The use of Layer 3 devices to manage Multicast Data on your CCTV network.

This document explains how IP Multicasting works, when to use it and what feature are required in the network.
Executive summary

The need for bandwidth is constantly increasing as numerous new cameras emerge in CCTV networks. The CCTV networks are expanded massively to accommodate the security requirements. To make CCTV networks more efficient, you can increase the bandwidth, or you can optimise the way data is sent.

Multicasting data is a way to optimise the way data is sent through a network. Multicasting is a type of communication between IP devices in a network that enables a computer to send one stream of data to many interested receivers without interrupting devices that are not interested. For these reasons, multicasting has become the favoured transmission method for most multimedia and triple play applications, which are typically large and use up a lot of bandwidth.

Multicasting not only optimises the performance of your network, but also provides enhanced efficiency by controlling the traffic on your network and reducing the loads on network devices.

Multicasting explained

There are three types of communication between devices in a network:

- **Unicast** - one device talks directly to another device
- **Broadcast** - one device talks to all devices
- **Multicast** - one device talks to a select group of other devices

In a conventional Ethernet network, most IP packets are sent using unicast transmission. Every device in a network can transmit and receive packets, which in unicast transmission are labelled with the address of the receiving device. Each device listens to all the other packets that are sent in the network and looks for packets that are addressed to itself. When a computer encounters a packet that is addressed to itself, it interrupts the processor and hands the packet to the operating system to process.

Unicast is great for communicating directly with one or a few other computers. However, if you want to communicate with a number of computers, unicasting become inefficient because a copy of each packet must be sent to every receiving unicast address. Unicasting uses up bandwidth fast, especially when sending large multimedia files, which already take up a lot of bandwidth. The same information must be carried multiple times to the group of computers that you are sending the information to, even across shared links.

Broadcast communication is used to communicate with all of the devices connected to a network using a special broadcast address. When packets are addressed to the broadcast address, all of the computers in the network pick up the packets and give them to the operating system for processing. Broadcasting is really useful if you need to send information to everyone on your network, but not everybody is always interested in receiving your information.

With multicasting, the source device sends out one stream of packets addressed to the multicast group's address and receivers who are interested in receiving the data can program their computers to listen for data that has their addresses. Multicasting enables one computer to send data to many interested receivers without interrupting devices that are not interested in the data.
How does IP Multicasting work?

The set of messages that enable devices to send IP multicast data to each other is called IGMP. IGMP stands for Internet Group Management Protocol. These messages allow devices in the network to add or remove themselves from groups, each group having a special group address. Once a group is established, any member of the group can send data to the special group address and the Multicast Enabled Switches and Routers in the network will know where all the other members of the group are and correctly copy the data only to other group members.

IGMP snooping
IGMP snooping enables switches to intelligently forward multicast packets to hosts that want to receive the packets instead of sending them to all ports on a virtual LAN (VLAN). IGMP snooping can passively snoop an IGMP Query. Report and Leave packets are sent between IP multicast routes and hosts to learn the multicast group membership of the packets. IGMP snooping checks packets as they move around a network, picking out group registration information and then configuring the multicast stream so that multicast traffic is only sent to ports that have members of the particular multicast group or groups. IGMP snooping does not generate any extra network traffic and significantly reduces the multicast traffic passing through your switches.

IGMP Querier
On each network, one of the Multicast enabled switches or routers takes on a special role called the IGMP Querier. Every so often, it sends out an IGMP Query message to all other multicast enabled devices in the network, asking them to report in which groups they are members. All other switches in the network listen in (or snoop) on these reports coming back from devices on the network, which are members of multicast groups. By snooping on these reports, they can learn which groups are in the network and which group members can be found on each of their physical switch ports. Then when some data addressed to a group comes in on one port, the snooping switch can correctly copy the data out of any other ports which it knows connects to other groups members.

Usually, the IGMP Querier is a router but in a network which does not have a router, this function must be provided by a multicast enabled device (i.e. L3 switch, NVR or VMS). Many managed switches support the IGMP snooping feature but not all switches support the IGMP Querier feature. For CCTV Systems involving just a LAN with no router connection to another network, it is important to make sure all the switches support IGMP snooping and at least one of them supports IGMP Querier.

Multicast Address Ranges
IP multicast groups are identified by a multicast group address. The IP specifications have a reserved address range that can used for multicast:

- IPv4: The 4 most significant bits in multicast addresses are 1110, which gives 2^{32} addresses in range: 224.0.0.0 - 239.255.255.255

Multicast Protocols
The Internet Group Management Protocol (IGMP) is a protocol used in IPv4 networks to manage multicast group membership. A recipient on an IPv4 network that wants to be a part of an IP multicast group must use IGMP to join the group. Adjacent routers also use IGMP for communication. Three versions of IGMP are defined, each newer version provides enhancements compared with the older version. In IPv6 networks multicast management is handled by the Multicast Listener Discovery (MLD) protocol.
The benefits of Multicasting

Multicasting optimises the performance of your network. Because only one multicast data stream is sent out, multicasting preserves bandwidth on your network and eliminates traffic redundancy. In contrast, the unicast environment sends out a separate copy of the data to each receiver.

Multicasting also provides enhanced efficiency controlling the traffic on your network and reducing load on network devices. The clients on your network are able to decide whether or not to listen to a multicast address, so packets are only sent to where they are required.

In addition, multicasting is scalable across different sized networks, but is particularly suited to WAN environments. It gives people in different locations access to streaming data files, like a video or live presentation without taking up excessive bandwidth or broadcasting the data to all users in the network.

Summary

IP multicasting optimizes the use of an IP network for point to multi-point communication. A data packet is only sent once through the network, even if it is destined to many recipients in a IP multicast group.

On a single physical segment in a network it is relatively simple. However, complications arise when multicasting is extended beyond a single physical network and multicast packets pass through a router.

The features you should look for in a switch are:

- IGMP snooping
- IGMP querier