Understanding IP Multicasting

White Paper

Document ID:	IC-135-TC001-1.3
Dated:	19 May 2008
Status:	Released

IndigoVision

Signatories

Chief Technical Officer..... Barry Keepence

Signature Not Verified

Digitally signed by Barry Keepence
DN: cn=Barry Keepence, o=IndigoVision, c=US
Date: 2008.05.19 11:39:10 +01'00'

Program Manager..... Alex Swanson

Signature Not Verified

Digitally signed by Alex Swanson
DN: cn=Alex Swanson, o=IndigoVision, c=GB
Date: 2008.05.19 11:05:28 +01'00'

Contents

1. Background

IP Multicasting is an extremely powerful feature of IP networks that allows CCTV video footage from the same camera to be efficiently viewed and recorded by multiple CCTV operators at the same time.

IndigoVision is often asked by partners for advice on specifying and configuring networks to support IP Multicasting.

This white paper explains how IP Multicasting works, when to use it and what features are required in network switches and routers. Example configurations are given for typical Cisco and 3Com switches.

2. IP Multicasting

2.1 What is Multicasting?

The term “broadcasting” is familiar to everybody in the context of radio broadcasts. In a radio broadcast, signals are sent from a transmitter to everybody within range of the transmitter. The signals are there, in your house or car, regardless of whether you have your radio turned on or not.

Rather than sending out information regardless of whether anyone is listening, a more efficient form of transmission would be to only send information “on-demand”. In other words, you have to ask the transmitter to send you the information. In such a system, only those people who have asked to receive the information will get it. An example of an on-demand system is the pay-movie services available in many hotels. The movie starts at a certain time but you only get to see it on your TV if you have asked for it.

On-demand systems require more sophisticated or intelligent transmitters and receivers. In a broadcast system the transmitter doesn’t need to know or care whether your receiver (your radio) is turned on and receiving the transmission. In an on-demand system, the receiver (the TV in your room) needs to be able to tell the transmitter (the movie server in the basement of the hotel) whether you’ve agreed to the charges and should be allowed to receive the movie.

In other words, the receiver and transmitter talk to each other.

In a CCTV system, the transmitters are cameras and the receivers are monitors, recorders or PCs.

Consider a CCTV system covering an airport. There may be several “Control Rooms” each with access to sets of cameras covering different areas or responsibility. For example one run by airport security with access to all cameras, one run by customs, one covering car parks one covering baggage handling etc. etc. Overall there are several hundred cameras and any one camera may be viewed and recorded by several different security guards from different control rooms at the same time. When an incident happens the demand on a single camera may be multiplied as many guards from the same control room all view the same camera. Lets say there are 10 distinct control rooms, each with 10 guards. There is one high bandwidth “core” switch which connects each of the 10 control rooms, and at each of the control rooms, an “edge” network switch gives each of the 10 guards access to the network. Individual cameras or groups of cameras are also connected to the “core” switch. (See Figure 1 below)

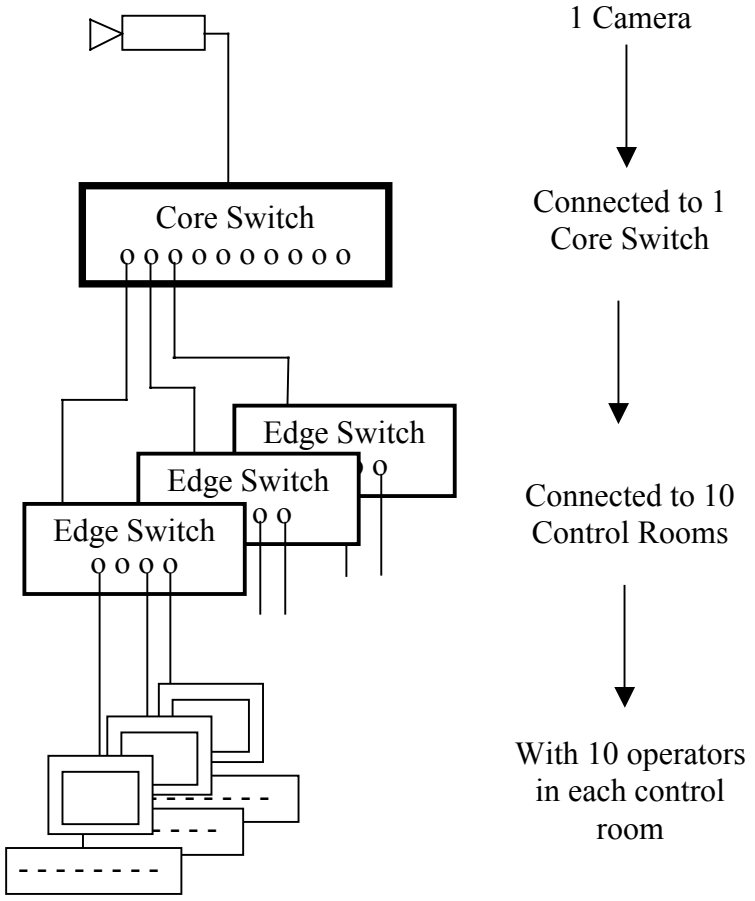


Figure 1 Camera must either send 100 Unicast data streams or 1 Multicast data stream

As more and more security guards decide to view or record a particular camera, there are two possible ways in which the camera could deliver video to each guard.

