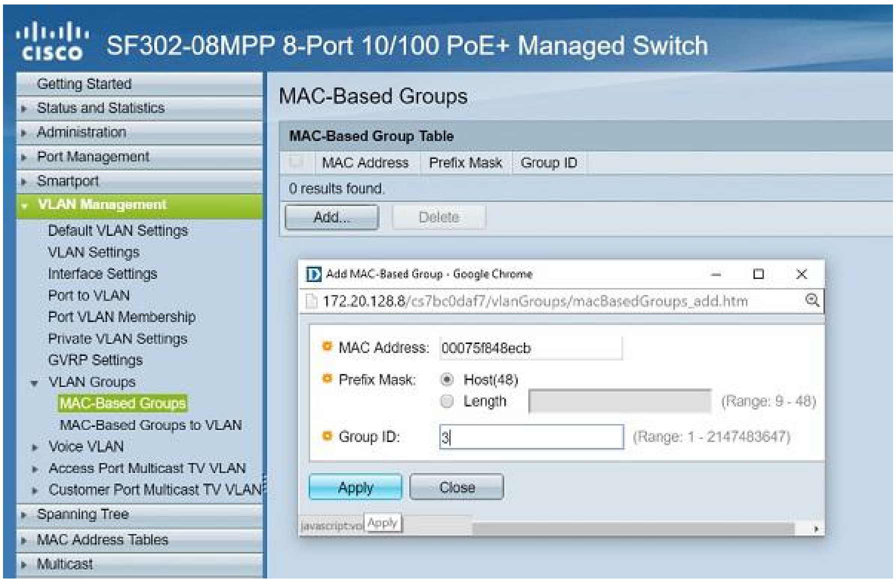
Dynamic VLANs

Dynamic VLANs assign a port based on its MAC address, credentials, or type of device. This provides greater flexibility, since devices may be plugged into any port, and rearranged as needed.

However, initial setup of dynamic VLANs more time-consuming, as the database or macros with the device identifiers or rules must be created, making them less commonly used, especially in surveillance as cameras, servers, and other equipment typically remains connected to the same port, and are not moved.

MAC Based VLAN Example

There are a few variations of dynamic VLANs. Below we provide an image from a managed switch that shows MAC based VLAN configuration. The switch will discover the MAC address of the device connecting to it and then add it to the appropriate VLAN based on the predefined policy.



MAC-Based Groups

MAC-Based Group Table

□	MAC Address	Prefix Mask	Group ID

0 results found.

MAC Address: 00075f848ecb

Prefix Mask: ● Host(48) ○ Length (Range: 9 - 48)

Group ID: 3 (Range: 1 - 2147483647)

Other Dynamic VLAN Options

Dynamic VLANs are also set via two other means, neither of which is common in surveillance:

- Macros/"Smart ports": This method uses protocols such as CDP/LLDP to automatically check the device type connected and assign it to a VLAN. This is commonly used in voice over IP and general network settings, but the vast majority of IP cameras do not support the required protocols, making it practically useless in surveillance.
- Active Directory/LDAP: Finally, devices which support Active Directory/LDAP may be assigned to a specific group in coordination with the domain controller. Few cameras support these protocols,

but it may be useful in assigning specific users (admins, security managers, guards, etc.) rights to view surveillance devices, regardless of which machine they log in from.

VLANs for Uplinks

There are two ways to handle VLANs in switch uplink ports.

- Dedicated VLAN per port: In switches with multiple uplink ports and few VLANs, specific uplink ports may be assigned to a single VLAN. This is the simplest method to use, though the number of VLANs must be fewer than the number of uplink ports.
- Shared trunk port: Second, traffic may be sent over a shared uplink port or ports, referred to as a trunk port. Traffic leaving trunk ports is tagged as specific VLANs using 802.1q (see above). This method is slightly more complex, but generally preferred as it allows for link aggregation for failover and/or higher uplink throughput.

VLAN Benefits

Increased security on shared networks is the main benefit of using VLANs. By segmenting traffic into multiple virtual LANs, surveillance may securely coexist on the same switch as general data or voice traffic. For practical purposes, the networks are invisible to each other so clients on the office LAN may not reach the surveillance VLAN.

Bandwidth Myths

In surveillance, VLANs are not used to save bandwidth, a popular myth. It is technically true that VLANs reduce the amount of traffic on the LAN, since broadcasts are not sent to the entire physical network, but only to the originating VLAN. However, this generally only impacts performance on very large networks, with hundreds of devices. In a 24-camera LAN, they will have little to no effect. If your surveillance cameras overload your IP network, other traffic on those switches will be impacted.

VLANs and QoS

One of the reasons VLANs are often seen as restricting or allocating bandwidth is because they are often used in conjunction with quality of service. QoS may be set by VLAN in most managed switches. A surveillance VLAN, for example, may receive higher priority as a whole than general data or voice VLANs.

Equipment Requirements

Implementing VLANs requires managed switches be used, as unmanaged switches offer no configuration capability. The vast majority of managed switches (both fully-managed and smart switches) available today are VLAN-capable. Users may see our switch recommendations for surveillance systems for more information.

VLAN Scenarios for Surveillance

How VLANs are applied varies, depending on the application:

- Small systems: In low camera count systems, such as small retail, VLANs are generally not used as low-cost unmanaged switches without VLAN support are most often deployed. Also, viewing is normally performed on the same computer as general office tasks, so creating VLANs would require routing be set up, adding cost.

- Converged network: When sharing a LAN with other services, often the case of schools and small or mid-sized offices, VLANs are normally implemented. It is not uncommon for these facilities to use one VLAN for data, one for VOIP traffic, and one for security, to better segment these services. Routing between the general office VLAN and security VLAN is normally required, to give select workers access to video.
- Dedicated network without VLANs: When using a dedicated, separate camera network, VLANs are often not needed or desired. If access from the general LAN is needed, the two separate physical networks are connected via router.
- Dedicated network with VLANs: In large systems, multiple VLANs may be used, even when using a dedicated security network. Cameras and clients are placed on separate VLANs, to prevent any potential tampering by users on monitoring stations directly access the cameras' web interfaces. When access control is deployed on the network, as well, many manufacturers recommend using a separate VLAN, as access systems may create broadcast traffic which may create issues in the surveillance system.

Conclusions

While the value of VLANs is significantly inflated by many, they do have some importance in shared LANs, preventing unauthorized access to video. However, VLANs are not a panacea in network security, and should be deployed only when necessary. Creating a truly converged network demands more configuration and coordination, not simply VLANs.

QoS

Along with VLANs, QoS is one of the most misunderstood topics in IP surveillance networks. Many purported "experts" claim it is required in any and all surveillance systems, but little clear guidance is given about why, leaving those new to the field confused. We cover the basics of QoS, what it is, how it is applied, and when it should be used.

We explain:

- What is Quality of Service
- How Quality of Service is Applied
- Limitations
- Practical Uses
- Setting up QoS

This is one of many tutorials on networking for surveillance. Others include: Wireless Networking for Video Surveillance, Network Addressing for Video Surveillance, Bandwidth Guide for Video Surveillance, Remote Network Access for Video Surveillance, Network Monitoring / SNMP for Video Surveillance, and more.

What is Quality of Service?

Quality of Service (QoS) refers to strategies used to manage available bandwidth for specific applications. Typically, it is applied when IP video or VoIP services are present on the same network as typical data traffic (file transfers, internet use, etc.). Video and voice are highly latency-sensitive, unlike these other services, and may be adversely effected if bandwidth is not managed, resulting in lost packets and high latency. These issues may result in dropped frames, degraded streams, camera disconnections or other undesirable or unpredictable effects.

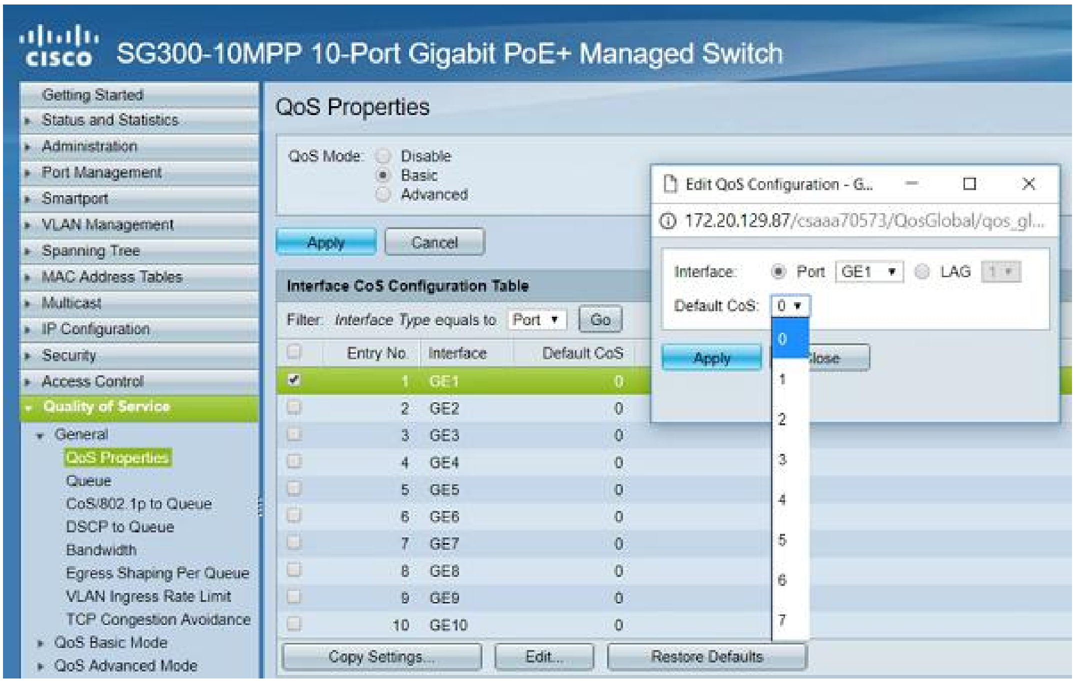
How QoS is Applied

There are three methods by which QoS is generally applied:

- By Application: Setting QoS by application is perhaps most common. This method categorizes and allocates bandwidth based on the type of application it serves. For example, FTP traffic may be assigned a lower priority than streaming video, to maintain higher frame rates and quality. Setting QoS by application requires that all components (cameras, switches, servers, etc.) support QoS, normally via DiffServ, the most common means today of tagging traffic by its application.
- By VLAN: Different VLANs may be assigned different QoS, allowing a security VLAN higher priority than the office LAN, so cameras, servers, and viewing clients receive a larger share of bandwidth. Setting QoS by VLAN requires that all devices support VLAN tagging, but QoS is set at the switch, requiring nothing further at end devices.
- By User: Finally, QoS may also be set by user. This is generally not used in security, but may still be preferred by network administrators or database workers who require a certain amount of

guaranteed bandwidth to perform their work, while those performing lighter tasks, do not. This method is more time-consuming to configure, since QoS setup must be tied to network login, adding additional complexity.

No matter which method is used, if QoS is desired, managed switches must be used, as QoS can not be configured on unmanaged switches. Below we provide an example of managed switch's QoS settings [Note: A Cisco switch is shown as they are most common in surveillance networks].



SG300-10MPP 10-Port Gigabit PoE+ Managed Switch

QoS Properties

QoS Mode: ○ Disable ● Basic ○ Advanced

Interface CoS Configuration Table

Filter: *Interface Type* equals to Port

	Entry No.	Interface	Default CoS
☑	1	GE1	0
□	2	GE2	0
□	3	GE3	0
□	4	GE4	0
□	5	GE5	0
□	6	GE6	0
□	7	GE7	0
□	8	GE8	0
□	9	GE9	0
□	10	GE10	0

Edit QoS Configuration - G...

172.20.129.87/csaaa70573/QosGlobal/qos_gl...

Interface: ● Port GE1 ○ LAG 1

Default CoS: 0

Some vendors, like Netgear, have unmanaged switches that honor IEEE 802.1p and DSCP priority tags.

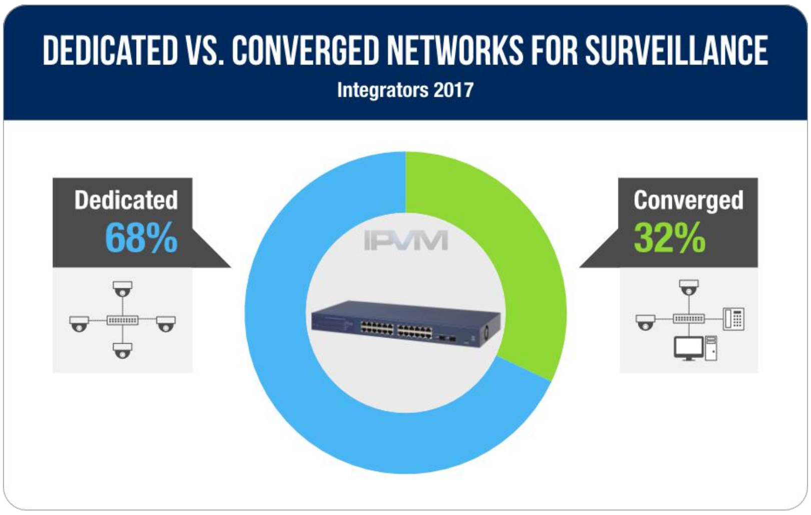
No Guarantees

QoS is a prioritization in most cases, and not a bandwidth guarantee, arranging the order in which packets / data are queued for sending. Some switches may offer bandwidth reservation, allowing specific services to receive only X amount of bandwidth, instead of a simple prioritization.

However, this is generally not used, as it is featured in more expensive enterprise switches, and restricted to trunk connections between switches or WAN connections. In most cases, prioritization via DiffServ is sufficient.

Dedicated vs Shared Network Use

For installations using a dedicated security network (most common in IP video), QoS will have little practical effect. Shown below are the statistics derived from integrator surveys which illustrate the large majority of surveillance networks are dedicated, and therefor likely will not benefit from QoS.



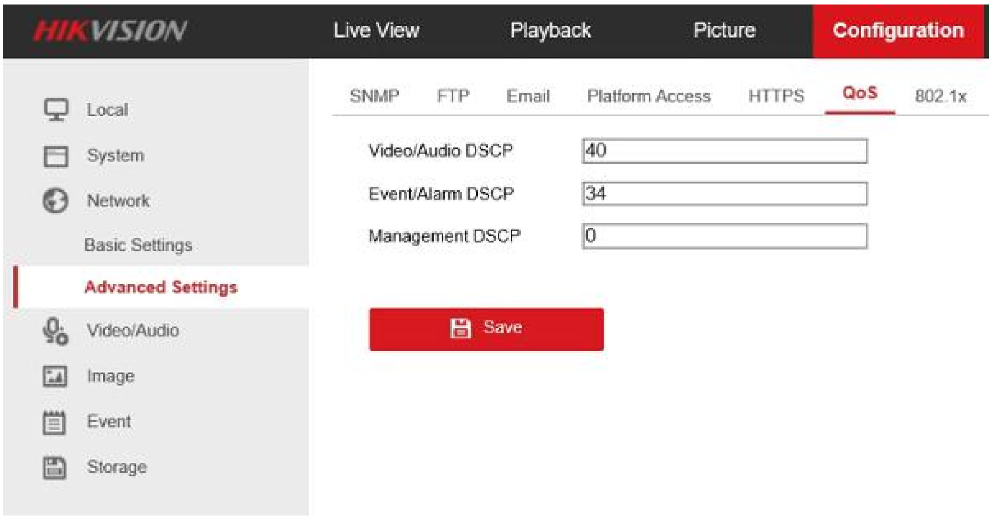
There may be potential gains if multiple systems, i.e., surveillance, access control, and IP intercom are used on the same network, but overall this is likely unnecessary.

In shared networks, QoS may be vital for systems of any size. In a four or eight camera system sharing a switch in a small retail or office applications, chances are that available bandwidth without QoS is sufficient. However, in larger systems, such as schools, mid-sized offices, campus environments, etc., QoS is more desirable, if not necessary, as these networks may easily become congested.

Setting Up QoS

For example, in a shared enterprise network, where IP surveillance, voice, and data all are present, QoS is generally set in one of two ways:

- First, by application, using DiffServ tagging to prioritize applications. Typically, voice is prioritized first, followed by video, then file transfer, internet data, and other general uses. Degradation to voice is most noticeable to users, while video may handle light latency better, making voice the higher priority. As an example we have an IP camera setup below. When using DiffServ, QoS must be configured in each camera, typically by entering a DiffServ code point (DSCP), which correlates to priority level, assigned in the switch. In some cameras, different DSCPs may be set for services such as audio, video, alarm, and management, so these functions are prioritized separately. Most, but not all, IP cameras supports DiffServ so check ahead if you plan to use this method. Below is DiffServ configuration for a Hikvision camera:



Video/Audio DSCP 40

Event/Alarm DSCP 34

Management DSCP 0

- Second, by VLAN. In this case, the entire voice VLAN, followed by security, and finally by file transfer and internet data VLANs would be assigned QoS as a whole. For the most part, this is effectively the same as QoS by application, but prioritizes all traffic on the VLAN, meaning that management tasks, audio, I/O data, and other non-video system functions all receive the same priority.

CBR vs. VBR for QoS

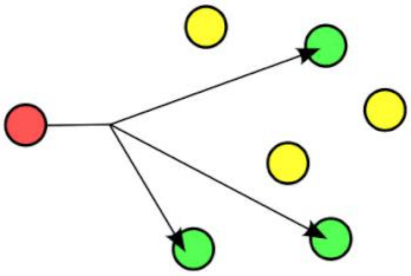
Even without a network enabled for QoS, you can set up your camera streams to improve quality of service. To do so, use MBR / VBR with bit rate caps, or CBR, as this will constrain cameras overloading your network. Combining the two will provide the most predictable results. Using CBR or bit rate caps provides a fixed bandwidth target, allowing easier estimation of throughput, while QoS provides prioritization of traffic, reducing latency and packet loss. Below, shows the bitrate options for a Hikvision camera.

Note: ***Click here to view the demo on IPVM***

Conclusions

Given most integrators prefer to run their surveillance systems on a dedicated network, QoS is generally not needed. In larger, shared networks, however, it becomes vital in preventing unexpected performance degradation.

Multicasting



Network bandwidth is a key concern in surveillance systems. While improvements in video codecs, such as smart codecs for H.264 and H.265, have reduced bandwidth needs somewhat, large systems still encounter issues with large amounts of video data. In this update, we'll look at the basics of multicast networks, a frequently-mentioned means of reducing bandwidth, where they will save bandwidth and where they won't.

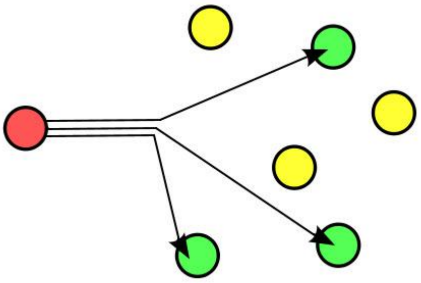
We explain:

- The Basics of Multicast
- Use in Surveillance
- Unicast / Mulitcast Combinations
- Network Support
- VMS Suppport

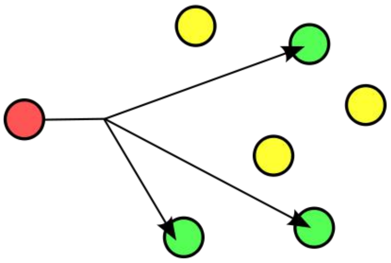
This is one of many tutorials on networking for surveillance. Others include: Wireless Networking for Video Surveillance, Network Addressing for Video Surveillance, Bandwidth Guide for Video Surveillance, Remote Network Access for Video Surveillance, Network Monitoring / SNMP for Video Surveillance, and more.

The Basics

In order to understand multicast's use in surveillance applications, users should understand the basics. In most typical network applications, unicast transmission is used. In this method, the source device, such as an IP camera, transmits as many copies of the video feed as are requested by destinations. The main drawback of this is inefficiency. If the camera is set to a 2 Mbps stream size, for example, four clients requesting video will utilize 8 Mbps of bandwidth. This image illustrates unicast transmission from the sender (red) to three recipients (green):



In multicast transmission, however, there is no direct connection between the source and destination(s). Destinations, such as surveillance clients, are joined in a multicast group, which receives a single copy of the video stream which is replicated to each client. So four viewers requesting a 2 Mbps stream will only use 2 Mbps of bandwidth, instead of the 8 Mbps used in a unicast network. The following image illustrates multicast transmission from the sender (red) to three recipients (green):



Use In Surveillance

Multicast is often cited as a must-have capability in any surveillance system. This is simply not the case. In systems with a limited number of destinations, such as one recording server and one or two viewing clients, multicast will save little bandwidth. True, it will potentially save the bandwidth of a stream, but in many cases this is negligible, as the network is rarely a bottleneck in smaller systems. In cases where recording and viewing use separate streams, one to the server, one to the client, no bandwidth will be saved, as each stream is only being sent to one destination.

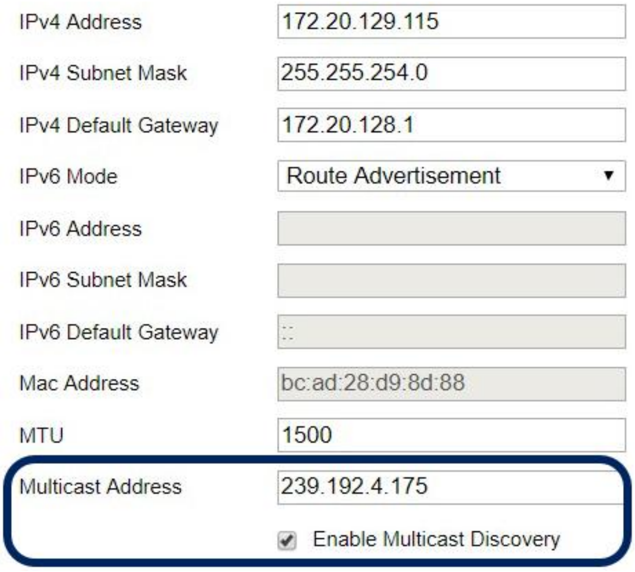
However, in larger deployments, where a larger number of cameras are viewed by a large number of clients, multicast may be critical. In municipal or corporate command centers, for example, half a dozen clients may be connected 24/7, with additional occasional users. Client usage may spike during critical events, as well.

Unicast/Multicast Combinations

In some cases, VMS systems may be capable of taking in a unicast stream and re-streaming it as multicast to clients. This can be useful when using cameras connected via means that don't support multicast, such as some wireless links or VPN connections. In this case, the VMS server makes a single connection to the camera and sends the stream out as multicast to a client, reducing bandwidth. In other cases, such as a client connecting through a VPN which does not support multicast, the VMS may transmit video from multicast cameras as a unicast stream. These features are typically limited to enterprise-level VMSs, however.

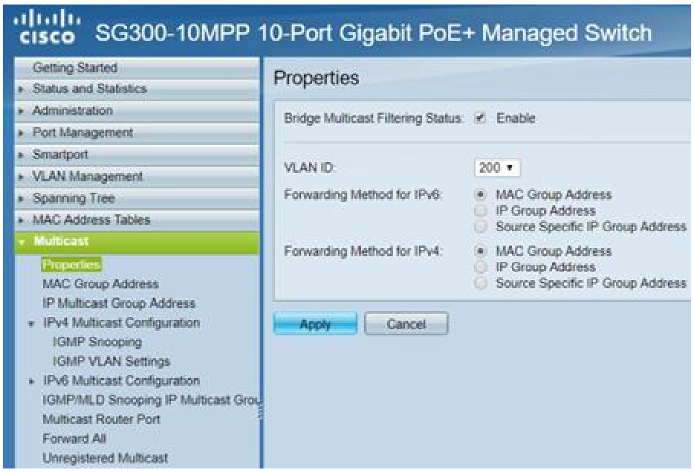
Network Support

Multicast IP addresses are designated as Class D, with an address range of 224.0.0.0 to 239.255.255.255. The following image illustrates multicast configuration on an IP camera though actual capabilities and configuration options may vary by manufacturer.



IPv4 Address	172.20.129.115
IPv4 Subnet Mask	255.255.254.0
IPv4 Default Gateway	172.20.128.1
IPv6 Mode	Route Advertisement ▾
IPv6 Address	
IPv6 Subnet Mask	
IPv6 Default Gateway	::
Mac Address	bc:ad:28:d9:8d:88
MTU	1500
Multicast Address	239.192.4.175
	☑ Enable Multicast Discovery

Multicast networks require that all components support IGMP (Internet Group Management Protocol), which manages the joining and leaving of multicast groups. IGMP is supported by most, if not all managed switches today. The image below shows a Cisco switch and the settings to setup Multicast for VLAN 200 and several ports



SG300-10MPP 10-Port Gigabit PoE+ Managed Switch

Properties

Bridge Multicast Filtering Status: ☑ Enable

VLAN ID: 200 ▾

Forwarding Method for IPv6: ● MAC Group Address ○ IP Group Address ○ Source Specific IP Group Address

Forwarding Method for IPv4: ● MAC Group Address ○ IP Group Address ○ Source Specific IP Group Address

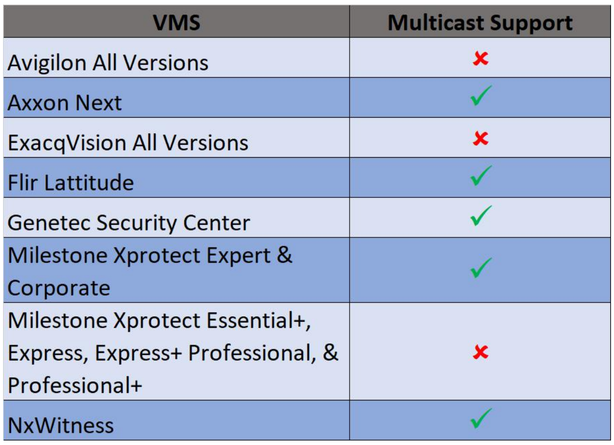
The majority of camera manufacturers support multicast streaming, as well. VMS support is limited, however, as shown below.

Multicast networks do add complexity to installation and troubleshooting. Unicast networks can be easily deployed by those with basic network experience, as the main concerns are the source and destination addresses. Most technicians have no issues IP addressing cameras and client machines. IGMP setup, performed in the switch, is simply beyond the scope of most low-level techs' training, however. Troubleshooting is also no longer as simple as checking a single source address and destination address, due to the creation of multicast groups, which are addressed separately. Combine this with the number of "moving parts" involved (cameras, clients, servers, and switches), all with their own multicast implementation and potential issues, and multicast is best left to experienced IT techs.

VMS Support

As mentioned, not every manufacturer supports multicast. Most major camera manufacturers now support multicast streaming, however some of the major VMS providers do not. A quick check of VMS players shows the following multicast support from each:

[[replace with chart from lightning / replace names with VMS word art]]



VMS	Multicast Support
Avigilon All Versions	✗
Axxon Next	✓
ExacqVision All Versions	✗
Flir Lattitude	✓
Genetec Security Center	✓
Milestone Xprotect Expert & Corporate	✓
Milestone Xprotect Essential+, Express, Express+ Professional, & Professional+	✗
NxWitness	✓

This noted, since multicast is complex to deploy and can depend on a number of networking components, we strongly advise checking detailed technical references on how well and easy it is to deploy multicast with your preferred VMS.

NTP / Network Time

Inaccurate time can lead to missing or inadmissible video, yet this topic is often overlooked, with cameras and servers left defaulted, synchronized to different sources or not at all. However, setting up a proper time server in a surveillance network often requires little time or money and can prevent or mitigate these potentially disastrous issues.

We review network time for surveillance, covering these key topics:

- Time protocols: NTP, SNTP, Windows Time
- How cameras handle time sync - on arrival vs camera timestamp
- How recorders / VMS synchronize time
- Time server options
- What you should sync
- IP vs Non-IP Cameras

Time Protocols

The most commonly used time protocol in surveillance (and the IT industry at large) is SNTP (Simple Network Time Protocol) which is a less complex version of NTP (Network Time Protocol). While NTP is consider more accurate, even the 'less' accurate SNTP is generally accurate within a millisecond, sufficient for video surveillance application. Both of these protocols are intended to synchronize computers and other network devices to within a few milliseconds of UTC (Universal Coordinated Time).

A time server running one of these protocols provides time to devices (cameras, client PCs, servers, etc.) which request it. This synchronization is most often performed every hour, though some may choose to run it more often, in cases where high accuracy is required.

