www.mayflex.com

White Paper

Understanding Ethernet switching for security professionals

Infrastructure.
Networking.
Electronic Security.

All together.

MAYFLEX

+ Introduction.

Understanding Ethernet switching for security professionals is designed to help the security installers who are already familiar with the traditional transmission methods used in analogue CCTV systems to understand the area of Ethernet switching and data transmission in network based CCTV systems.

+ What is Ethernet?

Ethernet is a technology that is used in local area networks (LAN) introduced in the early 1980's for interconnection of PC's and other office equipment. It became officially standardised in 1983 with the introduction of the IEEE 802.3 standard.

Security installers will be familiar with the transmission of video images in analogue CCTV systems over point to point cabling. However, with the move to IP based systems there is no longer a need to install separate cabling as the images are converted into data at the camera and transmitted across an Ethernet based network.

Ethernet uses a star topology which means individual cameras can be connected to the network via wired transmission cabling mediums. Wired mediums are typically twisted pair or fibre optic. A twisted pair cable consists of four pairs of twisted copper and is used with RJ-45 connectors which can transmit up to 100 metres to a localised Ethernet switch. Whilst fibre connections can operate over much longer distances of up to 70 km before they need to be connected to a switch.

There are three main types of Ethernet LAN technologies called Fast, Gigabit and 10 Gigabit.

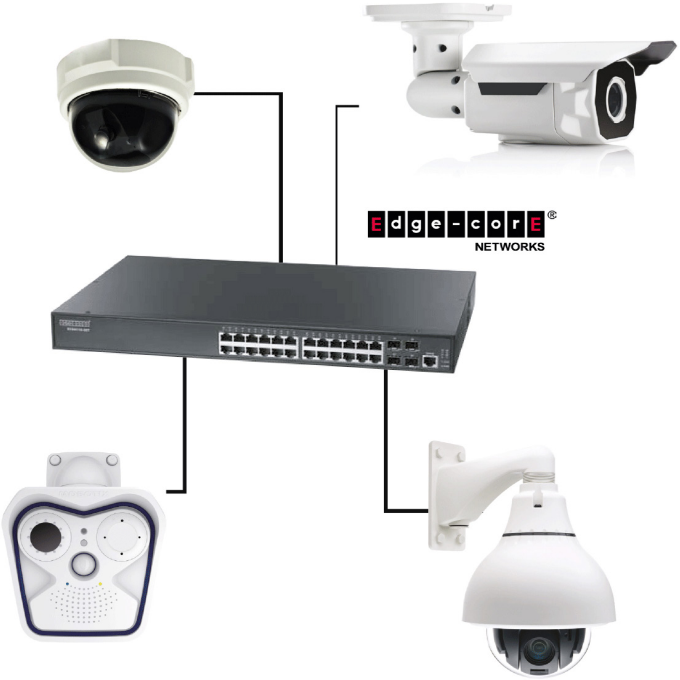
Fast Ethernet.

The Fast Ethernet standard (IEEE 802.3u) has been established for Ethernet networks that need higher transmission speeds. This standard raises the Ethernet speed limit from 10 Mbps to 100 Mbps with only minimal changes to the existing cable structure. Cabling is based on a twisted pair cable network made up of Category 5e cable with fibre optic cable often providing the backbone. Depending on what else is installed on the network a fast Ethernet network should provide the necessary bandwidth for smaller network video applications. However, when deploying PoE it may be necessary to consider and investigate the use of Category 6 cabling.

Most security devices connected to a network, such as a network camera, have 10BASE-T/100BASE-TX connections to enable them to be installed onto a LAN.

Gigabit Ethernet.

Gigabit Ethernet was developed to meet the need for faster communication networks with applications such as multimedia and Voice over IP (VoIP). Gigabit Ethernet runs at speeds 10 times faster than 100Base-T (1000Base-T).



Gigabit Ethernet, which can also be based on a twisted pair infrastructure or more commonly fibre optic cable, delivers a data rate of up to 1,000 Mbit/s (1 Gigabit/s) and is becoming the standard in new builds.

Typically used as an enterprise backbone. Existing Ethernet LANs with 10 and 100 Mbps cards can feed into a Gigabit Ethernet backbone to connect to switches, routers and servers

10 Gigabit Ethernet.

10 Gigabit Ethernet is the fastest Ethernet standard and provides a rate of 10 Gbit/s. It is based on either Category 6A or a fibre cabling network. 10 Gb Ethernet can easily be deployed within existing networks, providing a cost-effective technology that can support high-speed, low-latency requirements.