1. The camera could send a dedicated "stream" of video to each guard that has demanded to view the camera. Such a delivery system is called "**Unicast**". There is a dedicated "one-to-one" connection for every person watching the camera. In the worst case where everybody is watching the same camera, the camera would be streaming 100 copies of the video signal.

2. Alternatively, the camera could send out one signal into the core switch, and if the core and edge switches in each control room were clever enough, they could decide whether to forward the signal on to a specific security guard, depending on whether he had requested to view the camera or not. Such a delivery system is called "**Multicast**". It is a "one-to-many" information delivery system. In the worst case where all guards are watching the same camera, instead of serving 100 copies of the video signal, the camera would serve just 1 copy, the core switch would make 10 copies and each edge switch would make another 10 copies to send to each security guard in its control room.

Clearly, Multicast is a more efficient way of delivering information in an on-demand system. It does however require the switches that make up the network to have a certain amount of "intelligence". They must be able to join in the discussion that

happens between receivers and transmitters regarding who has demanded the information. They must also be able to make local decisions about whether to copy information to specific end points or not.

In an IP network as used by IndigoVision CCTV equipment, Multicasting is referred to simply as **IP Multicasting.** The "intelligent" boxes that make up the network are referred to as **Multicast Enabled Switches** and **Routers**. The transmitters are IP Cameras and the receivers are either Control Center viewing panes, Networked Video Recorders or Receiver codecs connected to analog monitors.

2.2 What types of CCTV installations are suitable for IP Multicasting?

From the example above, it is clear that the principal use for Multicasting is when there are multiple receivers all wanting to receive information from the same transmitter. In terms of CCTV installations, that would mean the same camera being viewed by multiple CCTV Operators and also possibly being recorded by one or more Networked Video Recorders.

If each of these receivers had a dedicated **Unicast** connection, then the camera would have to produce multiple copies of the video stream to send out on to the network – one copy to each receiver. Not only would this multiply the processing workload on the camera, it also multiplies the amount of data being put on the network.

IndigoVision video streams can be configured to have bandwidths anywhere between 32Kbps and 4Mbps depending on the desired quality and resolution. 1Mbps would be a reasonable example of a good quality video stream. Imagine a CCTV system where two operators and a recorder all in the same control room all want to view (or record) that camera with Unicast connections. The camera would produce a total of 3Mbps data onto the network – 1Mbps for each receiver.

Most Local Area Networks (LANs) in modern offices and buildings support bandwidths of 100Mbps so on the face of it 3Mbps from one camera is not a problem. What if the camera was not local to the operators but was somewhere more remote across a Wide Area Network (WAN)? Typical WAN bandwidths are 2Mbps (e.g. broadband) or even less for leased lines and wireless services. On such a WAN, suddenly 3Mbps from the camera becomes unsupportable. Using Multicasting, the camera could send out just one copy of the video stream using just 1Mbps. When this stream gets to the control room, an intelligent Multicast Enabled Switch could copy the stream to each of the three receivers (two guards and one recorder).

So one reason for using Multicasting is if the network bandwidth available between a transmitter (camera) and a receiver (live viewer or recorder) is restricted such as typically is the case with remote cameras.

Even on a LAN, you have to consider the processing load on the transmitter. An IndigoVision transmitter is capable of producing about 16Mbps total data. This means, with our example 1Mbps video stream from above, an IndigoVision camera could support up to 16 Unicast dedicated one-to-one connections to receivers. This would work and would probably cover most CCTV system requirements – how many systems need 16 simultaneous views of the same camera? However, what if the required video quality meant that the video stream was set to 4Mbps? Then suddenly, the transmitter will only support four Unicast connections. Once again, the solution is Multicast. With Multicast, because the transmitter is only sending out one stream, there is no processing restriction on the transmitter. It can send out one 4Mbps stream and the Multicast Enabled Switches will copy that stream as necessary to an **unlimited** number of receivers.

So, in summary, Multicasting is suitable for CCTV installations where:

1. The camera is remote from the control room on a WAN and more than one person wants to view (or record) the camera. i.e. where there are bandwidth restrictions.

2. The camera is local to the control room on a LAN but the combination of a higher quality video stream with multiple people viewing that camera means the camera's processing limit is reached.

In general, if three or more people want to view or record the same camera you should consider using Multicasting.