Surveillance devices often are not clear whether they support NTP or SNTP. It is common for devices to simply state 'time synchronization' instead of SNTP or NTP specifically. Despite this, they will work with varying time servers (described in a later section).

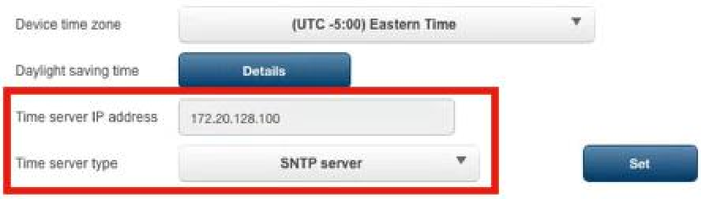
Windows Time

It's worth noting that Windows includes a time protocol of its own which has historically been used in many networks. However, configuring a time server using Windows Time requires users to edit the Windows registry, which many users may not be comfortable with. Additionally, it is notoriously inaccurate, with multiple seconds of drift common, so should not be used in surveillance

How Cameras Handle Time

The vast majority of current IP cameras, including low cost and consumer models, allow for automatic synchronization of the camera to a time server. Users typically simply enter the server IP address or hostname, port, and time zone, and the camera retrieves current UTC time and adjusts its on-board clock. This synchronization is typically performed hourly, though some cameras allow for a different interval to be set.

This image shows these typical settings:



Device time zone: (UTC -5:00) Eastern Time

Daylight saving time: Details

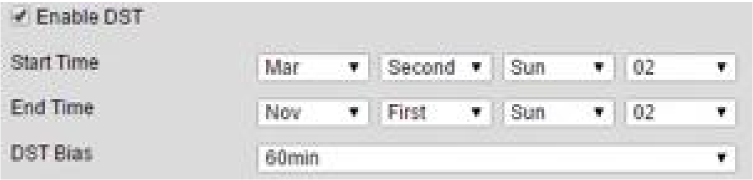
Time server IP address: 172.20.128.100

Time server type: SNTP server

Time Zones and Daylight Savings

Because time servers provide UTC, which applies no time zone or daylight savings (DST) adjustments, these settings must be configured in the camera. Each camera must be set to its local time zone. For DST, many devices include configurable options for start/end dates and time offset (typically 1 hour). Camera time is automatically adjusted when DST begins and ends.

These settings are shown in this sample image:



☑ Enable DST

Start Time: Mar ▾ Second ▾ Sun ▾ 02 ▾

End Time: Nov ▾ First ▾ Sun ▾ 02 ▾

DST Bias: 60min ▾

However, in some cameras, only an "enable DST" checkbox is provided, and users must manually set and reset time when daylight savings begins and ends. Care should be taken to ensure this is done, as inaccurate time will be provided if it is not.

Manual Sync

In addition to automatic sync options, many cameras also allow the time to be manually set. This is not recommended, as manual adjustment may easily be forgotten or incorrectly set, and adjusting time on even a handful of cameras may become tedious and time consuming.   Because each camera is changed manually, it is difficult to get the time on each camera to the same second, and could be a minute or more off.   Drifting will occur over time and can cause the cameras to be many minutes or more off.   In this case you may see obscure time differences (i.e. 6 minutes off, 18 minutes off, etc) between cameras and other devices on the network.

How Recorders / VMS Synchronize Time

There are two ways VMSes handle timestamps: stamping frames upon arrival, or using the camera's timestamp.

Stamping on Arrival

Stamping on arrival is exactly what it sounds like, with the VMS marking the time it receives each frame of video. This avoids issues caused by camera time being inaccurate, as the server is the sole source of time. In very large systems, or systems with high latency, it may take longer for frames from one camera to arrive than frames from another camera, which will cause video to be out of sync. However, this is rarely a practical concern, as time differences are very small (<1 second) and these issues are not common.

Using Camera Timestamps

Other systems use the timestamp added to video by the camera. If cameras are properly synchronized to a time server, this should not be an issue. However, if one or more cameras are using inaccurate time, issues may result, varying from annoying to severe.

If a camera's clock is fast by two hours, video on the VMS system will be marked as two hours off. Searching for video at the expected time will produce video from another time, while the desired video has actually been stored two hours in the future. This makes synchronized playback unusable. Worse, it may make video inadmissible in court, as the timestamps do not reflect the actual time a crime took place.

Verifying With VMS

IPVM recommends checking with your preferred VMS supplier on their approach. For example, Exacq uses the camera's timestamp while Milestone and Genetec use stamp on arrival.

Time Servers

There are three basic ways to serve time to a surveillance network:

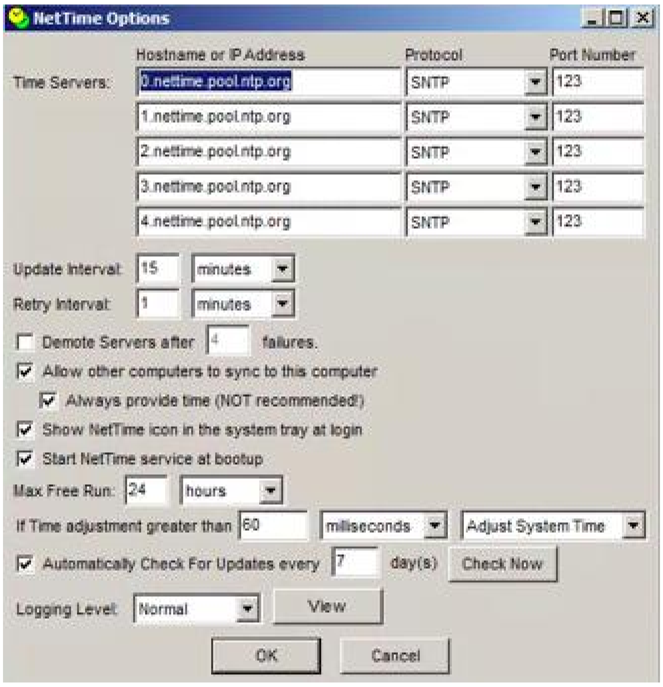
Public Servers

Public servers such as time.gov and ntp.org are most commonly used to synchronize time of PCs, though some cameras also use them by default. However, in order to use these servers, all devices must have internet access, which is often undesirable in surveillance networks. Also, using these servers for multiple devices is considered poor practice in the IT industry, as local servers greatly reduce traffic and requests made of public sources.

Private Servers

In a surveillance LAN, one (or more) servers may be configured as a time server. This machine then retrieves time from a public source such as ntp.org or is manually set, and serves time to all other devices in the network. This is most often configured via third party programs such as Meinberg NTP or NetTime.

This screenshot shows the setup of a typical NetTime server, in this case pulling from multiple sources, with a 15 minute synch frequency:



NetTime Options

Time Servers:

Hostname or IP Address	Protocol	Port Number
0.nettime.pool.ntp.org	SNTP	123
1.nettime.pool.ntp.org	SNTP	123
2.nettime.pool.ntp.org	SNTP	123
3.nettime.pool.ntp.org	SNTP	123
4.nettime.pool.ntp.org	SNTP	123

Update Interval: 15 minutes

Retry Interval: 1 minutes

□ Demote Servers after 4 failures.

☑ Allow other computers to sync to this computer

☑ Always provide time (NOT recommended!)

☑ Show NetTime icon in the system tray at login

☑ Start NetTime service at bootup

Max Free Run: 24 hours

If Time adjustment greater than 60 milliseconds Adjust System Time

☑ Automatically Check For Updates every 7 day(s) Check Now

Logging Level: Normal View

Since nearly any PC may be set up to act as a time server (including the VMS server), without much-increased load, private servers retrieving time from an Internet source is the most common time synching option in surveillance.

Dedicated GPS Servers

Finally, in systems where accurate time is required but the surveillance system is not connected to the internet, dedicated GPS based time servers are used. These devices retrieve time from GPS satellites via antenna, either mounted to a window or external, and act as NTP/SNTP servers for the rest of the network.

Dedicated GPS time servers sell for about $700 USD online (Veracity Timenet) and up. Advanced servers (such as Spectracom and Meinberg) with extremely precise nanosecond accuracy, redundant external antennas, and other advanced features sell for easily 2-3 times this price, or more.

Because of the added installation and material cost, GPS servers are typically only used in systems where the surveillance network is closed, without access to the internet.

IP vs Non-IP Cameras

Non-IP Cameras, like analog, HD analog, HD-SDI, do not have any concept or implementation of 'time'. The encoder or recorder these cameras connect to stamps time when video is received. In small systems, with only a single encoder or recorder, this generally results in the time of all cameras being synchronized. A time server, however, can still be beneficial to ensure the time is accurate. Moreover, if there are multiple recorders connecting to non-IP cameras, the same risk exists with those recorders being out of sync like multiple IP cameras.

What Should I Sync?

To avoid any potential problems, regardless of how the VMS server handles timestamps, we recommend that all cameras, VMS servers, and clients be synchronized to the same time source. Though it may not be necessary, entering time server information requires minimal time during initial setup and eliminates one potential source of issues.

Poll - Do You Time Synch?

Note: ***Click here to view poll results on IPVM***

Network Monitoring / SNMP

Surveillance systems typically rely on the the VMS to report issues, but this most often just means knowing a camera is "down" with no warning or detailed information.

Network monitoring systems can give users more insight into their network, from the camera to the switch to the VMS server, but are seen as too complex or expensive to be used in simple surveillance systems.

However, significant practical benefits can be gained by understanding these monitoring platforms, with free software available, and minimal setup time.

We cover these topics:

- What is SNMP?
- What are traps and requests?
- How do I monitor this data?
- What monitoring do cameras, servers, and other devices support?
- What is a MIB and how do I use them?
- What practical surveillance applications are there?

What Is SNMP?

Simple Network Management Protocol (SNMP) is used to monitor health and performance information of networked devices. This information is either requested by an "manager", such as an SNMP monitoring server, or sent as a message (called a "trap") by a device.

- Requests generally include variable information, such as CPU usage, bandwidth, disk write speed, etc.
- Traps are used to notify the manager of significant events, such as temperature alerts, power supply failures, camera tampering, etc., which do not have a variable status.

Network Monitoring Software

Devices are monitored using a specialized monitoring software which interprets SNMP requests and traps (as well as other protocols) and presents usable information, most often graphically. Devices such as cameras, servers, switches, etc., are added (much like adding cameras to a VMS) and one or more "sensors" associated with them. A sensor includes anything which may be monitored, such as pings, uptime, bandwidth, or throughput.

There are many network monitoring platforms available, all with varying featuresets and protocol support, both paid and free. Some popular platforms include:

- PRTG: Free for up to 100 sensors, license required for higher sensor counts.
- Spiceworks: Free
- WhatsUp Gold: License required
- ManageEngine: License required, 1000 sensor minimum.

We used PRTG because it is one of the most popular platforms available. Additionally, it offers a wide variety of sensor types (SNMP, Windows Management Instrumentation, SSH for Linux/MAC, HTTP, Ping, and more), and free licensing for up to 100 sensors.

Using Network Monitoring Systems

This video demonstrates the basics of adding devices as well as configuring and monitoring sensors in network monitoring software:

Note: Click here to watch the video on IPVM

SNMP Traps

Traps are monitored using a special type of sensor, simply called a receiver, which is used to receive and interpret trap data into usable information. In their raw form, traps contain complex syntax with pertinent information sometimes difficult to find or not in plain text. For example one manufacturer's traps look like this:

```
SNMPv2-SMI-v1::enterprises.3967.1.3.2.1.1.1 = 0

SNMPv2-SMI-v1::enterprises.3967.1.3.2.1.1.1 = 1
```

Without interpretation, this message is useless to the user. However, once the trap is translated into usable information, it may be used to create alerts or warnings upon specific events.

We review traps in this video:

Note: Click here to watch the video on IPVM

Device SNMP Support

SNMP supports varies by device, with cameras typically providing the least information, while servers and switches provide more detail.

Cameras

Most IP cameras do not support any information requests, so are limited to simple ping and HTTP sensors. Some, such as Axis, include more detail, such as Ethernet throughput, temperature, and local recording status, but this is rare.

Some cameras also include support for traps upon error, though for which events and how detailed varies widely. Most send traps only for critical failures, such as bad power supplies, temperature alarms, hardware failures, etc. Others may be configured to send a custom trap for any event on the camera.

Servers

Servers deliver more detailed information, including detailed performance metrics, such as CPU load, throughput in and out, memory usage, disk I/O, and more.

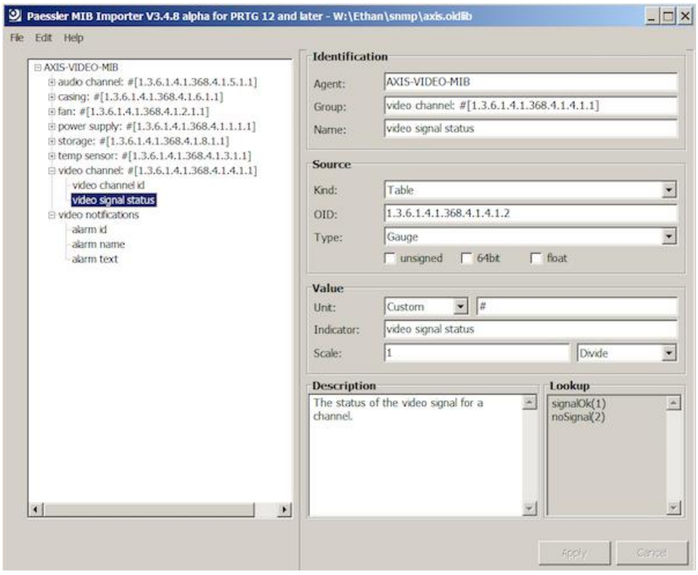
Managed Switches

Switches also deliver detailed information, typically on a port by port basis. Throughput in and out for each port may be viewed, along with errors, VLAN traffic, and more.

Dealing With MIBs

With so many unique device manufacturers with differing SNMP implementations, network monitoring developers cannot be expected to interface with and interpret all of them. Because of this, manufacturers may release MIB files (Management Information Base) which contain details on which requests and traps they support. These files are then imported into the network monitoring application which uses them to interpret SNMP data.

This image shows the contents of Axis' MIB files (publicly available for download), ready for import:


Paessler MIB Importer V3.4.8 alpha for PRTG 12 and later - W:\Ethan\snmp\axis.oidlib
File Edit Help
Apply
Cancel

```
⊟ AXIS-VIDEO-MIB
  ⊞ audio channel: #[1.3.6.1.4.1.368.4.1.5.1.1]
  ⊞ casing: #[1.3.6.1.4.1.368.4.1.6.1.1]
  ⊞ fan: #[1.3.6.1.4.1.368.4.1.2.1.1]
  ⊞ power supply: #[1.3.6.1.4.1.368.4.1.1.1.1]
  ⊞ storage: #[1.3.6.1.4.1.368.4.1.8.1.1]
  ⊞ temp sensor: #[1.3.6.1.4.1.368.4.1.3.1.1]
  ⊟ video channel: #[1.3.6.1.4.1.368.4.1.4.1.1]
      video channel id
      video signal status
  ⊟ video notifications
      alarm id
      alarm name
      alarm text
```

Identification

Agent: AXIS-VIDEO-MIB
Group: video channel: #[1.3.6.1.4.1.368.4.1.4.1.1]
Name: video signal status

Source

Kind: Table
OID: 1.3.6.1.4.1.368.4.1.4.1.2
Type: Gauge
☐ unsigned ☐ 64bit ☐ float

Value

Unit: Custom #
Indicator: video signal status
Scale: 1 Divide

Description

The status of the video signal for a channel.

Lookup

signalOk(1)
noSignal(2)

Surveillance Applications

There are several use cases for which network monitoring makes sense, including:

Camera Monitoring

While VMS systems provide basic information on cameras, including up/down status and throughput, SNMP and networking monitoring systems may provide more detail.

By monitoring pings, users can see not only if the camera is up or down, but increases in latency, as well. Further, using a sensor to check HTTP web page health of the camera's web interface shows whether the camera is responsive, regardless of whether it is pingable or not, which may commonly happen when cameras go bad. Finally, monitoring throughput out (whether on the camera itself or using a switch port), users can be alerted if the camera stream drops below extreme levels, which may indicate video loss, even if the camera is still shown as up and responding to pings.

Server/Recording Monitoring

Network monitoring systems can be used to monitor basic server performance, such as CPU and memory load, throughput, and more. While these parameters are available using Performance Monitor or other tools, using a monitoring system centralizes this information for multiple servers, and allows for better warning and error alerts from a centralized location.

Additionally, server disks may be monitoring to tell at a high level whether video is being recorded or not. By monitoring disk writes throughput per second, users may be alerted if this traffic drops below an expected level. For example, if cameras are being written to disk at a minimum of 12 Mb/s, and disk writes drop to 100 Kb/s, but cameras are still up and streaming, there is likely a server recording issue which users should investigate.

Example Devices and Alerts

This video reviews common devices and alerts which might be used in surveillance monitoring:

Note: ***Click here to watch the video on IPVM***

Network Cabling

Network Cabling

We teach the fundamentals of network cabling for video surveillance networks, how they should be installed, and the differences in testing them for production networks.

Specifically, we examine:

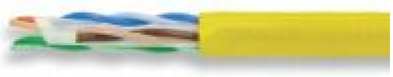
- Cat 5e vs. Cat 6a vs Cat 7a Basics
- Why More Than Cat 5e is Often Unnecessary for Video
- STP vs. UTP Overview
- When You Should Use STP
- Solid vs. Stranded vs. CCA
- Wiremapping
- Cable Identification
- Service Detection
- PoE Detection
- Cable Labeling
- Using Cable Trays & Hooks
- Importance of Cable Jackets
- Why Drawing Maps Is Vital
- Avoiding Excessive Service Loops
- Installation Specifications
- Crosstalk Defined
- Propagation Delay
- Cable Verifiers
- Cable Qualifiers
- Cable Certifiers
- Choosing Between Verifiers, Qualifiers and Certifiers

Cat 5e vs Cat 6a vs Cat7

Cat 5e and Cat 6a are the two most common UTP cables used today, while Cat 7 is a niche offering for super high bandwidth connections where fiber is not a viable option. All three types have similar construction, made up of four twisted pairs of copper wire in the range of 22-24 AWG under a single jacket. They do have some key differences, however:

- Cat 5e: Cat 5e is rated to a max operating frequency of 100 MHz. It's main use historically has been for Fast Ethernet (100Base-T), but it's capable of gigabit speeds using all four pairs, as well. Cat 5e uses 24AWG conductors, with few exceptions. The following image shows a partially stripped Cat 5e cable:

- Cat 6a: Cat 6a is rated to a max operating frequency of 500 MHz. A variant of gigabit Ethernet was created to take advantage of its better performance characteristics to use only two pairs for gigabit speeds and is capable of up to 10-gigabit Ethernet. However, most gigabit transmission still uses four pairs today. Cat 6a often uses 23 AWG conductors, which makes it less flexible and gives it a larger outside diameter, requiring more care in installation. Cat 6a cables also commonly use a physical barrier in the cable to maintain separate between pairs. The following image shows a stripped Cat 6a cable. The white separator can be seen in the middle of the pairs:



- Cat 7a: Even faster and with tighter cross-talk specifications than Cat 6a, Cat 7a cables are rated to a max operating frequency of 1000 MHz. While conductor wire gauge is typically unchanged from Cat 6a, the faster frequency of Cat 7a is a result of precise twist specifications, and the mandatory inclusion of a full braided shield and individual pair shield. Throughput is rated at the same 10-gigabit Ethernet capacity of Cat 6a, and the extra bandwidth capacity is unnecessary for typical video surveillance applications and unneeded for connecting cameras to switches. The image below shows the integral shielding in Cat 7a cables:

Aside from the physical characteristics, there are a number of other parameters which these cables are tested for, such as crosstalk (interference between conductors), attenuation (signal loss due to distance), and return loss (loss of signal power due to reflected signal). Cat 7a and Cat 6a also are tested for performance parameters Cat 5e is not, essentially for better interference rejection. These factors, combined with increased bandwidth, are what allow higher-rated cables to perform better.

Do I Need Cat 6a or Cat 7a?

Based on the above information, the question then becomes whether surveillance applications need this extra performance provided by Cat 6a or Cat 7a? No. IP cameras do not need gigabit Ethernet connections, and Cat 5e is more than enough for connecting cameras to switches.

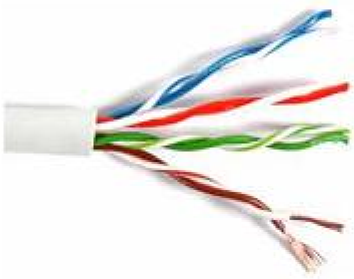
On the other hand, many IT organizations have standardized on Cat6a for their entire infrastructure, both for future proofing and for special need applications. Even if IP cameras do not require the extra capabilities of Cat 6a, such standardization may require all video surveillance devices to use Cat6a as well.

Where Cat 6a or Cat 7a does have potential, however, is in locations which may be more difficult environments. These include "noisy" facilities with a lot of RF or electromagnetic interference, which may create transmission errors. High temperatures also negatively impact cable performance, as throughput decreases as temperature increases. Finally, if a large number (100+) of cables are to installed in the same path, such as a cable tray, signal coupling can occur.

Cat 6a and Cat 7a's superior performance allows them to reject interference from these outside sources better than Cat 5e. Additionally, they simply allow for more headroom due to increased bandwidth. This means that while its performance may be decreasing due to any of the above factors, it has a better chance of maintaining a usable level of performance where Cat 5e could not. Substantially decreased performance can lead to blocking and ghosting in video, or just plain video loss.

STP vs. UTP Overview

A quick physical comparison between STP and UTP, or 'unshielded twisted pair' cabling reveals the primary differences. The image bellows the additional metallic shielding surrounding wire pairs in STP:



UTP: Unshielded Twisted Pair

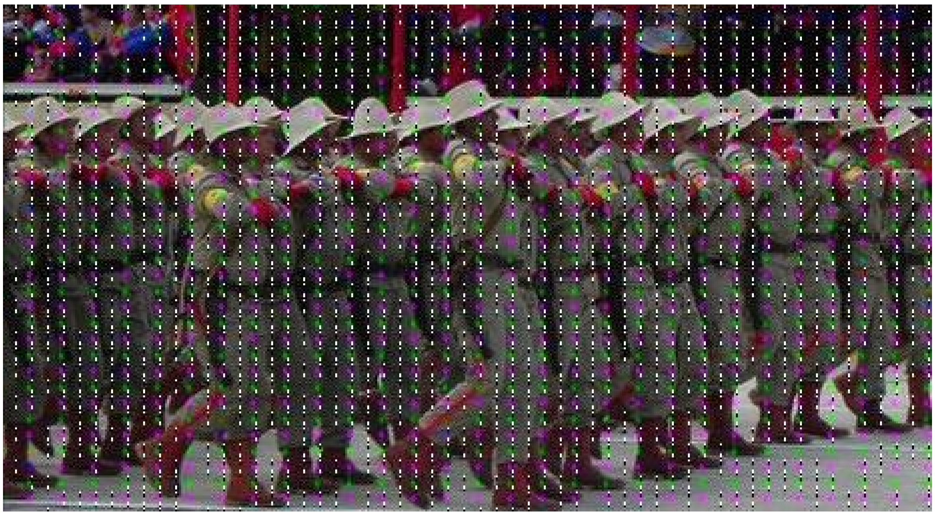
STP, or U/FTP: Shielded Twisted Pair

'Shielding' should not be confused with 'cable screening' where a single layer or metallic foil or mesh covers the entire bundle of wires. While the decision to individually wrap pairs versus gross wrap the entire bundle shares some of the same benefits, they are not equivalent to one other and result in different performance.

The common abbreviation for shielded twisted pair cable, 'STP', is sometimes noted as 'U/FTP' or 'Unscreened/Foil-shielded twisted pair'. As cabling standards develop and are refined over time, cabling products devoted to high-end data center applications have driven changes to the nomenclature. However, for most surveillance video applications 'STP' is most widely used.

Electrical Interference: Video Killer

In the video surveillance world, the emphasis is often on cameras and NVRs, with little attention to the cabling in between. When video quality problems arise, it can be a frustrating exercise to swap camera and tweak settings, only to discover problems are still present. However, taking a hard look at cabling can resolve maddening issues. Take the example in the image below:



Electrical interference in the cabling itself cause this type of problem. Not only does the cable transmit intended data streams, but it also can attract and transmit unwelcome 'noise'. A jacketed cable can serve as an 'ad-hoc antenna' helps emphasizes why cable shielding is sometimes critical.

The adage goes: "You're only as strong as your weakest link." This certainly applies to video networks, where the performance of world-class cameras and video recorders can be ruined by shoddy network design.

Physical Differences

The following list summarizes the tangible differences between UTP and STP.

- Metallic Foil Shield: A thin layer of foil, commonly aluminum, surrounds wire pairs. This layer is often called the 'drain', and must be properly terminated. Failure to adequately ground the drain can amplify the problems that STP attempts to mitigate.
- Thicker Jacket: The added layers of foil increase the weight add diameter to the cable bundle. As a result, a thicker plastic insulating jacket is needed, which adds rigidity. Overall, STP is heavier and

thicker compared to UTP, and may be more difficult to install as a result.

- Cores, Pull Strips, and Groundwires: Depending on the exact manufacturer and brand of STP, other features may be present not commonly found in UTP cabling. This includes plastic divider 'core' sprues, strings to aid stripping the jacket, and additional electrical grounding wires.

Functional Differences

Those additional physical features provide STP with properties that UTP does not possess.

- EMI resistance: The primary advantage of shielding is protection from environmental electromagnetic interference, or EMI. Because each pair is individually wrapped, the ability for ambient interference to permeate and carry down the cable is significantly minimized or eliminated.
- Isolated line noise: Interference can be a 'two-way street' in that unshielded cabling is a source itself of interference. In some applications, like sensitive medical imaging or manufacturing, normal ethernet cabling can be a uncontrolled conduit for interference. Again, the addition of pair shielding minimizes or eliminates this problem.
- Higher transmission rates: Some studies suggest that the reduction in noise increases the bandwidth capabilities of shielded cabling. However, these claims should be met with some caution. Any gross improvement in transmission rate has likely root cause in the tighter 'twisting' of cable pairs during manufacture rather than the

reduction in EMI. In any case, any additional increase in transmission speeds must also be supported by the terminating connectors. Transmission speeds are only as fast as Cat5E or Cat 6 terminations are rated, which mitigates the impact of this claim.

Cost Difference

Using STP adds between $20 to $40 per camera compared to UTP cabling, assuming cable runs of 150 feet, based on STP cable costs ~40% more than UTP and depending on how much additional labor or larger conduit is needed for the larger, heavier and more rigid STP.

Where should STP be used?

The simple answer: anywhere interference could be a problem. Since that alone is fairly obtuse, here are some common sources of interference that affect network video:

- Adjacent to High Voltage Wiring: Power wiring can interfere with data transmission even when run parallel to each other. Even wiring run a compliant distance apart within a grounded raceway can be a source of video interference. While no hard specification exists for when to use STP in this situation for video, best practices in data networking design follow that any data cabling sharing the same raceway, regardless of how it is contained in EMT or conduit, must be run using STP cable.
- Near Inductive Sources: Data cabling run near common electromechanical features like electric motors, power transformers, magnetic coils, or solenoids can introduce significant EMI. These sources are characterized by their 'inductive' properties, or their

reliance on magnetic fields for operation. Devices like HVAC equipment, ventilation fans, door maglocks, electrical switchgear, and industrial machinery can generate enough interference to degrade video quality.

- GSM Devices/Walkie Talkies: Common low powered communication radios disrupt data transmission. While a token handset may not be significant enough to be a problem, locating data runs near high powered repeaters or transmitters should be run using STP to eliminate problems.
- Fluorescent Light Fixtures: One of the biggest sources of EMI are these common light fixtures. Given the common occurrence of ethernet cables running directly overhead of these fixtures in acoustic tile ceilings, if cabling cannot be run in formal cable trays, it should be run using STP cable.

Practical Use

In our experience, the vast majority of all surveillance ethernet cabling has been run using UTP, and we have no significant issues to report. We went to our LinkedIn group to gauge how commonly STP is used, and a significant majority claim voted "seldom" to "never". Since specifying networks with appropriate shield is imperatively acknowledged in datacenter and networking design "best practices", is it also significant to specify in video network design?