The IEEE 802.3ae standard allows for distances between locations of 4 kilometres over single mode fibre. Shorter distances of up to 4 kilometres can be achieved using a multi-mode fibre.

+ Ethernet switching.

Ethernet switches connect together the CCTV cameras with other devices on the LAN. These connections are made via the structured cabling network over which the switch sends communications from one port to another. The number of ports can range from 4 to 48 depending on the application.

There are three types of switches used in security applications: unmanaged, partially (Smart) managed and fully managed.

Unmanaged Switches.

These are essentially plug and play switches which can be used on smaller systems and provide layer 2 switching and connectivity. They are simple to install and only require power to be operational. They come in 4 – 48 port versions and all the installer needs to do is to plug in the cameras and enter the appropriate password to gain access to the cameras.

Partially Managed Switches (Smart Switches).

Partially managed switches are slightly more to buy but offer additional features over and above the unmanaged switch. The installer can control port bandwidth, and create workgroups such as Quality of Service (QoS) and create VLAN's (Virtual Area Networks). Once a camera is installed onto a partially managed switch the communication is enabled and the installer has control over the configuration. They are useful if the installer wants to segregate different portions of his network and needs a little more information about the health of his network via a browser based interface.

Since these types of switches offer certain levels of management but are not as capable as fully managed switches it is recommended that they are used at the edge of the network or as the infrastructure for smaller – medium sized CCTV networks.

Fully Managed Switches.

These are the most expensive switches to use but have more functionality to them than unmanaged or partially managed switches. They deliver a comprehensive amount of features and the highest levels of security and offer more control over the features such as port bandwidth, security, and increased QoS and VLAN set up. These switches must be installed by a qualified network engineer to optimise the set up and would be installed at the core of a system.

Key additional features of fully managed switches include:

- Protect themselves and the network from deliberate or unintended Denial of Service attacks
- Have built in protection of the data plane and control
- Extensive VLAN capabilities that secure users and isolate devices
- Greater scalability
- Multiple ways of managing the switch

Port Forwarding.

Port forwarding is way of making a camera on a network available to a viewing station outside of the site it is installed on. Even though the network is behind a router. Its commonly used for video surveillance applications and remote viewing.

To remotely access cameras that are installed within a building on a LAN the user needs to access via the IP address of the router that connects the site or building to the internet. This router can be configured to associate an HTTP port number to a cameras IP address and an HTTP port. This process is called port forwarding.

Port forwarding works when the incoming data arrives at the router's external IP address along with its specific port number. The router then forwards the data to a specific device on the LAN. The router achieves this by replacing the sender's address with its own internal IP address. With outgoing data, such as remote video viewing the reverse happens and the video data is sent out over the Internet to its destination for storage and viewing.

+ Bandwidth.

With larger systems it is important to consider the issue of bandwidth. Ways to manage bandwidth requirements include:

1. Optimising camera set up
2. Using VLANs
3. Quality of Service

1. Optimising camera set up.

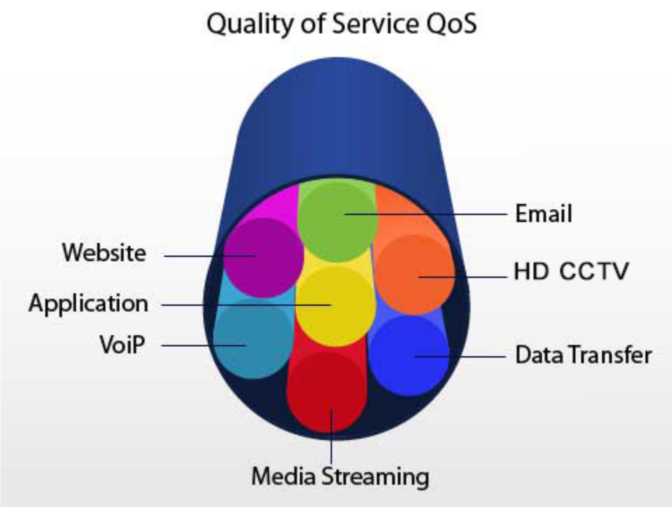
The settings of the IP cameras on a system dramatically affect the bandwidth usage. So It is very important to optimise the key settings of the cameras for picture quality, storage and bandwidth optimisation. For example, a 2 Megapixel camera will use approximately 6 MB of bandwidth at 25 frames a second whereas the same camera at 15 frames a second will only use 4 MB.