2.3 What types of CCTV installations are not suitable for IP Multicasting?

In general Multicasting is suitable for all CCTV installations.

There are three issues that are sometimes raised. These are discussed below with an explanation of how they can be overcome:

2.3.1 The Internet

IP Multicasting is generally not supported on public IP networks such as The Internet. On the other hand, not many security systems allow public access to their cameras.

If the reason you are using The Internet is to allow public access to a camera then the solution is to use the IndigoVision Internet Streaming Server (ISS). This product allows you to securely serve an IndigoVision camera to multiple receivers using standard media players such as Apple's QuickTime. The Internet Streaming Server uses Unicast rather than Multicast connections but it overcomes the restriction on the processing power of the camera.

If you are using a public network simply as a convenient pipe to transport your CCTV video between sites, then this can be done securely using Virtual Private Network (VPN) technology. VPNs support Multicasting so they are a possible alternative to a dedicated private WAN such as a leased line.

2.3.2 Complexity of Network Administration

This is the other disadvantage of IP Multicasting that is often quoted. Not all network administrators might be confident or experienced in configuring and managing support for IP Multicasting in their network switches and routers.

In fact enabling support for IP Multicasting is straight forward as this white paper aims to show below.

2.3.3 Existing legacy network infrastructure

Not all network switches are Multicast Enabled. The specific features a switch needs in order to support Multicast are detailed below. If you are installing your CCTV system on an existing IP network that has non-Multicast enabled switches then problems can arise. The default behaviour for a switch that does not support Multicast is for it to broadcast the data. That is, it will forward the data to every device on the network, even if it hasn't asked to receive the data. This causes unnecessary congestion on the network and often results in lost frames and jittery video.

These days it only tends to be very low-end unmanaged switches that do not support Multicast. If your CCTV operational requirements demand the use of Multicast and the existing network switches do not support it then part of the system design will be to upgrade the network switches. Fully managed edge switches with Multicast support can currently be bought for around $250 (£125)

2.4 How does IP Multicasting work?

2.4.1 How IP Multicasting works in a LAN

In the section “What is Multicasting?” above, it was shown that an important part of Multicasting was the ability of the receiver and transmitter to talk to each other regarding who was demanding video. Also for the network switches to participate in those discussions. This section will describe those conversations in more detail, in the context of IP CCTV systems.

The set of messages that IP Multicast enabled devices can send to each other is called **IGMP**. IGMP stands for **I**nternet **G**roup **M**anagement **P**rotocol. These messages allow devices on 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 on the network will know where all the other members of the group are and correctly copy the data only to other group members.

How do the switches and routers know where all group members are? 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 on the network, asking them to report on which groups they are members. All other switches on 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 on 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 any other ports which it knows connects to other group 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 switch. Many switches support the “IGMP Snooping” feature but not all switches support the “IGMP Querier” feature. For CCTV Systems involving just a Local Area Network (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”.

2.4.2 Example from the IndigoVision CCTV system

To illustrate how IGMP works, here is a description of the sequence of events when a CCTV operator chooses to view an IndigoVision camera using IP Multicasting.

- In Control Center, the operator drags a camera from the site list and drops it into a viewing pane.
- Control Center sends a proprietary message to the camera/codec to ask what its Multicast IP address is. Multicast IP addresses fall within an internationally agreed range from 224.0.0.0 to 239.255.255.255. IndigoVision codecs have a default Multicast IP address beginning 239.255 and ending with the last two bytes of its normal IP address. e.g. a codec with IP address 10.5.1.10 has default Multicast IP address 239.255.1.10. The Multicast IP address can be changed if necessary through the codec’s Advanced Network Configuration web page. If you

plan to change the default multicast address scheme care should be taken as some addresses within the allowed range are reserved, meaning routers will not forward them. In this case you should refer to your router administrator's guide.

- Having learned the Multicast "group" address of the camera, the Control Center PC then sends an IGMP Report message stating that it has joined the camera's group. The IGMP Report message is sent to the group address. Since that address is one of the special reserved list of Multicast addresses, it ends up going to the network router which is where the IGMP Querier resides. As this IGMP Report message passes through any Multicast Enabled switches along the way, they "snoop" the report and learn that the PC is now a member of the codec's group.

- The Control Center PC then tells the camera to start streaming video to its group address.

- The camera sends video data to its special Multicast group address. When this data passes through a Multicast Enabled switch, the switch "snoops" a look at the destination IP address, sees that it is a special Multicast address and looks up its own internal tables to see if should forward the data to any group members on its ports. In this way the video data arrives at the Control Center PC and does not get sent to any devices that aren't members of the group.

- Timers in the Multicast Enabled switches control group membership. Every so often the IGMP Querier sends out an IGMP Query to all devices on the network and they respond with IGMP Reports. If an IGMP Snooping switch does not see an IGMP Report from any hosts that it knew used to be in a group then it assumes the host has left the group and removes it from its internal tables. Multicast data for that group will not be forwarded to any hosts that did not respond to the IGMP Query.