When Is Using STP Mandatory?

Industry giant Axis Communications recently declared use of STP mandatory for outdoor cameras per the following whitepaper:

"Our recommendation is to deploy an STP network cable in demanding electrical environments. Examples of demanding indoor environments are where the network cable is located in parallel with electrical mains supply cables or where large inductive loads such as motors or contractors are in close vicinity to the camera or its cable.**It is also mandatory** to use an STP cable where the camera is used outdoors or where the network cable is routed outdoors."

This is a bold statement given that ~40% of all cameras are installed outside. Observing Axis' recommendation may not drive a significant increase in overall project cost but it is likely overkill relative to common problems faced.

Rather, our experience disagrees with the generalized application of STP. The smartest use of STP is where ethernet is run in the 'high risk' areas identified above, or where earth-grounding switches and endpoint devices is not possible.

Solid vs. Stranded vs. CCA

The build of cabling varies, generally in the manner the conductor is constructed. The material of the conductor itself is commonly copper or aluminum, with aluminum resulting in a cheaper, lighter, but less conductive wire type.

Conductor copper grades are higher performing, but are heavier and more costly. Because of the cost, using solid conductors is often replaced by 'stranded' varieties, which is composed of multiple 'threads' of copper wires twisted together into a single conductor.

However, the method often results in minute differences in resistance, with solid conductors being better than stranded types.

The differences between solid vs stranded is often more pronounced when copper strands are subbed out of copper plated aluminum conductor, called 'CCA' cable. While the least expensive of all cabling options, it can be a big performance difference:

1. The conductor are more brittle and prone to break during pulling.
2. CCA has higher resistance than copper, which results in more aggressive voltage drops and increased heat, a potentially big problem when using PoE.
3. CCA oxidizes when exposed, resulting in decreased efficiency and degraded performance.
4. CCA generally has higher attenuation which can increase flaws in video streaming.

Top 5 Cable Installation Tips

Here are our top 5 tips:

1. Label All Cables: One of the most costly oversights when running cable is neglecting labels. As we previously covered in our Cable Labeling Best Practices report, we address how a few minutes of labor to labeling things can save thousands of dollars in troubleshooting time later. Having the ability to quickly determine the specific cable a camera is using and where it is connected in a switch make quick work of eliminating lengthy 'hunt & peck' diagnosing efforts.

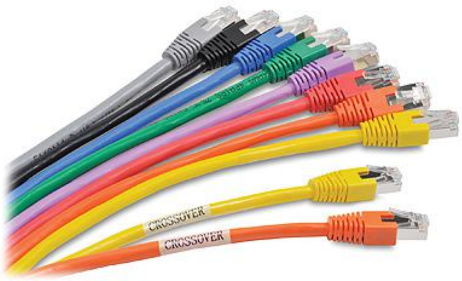
2. Use Cable Trays/Hooks/Tubing: Loose cabling above drop ceilings or along trusses have a way of becoming hopeless tangled messes over time.

Every time a ceiling tile gets popped or moved, the cables run atop get displaced. In Example 1 image above, the pictured state of the cabling is due to ceiling repair project that simply cast aside the network as an obstacle. Even after substantial reworking and re-stringing of cable, the system had problems with camera outages and unlabeled cable runs. The images below show examples of trays and hooks in use:

Cable Tray

Bridle Hook

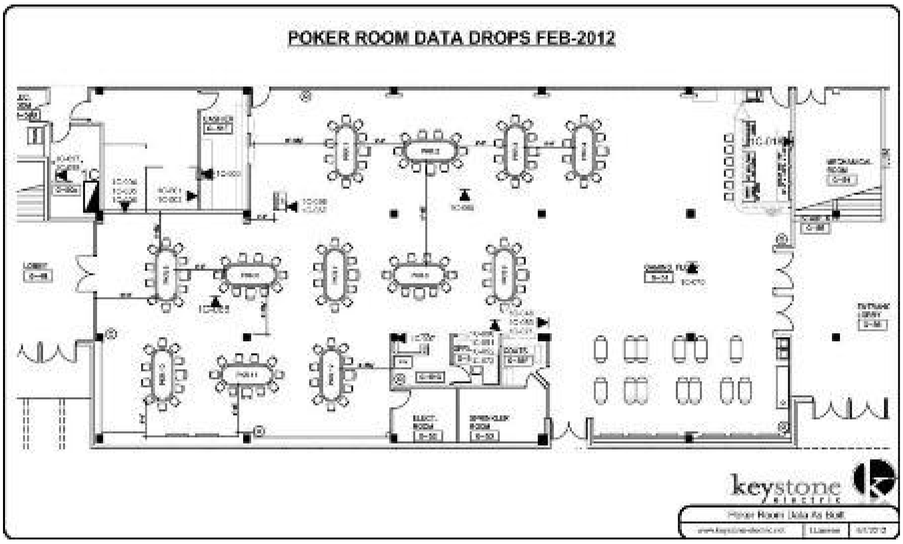
3. Jacket Color is Important: Using a specific color to denote cables belong to a certain system can be important. In Example 2 above, many colors are used but in a random fashion. Staying with a color scheme, even when not required by an overarching standard, will help eliminate 'monochromatic confusion' of lumping multiple data networks or low-voltage systems together.



Because 'blue' and 'gray' jacketed cables are the most common datacomm colors, and 'red' is reserved for fire system applications, the best 'standard stock' colors for video surveillance available at most distributors are greens, yellows, purples, and oranges. However many non-standard color options are available to choose from, and are only limited by order lead time and extra cost.

4. Draw a Map: Not only is drawing a map of cable runs and drops invaluable reference for surveillance maintenance, it also can be referenced by other projects that might disturb cabling. If the function of cabling is unknown, it can easily been seen as 'not critical' or even 'out of service'. However, a map of each run and it's scaled location on a floor plan makes it easy to locate and readily identifiable as part of a critical system. Ensuring that the information is accurate is vital when planning work, and every time work is performed that changes the location or index of cabling, the map must be updated.

For those performing in-depth or high volumes of design/installation cabling work, AutoCAD is the ideal platform to produce these maps (see our '[AutoCAD for Surveillance]' report), as they can easily be incorporated into official print sets. However, for incidental and occasional map drawing, a program like Visio (see our '[Visio for Surveillance]' report) is easier to navigate and use.



5. Don't Use Excessive Service Loops: One of the most common, and needlessly messy, habits of integrators is to pay out excessive amounts of cable as 'service loops' at the end of cable runs. Service loops should

contain a few feet of extra cabling to cover the inevitable camera shift or network rack movement. However, coiling up twenty or fifty feet at the end of runs 'just in case' needlessly drives cost and creates clutter.

For service loops, BICSI standards recommend 3m at the rack and 1m at the outlet or device. Note that it says RECOMMEND. It is recommended where practicable, and excessive loops are discouraged.

The performance impact of line interference and improper bend radii encouraged by lengthy service loops can negate any potential benefit the extra cable may provide in the future. Using 'long enough' loops reduces the amount of cable to troubleshoot, hang neatly in small spaces, and keep organized.

Installation Specifications

While no 'universal' code or spec exists for running cable, BICSI has published a number of 'best practice' guides for design and installation. Frequently, when installation specifications are mentioned in a bid or scope of work, a BICSI publication number is given. These documents define how installation work is to be executed,and almost universally recommend the 5 tips above as part of a network project. Among the commonly cited specs are:

- NECA/BICSI 607-2011, Standard for Telecommunications Bonding and Grounding Planning and Installation Methods for Commercial Buildings
- BICSI 002-2011, Data Center Design and Implementation Best Practices

- ANSI/BICSI 001-2009, Information Transport Systems Design Standard for K-12 Educational Institutions
- ANSI/NECA/BICSI 568-2006, Standard for Installing Commercial Building Telecommunications Cabling
- Electronic Safety and Security Design Reference Manual (ESSDRM)
- Telecommunications Distribution Methods Manual (TDMM)

Even if projects do not explicitly state work must conform to one or more of the spec guides, it is in the installer's best interest to take the guidelines to heart in order to keep the 'nightmares' at bay.

Cable Testing

Proper cable installation is key to trouble-free surveillance systems.

However, testing is often an afterthought, with problems only discovered when cameras have problems, resulting in increased troubleshooting, or even worse, reinstallation. Simple, inexpensive testers are available, which can easily prevent these issues without adding substantial install time.

The Three Main Test Tool Types

Verifiers, Qualifiers and certifiers and the 3 main test tool types to select from:

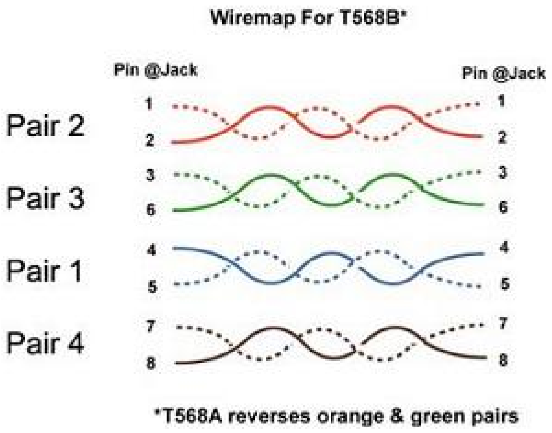
- Certifiers are the only of the three to test to EIA/TIA568B standards, which ensures manufacturer warranty and essentially guarantees link performance. Main downside is high price of ~$10,000, 4 to 5x of a qualifier.

- Qualifiers deliver a detailed technical test but is not standards-compliant, aiming primarily to give a 'real world' test at a lower price than certifiers.
- Verifiers provide only basic cable testing that misses issues such as crosstalk, loss, and skew. Their main upside is that the testers are, by far the cheapest, at only a few hundred dollars.

For more in depth information read our Network Cable Testing Guide

Cable Verifiers

Cable verifiers perform the most common tests needed to ensure basic cable performance, though exact features and functions vary by manufacturer. Verifiers consist of the handheld test unit itself, and one or more remote units, plugged into the far end of the cable to be tested. Some also allow testing of coax cables via F connector.



The most common features of verifiers are:

- Wiremap: Wiremap determines whether UTP is terminated correctly, with the correct pairs in the right place on the connector, typically to EIA/TIA 568A/B. This may be displayed graphically, via LEDs or numbers. Graphical wiremap is much simpler to use for the inexperienced, as it displays exactly which pins are the issue, and how they are crossed. In the case of coax cables, it simply shows whether there are any shorts between shield and center conductor.

- Length/distance to fault: The verifier determines the length of cable so installers may be sure UTP does not exceed 100m. This function also shows the distance to cable faults, such as breaks and shorts, so repairs can be made more easily.
- Cable identification: Each remote unit has a unique identifier, so that users may connect to multiple cables or jacks at once, and use the handheld unit to locate each. This can speed troubleshooting if cables are existing or mislabeled, instead of having to check a single cable at a time.
- Service detection: Many modern verifiers can detect the use of Ethernet, PoE, or POTS telephony on a cable, and which pairs are used. While this does not verify proper operation, it does show whether a cable is plugged into a switch or cross-connected to a phone line.

Verifiers generally do not save and store test results, a feature commonly found in qualifiers and certifiers, though some exceptions are available, such as the ByteBrothers RWC1000K.

This video below reviews the use of a typical verifier.

Note: ***Click here to watch the video on IPVM***

Product Options

Cable verifiers range in price from about $125-450 USD, with cost generally driven by graphic vs. LED display, display size, and number of functions.

Lower cost models such as the Ideal VDV II (~$125 online) provide a smaller display and numeric indication of wiremap compared to the graphical display in more expensive models. More fully featured options such as the Fluke MicroScanner (~$450 online) and ByteBrothers RWC1000K (~$400), offer a larger graphical wiremap display, or the ability to save test results.

Qualifiers

Qualifiers add some additional functions, but are not precisely calibrated and testing to standards, making them the middle ground between verifiers and certifiers.

The models typically include the wiremap, length, identification and service detection of verifiers, but add functions such as:

- Service testing: Instead of simply detecting Ethernet service on a cable, qualifiers runs simple tests to check cable bandwidth and basic issues and determine whether it will support 10/100, GbE, etc. These tests typically include crosstalk, though not to the level a certifier tests.
- PoE testing: Instead of simply indicating that PoE is present, qualifiers display measurements such as voltage and maximum wattage, which can indicate whether a port is 802.3af or 802.at, and troubleshoot issues with power budget.
- Saved test results: The vast majority of qualifiers record test results to on-board storage, so these may be printed out or stored at the end of a project for documentation.
- More detailed displays: Qualifiers display more detailed fault information than verifiers, showing the estimated distance to the

cable fault, and whether it's a short or crosstalk issue, often caused by crushed or damaged (but not cut) cables.

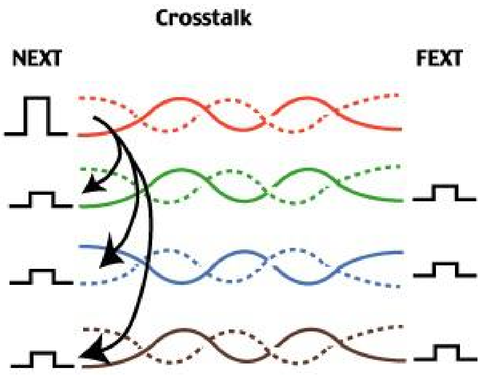
Product Options

Qualifiers are a large price increase over verifiers. The Fluke CableIQ sells for about $1,100 online, more than twice the price of their verifier model, the MicroScanner. Some, such as Ideal's SignalTek line (~$2,000 online), are priced even higher.

Qualifiers are not as widely available as verifiers, with Fluke, the Ideal SignalTek NT, and ByteBrothers Low Voltage Pro, being some of the most common and popular among installers.

Certifiers

Certifiers test cables to ANSI/EIA/TIA standards, running a full battery of tests, including those run by verifiers and qualifiers (wiremap, length), while adding others and running more in depth crosstalk testing.



These tests include:

- Crosstalk: This test measures the amount of signal which is leaked from one pair of a cable to another, or from one cable to another. This includes 6-8 different crosstalk tests (near end, far end, alien crosstalk, etc.) depending on the category of the cable being tested. Qualifiers simply test basic "crosstalk", without all of these detailed measurements.

- Propagation delay: This test is similar to latency, measuring the time it takes for signal to reach the far end of the cable.
- Delay skew: Skew tests measure the difference in delay among all four pairs of the cable. Significant differences can indicate cable faults or stressed cables.
- Insertion/return loss: These are measurements of the signal loss caused by connectors in the cable run (insertion loss) or by reflected signal back at the test point (return loss) typically caused by poor terminations or cable faults.

This PDF is a detailed test report produced by a cable certifier:

Product Options

Cable certifiers are far more costly than other testers, generally at least $5,000, though $10,000+ is not uncommon, with full kits including fiber optic adapters often selling for $20,000. In addition to initial cost, certifiers must be factory recalibrated periodically (every 2-3 years), which ranges from a few hundred to over a thousand dollars.

Due to the very strict tolerances required for calibrated testers such as these, only a handful of manufacturers sell cable certifiers, with the Fluke DSX and Ideal LANtek lines two of the most common.

What Do I Need?

In general, integrators should keep at least a verifier on hand. Wiremap and length are the key elements which should be tested in any cabling install, prior to devices being installed. It is common for at least one or two cables in an installation to have crossed or shorted pairs. Instead of simply guessing and/or re-terminating the cable without diagnosing the problem, a verifier may show exactly what is wrong.

Those doing mid-size installs with the budget to support it may want to invest in a qualifier. The ability to test services and document results may be used not only for installation and troubleshooting, but as a differentiator, since many integrators (especially small ones) do not provide these services or documentation.

Only in rare cases should integrators invest in a certifier, since the quantity of cables in most security projects is low, and full-blown certification tests not often required. In some instances, customers or RFPs may require a certifier be used, and test results documented as part of the closeout process. However, if this is only a periodic need, certifiers are available for rent for a few hundred dollars, well below their out of pocket cost, as well as the cost of maintaining their calibration.

Fiber Use and Testing

Most networks are twisted pair based (UTP/STP/ScTP, etc.), which is what we have covered above. For fiber links, see: Using Fiber Optics for Surveillance

STP vs UTP

For many video system designers, deciding which ethernet cabling to use is a quick decision: go with the cheapest. However, this overlooks the possibility cable, and the video it carries, needs extra protection against common electromagnetic interference.

Is the difference between cable types that significant? We examine shielded cable, look at how it can prevent video problems, and compare it to nonshielded alternatives.

We explain:

- How Electrical Interference Affects Video Quality
- What Shielded Cable Looks Like Compared To UTP
- Physical Differences Between Cable Types
- Other Names For STP
- Typical STP vs UTP Costs
- Use STP Against Common Sources of Interference
- Practical Use Is Limited, But Axis Disagrees

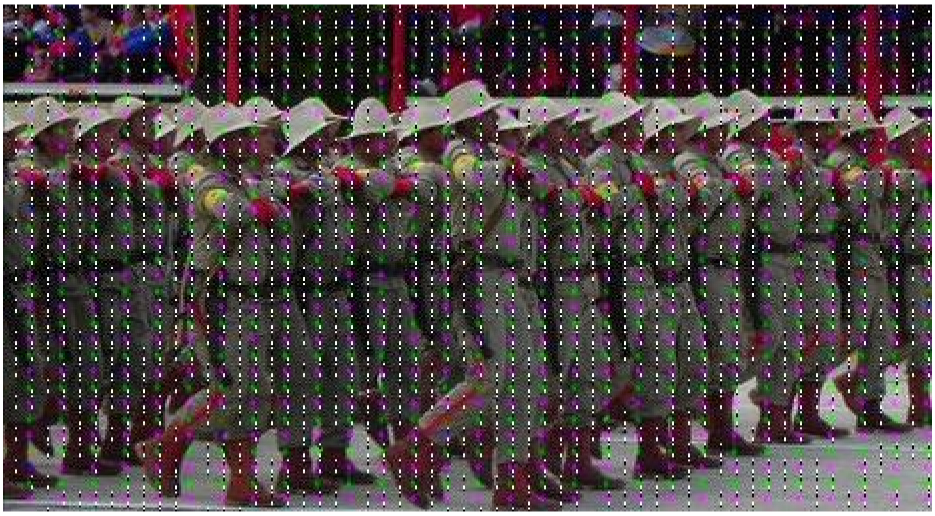
One Of Many Cable Tutorial Series

This tutorial is one of a number IPVM has addressing the topic of cabling. Others include: Cat 5e vs. Cat 6 for IP Cameras, Cabling Best Practices Guide, Network Cable Testing Guide, Grounding and Bonding for Video Surveillance, and more.

Electrical Interference Affects Video Quality

In the video surveillance world, the emphasis is often on cameras and NVRs, but little attention to the cabling in between. When video quality problems arise, it can be a frustrating exercise to swap camera and tweak settings, only to discover problems are still present.

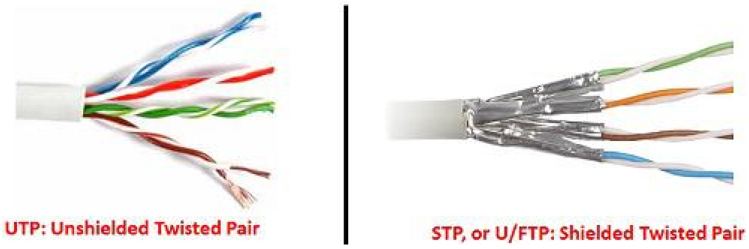
However, taking a hard look at cabling can resolve maddening issues. Take the example in the image below:



Electrical interference in the cabling itself cause this type of problem. Not only does the cable transmit intended data streams, but it also can attract and transmit unwelcome 'noise'. A jacketed cable can serve as an 'ad-hoc antenna' helps emphasize why cable shielding is sometimes critical.

'STP' Is Integrated Cable Shielding

A quick physical comparison between nonshielded UTP and STP, or 'shielded twisted pair' cabling reveals the primary differences. The image below shows the additional metallic foil shielding surrounding wire pairs in STP:


UTP: Unshielded Twisted Pair
STP, or U/FTP: Shielded Twisted Pair

'Shielding' should not be confused with 'cable screening' where a single layer or metallic foil or mesh covers the entire bundle of wires. While the decision to individually wrap pairs versus gross wrap the entire bundle shares some of the same benefits, they are not equivalent to one other and result in different performance.

Other Names For STP

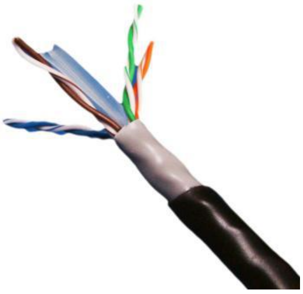
The common abbreviation for shielded twisted pair cable, 'STP', is sometimes called 'U/FTP' for 'Unscreened/Foil-shielded twisted pair' or 'S/FTP' for 'Shielded/Foil-screened twisted pair' instead. Especially for structured cabling specifications, some may use these alternate abbreviations to describe shielded cabling. However, in general use, the 'STP' abbreviation is most widely used.

Physical Differences Between Cable Types

The following list summarizes the tangible differences between UTP and STP.

- Metallic Foil Shield: A thin layer of foil, commonly aluminum, surrounds wire pairs. This layer is often called the 'drain', and must be properly terminated. Failure to adequately ground the drain can amplify the problems that STP attempts to mitigate.

- Thicker Jacket: The added layers of foil increase the weight add diameter to the cable bundle. As a result, a thicker plastic insulating jacket is needed, which adds rigidity. Overall, STP is heavier and thicker compared to UTP, and may be more difficult to install as a result.
- Cores, Pull Strips, and Groundwires: Depending on the exact manufacturer and brand of STP, other features may be present not commonly found in UTP cabling. This includes plastic divider 'core' sprues, strings to aid stripping the jacket, and additional electrical grounding wires. Below IS an outdoor rated cable with a center core that separates the pairs into quadrants within the jacket.



STP vs UTP Functional Differences

Those additional physical features provide STP with properties that UTP does not possess.

- EMI resistance: The primary advantage of shielding is protection from environmental electromagnetic interference, or EMI. Because each pair is individually wrapped, the ability for ambient interference to permeate and carry down the cable is significantly minimized or eliminated.
- Isolated line noise: Interference can be a 'two-way street' in that unshielded cabling is a source itself of interference. In some

applications, like sensitive medical imaging or manufacturing, normal ethernet cabling can be a uncontrolled conduit for interference that throws those instruments off. Again, the addition of pair shielding minimizes or eliminates this problem.

Cost Difference

Using STP adds between $20 to $40 per camera compared to UTP cabling, assuming cable runs of 150 feet, based on STP cable costs ~40% more than UTP and depending on how much additional labor or larger conduit is needed for the larger, heavier and more rigid STP.

Use STP Against Common Sources of Interference

Simply, STP should be used where interference could be a problem. To firm up where these places commonly are found, here are some places where interference could impact video quality:

Adjacent to High Voltage Wiring

Power wiring can interfere with data transmission when run adjacent to or too near each other. Even wiring run a compliant distance apart within a grounded raceway can be a source of video interference.

While no hard specification exists for when to use STP in this situation for video, best practices in data networking design follow that any data cabling sharing the same raceway, regardless of how it is contained in EMT or conduit, must be run using STP cable.

Near Inductive Devices

Data cabling run near common electromechanical features like electric motors, power transformers, magnetic coils, or solenoids can introduce significant EMI. Especially for industrial facilities, where these devices are common, shielding cable runs is an important protection.

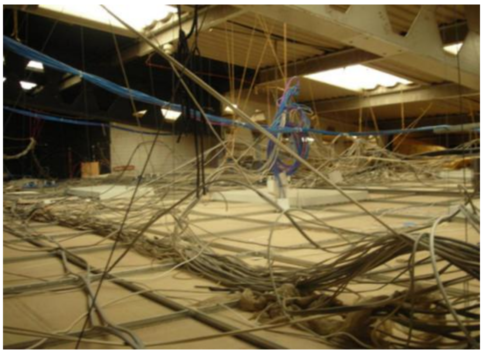
These sources are characterized by their 'inductive' properties, or their reliance on magnetic fields for operation. Cable proximity to devices like HVAC equipment, ventilation fans, door maglocks, electrical switchgear, and industrial machinery can generate enough interference to degrade video quality.

GSM Devices/Walkie Talkies

Common low powered communication radios disrupt data transmission. While a token handset may not be significant enough to be a problem, locating data runs near high powered repeaters or transmitters should be run using STP to eliminate problems.

Fluorescent Light Fixtures

One of the biggest sources of EMI are common light fixtures. Given the common occurrence of ethernet cables running overhead of these fixtures, if cabling cannot be run in formal cable trays on Conduit, it should be run using STP cable.



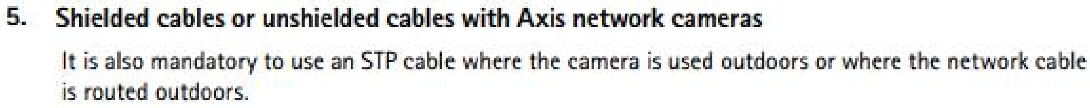
Even worse, there are many occasions where ethernet 'installed by others' is to be used for video. In many cases, cabling previously installed is the source of video quality problems that remain unfixed until the cable network is corrected.

Practical Use Is Limited

In our experience, the vast majority of all surveillance ethernet cabling has been run using UTP, and we have no significant issues to report. Since specifying networks with the appropriate shield is imperatively acknowledged in datacenter and networking design "best practices", it is generally suitable for video network design.

Axis: Mandatory STP Use Outdoors

Industry giant Axis Communications declared use of STP mandatory for outdoor cameras per the following whitepaper:



5. **Shielded cables or unshielded cables with Axis network cameras**

   It is also mandatory to use an STP cable where the camera is used outdoors or where the network cable is routed outdoors.

"Our recommendation is to deploy an STP network cable in demanding electrical environments. Examples of demanding indoor environments are where the network cable is located in parallel with electrical mains supply cables or where large inductive loads such as motors or contractors are in close vicinity to the camera or its cable. **It is also mandatory** to use an STP cable where the camera is used outdoors or where the network cable is routed outdoors."

This is a bold statement given that ~40% of all cameras are installed outside. Observing Axis' recommendation may drive a significant increase in overall project cost and is likely overkill relative to common problems faced.

Rather, our experience disagrees with the generalized application of STP. The smartest use of STP is where ethernet is run in the 'high risk' areas identified above.

Network Connectors

Fewer installation tasks are as nuanced as terminating cables and attaching connectors. Fortunately, this task is easy to manage and get right if the proper components and tools are understood.

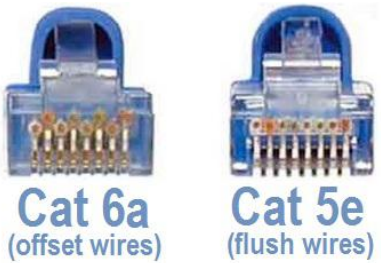
We explain:

- Connector Type vs Cable Type
- Single Piece vs Three Piece vs Connector Glands
- Tools Needed
- Cable Testing
- Termination Labor

Wire Size Impacts Connector Type

Physically connecting cameras to network cables is the job of the connector. For IP Cameras, this connection is done with RJ45 (sometimes called 8P8C) terminations. Regardless of the size of the raw cable used by the network, this connector must configure each of the component wires and twisted pairs for use in standard Ethernet jacks.

Because of wire size differences, the type of connector must match the network wire. Take a look at the image below:



While either connector will fit in an Ethernet port, the wires in a UTP bundle of Cat 6a are larger than those in Cat 5e. The difference in wire size (denoted by AWG or Gauge) can be seen evidenced by how the bigger Cat 6a wires must be offset or staggered inside the connector compared to the flush or straight orientation of the smaller Cat 5e conductors.

This difference is subtle, but critical because connector types must match the cable types they terminate. Cat 6a connectors should not be used to terminate Cat 5e cable because the fit and orientation of wires is critical to cable performance.

Single Piece Connectors

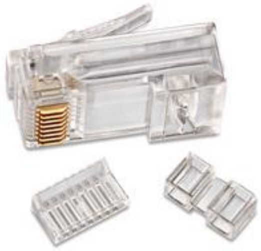
The most common and least expensive connector used is the single piece crimped style. Bare wires are inserted into the connector in a specific order so they contact individual pins at the end. After being fully inserted, a crimping tool is used to crimp the end of the connector, inserting the pins into the wires creating contact and a tight fit:

Single-piece Crimp (Cat 5e)

Because wire sizes are smaller with Cat 5e, these connectors are very common and inexpensive for use, costing about $0.05 - $0.10 each.