Some of the key camera settings include:

+ Video Compression
+ Streaming Mode
+ Frame Rate
+ Resolution
+ Video Quality

Of these settings the one which impacts bandwidth the most is the video compression format being used. The most common video compression formats in IP video cameras are: H.264, MPEG-4, MJPEG, MPEG-2, Wavelet and JPEG2000. Each of these compression formats have positive and negative features which are covered in a previous paper and the final decision of selecting one compression format over another is normally based on: Latency, Image quality, Storage requirement and the number of cameras on the system.

Of the main formats MPEG-4 and its successor, H.264, are the most efficient in terms of compression in terms of bandwidth utilisation and are usually the best choice when it comes to reducing storage requirements and optimising bandwidth without dramatically impacting video quality.



2. VLANS.

When installing a network based video system it is often the case that the IT department wish to segment the bandwidth intensive video on to a separate network in order to reduce the impact of bandwidth on other parts of the core network, which carry the main functions of the business.

This is achieved by installing a VLAN which is a “virtual” LAN, consisting of a number of devices which communicate privately on separate networks. To achieve this the network switches must be built on smart or managed Ethernet switches. Unmanaged switches cannot be used to create Virtual networks as they do not have the functionality or the graphical user interface to control them.

VLAN is a method for segmenting a network virtually and is achieved by splitting networks into logical groups where users in a group exchange data across the network. On a VLAN only devices within that VLAN can communicate with each other and access the network cameras.

So in summary the use of VLANs enables the logical grouping of camera devices, reduces the traffic on the network and therefore reduces bandwidth use. This means that using VLANs is often the preferred method used for video surveillance applications on data networks. An additional advantage of VLAN’S is that sensitive security applications can only be accessed by other users on the network which improves security by reducing the possibility of an unauthorised person gaining access to the video images.

3. Quality of Service.

The original design concept for LAN's was that all traffic was treated equally. This meant that all network traffic regardless of application used resources equally from the network and each user on the network had no guarantee of reliability or prioritised connectivity to the LAN.

The reality of course is that different applications such as video, VOIP and e-mail are all using the same network which means there needs to be control in how the network prioritises its resources.

This is achieved by using Quality of Service (QoS) which enables different network applications to co-exist on the same network without consuming each other's bandwidth.

Quality of Service (QoS) for networks is a set of standards used to ensure high-quality performance for critical applications such as security surveillance. Network administrators use QOS to manage resources on their networks to ensure the optimal level of service is delivered to all users for all applications on the network. The prerequisite for the use of QoS within a video network is that all switches and routers must support QoS.

Quality of Service, (QOS) is achieved by programming the smart switches to identify the type of content in a data packet and then prioritise this content according to pre-defined rules before forwarding the data on from the switch.

+ Summary.

The installation of a network based CCTV system can be a frustrating one for an installer more familiar with analogue technology and DVR based recording. However, it does not need to be complicated if the installer has built up his knowledge and understanding of Ethernet switching.

In this paper we have covered the basics of Ethernet switching and networks so that the installer can approach a network based system with more confidence and be able to deliver to their end user more flexibility and improved returns on their existing networks, which in turn maximises their total cost of ownership.

When designing an IP based video surveillance system, the variety of equipment available and the rapid pace of technology need to be balanced with the specific needs of the end user to ensure the best solution is delivered to the customer.

In terms of switch selection this means we recommend that an installer considers the system requirements at the design stage before selecting the appropriate switches.

The decision on switches should be based on four key factors:

+ Speed

+ Number of ports

+ POE versus non-POE

+ Stackable versus Standalone

It should be remembered that the switches deployed on today's network based video system will need to have longevity, and the flexibility to deal with future changes. Installers therefore will need to make important choices to determine the best network switch for a system, whilst keeping one eye on the future to make sure the switches purchased today are capable of meeting the future needs of the customer.

www.mayflex.com

Mayflex UK
Excel House
Junction Six Industrial Park
Electric Avenue
Birmingham B6 7JJ
United Kingdom

Tel +44 (0)121 326 7557
Email sales@mayflex.com
Website www.mayflex.com

Mayflex MEA DMCC
PO Box 293695
Office 11A, Gold Tower
Jumeirah Lakes Towers
Dubai
United Arab Emirates
Tel +971 4 421 4352
Email mesales@mayflex.com
Website www.mayflex.com

Certificate No. FS 547274

Certificate No. EMS 542863

Investor in Customers

CCTV User Group
Leading, Working, Delivering for ALL CCTV Users

IP UserGroup™ Affiliate Member

FIA The Fibreoptic Industry Association CORPORATE MEMBER

BICSI® CORPORATE MEMBER

All together.

Printed on paper made
from 75% recycled fibres.

MF1079_07/16

MAYFLEX