CHOOSING THE RIGHT SWITCH FOR VIDEO SECURITY APPLICATIONS

Whether you're protecting your home or business or utilizing the time-saving benefits of video analytics, a reliable stream of high-quality video is essential.

Managed vs. Unmanaged Switches

For applications involving more than just a few cameras, you need a network to connect the digital cameras to the servers that store and analyze video data. A switch enables multiple devices to be connected onto the same network, and to control or restrict how those devices communicate, you must have the ability to configure the switch. The amount of control you have depends on the type of switch: managed, unmanaged, or somewhere in between. Examining the benefits of each switch type lets you make the right decision for your specific application.

	Managed	Unmanaged
Control	You can control traffic, network design, security, power for connected devices and more. The switch can be controlled remotely with no need for a truck roll.	Switch behavior is entirely controlled by the manufacturer. To reboot, a person must be present to power cycle the switch.
Visibility	The switch provides full reports about its state and the traffic it is forwarding. It can generate alerts if user thresholds are breached.	The switch has no way of reporting its status or the type and amount of traffic its forwarding.
Resiliency	Many features enable the switch to control network issues and recover automatically from faults. Video quality is maintained despite disruptions.	The switch has few mechanisms to handle network disruptions. This can affect video quality or sometimes cause video loss.
Trouble-shooting	The switch can diagnose faults anywhere on the network to quickly resolve issues and proactively test the network to help prevent faults from occurring.	The switch cannot report its status. Therefore, other devices or tools must be used to diagnose problems.
Installation	Requires skilled personnel for best installation results.	Since there is no configuration required, most switches are plug and play—ideal for simple setups.
Flexibility	Several features allow the switch to change behavior to suit new network conditions. Some react in real-time to save manual intervention and provide superior network agility.	With no ability to alter its behavior, the switch cannot adapt to changing network requirements. This can lead to more frequent equipment refreshes.
Security	The switch can control users, network access, detection of intruders, and block unknown devices. Some threats can be blocked before they affect the rest of the network.	The switch can't prevent an attacker from gaining further network access. This is a major issue for public video surveillance applications.
Lifetime Cost	Higher upfront cost since the switch is more sophisticated, but operating costs are lower with fewer truck rolls and remote-control ability.	Unmanaged switches are not complicated, so their cost is low. However, operating costs may be higher since control is limited.

■ Recommended   ■ Sometimes recommended   ■ Not recommended

A word about cost…

Networks last a long time and require monitoring and maintenance for best results, so in planning your budget, it's crucial to consider both the purchase price and ongoing operating costs.

Purchase Price

Unmanaged switches are generally cheaper than managed switches because they are much simpler devices. However, this simplicity means they are unable to adapt to changes, so their useful lifespan may be shorter than a managed switch.

+

Operating Cost

Unmanaged switches must be physically touched to reboot them or change their configuration, which requires skilled engineers onsite. Travel costs, time and business disruption can be unwanted side effects of waiting for fixes. In contrast, managed switches can be remotely controlled, so changes can be made quickly with minimal cost and disruption.

=

$ Total Cost of Ownership (TCO)

Combines purchase price and operating cost over the long term, and can be lower with a managed switch, particularly if the switch is in a remote or hard-to-access location. Additionally, managed switches improve business agility because they can adapt to new requirements and take advantage of new opportunities.

So, how do you choose the right switch for your application?

The table below is a quick guide to the best switches to consider for different applications. An Allied Telesis WebSmart switch has some management ability, and can be a good compromise where a fully-managed switch is not ideal.

	Managed	**Websmart**	**Unmanaged**
Small (Less than 20 cameras in one location)	Managed switches give the most control and visibility and are preferred if the location is difficult to access.	Websmart switches are easy to set up, yet allow some remote management and monitoring functions.	Good option for easy plug and play setup. Switch should be accessible, and cameras securely located.
Medium (Up to 100 cameras in one location)	Best option if the network is not in a secure location, for example a shopping mall, public building or outdoor carpark.	Good for easy install with some remote troubleshooting ability for faster issue resolution.	Only use if all switches are accessible and all cameras are in a secure location.
Large (More than 100 cameras, or several locations)	Best choice for mission critical applications and those in remote or insecure locations. Lowest long-term cost.	Good option if budget is a priority, however network visibility and control limitations may add to operating costs.	Not recommended.

Why use Allied Telesis managed switches in your video surveillance network

Allied Telesis Autonomous Management Framework™

AMF is an intelligent automation tool that simplifies remote network management and lowers operating costs. It's ideal for distributed applications such as video surveillance because no skilled resources are required at the edge of the network, where the bulk of time and operating costs are spent.

Virtual Chassis Stacking™ (VCStack)

Surveillance networks must have a steady stream of high-quality video, which increases demands for high performance and reliability. VCStack ensures your network core performance, even if power outages or link failures threaten network disruption.

Advanced Security Features

Security is a paramount concern for networks that exist outside secured buildings. Our managed switches can detect and defeat attackers before they can disrupt operations, by scanning for threats and continuously blocking unauthorized access attempts.

Power over Ethernet (PoE)

For easier management and simplified installation, security cameras are usually powered from the network switch using PoE. Managed switches allow the user to control the flow of power to the camera, which is useful if a reset is required because it can be done remotely without the need for a truck roll.

Continuous PoE (CPoE)

Allied Telesis innovative CPoE allows power to be supplied to the camera while the switch reboots—usually a reboot causes the power to stop. This is ideal for $24/7$ surveillance operations where software updates can cause major disruption. With CPoE, the camera does not lose power and can store video locally during switch reboot, so nothing is lost

Loop Detection

In any network, loops must be avoided because they can create uncontrollable "storms" of traffic that block all other traffic. Loop Detection rapidly detects and shuts down any loops. A common feature in managed switches, this is also included in Allied Telesis unmanaged switches, because loops are easy to accidentally create and can be devastating to an unmanaged network.

» Try the Switch Selector at **http://bit.ly/MvUSwitches** to find the perfect model for your application.

Allied Telesis

NETWORK SMARTER