Three Piece Connectors

For larger wire sizes, especially Cat 6a, the exact orientation of staggered wires are important to maintain during cable termination. For this reason, extra pieces are needed to make the connector work. The basic idea of a single piece crimp connector is modified to include a 'liner' and a 'sled' that is used to precisely locate wires inside the crimp connector head:



3-piece Crimp (Cat 6a)

After the liner and sled is installed onto a cable end, the process of finishing a 3-piece connector is similar to a single piece style, where a special handtool crimps the body of the connector onto the cable bundle.

While less common and more difficult to install than a single piece connector, prices are still inexpensive costing about $0.20 - $0.40 each.

Compression Gland Connectors

A less common, but weather resistant and water-proof type of connector is often used for camera hung outside or in harsh environments. The exact installation process varies according to designs, but in general these multi-piece connector assemblies use special gaskets or glands for protecting internal wire connections and the overall termination piece.

This video demonstrates a compression gland connector used by Axis. Notice that while no special tools are required, the process for terminating a cable is ten or more steps that are very specific:

Note: ***Click here to watch the video on IPVM***

While pricing for compression gland connectors vary, they range from $5.00 to $25+ each.

Tools Needed

Terminating cables requires several specialized, but not expensive handtools. The main ones are:

- Jacket Stripper: This is a special blade that scores the outer jacket of the UTP bundle without cutting into individual pairs inside. This tool is needed to cleanly prepare the end of a cable for termination. These tools typically cost less than $15 each.

- Diagonal Cutters: This tool is used to trim individual wires to uniform length. In some cases, cutting bladed may be built-in to a Crimper or techs may prefer to use a knife. A pair of cutters sized for UTP wire typically cost about $10 - $15 each.
- Wire Strippers: Although some view this tool optional, a set of wire strippers for individually removing insulation jackets from wire pairs should be used instead of knives or cutters. While experienced techs may have 'a feel' for stripping jacket without damaging conductors, a wire stripper is designed to prevent damage. A set sized for low voltage wire sizes costs about $15 - $20 each.

- RJ45 Crimper: The handtool used to affix the connector to the end of the wire is most specialized and limited for general use for other jobs, but a hand crimper often combines several of the above tools and several different connector sizes into a multitool to keep toolbelts light. The crimper alone cost about $15 - $20, but specific connectors may require specific crimp tools.

These specialty tools are often assembled into kits available from low-voltage distributors and cost less than $50 for budget tools. However, unless attaching connectors is an infrequent task, technicians may find the quality and durability of premium kits valuable, with the cost of those reaching several hundred dollars which frequently add basic cable testers to the kit.

Cable Testing

A key aspect of creating cables and attaching connectors frequently overlooked is checking them for function. It is easy to create errors or incorrectly terminate connectors, and cable checkers are a quick way to verify work was done correctly.

The degree of checking can range from simple function checks all the way to detailed certification of wire runs, and testing units can range in price from $25 to $10,000+ depending on needed result. We cover this subject in detail in our Network Cable Testing Guide.

Termination Labor

The amount of time it takes to properly prepare and terminate a UTP cable is not long; someone who has done the process a few times can learn to complete the process in less than a minute (60 seconds) per termination, although factors like cable location, certification, and cable type can add several minutes to the typical quick process.

For example, if using STP or cable including a drainwire, installing the connector to maintain solid contact with that conductor usually slows the process down and may add 5 to 10 minutes to the normal termination process for checking continuity. And when weatherproof connectors are used, like the compression gland type mentioned above, the precise nature of installing cabling inside may add another 5 to 10 minutes per end.

Network Ports

Network ports are critical for remote video viewing and recording and without proper configuration, IP video will not work.

We examine:

- Why ports are used
- The format for ports
- How ports are assigned
- Well-Known ports for video surveillance
- Uncommon / manufacturer specific ports
- Risks of open ports
- Multiple port use for VMSes
- Using NMAP to scan ports

Why Ports Are Used

A computer will generally have a single IP address but will often communicate via different applications or services.

To accommodate this, IP addresses support multiple 'ports', up to 65,535. Ports (also called 'sockets') define particular channels for data to flow to points in a network, like from cameras to a recorder, or a recorder to a client. Ports help a computer know how to use the data it receives, so with any data streamed on a video port can be quickly processed for viewing, or emails can be received by an email client for reading, or web traffic by a browser and so on.

With the large range of ports available, significant portions of network traffic are assigned for specific use or specific applications, and this greatly speeds up the process of a computer's specific applications knowing which data applies and which data does not.

Port Format

The way particular ports are addressed is a variation of the IP address scheme. For example, an IPv4 address port is identified by adding a colon and port number at the end, like this (port index in bold):

192.168.0.223**:554**

When you visit a webpage, you might assume there is no port needed but that is only because web browsers handle that for you. For example, the IP address form IPVM.com is 192.34.63.49. Going to https://192.34.63.49and https://192.34.63.49:80 both take you to the IPVM homepage, it is just that the browser knows / assumes you mean port 80 when you type in "http://"

How are Ports Assigned?

Port numbers are assigned according to three groups, based on how general or how specific they are to general network applications.   All potential ports, from #0 to #65,535 are assigned accordingly:

- System Ports, from Port 0 - 1023: System Ports are assigned by IANAas standards per RFC6335. These are reserved for general, well-known uses.
- User Ports, from Port 1024 - 49151: User Ports are assigned by IANAper RFC6335. These are for specific software operation

use. Many surveillance and security platforms have port reservations in this group.

- Dynamic Ports, from Port 49152 - 65535: Dynamic Ports are not assigned. This block is essentially not administrated and kept open for general use, often for private or temporary assignments within a network. This is what surveillance manufacturers often use for their own internal communications between their servers/recorders and clients.

The group responsible for assigning port functions, Internet Assigned Numbers Authority (IANA), is part of the same oversight group that assigns IP Address allocations and a number of other 'root level' administrative IDs in modern internet and network use.

Well-Known Ports

When it comes to typical ports being used by surveillance, the most generally open and used ports are found in the 'System' group, including:

- Port 80: HTTP (Hypertext Transfer Protocol) for general websites and web traffic
- Port 21: FTP control for file transfer, including image files
- Port 22: SSH, or secure shell transfer for port forwarding and secure portal logins
- Port 23: Telnet, or unencrypted text communication, often used for 'command line control' of cameras and even servers.
- Port 443: Secure Socket Layer, or 'secured' HTTP traffic. Uncommonly used to secure video streams.
- Port 554: RTSP (Real Time Streaming Protocol) for video, used widely and a pre-requisite for ONVIF streams

There are many well-know ports, though most are not relevant to surveillance applications. See a full list of 'well-known' ports here.

Uncommon / Manufacturer Specific Ports for Video Surveillance

However, many surveillance systems use port assignments that are specifically reserved for their use. Some of these reservations include:

- Port 2804: March Networks Digital Video Recorders and Enterprise Service Manager
- Port 22609: Exacqvision video client
- Port 37777/78: Dahua video forwarding port
- Port 38880: Avigilon ACC video client
- Port 49152: UPnP device discovery protocol

Port Security Risk

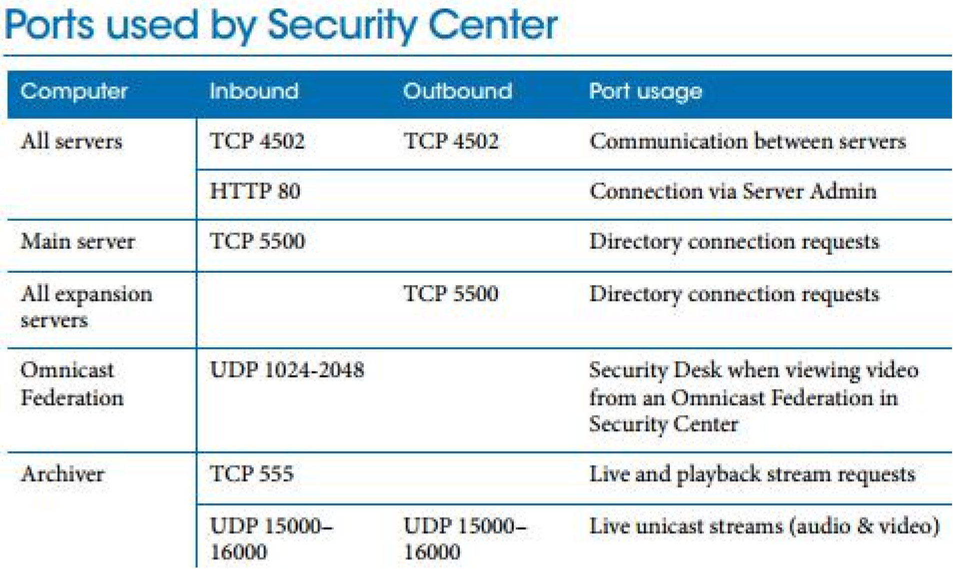
In many cases, surveillance platforms will use 'uncommon' user or dynamic ports that must be approved to pass traffic through security firewalls for use.   If these port assignments are not known and approved, video surveillance systems will not work.

Best security practices for networks often require blocking traffic all ports but those explicitly allowed for recognized use. In general, part of 'locking down' a network includes turning off ports in firewalls regardless of which IP address the originate from. This mitigates the risk of harmful viruses or other exploits from sliding through into a network.

This cyber security report shows the default ports that open on cameras from ten manufacturers.

Multiple Port Use Common

Surveillance systems generally use multiple ports during operation. Despite a camera or a recorder having just one IP address, that single resource may have many different ports collecting or sending data.   In general, opening up the requisite ports needed by the surveillance system is part of the initial configuration process, with VMSes typically publishing a list of needed ports like this one from Genetec.



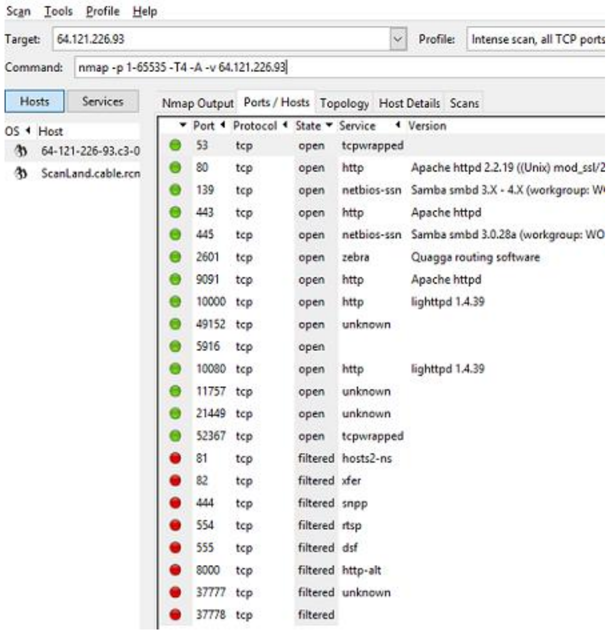
Ports used by Security Center

Computer	Inbound	Outbound	Port usage
All servers	TCP 4502	TCP 4502	Communication between servers
	HTTP 80		Connection via Server Admin
Main server	TCP 5500		Directory connection requests
All expansion servers		TCP 5500	Directory connection requests
Omnicast Federation	UDP 1024-2048		Security Desk when viewing video from an Omnicast Federation in Security Center
Archiver	TCP 555		Live and playback stream requests
	UDP 15000–16000	UDP 15000–16000	Live unicast streams (audio & video)

NMAP Port Scanning Tools

Because surveillance systems can open many ports, minimizing the group to just those that are needed is a key network security step.

Especially given recent hacking exploits taking advantage of ports opened by surveillance systems, tools like NMAP can be used to find what ports must be opened and which ports can be closed by turning off unneeded or unused features like UPnP, Telnet, and FTP. Below we provide a screenshot of an NMAP scan.



Target: 64.121.226.93

Profile: Intense scan, all TCP ports

Command: nmap -p 1-65535 -T4 -A -v 64.121.226.93

OS	Host
	64-121-226-93.c3-0
	ScanLand.cable.rcn

	Port	Protocol	State	Service	Version
🟢	53	tcp	open	tcpwrapped	
🟢	80	tcp	open	http	Apache httpd 2.2.19 ((Unix) mod_ssl/2
🟢	139	tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: W
🟢	443	tcp	open	http	Apache httpd
🟢	445	tcp	open	netbios-ssn	Samba smbd 3.0.28a (workgroup: WO
🟢	2601	tcp	open	zebra	Quagga routing software
🟢	9091	tcp	open	http	Apache httpd
🟢	10000	tcp	open	http	lighttpd 1.4.39
🟢	49152	tcp	open	unknown	
🟢	5916	tcp	open		
🟢	10080	tcp	open	http	lighttpd 1.4.39
🟢	11757	tcp	open	unknown	
🟢	21449	tcp	open	unknown	
🟢	52367	tcp	open	tcpwrapped	
🔴	81	tcp	filtered	hosts2-ns	
🔴	82	tcp	filtered	xfer	
🔴	444	tcp	filtered	snpp	
🔴	554	tcp	filtered	rtsp	
🔴	555	tcp	filtered	dsf	
🔴	8000	tcp	filtered	http-alt	
🔴	37777	tcp	filtered	unknown	
🔴	37778	tcp	filtered		

For more details on how NMAP can identify and help minimize open port security risks, see our: NMAPing IP Cameras note.

Cabling Best Practices

Surveillance cabling can be a huge problem. Poorly installed and maintained networks are often costly, lengthy, frustrating ordeals to manage.

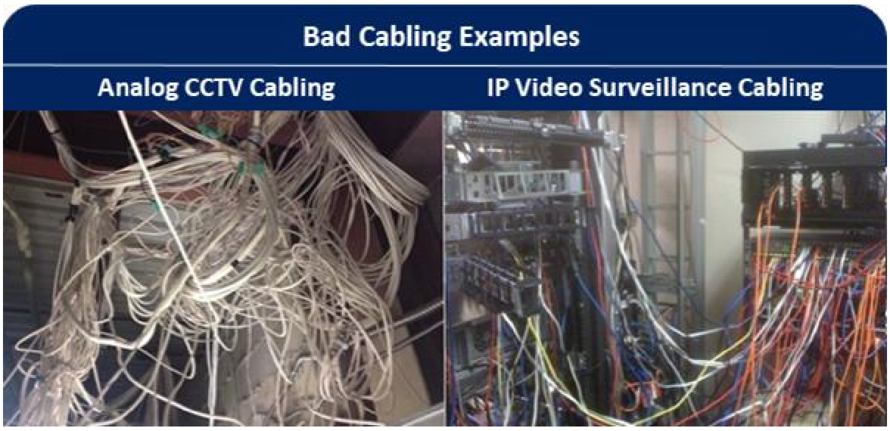
While keeping cables organized is not an advanced topic to understand and practice, in this note we address a few basic rules can go far in preventing "cabling nightmares."

We explain:

- Real Life Examples
- The 5 'Best Practices' That Make A Difference
- Cabling Specifications

Real-Life Examples

Just about every integrator and installer has example stories to share of video surveillance networks that are a mess. In the snapshots below, we share some member photos depicting just these 'nightmare networks':



Top 5 Tips

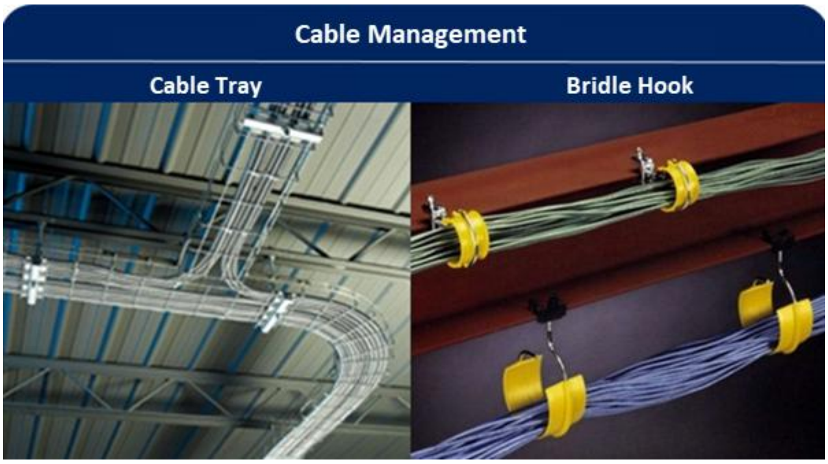
Here are our top 5 tips:

1. *Label All Cables*

One of the most costly oversights when running cable is neglecting labels. As we previously covered in our Cable Labeling Best Practices report, we address how a few minutes of labor in labeling can save thousands of dollars in troubleshooting time later. Having the ability to quickly determine the specific cable a camera is using and where it is connected in a switch make quick work sorting through big bundles of cable looking for one specific cable.

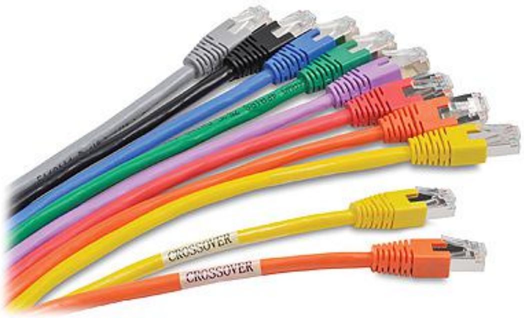
2. *Use Cable Trays/Hooks/Tubing*

Loose cabling above drop ceilings or along trusses have a way of becoming hopeless tangled messes over time. When ceiling tiles get popped or moved, the cables run atop get displaced. Even after substantial reworking and re-stringing of cable, the system had problems with camera outages and unlabeled cable runs. The images below show examples of trays and hooks in use:



3. *Jacket Color is Important*

Using a specific color to denote cables belong to a certain system can be important. In Example 2 above, many colors are used but in a random fashion. Staying with a color scheme, even when not required by an overarching standard, will help eliminate 'monochromatic confusion' of lumping multiple data networks or low-voltage systems together.

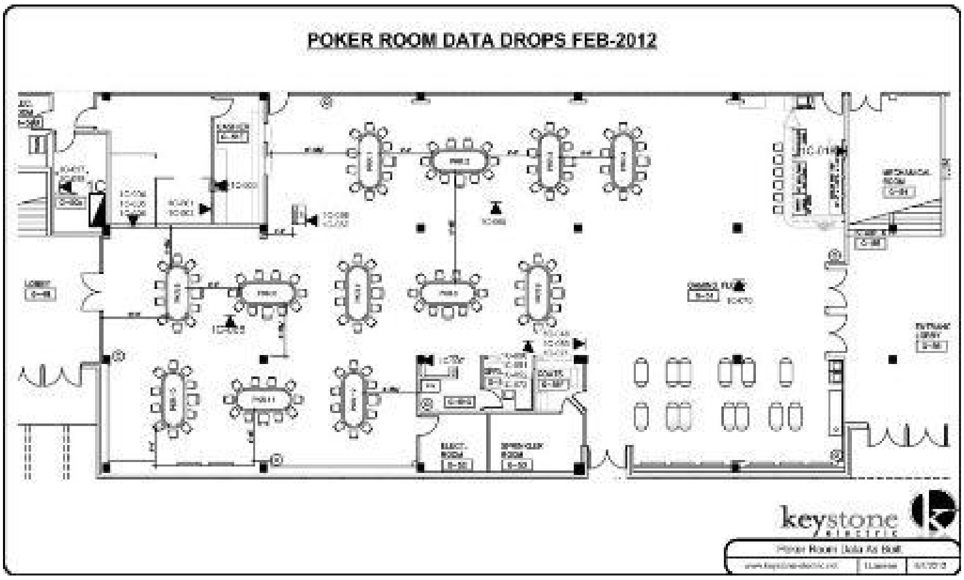


Because 'blue' and 'gray' jacketed cables are the most common datacomm colors, and 'red' is reserved for fire system applications, the best 'standard stock' colors for video surveillance available at most distributors are greens, yellows, purples, and oranges. However many non-standard color options are available to choose from, and are only limited by order lead time and extra cost.

4. *Draw a Map*

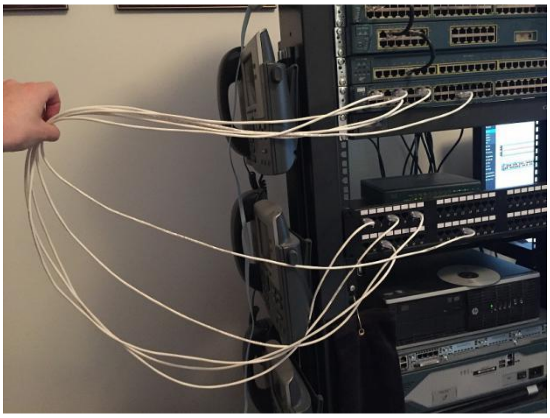
Not only is drawing a map of cable runs and drops invaluable reference for surveillance maintenance, it also can be referenced by other projects that might disturb cabling. If the function of cabling is unknown, it can easily been seen as 'not critical' or even 'out of service'. However, a map of each run and it's scaled location on a floor plan makes it easy to locate and readily identifiable as part of a critical system. Ensuring that the information is accurate is vital when planning work, and every time work is performed that changes the location or index of cabling, the map must be updated.

For those performing in-depth or high volumes of design/installation cabling work, AutoCAD is the ideal platform to produce these maps (see our '[AutoCAD for Surveillance]' report), as they can easily be incorporated into official print sets. However, for incidental and occasional map drawing, a program like Visio (see our '[Visio for Surveillance]' report) is easier to navigate and use.



5. *Don't Use Excessive Service Loops*

One of the most common, and needlessly messy, habits of integrators is to pay out excessive amounts of cable or use significantly over-length patch cords as 'service loops' at the end of cable runs. Service loops should contain a few feet of extra cabling to cover the inevitable camera shift or network rack movement. However, coiling up twenty or fifty feet at the end of runs, or using 10' path cords when 3' is all that is needed 'just in case' needlessly drives cost and creates clutter.



For service loops, BICSI standards state 3m at the rack and 1m at the outlet or device, recommended where practicable, and excessive loops are discouraged.

The performance impact of line interference and improper bend radii encouraged by lengthy service loops can negate any potential benefit the extra cable may provide in the future. Using 'long enough' loops reduces the amount of cable to troubleshoot, hang neatly in small spaces, and keep organized.

Specifications

While no 'universal' code or spec exists for running cable, BICSI has published a number of 'best practice' guides for design and installation. Frequently, when installation specifications are mentioned in a bid or scope of work, a BICSI publication number is given. These documents define how installation work is to be executed,and almost universally recommend the 5 tips above as part of a network project. Among the commonly cited specs are:

- NECA/BICSI 607-2011, Standard for Telecommunications Bonding and Grounding Planning and Installation Methods for Commercial Buildings
- BICSI 002-2011, Data Center Design and Implementation Best Practices
- ANSI/BICSI 001-2009, Information Transport Systems Design Standard for K-12 Educational Institutions
- ANSI/NECA/BICSI 568-2006, Standard for Installing Commercial Building Telecommunications Cabling
- Electronic Safety and Security Design Reference Manual (ESSDRM)
- Telecommunications Distribution Methods Manual (TDMM)

Even if projects do not explicitly state work must conform to one or more of the spec guides, it is in the installer's best interest to take the guidelines to heart in order to keep the 'nightmares' at bay.

Direct Attached vs Jack & Patch

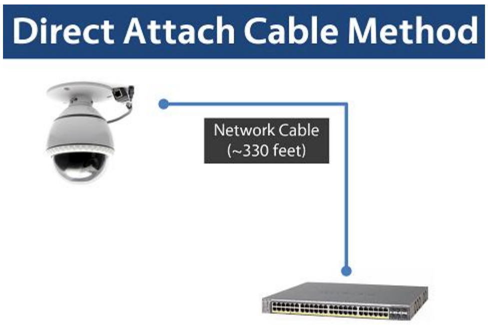
An ongoing debate rages about how the IP camera cables should be terminated.

This argument surrounds two common options:

- 'Direct Attached', where the first terminates the field cabling with an RJ45 modular plug, and connects it directly to the camera.
- 'Jack & Patch': where the cables are first terminated to a jack or patch panel, and then connected to security devices by patch cord.

The Two Methods

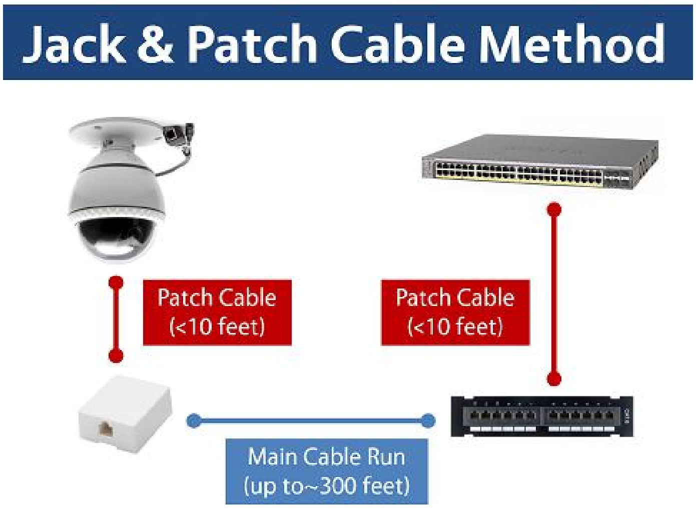
Direct Attach Method: The most common method of attaching devices to a network is simply plugging each terminated end into a device. Cables are run directly to a switch and to a camera or controller in the field, using an RJ45 modular plug at both ends of the cable. Testing is performed from these plugs across the length of the single cable.



However, many cite a second more permanent method is better despite being more complex:

Jack and Patch Approach: According to the 12th Edition of BICSI's TDMM and prior, all horizontal cabling should be terminated in the closet end on a patch panel, and in the field, on a jack. Starting in later editions, this requirement was relaxed for security equipment and other installations where accessibility may be difficult or tampering may be a risk.

Connections are made from the patch panel to switch, and from the jack to device with patch cords. The resulting section of cable from patch panel to jack is called the 'permanent link'. Typically jacks are installed in a wallplate for interior cameras, and patch from the plate to the camera. In exterior applications, jacks are commonly mounted in junction boxes.



The Heart Of The Debate

The major issue driving this debate is the 'modified permanent link' which modular plugs create. Since cables are specified by standards to be terminated in the typical link fashion, testers were created to test the normal permanent link, resulting in not-quite-accurate tests when testing through a modular plug. How inaccurate these results are is debatable, and in practical terms, negligible.

Building automation systems have used the direct attach method for years, as it was recognized by TIA standards that in some cases a jack and patch cable are impractical or unserviceable. Current Editions of BICSI's Electronic Safety and Security design reference have come to the same conclusion.

However, it should be noted that security applications break other fundamental rules of BISCI standards, such as each outlet being mounted 18" above finished floor with two cables run to it. Security devices, just like BAS devices, are application-specific, and different standards apply while respecting original intent where possible.

Which Method Should I Use?

While, practically speaking, there is nothing wrong with either of these methods, and much is left up to preference, directly attaching plugs is generally preferred by the majority of integrators. There are two main drawbacks which may be a problem when using this method:

- Cable flexibility: In UTP cable used for horizontal runs, each of the eight conductors (four pairs) is made from a solid copper conductor. In patch cables, each conductor is made up of multiple thin copper strands. This makes the conductor, and in turn, the entire cable, more flexible. For this reason, patch cables may be able to fit into tight domes where sharp bends are without straining or pinching the cable where solid conductor cable would have issues. Strictly speaking, however, according to standards, bend radius is four times the diameter of the cable, regardless of solid or stranded construction.
- Modular plug construction: While Cat 5e cable is almost always 24 AWG, some manufacturers of Cat 6 and higher cables have sized

conductors up to 23 AWG. Care should be taken when selecting cable/modular plug combinations, to make sure the plug will handle larger-gauge wire, or it may not work properly, or simply not at all.

Users should be aware of challenges in specific applications, as well:

- Interior cameras: When installing interior cameras, the key consideration is where the camera will be mounted. If the cameras are to be wall-mounted, or in the case of warehouse or other open-ceiling environments, installing jacks is simple, either in a surface-mount or recessed box with wallplate. When using ceiling-mounted domes, however, installation is trickier. As discussed in our installation issues update, exposed connections are not allowed by code above drop ceilings. This means that, unless the dome has room enough to install a jack inside it (which is unlikely), a junction box must be provided to house the connections, making the direct attach method much simpler.
- Exterior cameras: Using jacks in exterior locations can be much trickier than their interior counterparts. If using box cameras, a jack may be located in the housing. However, exterior domes are as unlikely as their interior counterparts to have enough space to locate a jack and patch cable. If an enclosure is provided, for surge protection, wireless equipment, or other needs, the jack may be located there. In most cases, however, the direct attach method will be simpler.