- If the Control Center Operator stops viewing video, Control Center sends an IGMP Leave message to explicitly let the IGMP Querier (and any IGMP Snooping switches) know that it is no longer part of the camera's group. If the Operator's PC suddenly leaves the network (e.g. power cut) then the normal timeout mechanism will ensure that switches stop forwarding data to the PC's port.

- Irrespective of the IGMP timeout mechanism, IndigoVision cameras and codecs also operate a timeout mechanism to keep track of group members. If a receiving Control Center PC or Networked Video Recorder stops sending a regular keep-alive message to the camera, the camera removes them from its list of current media connections. In this way, if all group members disappeared unexpectedly, the camera would know to stop sending video data to the Multicast group address.

2.4.3 How IP Multicasting works in a Private WAN (Leased Lines or Private Network)

In a private Wide Area Network, routers are used to connect two or more Local Area Networks. As described above, the router located in each Local Area Network usually provides the IGMP Querier function for that local network. This means it learns about all the groups on its Local Area Network.

Each router also needs to find out which groups exist on all the remote networks making up the WAN so that it can forward group messages correctly across the WAN. The routers could forward all the local reports they receive from individual devices on their local networks to all other routers they know about, but this would be very inefficient. Instead, routers use a different protocol or set of messages to exchange information in bulk about which groups they each have locally.

There are a number of such protocols that exist to allow routers to exchange multicast routing information. Examples include MOSPF and the PIM family of protocols.

This white paper will not attempt to explain the details of how these multicast routing protocols work. From a CCTV system perspective, the network provider e.g. a Telecoms company or Wide Area Service Provider usually provides support for Multicasting across a WAN. You need to make sure when specifying the system that support for IP Multicast is stated as a requirement.

2.4.4 How IP Multicasting works in a Public WAN (The Internet)

As stated above, public networks do not typically support IP Multicasting. The solution in this case is to connect your various remote sites in a Virtual Private Network (VPN). VPN support is a feature of the routers that connect your office to the Internet. It allows the routers to set up a secure, virtual pipe between two sites across the Internet. You are effectively extending the Local Area Network from your control room across the Internet into your remote sites. This means devices at both ends of the VPN can talk to each other as though they were local to each other. This includes being able to send data to Multicast group addresses. Also, devices in either location can receive queries from the IGMP Querier and switches in both locations can snoop on reports that may come from both locations.

From a CCTV system perspective, you need to make sure that your Internet Service Provider (ISP) supports VPNs and that the routers you specify to connect to the Internet also support VPNs. Most ISPs and routers support VPNs.

2.4.5 IGMP Versions

The set of messages and functions covered by IGMP has developed over the years and currently 3 versions of the protocol exist. Each version is backwardly compatible with the previous version.

IGMP V1 provides the basic functionality described above. The IGMP Querier is statically assigned by the network administrator to be one specific router or switch.

IGMP V2 introduces a more robust and automatic selection process for deciding who is the IGMP Querier. All devices capable of being an IGMP Querier agree which one device is the current IGMP Querier. If this device fails then one of the other devices automatically takes over the job. IGMP V2 also introduces an explicit “Leave” message which allows devices to notify the IGMP Querier when they want to leave a group. Under IGMP V1, devices are eventually timed out of a group if they fail to respond to an IGMP Query.

IGMP V3 adds extra functionality by allowing group members to state which particular devices they either want or don’t want to receive data from, even if they are all legitimate members of the group.

IndigoVision products all support IGMP V2. This provides compatibility with a wide range of network switches and routers from various vendors.