No matter which method is used, care must be taken during installation. Maximum cable pulling tension and not exceeding bend radii should be observed. All components should be Cat 5e or Cat 6 rated, including mod plug and patch cables. If all of these are followed, connections should experience few issues.

Cable Installation

BICSI

Spend enough time around networks and eventually someone will mention BICSI, the oft-referenced but only vaguely known standards body prevalent in the IT world. The question is: how do BICSI and their guidelines practically affect your surveillance installation? We look at this question, key things to know, and other areas they cover.

Specifically, we explain:

- The TDMM
- The RCDD Credential
- Standards vs. Codes
- Modular Plugs
- Terminating to Patch Panel
- Testing Cables
- Cable Labeling
- Cable Supports
- Firestops
- Telecommunications Rooms
- Grounding / Bonding
- Power Distribution

BICSI Overview

BICSI (Building Industry Consulting Service International) is a standards-making body focused on IT and related industries, such as life safety, security, audio-visual, and more. They are best known for publishing two manuals which effectively serve as the de facto standards of the cabling industry:

- Telecommunications Distributation Methods Manual (TDMM)): This publication covers design and planning of network systems, covering cabling, bonding/grounding systems, cable supports, equipment room planning, space calculations, and more. It also forms the basis of the Registered Communications Distribution Designer (RCDD) credential. The TDMM is a huge amount of material, with the 13th edition over 2100 pages, with most of it irrelevant to surveillance.
- Information Technology Systems Installation Methods Manual (ITSIMM): The ITS installation manual focuses on actual installation issues, such as how cable should be terminated and supported, firestopping methods, planning cable paths and spaces, etc. This manual is used as the study material for BICSI's certified installer program.

BICSI publishes other manuals, as well, covering electronic safety and security, data centers, project management, and more, but they are generally not utilized as much as the above.

These manuals are not cheap. BICSI sells the TDMM for $365 USD ($295 for members) online. The ITSIMM is less expansive, but still $205 ($185 member).

The RCDD Credential

The RCDD is BICSI's design credential, generally pursued by those actively doing design and engineering of network infrastructure on a regular (if not daily) basis. Because it uses the TDMM as its reference material, it is a lot of material to know (over 2100 pages), with work experience requirements and references required, and a closed book proctored exam.

For the vast majority of designers in the security industry, the RCDD is unnecessary. Most of the material covered is general to cabling and other infrastructure and not regularly used.

BICSI's Electronic Safety and Security credential was their only credential relevant to security, but was not really respected or required, with few outside of the BICSI set even aware of its existence. BICSI retired the credential at the end of 2015.

Standards, Not Codes

Note that unlike NFPA or IEC, BICSI publishes standards, not codes. This means that while the material they contain is often viewed as best practice, building inspectors and other code officials do not require systems to be installed to standards, and do not issue fines for breaking standards.

The most common area BICSI standards are used is in large construction projects, where the TDMM covers most of Division 27 of the CSI spec. While security is contained in Division 28, cables installed for it must be in accordance with 27. These projects are typically (but not always) bid projects, with telecom just one part of a much larger project.

Outside of construction, IT departments in large facilities (corporate, campus, government, etc.) are typically most concerned with BICSI standards as they have much more network infrastructure to install and maintain than smaller facilities. Adherence to standards (especially testing, supports, labeling, etc.) helps to ease upkeep and keep ceilings and equipment rooms neater. Since multiple contractors are typical in these facilities, installing multiple systems over the course of years may quickly lead to confusion as to what cable is used for what, where it goes, etc.

Key Areas

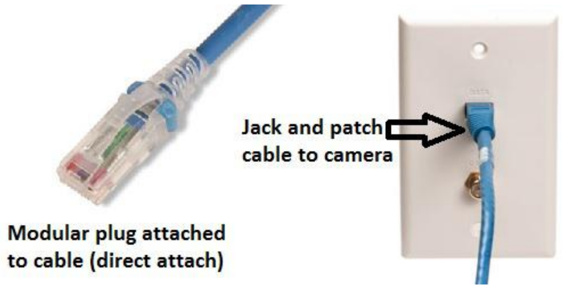
Cables installed for surveillance or access control generally make up only a small percentage of the overall project, and are often added separately (if not as an afterthought). However, surveillance professionals should know enough to properly install cables so they follow the same standards as the rest of the facility. Even in buildings where the owner is not concerned with standards, installing cables properly may decrease installation and troubleshooting time, and provide a more professional appearance.

Below are some key points relevant to surveillance from the TDMM and ITSIMM:

Modular Plugs Are OK

One of the biggest debates in the BICSI crowd in recent years was whether connecting a cable to a camera with a modular plug (instead of a jack and patch cord) was acceptable. This practice was technically against standards, which required a permanent link (the section of cable installed in the walls/ceiling of a building) to terminate in a jack at both ends, and be connected to equipment via patch cords. Partly this was for testing purposes, as cable certification equipment was calibrated to use test cords which required jacks be installed.

However, in the past 2-3 years, driven by the ESS standard, BICSI has approved the use of modular plugs, referred to as the "direct attach" method, creating a "modified permanent link", with the patch panel side terminating to a jack, but the device end terminated with a plug.



Current testers have included different adapters to account for this change. Note that installers must be careful to use category (5e/6, etc.) rated mod plugs when using this method. While terminating to a modular plug is acceptable at the device end, cables are required to be terminated to a patch panel at the head end. They may not be terminated with a plug and connected directly to a switch, a common practice in many small surveillance deployments.

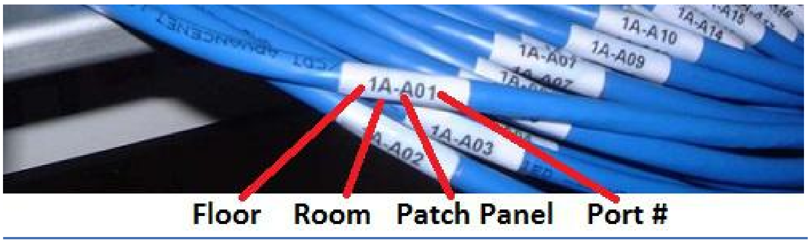
For more on this debate, see our: IP Camera - Direct Attached vs Jack & Patch note.

Cable Testing

In most cases, security integrators do not certify and document every cable they install. However, by BICSI standards, this is required. A record of each cable's test performance (wiremap, crosstalk, etc.) is recorded by the tester and kept for verification, typically electronically. Aside from standards, test records are also usually required by cable/component manufacturer warranty.

Labeling

When adding cables to a standards-compliant installation, security installers should follow the labeling scheme in place. Typically this includes identifiers for which room, rack, patch panel, and port a cable terminates in. Labeling is a big topic in BICSI design, with its own standards, and these schemes can be fairly complex.



Cable Supports

Standards specify that cables should be supported every 48-60 inches or installed in cable tray or conduit. Technically, cable is to be pulled, then placed into supports (lifted onto tray or into J-hooks), but this is rarely done in practice as ceiling obstructions make it impractical.

Maintain Firestopping

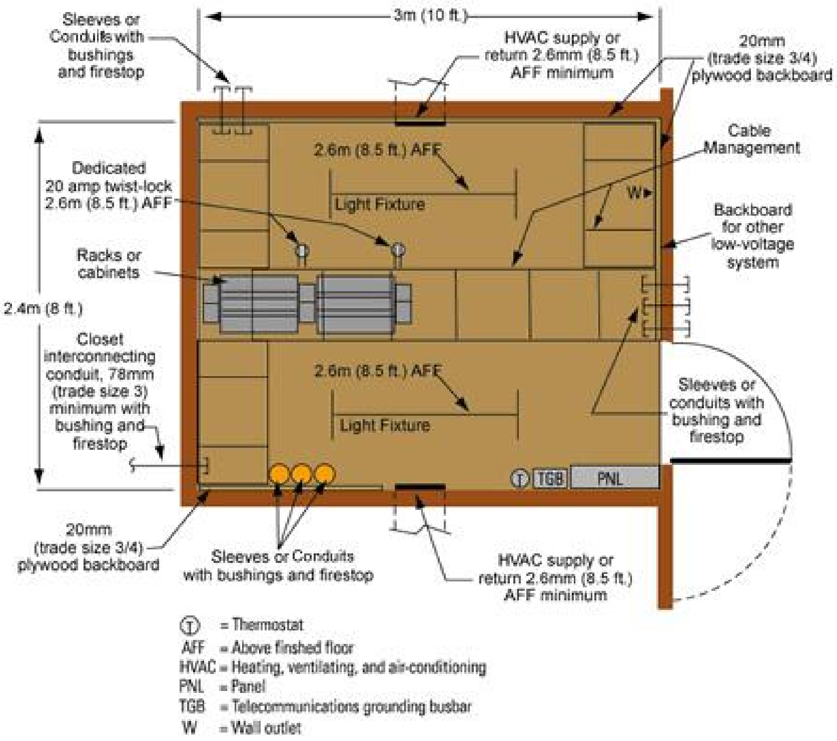
When adding cables to an existing (or new) installation, users should be careful to repair any firestopped pathways they may have disturbed, or apply firestop to new ones created. Readers may see our Cabling Through Firewalls guide for full information on methods.

Other Areas Covered

Aside from the practical areas above, the TDMM covers many infrastructure topics which may be of interest to some, but most installers and designers do not need to know by rote, including:

Telecommunications Rooms

The TDMM provides an entire chapter of guidelines for how telecommunications rooms (TCs, IDFs, MDFs, ERs, etc.) should be located, sized, and laid out. This chapter may be of interest to security designers as space for equipment may not be considered by the original designer, whether it requires rack space, such as servers or NVRs, or especially wall-mounted access control or intrusion detection equipment or power supplies.


Sleeves or Conduits with bushings and firestop
3m (10 ft.)
HVAC supply or return 2.6mm (8.5 ft.) AFF minimum
20mm (trade size 3/4) plywood backboard
Cable Management
2.6m (8.5 ft.) AFF
Light Fixture
W
Dedicated 20 amp twist-lock 2.6m (8.5 ft.) AFF
Backboard for other low-voltage system
Racks or cabinets
2.4m (8 ft.)
Closet interconnecting conduit, 78mm (trade size 3) minimum with bushing and firestop
2.6m (8.5 ft.) AFF
Light Fixture
Sleeves or conduits with bushing and firestop
TGB
PNL
20mm (trade size 3/4) plywood backboard
Sleeves or Conduits with bushings and firestop
HVAC supply or return 2.6mm (8.5 ft.) AFF minimum
T = Thermostat
AFF = Above finshed floor
HVAC = Heating, ventilating, and air-conditioning
PNL = Panel
TGB = Telecommunications grounding busbar
W = Wall outlet

Grounding/Bonding

The TDMM specifies the use of a dedicated telecommunications grounding/bonding infrastructure, consisting of a dedicated grounding backbone run to each telecommunications room, terminated to a grounding busbar (TGB). Equipment and racks are then connected to this busbar for proper ground. Security equipment requiring a ground (often needed in access control for proper operation) should connect to this busbar.

Power Distribution

Finally, another chapter covers power distribution, including power conditioning and protection, as well as UPS systems. It does not specifically warrant the use of either protection or UPS systems, but gives guidelines on selection and sizing. If security servers and equipment are being added to an existing UPS or power system, designers should consult with the owner, and be careful new equipment does not overload existing circuits or reduce backup power capacity.

Cable Strapping

Many say using zip ties is asking for problems. And BICSI prohibits them. But many video surveillance integrators use them regularly. What should you do?

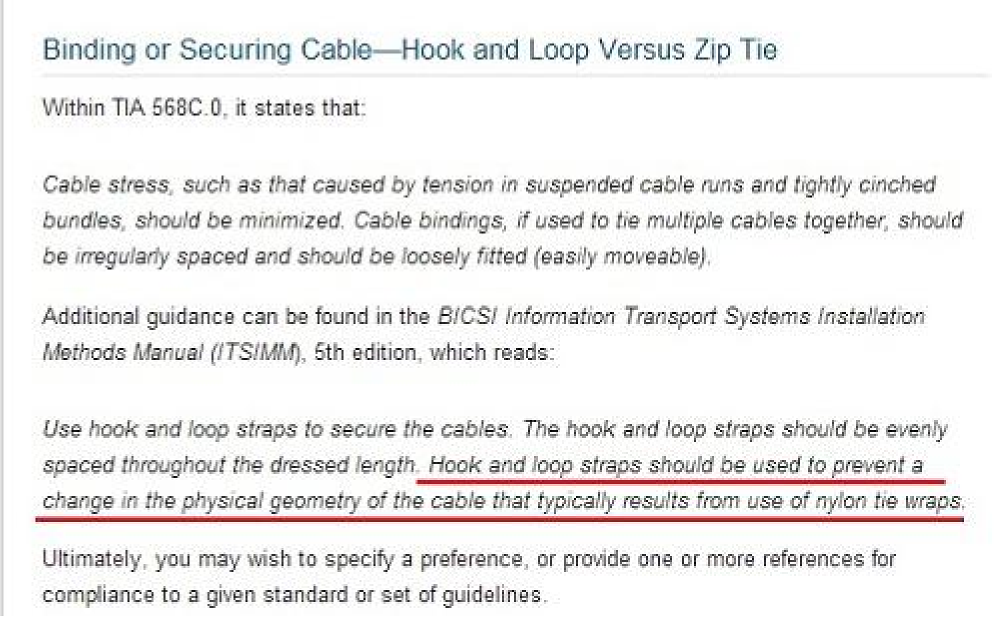
We contrast and explain the tradeoffs between:

- Zip ties (often Nylon)
- Hook and Loop Straps (also called Velcro)
- Cable Lacing (Typically Waxed String)

Zipties Are Bad: Myth or Fact?

Cabling standards authority BICSI takes a strong stance on the matter, essentially forbidding zipties and recommends Hook and Loop Straps instead.

From the BICSI Information Transport Systems Installation Methods Manual (ITSIMM):



Binding or Securing Cable—Hook and Loop Versus Zip Tie

Within TIA 568C.0, it states that:

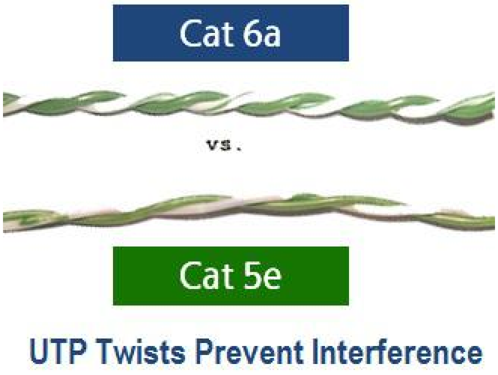
Cable stress, such as that caused by tension in suspended cable runs and tightly cinched bundles, should be minimized. Cable bindings, if used to tie multiple cables together, should be irregularly spaced and should be loosely fitted (easily moveable).

Additional guidance can be found in the *BICSI Information Transport Systems Installation Methods Manual (ITSIMM)*, 5th edition, which reads:

Use hook and loop straps to secure the cables. The hook and loop straps should be evenly spaced throughout the dressed length. Hook and loop straps should be used to prevent a change in the physical geometry of the cable that typically results from use of nylon tie wraps.

Ultimately, you may wish to specify a preference, or provide one or more references for compliance to a given standard or set of guidelines.

To understand the potential risk to video, the fact that network Category cable types are composed of twisted conductor pairs is important:



In order to preserve the best possible video signal, the internal twists must not be bent or kinked out of shape and alignment. The 'ziptie risk' is that overly tight ratcheted straps will physically displace conductors and create an interference point and potentially be disastrous for performance -sensitive IP video traffic.

But Is This A Practical Issue?

Despite BICSI's stance against zipties, examples of problems in using them are uncommon. Indeed, professional data centers with hundreds of server racks use them and claim they are not a source of performance problems:

Note: Click here to view the video on IPVM

Proponents of zipties claim that as long as the strap is not tightly ratcheted to the cable jacket, but installed with only light contact between the strap and cable the delicate twists of category cable will not be disturbed.

However, it is worth pointing out that reusing zipties is frequently not possible and they must be cut for removal during cable moves, adds, or changes. Other cable management products like Hook and Loop Straps can be reused, can be detached quickly, and make deformation of the secured cable difficult.

Zipties Examined

The most maligned method is also the least expensive and requires no special training or tools to use, although clipping ties so that no sharp 'alligator teeth' remain is necessary to prevent deep scratches or lacerations from future arms brushing against them. Bulk packs of zipties are available such they cost less than $0.02 each, in variable lengths, and variable base materials rated for harsh or hazardous environments.

In general, Zipties are single-use fasteners only because removing them often requires destroying them. However, due to their great strength and ratcheting design, they hold bundles of cables tightly for decades with no need for maintenance.

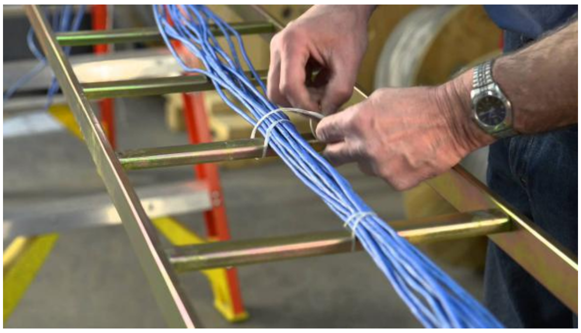
Hook and Loop Straps Examined

The cable strapping method BICSI recommends are softer fabric strips of Velcro, or generically "Hook and Loop' material. Because of widespread adoption in cabling, many options and lengths of these straps are available. However, the typical cost of these straps are higher, often costing $0.10 or more each.

Another potential issue with these straps in they can work loose over time, especially when exposed to harsh environments. This can mean that periodic tightening in difficult environments may be required.

Cable Lacing Examined

While replaced by more modern strapping methods, technique and trade skill intensive cable lacing is sometimes still seen or used in environments using great numbers of cables. Other environments subject to continual motion or harsh environment swings like ships or offshore oil platforms employ this method because of high dependability and inert waxed cord strapping.



While the cost of a spool of lacing tape/cord is low (1000 feet for ~$30), the cost of installing it in a neat fashion with tight knotting can take years of practice to perfect. Novices are not likely able to install Cable Lacing to professional standards without training and experience, and the overhead required accounts for its relative lack of widespread use.

Cable Testing

Proper cable installation is key to trouble-free surveillance systems.

However, testing is often an afterthought, with problems only discovered when cameras have problems, resulting in increased troubleshooting, or even worse, reinstallation. Simple, inexpensive testers are available, which can easily prevent these issues without adding substantial install time.

We examine:

- Wiremapping
- Cable Identification
- Service Detection
- PoE Detection
- Crosstalk
- Propagation Delay
- Cable Verifiers
- Cable Qualifiers
- Cable Certifiers
- Choosing Between Verifiers, Qualifiers and Certifiers

The Three Main Test Tool Types

Verifiers, Qualifiers and certifiers and the 3 main test tool types to select from:

- Certifiers are the only of the three to test to EIA/TIA568B standards, which ensures manufacturer warranty and essentially guarantees link performance. Main downside is high price of ~$10,000, 4 to 5x of a qualifier.

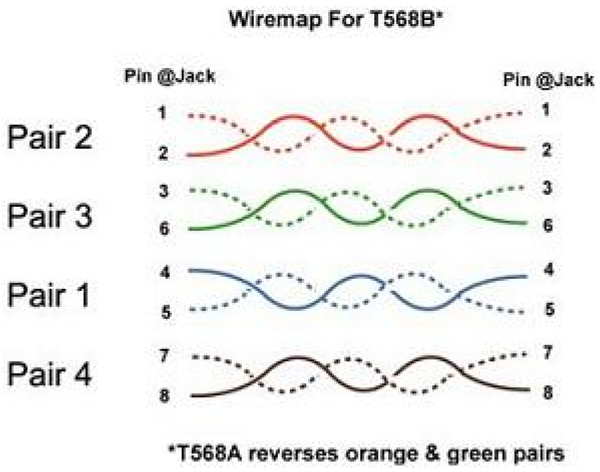
- Qualifiers deliver a detailed technical test but is not standards-compliant, aiming primarily to give a 'real world' test at a lower price than certifiers.
- Verifiers provide only basic cable testing that misses issues such as crosstalk, loss, and skew. Their main upside is that the testers are, by far the cheapest, at only a few hundred dollars.

Cable Verifiers

Cable verifiers perform the most common tests needed to ensure basic cable performance, though exact features and functions vary by manufacturer. Verifiers consist of the handheld test unit itself, and one or more remote units, plugged into the far end of the cable to be tested. Some also allow testing of coax cables via F connector.

The most common features of verifiers are:

- Wiremap: Wiremap determines whether UTP is terminated correctly, with the correct pairs in the right place on the connector, typically to EIA/TIA 568A/B. This may be displayed graphically, via LEDs or numbers. Graphical wiremap is much simpler to use for the inexperienced, as it displays exactly which pins are the issue, and how they are crossed. In the



case of coax cables, it simply shows whether there are any shorts between shield and center conductor.

- Length/distance to fault: The verifier determines the length of cable so installers may be sure UTP does not exceed 100m. This function also shows the distance to cable faults, such as breaks and shorts, so repairs can be made more easily.
- Cable identification: Each remote unit has a unique identifier, so that users may connect to multiple cables or jacks at once, and use the handheld unit to locate each. This can speed troubleshooting if cables are existing or mislabeled, instead of having to check a single cable at a time.
- Service detection: Many modern verifiers can detect the use of Ethernet, PoE, or POTS telephony on a cable, and which pairs are used. While this does not verify proper operation, it does show whether a cable is plugged into a switch or cross-connected to a phone line.

Verifiers generally do not save and store test results, a feature commonly found in qualifiers and certifiers, though some exceptions are available, such as the ByteBrothers RWC1000K.

This video below reviews the use of a typical verifier.

Note: ***Click here to view the video on IPVM***

Product Options

Cable verifiers range in price from about $125-450 USD, with cost generally driven by graphic vs. LED display, size, and number of functions.

Lower cost models such as the Ideal VDV II (~$125 online) provide a smaller display and numeric indication of wiremap compared to the graphical display in more expensive models. More fully featured options such as the Fluke MicroScanner (~$450 online) and ByteBrothers RWC1000K (~$400), offer a larger graphical wiremap display, or the ability to save test results.

Verifiers can easily pay for themselves the first time they are used for a trouble ticket.   They are able to report line breaks and the distance from the verifier, saving time on discovery / troubleshooting.

Qualifiers

Qualifiers add some additional functions, but are not precisely calibrated and testing to standards, making them the middle ground between verifiers and certifiers.

The models typically include the wiremap, length, identification and service detection of verifiers, but add functions such as:

- Service testing: Instead of simply detecting Ethernet service on a cable, qualifiers runs simple tests to check cable bandwidth and basic issues and determine whether it will support 10/100, GbE, etc. These tests typically include crosstalk, though not to the level a certifier tests.
- PoE testing: Instead of simply indicating that PoE is present, qualifiers display measurements such as voltage and maximum wattage, which can indicate whether a port is 802.3af or 802.at, and troubleshoot issues with power budget.

- Saved test results: The vast majority of qualifiers record test results to on-board storage, so these may be printed out or stored at the end of a project for documentation.
- More detailed displays: Qualifiers display more detailed fault information than verifiers, showing the estimated distance to the cable fault, and whether it's a short or crosstalk issue, often caused by crushed or damaged (but not cut) cables.

Product Options

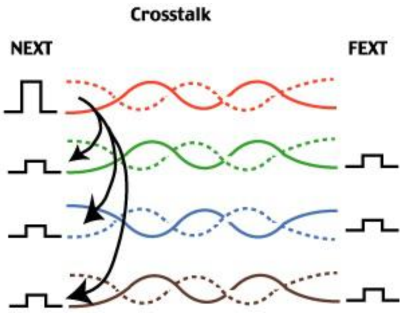
Qualifiers are a large price increase over verifiers. The Fluke CableIQ sells for about $1,100 online, almost the times the price of their verifier model, the MicroScanner. Some, such as Ideal's SignalTEK NT line (~$2,000 online), are priced even higher.

Qualifiers are not as widely available as verifiers, with Fluke, the Ideal SignalTEK NT, and ByteBrothers Low Voltage Pro, being some of the most common and popular among installers.

Certifiers

Certifiers test cables to ANSI/EIA/TIA standards, running a full battery of tests, including those run by verifiers and qualifiers (wiremap, length), while adding others and running more in depth crosstalk testing.

These tests include:



- Crosstalk: This test measures the amount of signal which is leaked from one pair of a cable to another, or from one cable to another. This includes 6-8 different crosstalk tests (near end, far end, alien crosstalk, etc.) depending on the category of the cable being tested. Qualifiers simply test basic "crosstalk", without all of these detailed measurements.

- Propagation delay: This test is similar to latency, measuring the time it takes for signal to reach the far end of the cable.
- Delay skew: Skew tests measure the difference in delay among all four pairs of the cable. Significant differences can indicate cable faults or stressed cables.
- Insertion/return loss: These are measurements of the signal loss caused by connectors in the cable run (insertion loss) or by reflected signal back at the test point (return loss) typically caused by poor terminations or cable faults.

This PDF is a detailed test report produced by a cable certifier.

Product Options

Cable certifiers are far more costly than other testers, generally at least $5,000, though $10,000+ is not uncommon, with full kits including fiber optic adapters often selling for $20,000. In addition to initial cost, certifiers must be factory recalibrated periodically (every 2-3 years), which ranges from a few hundred to over a thousand dollars.

Due to the very strict tolerances required for calibrated testers such as these, only a handful of manufacturers sell cable certifiers, with the Fluke DSX and Ideal LANtek lines two of the most common.

What Do I Need?

In general, integrators should keep at least a verifier on hand. Wiremap and length are the key elements which should be tested in any cabling install, prior to devices being installed. It is common for at least one or two cables in an installation to have crossed or shorted pairs. Instead of simply guessing and/or re-terminating the cable without diagnosing the problem, a verifier may show exactly what is wrong.

Those doing mid-size installs with the budget to support it may want to invest in a qualifier. The ability to test services and document results may be used not only for installation and troubleshooting, but as a differentiator, since many integrators (especially small ones) do not provide these services or documentation.

Only in rare cases should integrators invest in a certifier, since the quantity of cables in most security projects is low, and full-blown certification tests not often required. In some instances, customers or RFPs may require a certifier be used, and test results documented as part of the closeout process. However, if this is only a periodic need, certifiers are available for rent for a few hundred dollars, well below their out of pocket cost, as well as the cost of maintaining their calibration.

Fiber Use and Testing

Most networks are twisted pair based (UTP/STP/ScTP, etc.), which is what we have covered above. For fiber links, see: Using Fiber Optics for Surveillance

Grounding and Bonding

One of the most misunderstood and sloppiest elements of network design, grounding and bonding mistakes can lead to big problems.

We explain the key elements involved including:

- Differences between grounding and bonding
- The purpose of bonding and grounding in surveillance
- Published standards covering bonding and grounding
- Rack ground traps
- Chassis screws/bolts
- Third plug prong
- Camera side grounding
- Cable shield grounding
- Ground loop problems

Grounding vs Bonding Explained

Following the precept that electricity follows the path of least resistance, grounding and bonding is the practice of installing electrically sensitive equipment to an engineered point

- Grounding (also called Earthing): Connecting electrical equipment directly to a low impedance path to the earth.
- Bonding: Bonding connects all potentially sensitive equipment together. While not explicitly 'grounded', bonding typically is tied to a formal earth ground point, usually a bus bar or buried electrode.

Essentially, Grounding and Bonding describe different steps in the same process; a grounded system is the goal, and bonding is the process of connecting gear together for that purpose.

Purpose

The necessity of bonding and grounding in a surveillance system is two fold:

- Safety: Anytime metal is in direct contact with electricity, it can conduct errant currents. The only way to prevent the metallic chassis, enclosures, racks, or conduit from being an electrocution risk is to ensure it is bonded and connected to an earth ground. Even ethernet networks can conduct or become traps for deadly currents, and the general principles that apply to high-voltage systems also apply to low-voltage work.
- Signal Integrity: This is achieved by both grounding and bonding. Even non-hazardous currents can greatly disrupt the quality and transmission of electrical impulses, typical to ethernet traffic. To a lesser extent than safety, ground provides an outlet for these potentially disruptive currents.

In a typical surveillance system, any of the devices that are in close proximity to high-voltage sources - like ethernet switches or servers plugged into wall main outlets, and the cables and other devices connected to that equipment - need to be properly grounded, and bonding is typically the prescribed method of doing so.

Published Standards

Proper grounding and bonding for network attached systems are described in two primary resources:

- TIA-942: As electrical safety applies to data center designs, this specification describes minimum provisions for grounding within a computer network utility.
- TIA-607-A/B: This substandard specifically describes the methods of grounding and bonding mandated by TIA-942.

Together both of these documents form the basis of how surveillance systems are properly bonded and grounded, including the three methods described below.

Surveillance System Grounding

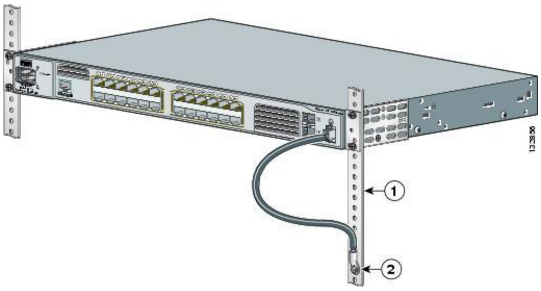
For video networks, three major types of grounding and bonding methods are employed:

- Rack Ground Taps
- Chassis Screws/Bolts
- Third Plug Prong

In general, any or all of these methods should be used where presented. These methods rely on the availability and proper installation of a formal earth ground point designed into the architectural and electrical plans of a facility. In most cases, this will be readily available within a data center or server room in the form of a TGB or TMGB points.

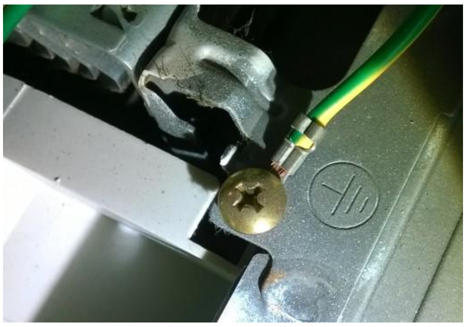
Rack Ground Taps:

Most rackmount equipment is incidentally grounded through contact of the mounting screws securing the devices to the rack. However, in many cases, a more deliberate method is called for that typically involves attaching a grounding wire to the chassis and rack by way of a bolted lug. This method is described in the installation instructions of the rack-mounted device, with the appropriate hardware and mounting instructions included with those devices. A typical example from a rackmount switch is shown below:



Chassis Screws/Bolts:

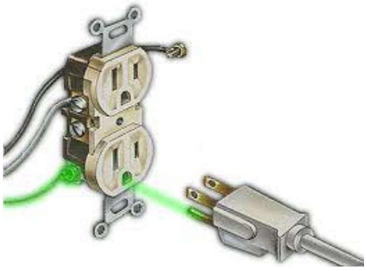
In other cases, a single screw or wire (often color-coded green) is located on the metal mount or chassis of a device. Cameras designed for mounting onto or in electrical junction boxes, or midspan PoE injectors are prime examples where this method is found.   The 'grounding point' where bonding cables or ground wires can be physically attached to the unit is typically marked with a universal 'ground point' symbol:



For this type of grounding to be adequate, the attached wire must itself be properly connected to a bond or ground point at the other end.

Third Plug Prong:

The most common type of grounding utility is also the least effective at preventing surveillance system issues. Modern electrical devices include a third prong designed into the modular plug and outlet connector. The image below shows how this prong comes into contact with the (green) ground wire attached to the outlet plug inside the wall:



However, this type of ground often is purely to maintain safety of the chassis by creating a path of least resistance between the device's internal power supply, the enclosure, and the main electrical circuit. The grounding property of this type of loop may not address any cabling or devices in turn connected to the device by a network. As such, most switches and power supplies include other methods of grounding in addition to a three-pronged plug.

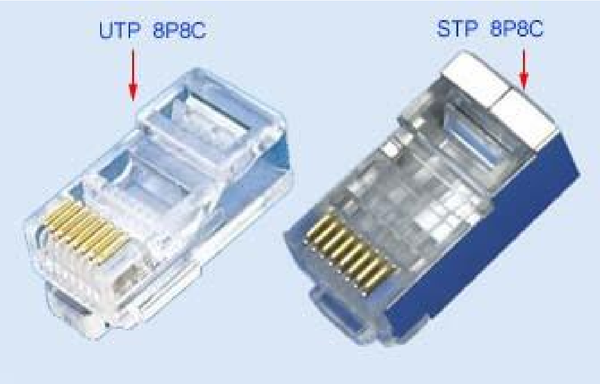
Camera Side Grounding: When the equipment and cabling leading to a discrete camera is grounded, concerns about grounding the camera itself are typically mitigated due to the source of electrocution being at the switch or power supplying equipment. When the cable connecting a camera is grounded, the camera is essentially bonded by the cable to a ground point.

Typically, the biggest threat of shock or electrical damage on the camera side is presented by lightning. If lightning strikes near the camera, the cable can become a conduit for very dangerous extremely high voltages. A 'lightning arrestor' is typically used to isolate the surge of current as close to the camera as possible.

Cable Shield Grounding?

Some varieties of cable include shielding or metallic grounding elements within the bundle. Most commonly STP (Shielded Twisted Pair) typically includes a foil sheath that surrounds pairs or the entire group of pairs that must be grounded to dissipate potential harmful electrical interference.

For STP cables, most shielding is designed to be grounded at the ethernet jack at the switch. However, maintaining conductive contact with the switch port and the cable's shield requires the connector itself to be conductive. For example, note the difference between the 'UTP' and 'STP' types below:



The 'STP' type is clad in a metallic surround that keeps the cable shield in contact with the grounded jack. In order to preserve the property of shielding, UTP style connectors cannot be used properly with STP cabling.

Ground-Loop Problems

In analog CCTV systems, when cameras and recorders are ground to points with different potentials, the cable stretching between those two points can become the host for small but disruptive currents commonly called 'ground loops'. With the signal impedance of analog CCTV video signals being especially sensitive to these currents, isolators or blockers are commonly used to trap and remove those currents.

With IP video, this is not a common problem simply due to the twisted pair properties of UTP cabling. The cabling design makes it much more difficult for such a current to interfere and travel in a 'loop' of cable, and therefore is not a practical issue.

Network Design & Security

Network Security

Keeping surveillance networks secure can be a daunting task, but there are several methods that can greatly reduce risk, especially when used in conjunction with each other.

We look at several security techniques, both physical and logical, used to secure surveillance networks, including:

- Network Hardening Guides
- Passwords
- LDAP / Active Directory Integration
- VLANs
- 802.1X Authentication
- Disabling Switch Ports
- Disabling Network Ports
- Disabling Unused Services
- MAC Address Filtering
- Locking Plugs
- Physical Access Control
- Managing Network Security For Video Surveillance Systems

Network Security Critical

More than ever, network security has become a key issue, with published vulnerabilities, hacks, and botnets on the rise.

In previous years, incidents were few and far between, with Hikvision the most notable target (see: Hikvision Hacking And Chinese Province

Warning, The Hikvision Hacking Scandal, The Hikvision Hacking Scandal Returns, finally resulting in their "Anti Hacking" Firmware).

Previously, major vulnerabilities (and their effects) were reported in other major manufacturers, including:

- Axis Critical Security Vulnerability: A vulnerability allows attackers to remotely initiate a telnet connection, allowing the attacker to take over the device, reboot it, power it down, etc.
- Hacked Dahua Cameras Drive Massive Cyber Attack: As part of the Mirai botnet, hacked Dahua cameras (and others) took down major internet sites and even an entire country.
- Sony IP Camera Backdoor Uncovered: Attackers can remotely enable telnet on cameras, combined with a hard coded backdoor account which allows users to take over the device.

See our Listings of Video Surveillance Cybersecurity Vulnerabilities and Exploits for more information on these and other issues, including new ones as they occur.

Because of the severity of these incidents and their increasing frequency, it is critical that users understand the basics of cyber security for surveillance systems, and how to protect against simple attacks at the very least.

Network Hardening Guides

In the IT industry at large, network hardening guides are common, outlining recommendations (as an example, see this Cisco hardening guide) to make the network more secure. Many/most of these recommendations apply to surveillance networks, as well, including controlling physical and login address, securing passwords, disabling ports, etc.

However, many recommendations may be above and beyond what many IP video integrators are capable of, or what is practical for a given system. Complex authentication schemes such as 802.1x, LDAP integration, SNMP monitoring, etc., are simply not worth the time/cost to implement for many systems, given the limited risk.

Surveillance Hardening Guides Rare

Unlike IT, surveillance specific hardening guides are rare, with only a handful of guides available from manufacturers.

- Axis cyber hardening guide
- Bosch IP Video and Data Security Guidebook
- Dahua best practices
- Genetec cyber hardening guide (requires partner login)
- Milestone cyber hardening guide

The exact recommendations in each of thees guides vary, but most are divided into basic and advanced levels, depending on the criticality of the installation.

The Axis guide, for instance, varies from demo only (not production use) to highly secure enterprise networks, and include basic best practices, such as strong passwords, updating firmware, and disabling anonymous access, through more complex practices, such as 802.1x authentication, SNMP monitoring, and syslog servers.

While the these guides are manufacturer-specific, providing instructions pertinent to the camera or VMS, many recommendations are useful across all manufacturers, and fall in line with IT industry best practices, and the practices discussed below.

Strong Passwords

Strong passwords are the most basic security measure, but unfortunately, ignored by many users. Many surveillance systems are deployed in the field with default passwords on all equipment, including cameras, switches, recorders, and more (see our IP Cameras Default Passwords List). Doing so may make it easier for techs to access cameras but also make it simple for anyone to log into one's cameras (see: Search Engine For Hacking IP Cameras).

At the very least, all surveillance network devices, including cameras, clients, and servers, should be changed from the defaults with strong passwords, documented in a secure location. This prevents access to the network using simple password guessing, requiring a more skilled attacker and more complex methods.

Some manufacturers require changing the default password when connecting for the first time (see a comparison of how Axis, Dahua and Samsung set passwords). Indeed, an upcoming ONVIF Profile (Q) would make changing default passwords mandatory, though how well that is adopted remains to be seen.

LDAP/AD Integration

Using LDAP/Active Directory (AD) integration, VMS permissions are assigned to network users managed by a central server (also called single sign-on). Since these user accounts often implement password strength and expiration rules, this integration may improve security over local VMS accounts which do not have these restrictions. This reduces administration overhead, since individual accounts do not to be created and maintained.

Typically, LDAP use is restricted to larger, enterprise systems, since many small installations do not have an LDAP server implemented. Some small or midsize systems which are installed in larger entities, especially education and corporate facilities, may use LDAP as these organizations are likely to use it for their network access control.

LDAP / AD could theoretically be used for IP cameras, but, in practice is not. ActiveDirectory, as a Microsoft offering, is not supported by almost any IP camera, which typically run on Linux. One Windows IP camera claimed to do so, but it has not gained any meaningful market share.

Firewalls/Remote Access

To prevent unauthorized remote access, many surveillance systems are not connected to the internet at all, instead on a totally separate LAN. This reduces risk, but may make service more difficult, as updates to software and firmware, usually simply downloaded, must be loaded from USB or other means.

Those systems which are connected are typically behind a firewall, which limits inbound/outbound traffic to only specific IP addresses and ports which have been authorized. Other traffic is rejected. Properly implemented, this may prevent the vast majority of attacks.

Remote Access Risks

For devices which require remote access, VMSes and cameras may require one or more ports to be open. However, each open port presents a possible opportunity for an attacker. Exactly how many and which varies by the VMS. Users should refer to manufacturer documentation for which ports must be open if remote access is required (for maintenance or remote viewing), and we list some examples in our Network Ports for IP Video Surveillance Tutorial.

P2P/Cloud Access

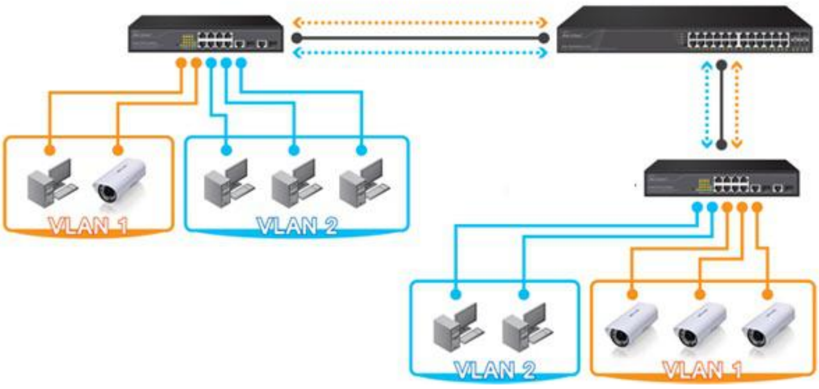
Alternatively, some manufacturers allow for "phone home" remote access, which sets up a secure tunnel via an outbound connection without requiring open ports, reducing risks. Many cameras and recorders use cloud connections for remote access, such as Hikvision EZVIZ, Eagle Eye Cloud VMS, and Genetec Cloud. Additionally, many remote desktop services use similar technology, such as LogMeIn, TeamViewer, SplashTop, etc.

We discuss these methods in our Remote Network Access for Video Surveillance tutorial.

VLANs

Virtual LANs (shortened to VLANs) improve security by segmenting traffic into multiple virtual networks. So while other services, such as IP based surveillance equipment or general office LAN traffic, may exist on the same physical switch, for practical purposes the networks are invisible to each other, and unreachable.

For example, in the image below, the camera and NVR on VLAN 1 may not be reached by the office PC on a separate VLAN, nor could a user on the NVR (VLAN 1)"see" traffic on the PC VLAN (VLAN 2).



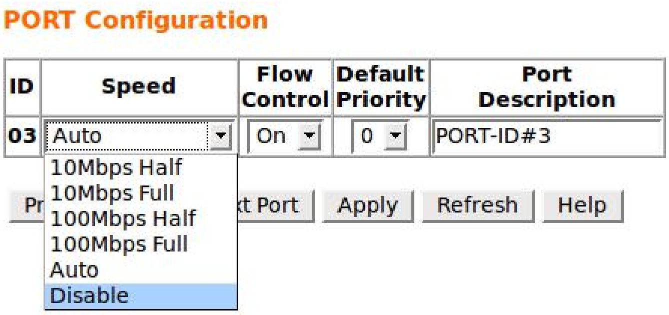
VLANs are most commonly set up using 802.1Q tagging, which adds a header to each frame containing VLAN information. This header is interpreted by the switch and traffic forwarded only to other devices on the same VLAN.

Note that while traffic may not be intercepted across VLANs, bandwidth constraints still exist. Numerous large video streams may negatively impact VOIP and office application performance, while large file transfers may affect the surveillance network. Because of this, VLANs are also most often deployed in conjunction with Quality of Service (QoS), which prioritizes network traffic, sending video packets ahead of file transfers, for example, so video quality is not impacted.

See our VLANs for Surveillance guide for further information.

Disabling Unused Switch Ports

Another easy but typically overlooked method of keeping unauthorized devices from accessing a switch is to disable all unused ports. This step mitigates the risk of someone trying to access a security subnet by plugging a patch cable into a switch or unused network jack. The option to disable specific ports is a common option in managed switches, both low cost and enterprise:



PORT Configuration

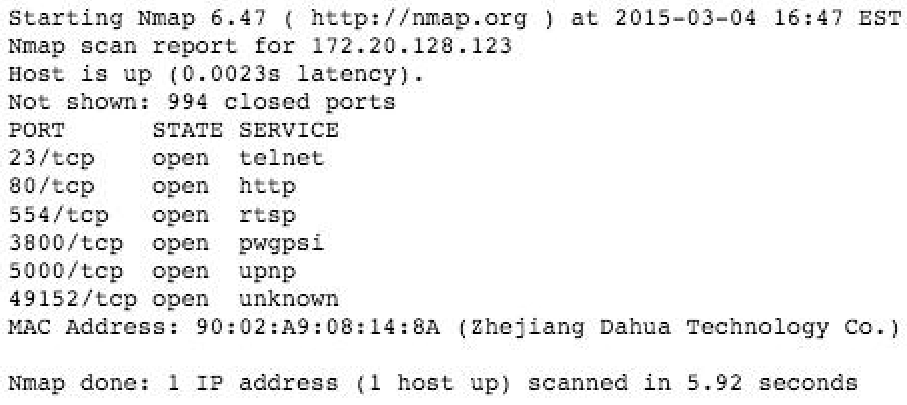
ID	Speed	Flow Control	Default Priority	Port Description
03	Auto	On	0	PORT-ID#3

While effective at narrowing the number of potential access points, this step does not necessarily prevent unauthorized access to a network, as someone could potentially unplug a device (camera, workstation, printer) from a previously authorized port or jack and access its port, unless measures such as MAC filtering or 802.1X are in place.

Disabling Unused Network Ports

Many cameras ship with unneeded network ports turned on, such as Telnet, SSH, FTP, etc., as we found in our NMAPing IP Cameras Test. These ports are favorite targets of hackers (as illustrated by bitcoin miners and buffer vulnerabilities found in Hikvision Cameras).

A quick 30 second scan of a popular IP camera reveals multiple open ports other than those expected for web access and video streaming (80/554):



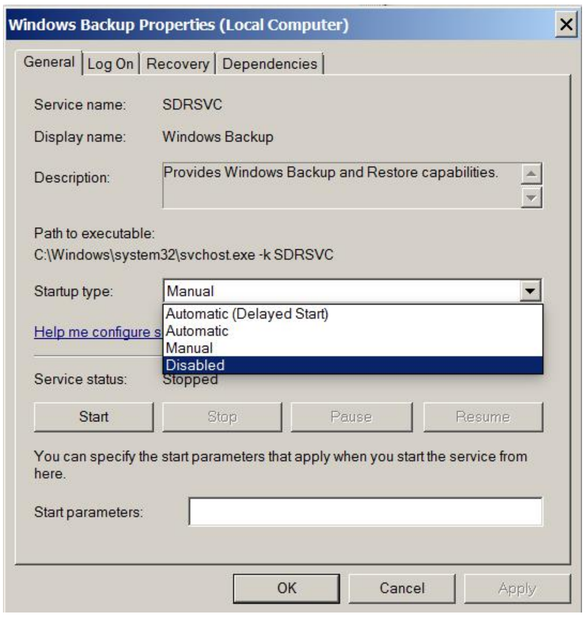
```
Starting Nmap 6.47 ( http://nmap.org ) at 2015-03-04 16:47 EST
Nmap scan report for 172.20.128.123
Host is up (0.0023s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
554/tcp   open  rtsp
3800/tcp  open  pwgpsi
5000/tcp  open  upnp
49152/tcp open  unknown
MAC Address: 90:02:A9:08:14:8A (Zhejiang Dahua Technology Co.)

Nmap done: 1 IP address (1 host up) scanned in 5.92 seconds
```

These ports should be disabled wherever possible to prevent potential attacks.

Disabling Unused Services

Unnecessary services on viewing workstations and servers should be turned off. These may include manufacturer-specific update utilities, various Microsoft update services, web services, etc. These unneeded services may act as a backdoor for hackers or viruses, consume additional processor and memory, and increase startup time.

These services should be disabled or set to operate only when manually started, as seen here in Windows:



Windows Backup Properties (Local Computer)

Service name: SDRSVC

Display name: Windows Backup

Description: Provides Windows Backup and Restore capabilities.

Path to executable:
C:\Windows\system32\svchost.exe -k SDRSVC

Startup type: Manual

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

OS and Firmware Updates

OS and firmware updates are a matter of some debate, with some users installing every available Windows Update, for example, while others insist that these updates may break VMS software or camera integrations.

However, these updates (especially Windows Update) often include patches to newly discovered security vulnerabilities, such as the Heartbleed SSL vulnerability, which affected millions of computers worldwide. Patches for these significant issues should be installed.

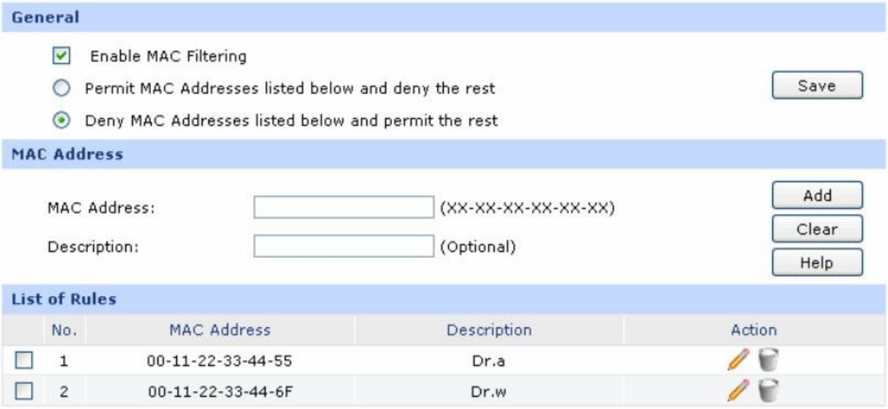
Other, more routine, updates may be optional. Users especially concerned about compatibility issues should contact their camera/recorder/VMS manufacturers to see their recommendations for applying updates or not.

MAC Address Filtering

MAC address filtering allows only a specific list of devices to connect to the switch. Other devices plugged into the switch are ignored, even if the port previously was used by a valid device. MAC filtering is possible only using managed switches.

In surveillance networks, MAC filtering is typically easy to administer. Once all cameras, clients, and servers are connected, it is enabled, and connected devices' MACs added to the whitelist. Since these devices in a surveillance network are rarely changed out, little extra maintenance is required. In other networks where devices may frequently be added or removed, administrators may find filtering more cumbersome to administer.

This image shows MAC filtering options in a typical managed switch interface:


General

☑ Enable MAC Filtering

○ Permit MAC Addresses listed below and deny the rest

● Deny MAC Addresses listed below and permit the rest

MAC Address

MAC Address: (XX-XX-XX-XX-XX-XX)

Description: (Optional)

List of Rules

	No.	MAC Address	Description	Action
□	1	00-11-22-33-44-55	Dr.a	
□	2	00-11-22-33-44-6F	Dr.w	

See our Network Addressing for Video Surveillance Guide for more discussion and a basic overview of MAC addresses.

802.1X

802.1X requires devices trying to connect to the network to have proper credentials to be allowed on. This blocks random devices or attackers from just jumping on a network.

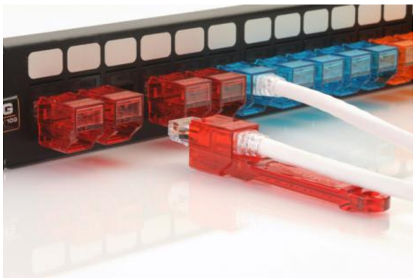
Using 802.1X, a "supplicant" (client such a camera, PC, etc.) attempts to connect to network via a switch or WAP (called the "authenticator"). The authenticator then checks the credentials of the supplicant with a server, call the authentication server (typically using a protocol called RADIUS, and grants or denies access accordingly.

While 802.1X provides strong security, setting up a network to support it can be cumbersome and involved. Not only must connected devices (cameras, WAPs, client PCs, NVRs, etc.) support 802.1X integration, all switches must, as well. Each of these devices must be individually configured for 802.1X, adding additional configuration time to the install.

Because of these factors, which increase cost and administration overhead, 802.1X is rarely used in all but the most complex enterprise surveillance networks, with users opting for simpler security measures instead.

Locking Plugs

Another layer of security that physically prevents connection or tampering with network cabling by unauthorized devices are port plugs and cable locks. These devices mechanically lock a cable into a switch, patch panel, or wall jack, or fill unused switch ports, and may only be removed with a proprietary tool.



While these types of locks are effective at stopping casual tampering, they are not unbeatable or indestructible, and a determined intruder may simply be able to force them out or pry them loose given enough time. As such, locking plugs should be considered part of a good network security program, but not the only element.

For a deeper look, read our Locking Down Network Connections update.

Door Locks and Physical Access

Finally, best practices call for controlling access to the most vulnerable areas of a network, the rooms, closets, or racks where surveillance servers and switches are typically mounted. By reducing the potential availability of these areas, many risks from determined or even inadvertent threats can be avoided. If doors cannot be secured, individual rack cages or switch enclosures should be. Most modern IT cabinetry includes security equipment as standard options:

As a result, many facilities employ electronic access control on server or network equipment rooms. However, even non-exotic mechanical keys and locks can do a great job of protecting sensitive areas when properly managed.

Managing Network Security For Video Surveillance Systems

While all the steps below may improve security on their own, they are most effective when documented as part of a written (and enforced) security policy.

In surveillance, this policy is up to the individual install, but generally it comes from one of two places:

- End user: When the surveillance network is part of a larger corporate/enterprise LAN (whether sharing switches or dedicated), end users most likely control the security policy for all network devices, and may force these requirements upon integrators (for better or worse).
- Integrator: If an end user does not have a security policy in place, the installing integrator may choose to create one as part of their documentation, requiring it to be followed in order for the warranty to be enforced and limit liability in case of a breach.

Vulnerabilities & Exploits

This list compiles reported exploits for security products, and is updated regularly.

We have summarized exploits by date and by manufacturer, providing a brief description of the exploit along with affected product(s) and firmware version(s), when known.

Historical List Of Exploits

This list contains a summary of known exploits in reverse chronological order. Additional details are provided in a section for each manufacturer below. Manufacturers with an asterisk (*) next to their name indicate products that were OEM'd under multiple brand names beyond the original manufacturer listed.

- December 2017 - Axis Vulnerabilities linked to DHCP and UPnP libraries in BisyBox, and vulnerability in CGI executables
- November 2017 - Hikvision Wifi cameras have hard-coded SSID, allows for rogue access point attack (7)
- November 2017 - Vivotek remote stack overflow vulnerability (3)
- November 2017 - Dahua Hard-coded backdoor credentials in camera and NVR firmware (6)
- October 2017 - Uniview recorders vulnerable to admin password retrieval backdoor
- August 2017 - Hikvision Tools allows admin password reset in older firmware (6)
- August 2017 - Hikvision iVMS-4200 stores passwords with reversible encryption (5)
- August 2017 - NeoCoolCam - iDoorbell product buffer overflow vulnerability allow various exp loits
- July 2017 - Dahua - Buffer overflow vulnerability in password field (5)
- July 2017 - Vivotek - CGI script exploits (2)

- July 2017 - Axis - Buffer overflow vulnerability in 3rd party software toolkit used for ONVIF (3)
- June 2017 - FLIR - Vulnerabilities allow remote code execution, unauthenticated viewing of live images, and reveal hard-coded accounts
- June 2017 - Persirai botnet attacks various consumer/SMB-oriented cameras.
- May 2017 - Hanwha - User can exploit cached data from a previous session to gain access to certain recorders
- March 2017 - Hikvision - Backdoor allows unauthorized access to admin interface (4)
- March 2017 - Axis - Multiple vulnerabilities related to CSRF attacks (2)
- March 2017 - Dahua - Backdoor allows attacker to read user/password list (4)
- March 2017 - Ubiquiti - Command injection vulnerability
- February 2017 - Geutebrück - Authentication bypass.
- February 2017 - Dahua - Multiple vulnerabilities in DHI-HCVR7216A-S3 recorders (3)
- December 2016 - Sony - Attackers can remotely enable telnet on cameras.
- December 2016 - Hikvision - hik-online.com servers susceptible to XXE exploit. (3)
- November 2016 - Milesight - Cameras have a number of vulnerabilities that allow remote exploit.
- November 2016 - Siemens - Remote privilege escalation possible via exploiting web interface.
- October 2016 - NUUO - Insecure default credentials. (2)
- October 2016 - Dahua*, XiongMai - Mirai botnet. (2)
- September 2016 - AVer - EH6108H+ DVR Multiple vulnerabilities
- August 2016 - NUUO - Remote root exploit and remote command injection vulnerability. (1)
- July 2016 - Axis - Remote root exploit. (1)
- July 2016 - Pelco - Digital Sentry hard coded username/password backdoor.
- March 2016 - TVT* - Remote code execution.
- March 2016 - HID - Command injection vulnerability allows attacker full control of device.