2.5 What features do I need to look for in a switch?

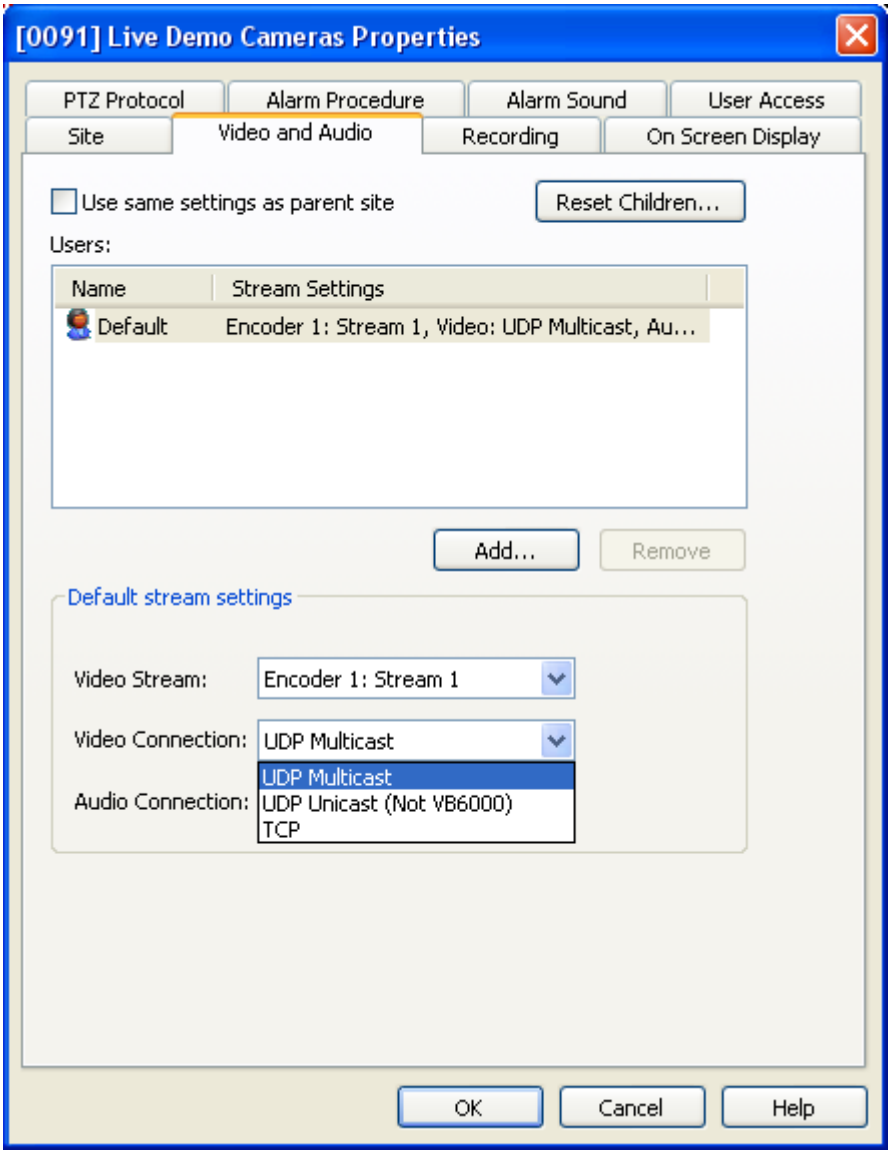
1. IGMP V2 support.
2. IGMP Querier support.
3. How many multicast groups are supported? Smaller edge switches typically support up to 64 groups. Larger core switches typically support thousands of groups. As an example, imagine a CCTV system with 200 cameras all being fed back to a central control room where there are just two guards each with

a PC. Both guards can access the same cameras and all cameras are being recorded so Multicast is being used. This means there are 200 Multicast groups – one for each camera. Even though a cheap low-end switch might be enough to provide network access for the two guards, care must be taken to specify a switch that supports at least 200 Multicast groups since the guards need to access any camera at any time.

2.6 Example configurations:

2.6.1 IndigoVision settings: Live View through Control Center

In Control Center, the administrator decides whether Multicast connections are to be made to one or more cameras. This is set as a property of either an individual Camera, a sub-site or the entire site. From within the Site Setup view, right click on a camera, sub-site or site and select the Properties menu option. Then select the "Video and Audio" properties tab (see screenshot below).