- Febrary 2016 - Unknown DVR OEM - Authentication bypass, other issues.
- August 2015 - Dedicated Micros - Devices have no default password, allowing full access.
- June 2015 Avigilon - ACC - Allows attackers to read arbitrary files.
- October 2014 - Bosch - 630/650/670 Recorders - Multiple exploits allow an attacker to get root console and also retrieve config data.
- September 2014 - Hikvision - 7200 series NVRs - Buffer overflow to gain root access. (2)
- November 2013 - Dahua* - DVR's/NVR's - Execute admin commands without authentication (1)
- November 2013 - Vivotek - RTSP stream authentication can be bypassed. (1)
- August 2013 - Hikvision - IP Cameras - Remote root exploit. (1)

Exploits For Specific Companies

Aver

Firmware version X9.03.24.00.07l, and possibly earlier versions, contain multiple vulnerabilities including hard-coded admin-level accounts and authentication bypass exploits. Additional details in CERT report.

Avigilon

ACC versions prior to 4.12.0.53 and prior to 5.4.2.21 allowed for arbitrary files to be retrieved through specially crafted URLs, giving anyone with remote access to the server the ability to access files at will, without authentication, making this a critical vulnerability. Additional details are in the CVE Report for this vulnerability.

Axis

(4) Axis announced patches for vulnerabilities common to DHCP and UPnP code in BusyBox Linux, and also for information disclosure vulnerabilities in CGI executables. Additional details in Axis 5 Vulnerabilities Examined.

(3) An exploit in a toolkit used for ONVIF support in Axis, and other brands, was discovered. While it has the potential to impact multiple products, proof-of-concept code was only developed/shown for Axis products.

(2) A Google researcher identified multiple vulnerabilities in Axis cameras. The vulnerabilities are relatively low risk, and are primarily patched in newer firmware, but could have the potential to disable or alter camera functionality if successfully used.

(1)Products with firmware from versions 5.20.x to 6.2.x had a vulnerability that allowed for an attacker to gain access to a root console on the device, allowing them full control of the device. Attackers did not need to know usernames/passwords, or other information about the product in order to exploit it, making this an extremely severe vulnerability. Axis issued a press release on this exploit, and IPVM covered the Axis exploit as well.

Bosch

DVR 630/650/670 units with firmware version 2.12, and possibly older versions, are vulnerable to exploits where attackers can send specially-crafted URLs to the device to enable telnet access, which provides a root console that does not require authentication. No special software is required to carry out this attack. Vulnerability details and proof of concept examples are listed in ExploitDB under ID 34956.

Dahua

(6) Hard-coded credentials were found in firmware for cameras and NVRs, allowing for rogue firmware uploads. Additional detail: Dahua Hard Coded Credentials Vulnerability.

(5) A buffer overflow vulnerability was discovered in Dahua cameras where excessive-length password text can be entered, triggering an overflow. Additional coverage: Dahua Suffers Second Major Vulnerability, Silent.

(4) Dahua cameras and DVRs/NVRs expose a config file containing username/password info to unauthenticated HTTP requests. Additional coverage: Dahua Backdoor Uncovered.

(3) Vulnerabilities found in Dahua's DHI-HCVR7216A-S3 recorder, including cleartext passwords, auto-admin login allows data sniffing, admin password bypass, unencrypted communications allows man-in-the-middle attack.

(2) Dahua camera and NVR firmware prior to January 2015 shipped with telnet enabled, which coupled with well-known admin credentials allowed attackers to gain access to a root shell and exploit the device. The most popular exploit was the Mirai botnet, which took down internet sites and service providers in October 2016. Products OEM'd from Dahua, which include multiple brands such as FLIR and Honeywell, were also affected.

(1) Recorders with firmware 2.608 could be exploited to accept certain admin commands without authentication, allowing an attacker to retrieve configuration information from the device to change user passwords. ExploitDB contains additional details under ID 29673

Dedicated Micros

Dedicated Micros DVRs, including at least DV-IP Express, SD Advanced, SD, EcoSense, and DS2, ship with no default credentials, and insecure protocols enabled. This can allow attackers to take over the device and/or to sniff network traffic during setup. Additional details in VU 276148.

FLIR

Multiple vulnerabilities, with no firmware fix, including ability to see live images without authentication, remote code execution, and hard-coded accounts, outlined in Beyond Security disclosure. Additional details and analysis in: FLIR Thermal Camera Multiple Vulnerabilities, No Fix.

Geutebrück

In G-Cam/EFD-2250 with firmware version 1.11.0.12 an authentication bypass vulnerability has been identified. The existing file system architecture could allow attackers to bypass the access control that may allow remote code execution. Details in ICS CERT Advisory.

Hanwha

SRN-4000, SRN-1673S, SRN-873S, and SRN-473S recorders have a vulnerability in some firmware versions where a user who was previously logged into an affected device and use cached data/files to gain access to the same recorders management interface, bypassing the standard authentication screen. Additional detail in the ICS-CERT release and Hanwha Vulnerability Analysis report.

HID

VertX and EDGE systems with firmware prior to March 2016 are susceptible to a command injection exploit, where an attacker can cause the controllers to lock or unlock doors without authentication, as well as perform a number of other functions on the controller. This vulnerability was detailed on Trend Micro's blog, technical details can be found in this github repository.

Hikvision

(7) Some Hikvision Wifi cameras attempt to connect to SSID "davinci" by default, allowing an attacker to setup a rogue access point with this SSID to gain access to camera for further exploit.

(6) Hikvision's algorithm for generating security codes to reset admin passwords is cracked, with tools released to enable easy code generation.

(5) iVMS-4200 has password recovery feature that divulges admin password encrypted with reversible method.

(4) A potential vulnerability was first reported in March 2017, and then verified in a US Department of Homeland Security release. Attackers can bypass authentication measures to get access to admin-level features in the web interface of affected Hikvision cameras.

(3) A security researcher found hik-online.com servers vulnerable to an XML External Entity (XXE) exploit. This vulnerability allowed the researcher to retrieve arbitrary files from the server, exposing users to the risk of having data on the public IP/port of their registered devices exposed. Further coverage available in our Hikvision cloud server vulnerability report.

(2) NVR's with firmware 2.2.10, and possibly other versions, contain a vulnerability that allows for a buffer overflow attack, enabling attackers to gain control of the device. This vulnerability was examined and described by research firm Rapid7. Hikvision

(1) Hikvision IP cameras with firmware v4.1.0 b130111, and possibly other versions, can be attacked to gain access to the admin account, bypass authentication entirely using hard-coded credentials, or to execute arbitrary code through a buffer overflow attack. Core security issued a report detailing these exploits.

Milesight

Milesight camera firmware prior to ~November 2016 may contain a number of vulnerabilities including hard-coded credentials and the ability to execute admin commands via unauthenticated CGI calls, making the cameras highly vulnerable to attacks.

NeoCoolCam

HTTP and RTSP service are vulnerable to multiple forms of buffer overflow attacks. Devices use uPNP to open ports in firewall, making them exposed by default in many installs. ~170K units impacted. Full details in Bitdefender whitepaper on NeoCoolCam vulnerability.

Nuuo

(2) Nuuo NT-4040 Titan firmware version NT-4040_01.07.0000.0015_1120, contains default credentials of admin:admin, and localdisplay:111111. A remote network attacker can gain privileged access to a vulnerable device. Further information can be found in CERT Vulnerability Listing for this issue.

(1) Multiple devices, including the NVRmini, NVRmini2, Crystal, Titan and NVRSolo with firmware prior to 3.0.8 have multiple vulnerabilities that allow for remote code execution, remote root exploit, remote file deletion, and other attacks. Exploits are listed on ExploitDB under multiple IDs, including: 40200, 40209, 40210, 40211, 40212, 40213, 40214, 40215. Each of these represents a critical vulnerability that is easy for an attacker to execute against the device.

Unknown DVR OEM

An unknown manufacturer of DVR's sold under various brands has firmware with multiple exploits, including ability to bypass authentication and get telent access. Details can be found on the researchers blog.

Pelco

Digital Sentry products running firmware prior to 7.13.84 contained a hard-coded admin account that could be used to take full control of the device by a remote attacker. IPVM covered this vulnerability when it was made public, and CERT also contains additional details.

Sony

Attackers can remotely enable telnet on Gen 5 and Gen 6 cameras with firmware prior to 1.86.00 and 2.7.2 respectively, enabling them to potentially login as root. Additional details in our coverage of this exploit.

Siemens

Specially crafted URLs allow an attacker to gain admin-level privileges on affected cameras. List of affected cameras and recommended firmware versions to resolve this issue are provided by Siemens.

TVT

Specially crafted URLs can be used to cause the recorders manufactured by TVT to execute arbitrary commands. At least 79 distinct brands OEM'd these units, including well-known brands like ADI and Q-See. Rotem Kerner documented the exploit on his site, and also provided IPVM with additional details on how he crafted the exploit.

Ubiquiti

A command injection vulnerability was reported in firmware prior to AirOS 8.0.1. Relatively low risk of exploit, but could enable severe holes in network, such as reverse shells, if properly executed.

Uniview

Admin password hash can be retrieved from Uniview recorders, and then used to login as admin, allowing full access. Details covered in Uniview Recorder Backdoor Examined.

Vivotek

(3) Potential for stack overflow, likely resulting in denial of service, via malformed URL calls. Details in Vivotek Remote Stack Overflow Vulnerability.

(2) CGI scripts on Vivotek cameras can be used to access files and run commands as root. Additional coverage: Wrongly Accused Critical Vulnerability for Vivotek

(1) Firmware 0105a, 0105b, and possibly other versions, are susceptible to having RTSP authentication bypassed, allowing video streams to be viewed without authentication. Firmware after 0301c should not be affected. Additional information from Core security: Vivotek RTSP auth bypass.

XiongMai

Xiongmai firmware prior to January 2015 shipped with telnet enabled, which coupled with well-known admin credentials allowed attackers to gain access to a root shell and exploit the device. The most popular exploit was the Mirai botnet, which targeted Dahua and Xiongmai devices, and took down internet sites and service providers in October 2016. Due to Xiongmai being primarily an OEM component supplier, many affected products were sold under alternate brands.

Wireless Networking

Wireless networking remains a niche for video surveillance applications. One of the key factors is that it is much different, if not harder, than deploying wireline networks.

We break down the key elements of wireless networking for video surveillance:

- Topology: PTP vs PtMP vs Mesh
- Antennas: Internal vs External
- Antennas: Omnidirectional vs Directional
- Antennas and Gain
- Free Space Path Loss
- Frequencies Including Licensed and Unlicensed Ranges
- MIMO Radios
- Bandwidth Planning
- Transmission Range
- Wireless Products Specializing for Surveillance
- Maintenance

Topology

There are three basic wireless network topologies in use in surveillance, with varying uses depending on where and how cameras are deployed:

Point-to-Point

Point-to-Point

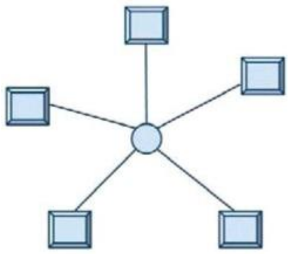
First, and most common are point-to-point (PtP) wireless links. In PtP networks, a single radio at the device location is connected to a single radio connected to the surveillance network. PtP links are used in two common applications:

- Connecting cameras: Most commonly, PtP radios are used to connect cameras from a single location (such as a parking lot pole, for example) to a surveillance system.
- Wireless backhaul: Point to point is also used in backhaul applications, connecting two buildings together or connecting a multipoint base station to another point in the network.

Directional antennas are most often used in PtP applications, with multi-mile ranges possible. Many different frequency options are available, from 900 MHz, to 2.4 and 5.8 GHz, and higher.

Point-to-Multipoint

In point-to-multipoint (PtMP) wireless links, a single radio acts as base station, connected to the central network, with multiple radios transmitting to it. The radios used in PtMP setups may be the same as PtP in many cases, though some manufacturers use special radios for the base station to handle higher data rates possible when connecting numerous client radios.



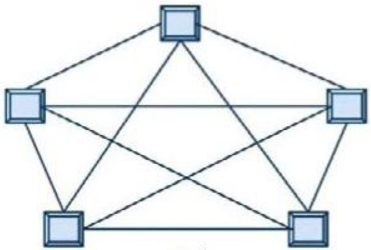
Point-to-Multipoint

PtMP is used in applications where multiple cameras must be dispersed around the area, without dedicated wired connectivity, with each camera sending video to the base station. These systems range in size from a handful of cameras in a parking lot to city-wide surveillance systems, where clusters of cameras are connected via PtMP before being backhauled through other means.

PtMP base stations typically use omnidirectional or wide angle directional antennas (such as sectors), depending one whether cameras are located in all directions or in one general direction. PtMP client radios most often use narrower directional antennas.

Mesh

In a mesh network, each wireless node connects to two or more other radios, providing more than one path for network traffic. If one link fails, data is rerouted to another path, reducing the chance of a total outage. However, if failover is desired, the mesh must be carefully designed to handle failed links, or traffic from one may quickly overload another.



Mesh

Mesh radios are typically more expensive than PtP or PtMP models, and more time-consuming to configure.

Because of the added expense involved in mesh networks, it is most often seen in city surveillance, one of the few applications with both the budget and need for these failover capabilities.

Mesh radios may use any type of antenna, depending on the distance to other nodes, and how many it is connecting to.

Internal Antennas for IP Cameras

Having wireless built into an IP camera is statistically rare and the cameras that do have integrated wireless, typically have short ranges and are marketed for consumer use, not professional. Less than 3% of IP cameras have built-in wireless and 90% of those are cube cameras.

As such, much professional video surveillance applications use a 'regular' IP camera connected to an external wireless node / radio that supports external antennas.

Antenna Types - Omnidirectional vs Directional

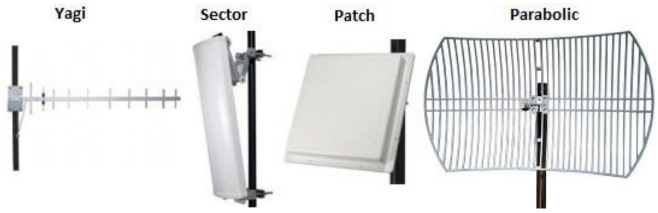
There are two fundamental types of external antennas used in wireless networking: omnidirectional and directional.

Omnidirectional

Omnidirectional antennas radiate signal in all directions. Most users are familiar with this type of antenna as it is typically included with consumer wireless routers, the black "rubber ducky" style seen below. Outdoor models function the same way, but may be much larger (3-5' long), depending on desired gain.

Directional

Directional antennas are available in numerous styles with varying beamwidths. Some provide tight coverage, 15 degrees horizontal or less, while other may be wide, over 100 degrees. Note that antenna type (yagi, sector, patch, parabolic, etc.) does not necessarily reflect beamwidth, and a wide variety of options are available in each form factor.



Performance Tradeoffs

Selecting the proper antenna depends on many factors, but essentially comes down to these tradeoffs:

- Omnidirectional antennas are easiest to set up, requiring little or no alignment, but offer the shortest range. They should be used only when required to connect multiple cameras to a base station, for example.
- Directional antennas such as patch and sector provide better range performance due to their narrower beam pattern. They are most commonly used both as external antennas and those built into all-in-one radios. They may often be aimed by sight instead of requiring more complex signal strength metering and aiming, and are forgiving of small changes due to wind, sway, and vibration.
- Highly directional antenna such as parabolic provide the strongest signal, but are difficult to aim due to their narrow beamwidth, often requiring experienced technicians to install. These antennas are most often aimed using lasers, signal strength meters, and other more complex means, and are more susceptible to performance issues due to sway or vibration than other types.

Antennas and Gain

Gain is important because the higher the gain, everything else being equal, the further the signal can transmit and more likely it can deal with obstructions. Omnidirectional antennas are often as low as 3dB while directional antennas can be 24dB or higher.

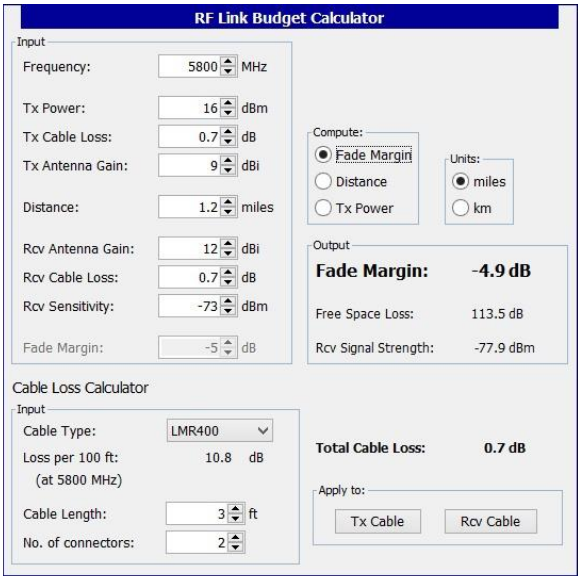
Free Space Path Loss

In this section, we introduce the basics of figuring out how far a signal can transmit, aka calculating free space path loss, for more, see: Training: RF for Wireless Surveillance.

The factors that drive how far one can transmit include:

- The frequency being used: higher the frequency, the shorter one can go (e.g., 5.8Ghz, everything else equal, has shorter range than 2.4Ghz).
- The gain of the antennas being used: the higher the gain (e.g., 24dB instead of 12dB), the farther one can go.
- The sensitivity level the receiver requires. The higher the level, the easier it is to meet but typically less bandwidth is available (e.g., -96dBm vs -74dBm for higher bandwidth levels).
- The transmission power of the radio. Most surveillance wireless systems use licensed frequencies which cap how much power can be put out, constraining how far the signal can go (unlike, e.g., a TV station which is comparatively 'blasting' out transmissions at much lower frequencies).

Because of the complex calculations required in FSPL, RF link budget calculators are most often used, with user inputting distance, frequency, antenna and cable information, and receiver sensitivity. The output of one of these calculators for a sample 5.8 GHz link is shown below.



RF Link Budget Calculator

Input

Frequency: 5800 MHz

Tx Power: 16 dBm

Tx Cable Loss: 0.7 dB

Tx Antenna Gain: 9 dBi

Distance: 1.2 miles

Rcv Antenna Gain: 12 dBi

Rcv Cable Loss: 0.7 dB

Rcv Sensitivity: -73 dBm

Fade Margin: -5 dB

Compute: ● Fade Margin ○ Distance ○ Tx Power

Units: ● miles ○ km

Output

Fade Margin: -4.9 dB

Free Space Loss: 113.5 dB

Rcv Signal Strength: -77.9 dBm

Cable Loss Calculator

Input

Cable Type: LMR400

Loss per 100 ft: 10.8 dB
(at 5800 MHz)

Cable Length: 3 ft

No. of connectors: 2

Total Cable Loss: 0.7 dB

Obstructions & Line of Sight

Though some frequencies may penetrate obstructions better than others, wireless links should ideally have clear line of sight (LOS) between radios for best performance. Obstructions impact performance in three key ways:

- Absorption
- Reflection
- Multipath Propagation

When RF hits an obstruction, some of the signal is absorbed and/or reflected, reducing the level of signal reaching the receiving end. How this impacts performance depends on the material. For example, drywall and wood studs (common home and office construction materials) absorb relatively little signal. By contrast, heavy concrete, brick, and steel construction found in older buildings absorb and reflect much more power, resulting in high attenuation.

Multipath is a partial reflection of the signal from its intended path, resulting in it being received out of sync with the stronger non-reflected transmission, reducing link quality. Highly reflective surfaces such as water and glass, as well as foliage, are prone to multipath propagation even at shorter ranges.

Frequency Selection

Frequency impacts wireless performance in two ways:

- Throughput: Simply put, the higher the frequency, the higher the maximum theoretical throughput. High frequency radios may easily transmit 1 Gbps speeds, while lower frequencies are limited to 2-5 Mbps.
- Penetration: Due to their larger wavelength, lower frequencies are better able to penetrate and overcome partial or total obstacles. Low frequencies (900 MHz, 2.4 GHz, etc.) may function in non-line of sight (NLoS) applications, while 20 or 40 GHz high frequency radios may see performance degraded by rain or fog due to moisture in the air.

Because of this, users must carefully consider the maximum required throughput, obstacles in the wireless transmission path, how they may possibly be overcome, and how critical potential outages may be.

These are the frequencies typically in use in surveillance systems:

2.4/5.8 GHz

These frequencies are unlicensed, free for use by anyone, and most often used in typical surveillance applications such as connecting cameras across a parking lot, between two buildings, etc. Throughput varies depending on transmission technology and number of radios (see MIMO, below) used, but is typically in the range of ~25-40 for single radios, and 150 or more for MIMO models.

However, these two bands are also used by 802.11 (a/b/g/n/ac) networks in use in homes and business, increasing the potential for interference. 5.8 Ghz was previously more common in surveillance as it was less crowded than the 2.4 band, but with 802.11n (and now 802.11ac) access points common in both home and commercial settings, its advantage has been greatly reduced.

2.4 GHz may be used in shorter or lower throughput non-line of sight applications, as it may penetrate obstacles such as light tree cover. However, 5.8 GHz generally requires line of sight.

Additionally, 2.4 and 5.8 GHz are less able to penetrate obstacles than lower frequencies, making line of sight (LOS) key when deploying radios in these bands. In professional video surveillance, 5.8Ghz is more frequently used than 2.4Ghz as it is relatively less crowded.

900 MHz

900 MHz is the most common non-line of sight frequency, and is most often used when cameras do not have a clear view of the base station, such as parks or other areas with foliage cover.

Its lower frequency band is better able to penetrate obstacles than 2.4 or 5.8 GHz radios. This penetration comes with a tradeoff, however, as 900 MHz wireless links typically have much lower throughput than higher frequencies, as low as a few Mbps to 15-20 at maximum.

The 900 MHBz frequency band, like 2.4 and 5.8 GHz, is also crowded and may experience interference issues, as it is commonly used by many consumer products, such as wireless phones and microwave ovens.

Licensed Bands

Some frequencies of the wireless spectrum are reserved for public safety use. In the US, 4.9 GHz is regulated for this reason, and those entities (typically, but not always, government entities) wishing to deploy radios in this band must apply for use. Other governments may reserve different bands.

Because the government restricts who may use the 4.9 GHz band and on what channels in each area, interference issues are lessened compared to unlicensed frequencies. Because it is restricted to public safety use, it is most often seen in city surveillance, used by police and other emergency personnel.

Other Available Frequencies

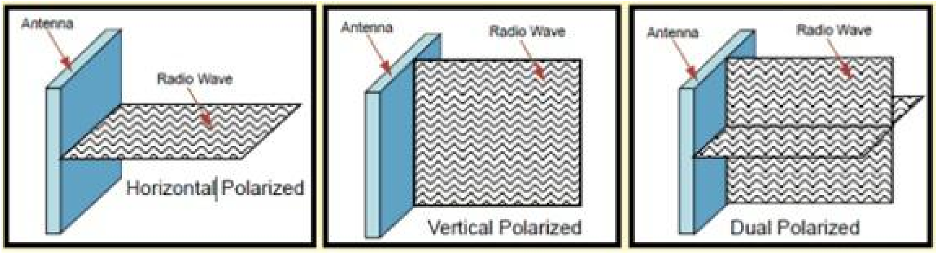
There are two other types of radios which see limited use in surveillance:

- TV white space: A recent development in wireless, TV white spacefrequencies were first opened up to wireless network use in 2010. These radios use frequencies in the VHF/UHF range which were vacated in the switch from analog to digital broadcast TV. Since they use lower frequencies (between 54 and 806 MHz), white space radios are better able to penetrate obstacles, but throughput is lower than even 900 MHz, topping out at about 16 Mb/s in currently available product options.

- >5 GHz: Wireless radios are also available in a number of frequency ranges above 5.8 GHz, such as 10, 40, 60, or 80 GHz, with high bandwidth capacity, commonly up to 1 Gb/s. These frequencies are much more susceptible to interference due to environmental conditions such as rain, snow, and fog, however, and are generally not used in surveillance because of this.

MIMO Radios

MIMO, short for Multiple In Multiple Out, spreads radio signal across two or more paths to increase bandwidth and resistance to interference. MIMO radios may use two or more distinct antennas, or more commonly a dual-polarized antenna, which transmits both of these signals at once, with the beamwidths rotated 90 degrees. This image illustrates single versus dual-polarized antennas:



Bandwidth Planning

Environmental and site conditions may impact bandwidth significantly, especially as frequencies increase. 5.8 GHz frequencies and below are generally not affected by any but the most severe weather, such as heavy snow or torrential rain. Frequencies above this, however, may be impacted greatly, and thus should not be used for critical surveillance links. Aside from weather, slight changes in site conditions, such as foliage growing into the path of transmission, or antennas shifting slightly may cause intermittent issues, decreased bandwidth, or complete loss of link.

Manufacturer Bandwidth Claims

Be careful about manufacturer bandwidth claims. As a general rule of thumb, discount specified bandwidth levels by 50% to 75% when estimating potential for real world surveillance use. The good news is that even with such caution, wireless bandwidth even for a single HD camera (~2-8 Mb/s) is generally easy to deliver on a dedicated PtP link. However, as wireless video systems get bigger and more complex, more careful estimation and testing becomes critical.

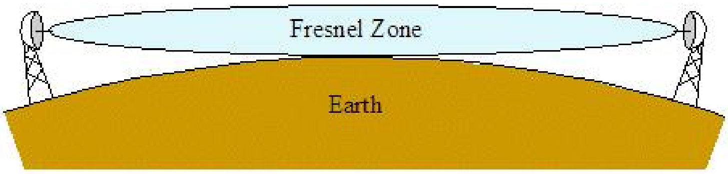
Transmission Range

There are no hard and fast rules for transmission range in wireless networks. Distances are affected by issues such as obstructions, frequency used, transmission power, and antenna gain.

In typical installations where line of sight is possible, such as parking lots, distance is not much of a challenge when standard antennas in PtP or PtMP configurations.

However, while multi-mile wireless links are easily possible with the right equipment, many users will find the calculations required in these scenarios challenging, and novice users should seek assistance from the manufacturer or experienced integrators.

Additionally, the longer the link, the more precise antenna alignment must be, making installation more difficult. Multi-mile links even must take the curvature of the earth into account, as it may become an obstacle to wireless transmission at long ranges, as seen here:



Wireless Products for Video Surveillance

Since cameras rarely have built-in wireless, typically surveillance systems will use specialist wireless equipment instead of trying to connect to a home or SMB wireless router.

In the 2000s, there was a lot of money and interest in mesh networking but the high cost ($3,000+ per link was common) and complexity has relegated that mostly to high-end, complicated projects. Most wireless surveillance users typically deploy PTP or PtMP systems, generally with lower cost systems (Ubiquiti is the most common). For more on wireless product preferences, see: Favorite Wireless Video Surveillance Manufacturers.

Maintenance

Because wireless links are sensitive to fluctuations in site conditions, routine maintenance is a key concern in any deployment. Antenna alignment should be checked, connectors should be checked for corrosion, foliage in the path of the link should be trimmed, and more. We examine these issues in-depth in our Wireless Surveillance Recommendations.

Remote Network Access

Remotely accessing video is difficult for 3 reasons.

- Private Networks: Almost all video surveillance uses private IP addresses, that are by definition, not accessible directly over the public Internet.
- Firewalled: Most video surveillance systems are firewalled and blocked from direct access to the public Internet.
- Dynamic Addressing: Many home, small business and remote locations use dynamic public IP addresses, so even if you could reach the private network through the firewall, the risk remains of the public IP address changing and disrupting access.

Five Remote Access Options for Video Surveillance

We explain how the five most common remote access options for video surveillance work:

- Port forwarding
- Universal Plug and Play (UPnP)
- Dynamic DNS
- Virtual Private Networks (VPNs)
- Cloud / 'Phone Home' (e.g., Hikvision EZVIZ, Axis AVHS, Nest Cam)

(Related: Network Addressing for Video Surveillance Guide and Converged vs. Dedicated Networks For Surveillance).

Cyber Security Is Critical

Before putting any surveillance system on the internet, it is critical that users understand the risks involved. Several major vulnerabilities have been reported, in major manufacturers' cameras, including:

- Hikvision Cloud Security Vulnerability: A critical vulnerability in Hikvision's global cloud servers allowed an attacker to remotely take over the server and get access to sensitive customer data.
- Axis Critical Security Vulnerability: A vulnerability allows attackers to remotely initiate a telnet connection, allowing the attacker to take over the device, reboot it, power it down, etc.
- Hacked Dahua Cameras Drive Massive Cyber Attack: As part of the Mirai botnet, hacked Dahua cameras (and others) took down major internet sites and even an entire country.
- Sony IP Camera Backdoor Uncovered: Attackers can remotely enable telnet on cameras, combined with a hard coded backdoor account which allows users to take over the device.