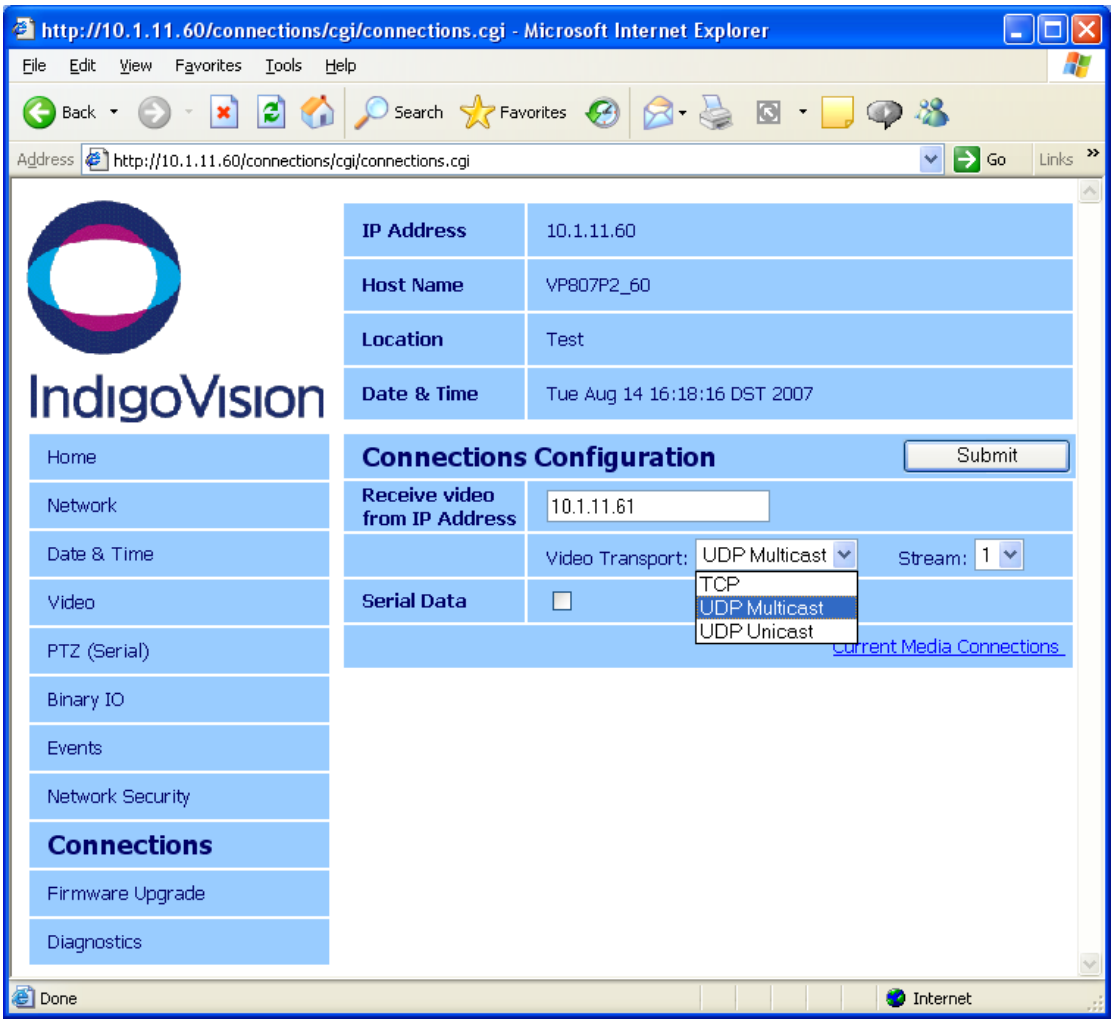


The "Video Connection" control offers a choice of UDP Multicast, UDP Unicast or TCP. Choosing "UDP Multicast" means all live views of that camera or site will be made using IP Multicasting.

2.6.2 IndigoVision settings: Live View through an analog Monitor

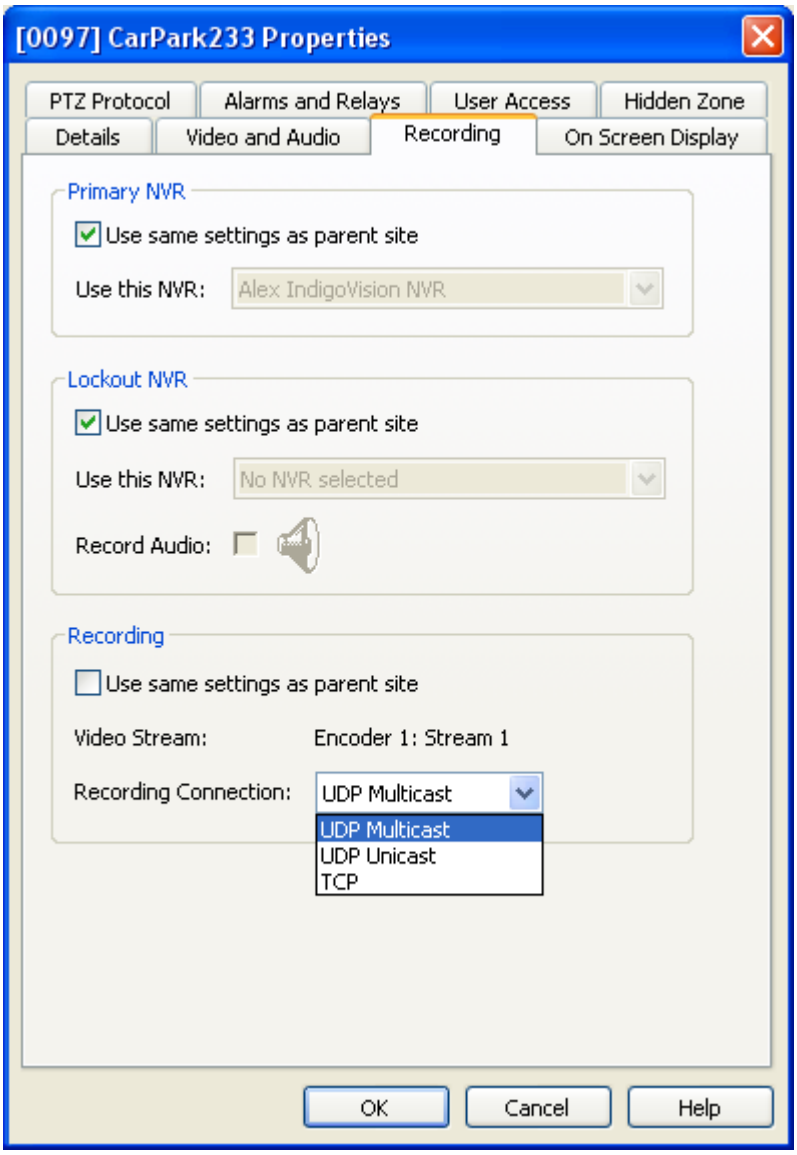
If you are setting up a point-to-point link between a camera and a monitor using Control Center to drag a camera icon onto a monitor icon then the type of connection made (Multicast or not) will be defined by the camera's "Video Connection" property as shown in the screenshot above.