See our Directory of Video Surveillance Cybersecurity Vulnerabilities and Exploits for more information on these and other issues, including new ones as they occur.

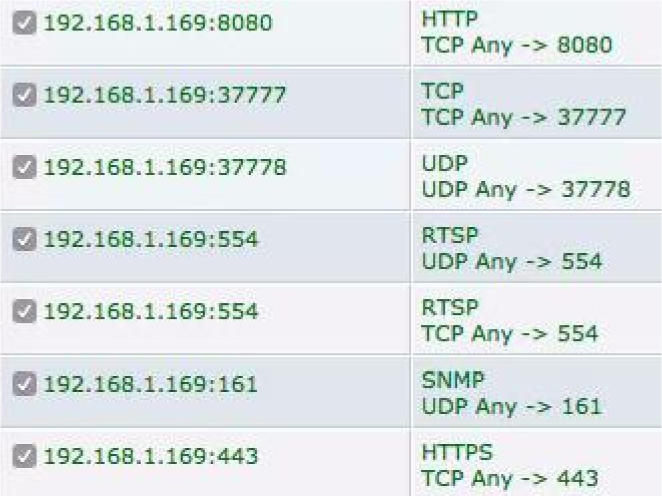
Because of the severity of these incidents and their increasing frequency, it is critical that users understand the basics of cyber security for surveillance systems, and how to protect against simple attacks at the very least.

We strongly recommend reviewing Network Security for IP Video Surveillance before proceeding.

Port Forwarding

Port forwarding maps the private IP address of the recorder or IP camera to the public IP address of a user's router so that it can be remotely accessible. Doing so requires router configuration changes complicated enough that most networking novices will struggle doing it correctly.

To access a camera or recorder, ports 80 (HTTP) and 554 (RTSP video streaming) are most often used and most often opened. Some systems require additional ports to be opened for configuration, control, or authentication, as well. For example, this image shows all the ports forwarded by a Dahua DVR in consumer router:



☑ 192.168.1.169:8080	HTTP TCP Any -> 8080
☑ 192.168.1.169:37777	TCP TCP Any -> 37777
☑ 192.168.1.169:37778	UDP UDP Any -> 37778
☑ 192.168.1.169:554	RTSP UDP Any -> 554
☑ 192.168.1.169:554	RTSP TCP Any -> 554
☑ 192.168.1.169:161	SNMP UDP Any -> 161
☑ 192.168.1.169:443	HTTPS TCP Any -> 443

Note that if multiple devices are to be viewed via the internet, different external ports must be mapped to their internal ports, as forwarding the same port to two devices results in errors.

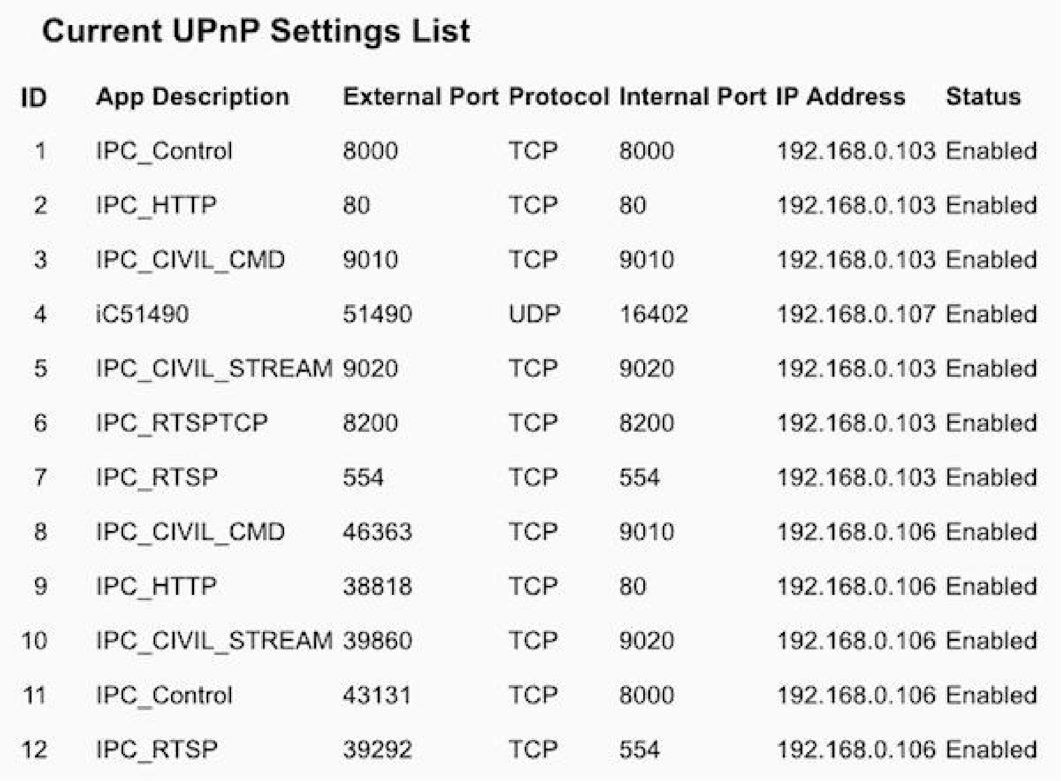
For example, if two NVRs are to be viewed remotely using IP address 145.10.234.12, and both use port 80, mappings may look like this:

- NVR1: 145.10.234.12:8080 ---> 192.168.3.8:80
- NVR2: 145.10.234.12:8081 ---> 192.168.3.9:80

Universal Plug And Play

Universal Plug and Play (UPnP) is a set of protocols which automate device discovery and configuration on a local network. One of the aims of UPnP is eliminating manual port forwarding (above), allowing a UPnP device to automatically create port mappings in a router without any intervention from the user.

For example, the image below shows UPnP port forwarding automatically triggered by three separate Hikvision IP cameras (multiple ports per camera):



Current UPnP Settings List

ID	App Description	External Port	Protocol	Internal Port	IP Address	Status
1	IPC_Control	8000	TCP	8000	192.168.0.103	Enabled
2	IPC_HTTP	80	TCP	80	192.168.0.103	Enabled
3	IPC_CIVIL_CMD	9010	TCP	9010	192.168.0.103	Enabled
4	iC51490	51490	UDP	16402	192.168.0.107	Enabled
5	IPC_CIVIL_STREAM	9020	TCP	9020	192.168.0.103	Enabled
6	IPC_RTSPTCP	8200	TCP	8200	192.168.0.103	Enabled
7	IPC_RTSP	554	TCP	554	192.168.0.103	Enabled
8	IPC_CIVIL_CMD	46363	TCP	9010	192.168.0.106	Enabled
9	IPC_HTTP	38818	TCP	80	192.168.0.106	Enabled
10	IPC_CIVIL_STREAM	39860	TCP	9020	192.168.0.106	Enabled
11	IPC_Control	43131	TCP	8000	192.168.0.106	Enabled
12	IPC_RTSP	39292	TCP	554	192.168.0.106	Enabled

However, in practice, UPnP is unreliable in many cases. In many business networks, large and small, UPnP functions are turned off, requiring manual port forwarding. In consumer use, port mappings may not function properly, may be added more than once, may conflict with other devices, or may simply not be added at all. Making things worse, error information is rarely available when UPnP port mapping fails, leaving the user without any means of troubleshooting.

Because of these reasons, manual port forwarding has proven more reliable in commercial surveillance, with UPnP typically left to consumer use.

Dynamic DNS

Typically, ISPs do not provide static IP addresses to residential and small business accounts (without an additional charge), so over time, the public IP address assigned to them may change. For example, the public IP address of your house may be 84.32.34.111 today but tomorrow it could be 84.32.34.119. If your remote video client is configured to connect to 84.32.34.111, tomorrow it would fail.

Dynamic DNS services resolve this IP address to a simpler hostname, e.g. Site2-NVR3.dyndns.org instead of 10.132.4.3. The DDNS service updates the IP address corresponding to each hostname periodically, or automatically detects changes and updates immediately in some cases.

In surveillance DDNS is most commonly used with DVRs/NVRs. Many manufacturers host their own private DDNS services free to users who purchase their equipment (though Hikvision no longer does), and many, if not most, modern DVRs include a built-in DDNS client, used to keep the device's IP address up to date.

DDNS is rarely used to connect individual cameras to a VMS, since the device failing to update its IP address upon a change will render it unreachable, resulting in lost video and requiring a site visit to repair.

Dedicated Virtual Private Networks

The most common option historically for larger organizations to connect remote cameras and sites is a dedicated VPN, typically using hardware appliances (such as SonicWall or Cisco firewalls) located at each site. This appliance creates a tunnel through the internet to the server location, effectively creating a single video network, despite being in disparate locations.

In surveillance, dedicated VPNs are generally used only used in larger multi-site installations. VPN appliances have historically cost $300-500 per site, though prices are dropping, with some options dropping to $100 or less. However, VPN configuration is beyond the expertise of many/most surveillance techs, making it less common.

Cloud / 'Phone Home'

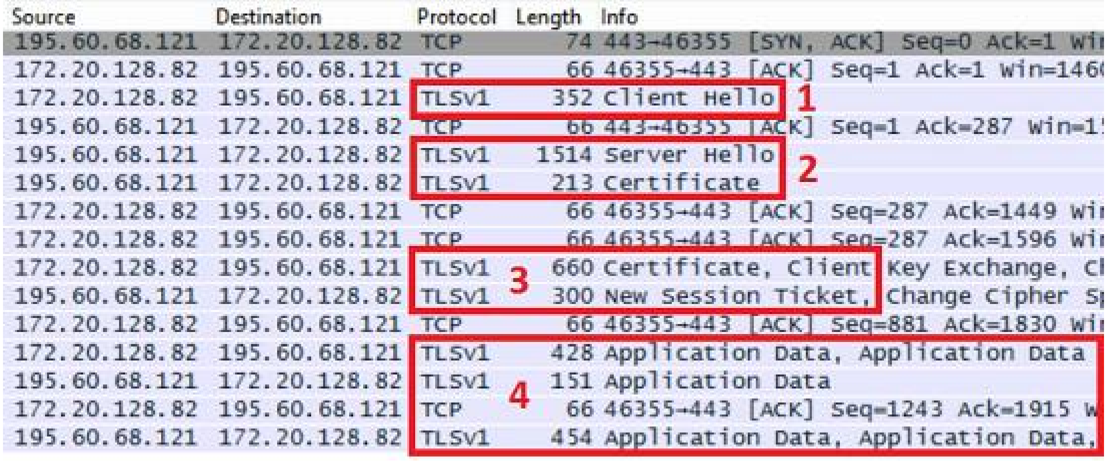
To eliminate the complexity and potential for errors involved in manual port forwarding, UPnP, and Dynamic DNS, cloud connections have become more prevalent. Cloud connections are a form of VPN (sometimes called application specific VPNs) which requires limited or no user interaction to configure.

Several manufacturers offer their own cloud platforms, such as Axis Companion, Hikvision (Ezviz / Hik-Connect), Dahua Easy4IP, FLIR Cloud, and more. Consumer/Internet of Things cameras and security/home automation systems typically also use this type of connectivity, such as Nest Cam, Samsung SmartCam, Canary, or Scout.

Cloud connections are generally made via a secure TLS (transport layer security, an encryption protocol) tunnel, set up via these basic steps (noted on the image below):

1. Initiating device sends a HELLO message to request a connection.
2. Server sends HELLO along with a security certificate.
3. A handshake is performed and a secure tunnel is set up.
4. Once the TLS tunnel is in place, data sent through it is encrypted, with protocol and data specifics obscured (shown only as "application data" in the example below).

Below is a Wireshark trace for an Axis camera with AVHS enabled:



```
Source          Destination     Protocol  Length Info
195.60.68.121   172.20.128.82   TCP           74 443→46355 [SYN, ACK] Seq=0 Ack=1 Wi
172.20.128.82   195.60.68.121   TCP           66 46355→443 [ACK] Seq=1 Ack=1 Win=146
172.20.128.82   195.60.68.121   TLSv1        352 Client Hello
195.60.68.121   172.20.128.82   TCP           66 443→46355 [ACK] Seq=1 Ack=287 Win=1
195.60.68.121   172.20.128.82   TLSv1       1514 Server Hello
195.60.68.121   172.20.128.82   TLSv1        213 Certificate
172.20.128.82   195.60.68.121   TCP           66 46355→443 [ACK] Seq=287 Ack=1449 Wi
172.20.128.82   195.60.68.121   TCP           66 46355→443 [ACK] Seq=287 Ack=1596 Wi
172.20.128.82   195.60.68.121   TLSv1        660 Certificate, Client Key Exchange, Cl
195.60.68.121   172.20.128.82   TLSv1        300 New Session Ticket, Change Cipher S
172.20.128.82   195.60.68.121   TCP           66 46355→443 [ACK] Seq=881 Ack=1830 Wi
172.20.128.82   195.60.68.121   TLSv1        428 Application Data, Application Data
195.60.68.121   172.20.128.82   TLSv1        151 Application Data
172.20.128.82   195.60.68.121   TCP           66 46355→443 [ACK] Seq=1243 Ack=1915 W
195.60.68.121   172.20.128.82   TLSv1        454 Application Data, Application Data,
```

Though shown only as "Application Data" above, once the tunnel is set up, typical protocols such as HTTP(S), RTSP, TCP, UDP, etc., are used for camera control and streaming.

Cloud / 'phone home' connections are the easiest and most reliable overall to provide remote access to home and small business. However, for corporate or business users, IT administrators may be concerned about allowing these devices to 'get around' their firewalls.

Push To Move To Cloud

While DDNS and port forwarding have been popular for years, there has been a push to move to cloud services in the past year, at least in part due to the increase in exploits and cyber attacks.

The best example of this is Hikvision's discontinuation of their free HiDDNS service, forcing users to move to their Hik-Connect cloud platform or a third-party, typically paid, DDNS. Unfortunately, this change was made with little warning, contradictory documentation, and uninformed tech support, leading to much confusion about when services would be discontinued or how new features would work. See our report Hikvision Discontinued 'Migration' Tested for more information.

Also note that while cloud services may be more secure as video and other data is transferred via secure tunnel, security is moved from the control of users to the manufacturer/developer providing the service, as well as those providing hosting services. This means that, for example, if Hikvision's EZVIZ service, Dahua Easy4IP, or Nest are breached, all users of the service are likely to be impacted, instead of more limited numbers normally associated with targeted hacks.

UPS Backup Power

Backup power for surveillance systems generally rely on batteries, especially since UPSes for computers are common and easily available.

However, uncertainty in picking the right backup power supply sized with the right batteries is a common problem, and the pitfalls of poor selection stretch beyond just having a weak system.   In the note, we look at battery backup, the most common method for surveillance power backup.

We examine:

- UPSes run time delivered
- Understanding UPS power units of measure
- How to calculate surveillance system wattage
- Using runtime graphs to determine supply duration
- How much backup runtime is needed
- Common factors affecting runtime
- Why consumer UPSes often are too weak
- Why battery equipped power supplies may not be enough
- Why commercial UPSes are often the best choice
- Using generators for longer runtimes

UPS = Runtime Less Than 2 Hours

As a general rule of thumb, unless you are going to deploy huge arrays of batteries, providing runtime of days for even a small surveillance system (say 100W) is not feasible with UPSes, which are almost always designed run for a few hours or less. Typical runtimes last from a few hours to tens of minutes. The rationale is because UPSes are designed to bridge gaps in the main supply, not to replace them for days on end.

Generators For Longer Time

For backup power lasting more than an hour or two, generators should be used. For more on generators, see Generator Backup Power for Surveillance.

UPS Power Units of Measure

Calculating power can be confusing unless basic units are defined. For UPSes, three basic units are used to establish the relative size and runtime of a UPS.

Watts: For a general idea of how much power a devices needs, Watts are used. This power unit normalizes voltage into the figure, so comparing devices that run at 12 VDC or 110 VAC can be done with no conversion. Watts does not offer an idea of demand over time, but demand at a moment. UPSes often express output power in Watts, and some finders offer the option to search products using it like this example Tripplite calculator. Specific examples include this APC 500W unit, Tripp-lite 540 W unit, and CyberPower 900W unit. Despite being one of the more useful ratings for selection purposes, the wattage rating is not often the leading power value in product designations and may be buried in the tech specs.

Volt/Amps (VA): Many UPSes express power capacity with Volt Amps, which is an alternative power unit. However, the unit is typically limited to describing DC outputs only (it does not apply accurately to AC reactive loads) while most UPS powered devices like servers, switches, or NVRs use

AC. UPSes use this term often to describe the capacity rating of their internal batteries, which are DC, but the full amount of power they claim is typically not available due to losses. The actual wattage available for backup power use will be less than the theoretical VA rating of the unit. Most UPSes use VA as the primarily capacity attribute, like this APC 350 VA unit that provides 200 W, this Tripp-lite 1500 VA unit that provides 900 W, and this CyberPower 1350 VA unit that provides 810 W.

Watt/Hours (Wh): For a measure of power over time, other units like Watt/Hours are needed. Simply defined, 1 Watt Hour supplies 1 Watt over 60 minutes. UPSes do not provide this value as a spec sheet number because their capacities are almost always less than an hour and demands are often dynamic. Instead, they include Runtime Charts or Graphs that help establish how long a given device supplies power at a given watt load.

To establish how much time a UPS can supply backup power, total system power demand must be calculated first:

System UPS Calculation

The total system wattage combines the power needed by all system components, including cameras, switches, and recorders or servers. The calculation of total wattage follows this formula:

(Number of cameras * Watts consumed by camera) + (Power used by recorders) + (Switch Power)

So for an example small system using 8 cameras, an NVR appliance, and an 8 port switch:

(8 cameras * 6 W) + (70W NVR) + (1.5W Switch) = ~125 W total

System Wattage vs. UPS Wattage

Though device loads and UPSes are both frequently described with the same unit, watts (e.g., an NVR might need 30w or 70 watts, etc. and a UPS might be rated for 300 watts or 700 watts, etc.), these cannot be easily related. For example, a 30 watt NVR connected to a 300 watt UPS will not run anywhere close to 10 hours, even if one (wrongly) assumes UPS wattage can be divided by device wattage.

In practice, runtime / backup time is generally quite short. For example, this 900W unit can only run a 900W load for ~5 minutes and a 450W one for ~14 minutes.

You must check the UPS runtime graph / chart to determine how long of backup the UPS will provide.

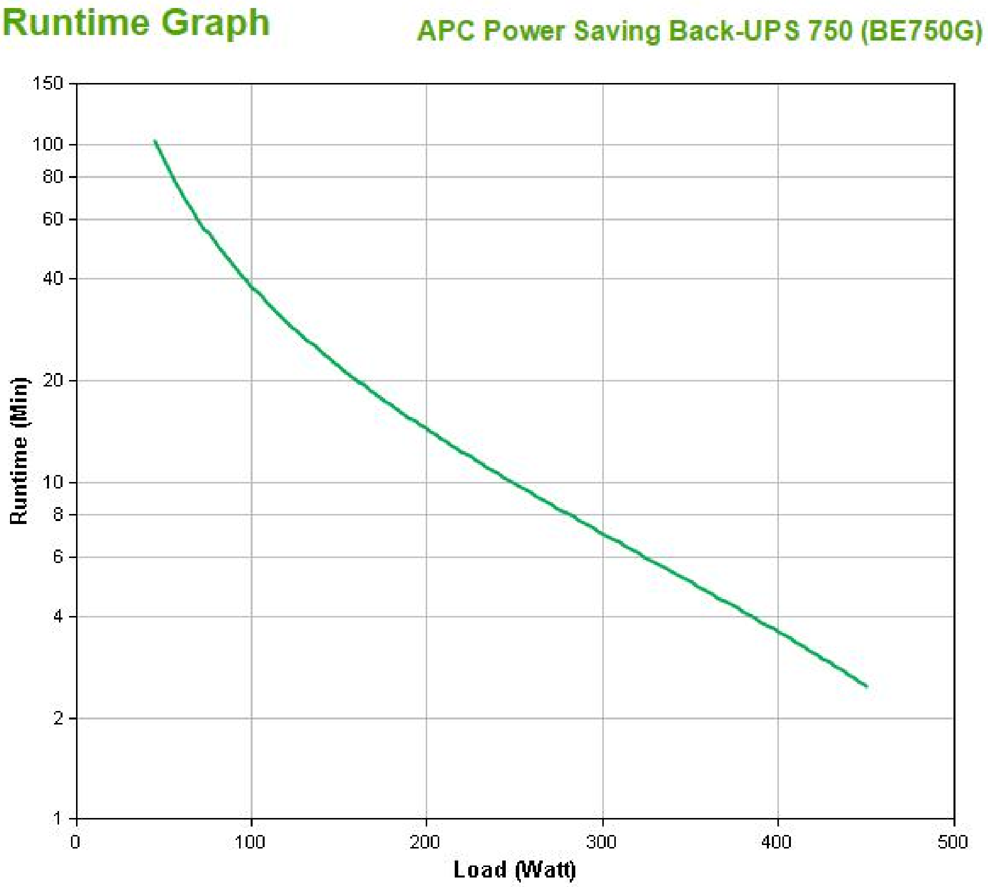
Runtime Graphs / Chart

Runtime graphs (or charts) show how much backup time a given UPS will deliver for a given load.

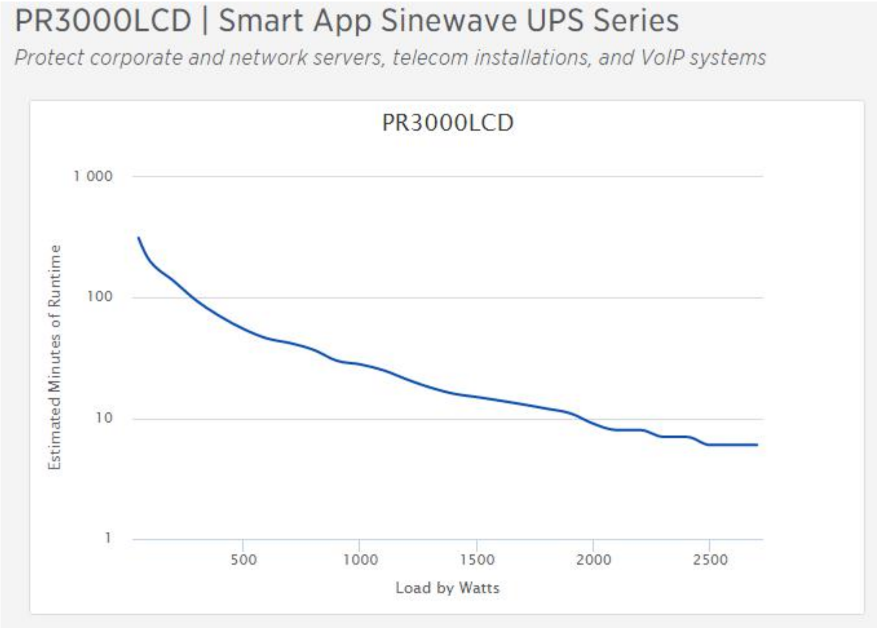
Some UPSes are designed to be more efficient at delivering low wattages, others are more efficient at higher values.   Other UPSes are just designed to be cheap to purchase, so buying UPSes based on Wattage or VA ratings alone is a mistake. The battery types and number of batteries affect the total runtime abilities of a UPS, resulting in mixed UPS mixed performance. Instead, the Runtime values will display performance in a usable way.

Once total demand wattage is known, a Runtime Graph will help pin down how much battery capacity is available for how long. UPS manufacturers typically express power runtime as a curve for system watt load, like the examples below:

Example A:



Example B:


PR3000LCD | Smart App Sinewave UPS Series

Protect corporate and network servers, telecom installations, and VoIP systems

These graphs display how the load variation affects minutes of battery power. For example, for UPS Example A, a load of 50W will last approximately 100 minutes, but a maximum 450W load will last ~3 minutes. For UPS Example B, a 50W loads will last over 300 minutes, a 450W load will last ~60 minutes, and a maximum 2700 W load will last 6 minutes.

While most manufacturers publish unit runtime charts, if they are not available for a UPS unit, then battery runtime calculators from the manufacturer (or white label reseller) are an equivalent alternative.

Once total power demand is known, finding the right backup source can be selected. Battery backups are typically available in three different types:

Consumer UPS Options

The most common battery backup are small battery equipped surge protectors, typically designed for general office use, and are designed to plug into 120VAC wall outlets. However, these units typically are not

built with enough battery power to run attached devices for more than a few minutes and are not good solutions for surveillance systems.

Take this example 450W consumer-grade UPS, for our surveillance system using 125W, the backup power would only last around 30 minutes, which could be too short to be useful depending on typical outage durations. These units are not always field serviceable, and even routine maintenance like battery replacement is not always an option. Some consumer units are instead designed as disposable.

Price

Consumer grade UPS units are frequently available between $100 - $500 for most battery configurations, with the biggest units typically sized for 1000W or under.

Battery Backed Power Supplies

Another surveillance system ready option are traditional low-voltage power supplies equipped with batteries in the enclosure. This option usually is useful to non-PoE powered cameras only, since only low voltage hardwired cameras are wired to them.

Product lines like the Altronix ReSurv or LifeSafety Power Helix are designed specifically for surveillance camera use, with 12/24V individually fused outputs in a locking can. However, these power supplies are useful only for camera power and other system components like switches and recorders need additional backup power sources.

Price

Battery backup power supplies are typically the most cost efficient way to add batteries to non-PoE cameras. While a typical 8 - 12 channel power supply can cost $175 - $200, this is only ~$40 - $80 more expensive than typical non-battery equipped equivalent models.

Commercial UPS Options

With consumer UPSes and battery equipped power supplies being undersized, bigger more capable battery backup solutions are available, but at prices well above typical consumer models.

Commercial UPSes are generally available as minitower or rackmounted units, and the physical larger footprint contains more batteries offering much longer runtimes. For example, this configuration (Tripp-Lite SU1500RTXLCD2U +1 BP48V24-2U) will run our example 125W system above for over 6 hours, or 360 min.   These units often include network monitoring tools that notify when mains power drops, batteries are weak, and general unit health checks. In general, internal battery packs can be replaced as modules for less than 30% the cost of the full device.

Commercial UPSes may not use single phase, 120 VAC 'plug-in' power, but require multiple phase or 220/240/477VAC power. Unlike consumer units that can be dropped anywhere wall power is available, commercial units typically require dedicated power circuits.

Examples of these heavy-duty UPSes are available from APC, Dell, and Eaton among others.

Price

Most commercial UPSes cost at least $500, with totals reaching thousands of dollars when extra battery units are added. While the most expensive option, these unit typically offer the longest runtimes and the most wattage.

Factors Impacting Runtime

Runtimes listed on graphs and specification sheets generally carry a disclaimer warning against shorter than expected durations. These disclaimers mention that battery life and, environmental condition around UPS can shorten times.   Here is why:

Battery Age: Over time, every battery will lose it's ability to store and regenerate a charge, due to the decay of the internal cathode and anodes. For a typical wet-cell battery, the same chemical reaction that excites electrons in a cell will eventually lose potency over time, or may even lead to the destruction on the cell itself. In most cases, the batteries inside a UPS will have a lifespan of 3 - 5 years before needing to be replaced. However, before then a battery can become weaker than what is stated on the specsheets.

Environment: Cold Batteries are characteristically less efficient than warm ones, and cells installed in semi-corrosive environments can experience conductivity problems as corrosion takes place.   If batteries are not kept in temperate, environmentally controlled areas, they can prematurely fail or operate under rated capacity. In many cases, outdoor UPSes include heating elements or pads to keep cell temperature above freezing to avoid damage and improve performance.

Temporary Loads: Camera options like IR illumination, PTZ motor movement, heaters, or blowers can drive intermittent loads that are not typical were not accounted for during estimates, and
these non-typical loads can reduce battery power times.

Extended Runtimes Need More Power

When extended runtimes (days, not hours) are needed, alternative backup power sources like generators or large capacity battery arrays are more cost effective with longer supply times and lower operational costs. See our Generator Backup Power for Surveillance note for more detail on those options.