If you are not using Control Center but instead are using the receiver codec's web interface then you can choose to use IP Multicast through the "Video Transport" setting on the "Connections" web page. (see screenshot below).



2.6.3 IndigoVision settings: Recording to a Networked Video Recorder

To configure recordings to be made using IP Multicast, once again you should use the Properties dialog for either a specific camera or a site within Control Center Site Setup view. This time go to the “Recording” properties tab and in the Recording section, select the type of “Recording Connection” to be UDP Multicast (see screenshot below).

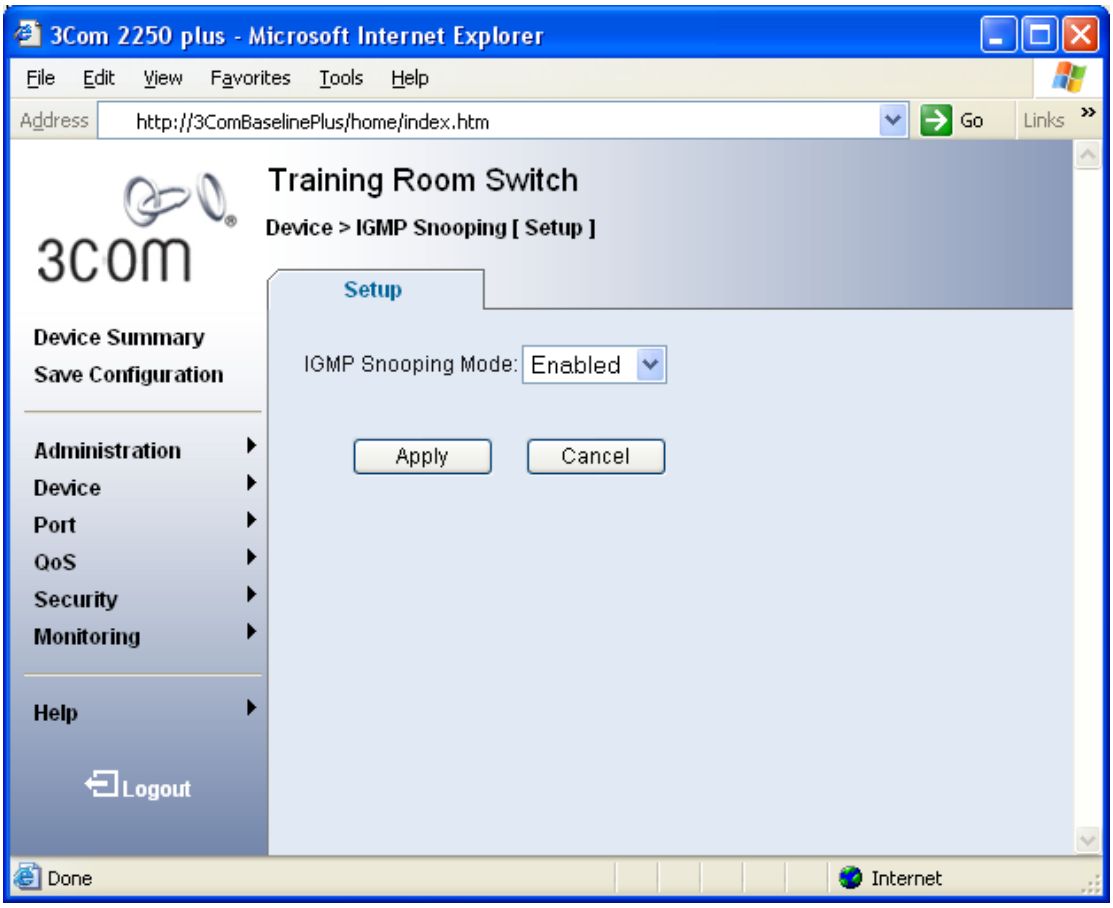


2.6.4 Example switch settings: 3Com Baseline Plus switch

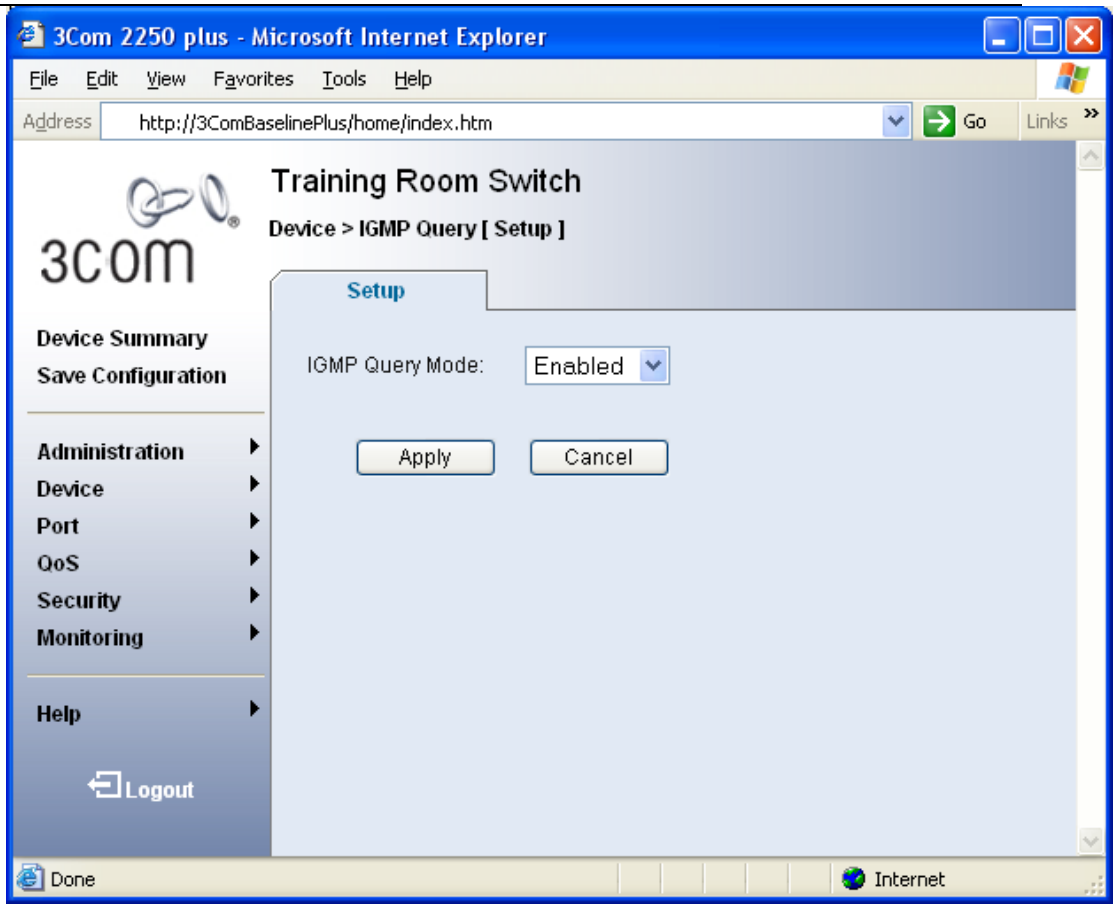
Many network switches have web interfaces that allow network administrators to configure their settings. The 3Com Baseline Plus family of switches is a typical edge switch which supports all the features required for IP Multicast:

- IGMP V2 Snooping
- IGMP Querier
- Up to 64 Multicast groups.

By default, IGMP Snooping is enabled. To check your configuration and if necessary enable IGMP Snooping select the 'Device -> IGMP Snooping' menu option and choose "Enabled".



The IGMP Querier function is not enabled by default. To enable IGMP Querier go to the 'Device -> IGMP Query' menu option and choose "Enabled". You can enable the IGMP Querier function on all the switches on your network. Using IGMP V2 messages they will agree amongst themselves which is the currently active Querier.



2.6.5 Example switch settings: Cisco Catalyst 2960

Cisco switches may also have a web interface but they also are often configured using a command line interface through a Telnet login. Supporting Multicasting across multiple routed networks does require deeper knowledge of Cisco configuration than this white paper can give. Refer to the available Cisco documentation for further information on this.

For Local Area Networks, the two basic features (IGMP Snooping and IGMP Querier) are easily configured.

By default IGMP Snooping is enabled. To check your configuration and if necessary enable IGMP Snooping, issue the following commands at the Cisco command line prompt:

```
Switch# configure terminal
Switch(config)# ip igmp snooping
Switch(config)# end
```

By default IGMP Querier is not enabled. To enable the IGMP Querier function, issue the following commands at the Cisco command line prompt:

```
Switch# configure terminal
Switch(config)# ip igmp snooping querier
Switch(config)# end
```

If you make a change to your configuration it is normal to save your changes so that they are re-used the next time the switch starts. The command to do this is:

```
Switch# copy running-config startup-config
```