

Enhancing Network Quality and Video Transmission

Optimized IGMP for IP Surveillance

Video Multicasting

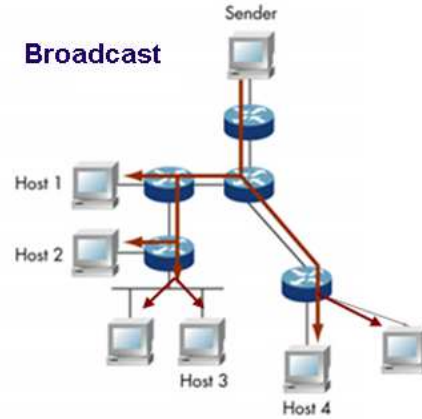
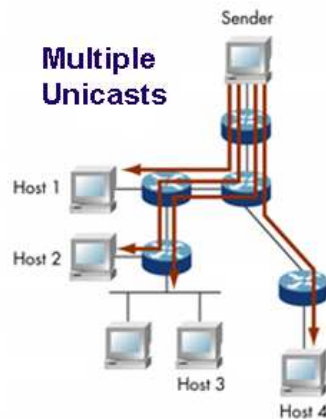


In the emerging market of IP surveillance, network communication is the key to provide a high quality and efficient video streaming. Various communication protocols are being used by vendors, each affecting on the quality of the data transmission differently. This document provides an executive introduction to IP surveillance video multicasting. It presents the advantages of multicasting over other network communication technologies as well as the importance of Internet Group Multicast Protocol (IGMP) integration for video traffic transmission. The paper mainly highlights the deployment benefits of Korenix switches for assuring the high quality and optimized communication in an IP surveillance network.

Multicast - Efficient One-to-Many Video Delivery

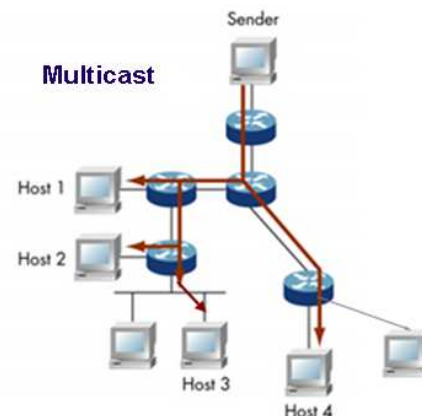
In a legacy IP surveillance network the video streams are transmitted from cameras to the PCs in different ways. However, mainly 3 basic methods of communication over an Ethernet IP network are being used: Unicast, Broadcast and Multicast.

In **Unicast** technology IP camera sends an individual streaming for each client who is willing to see the images. However, more is the client number, higher is the required network bandwidth and larger is the loading of the IP camera. As a result, by sending each receiver a duplicate copy, Unicast makes the sender busy and consumes network bandwidth and IP camera computing power.



Opposite to it, in **Broadcasting**, the image is sent from a single IP camera to all the devices connected to the LAN at a time. As a result, some cameras receive the information when they don't quite need it. Hence, there is the waste of network bandwidth which obviously downgrades network transmission quality.

Compared to Unicast and Broadcast, **Multicast** fits the need of one-to-many transmission more efficiently. It uses network resources smartly by sending video data from a single device to multiple receivers simultaneously. It optimizes system resources and enables data transmission to multiple system elements with reduced latency and increased coherency. With Multicast, even when the client number is increasing, the network bandwidth is still the same, as is the loading of the IP camera, too.



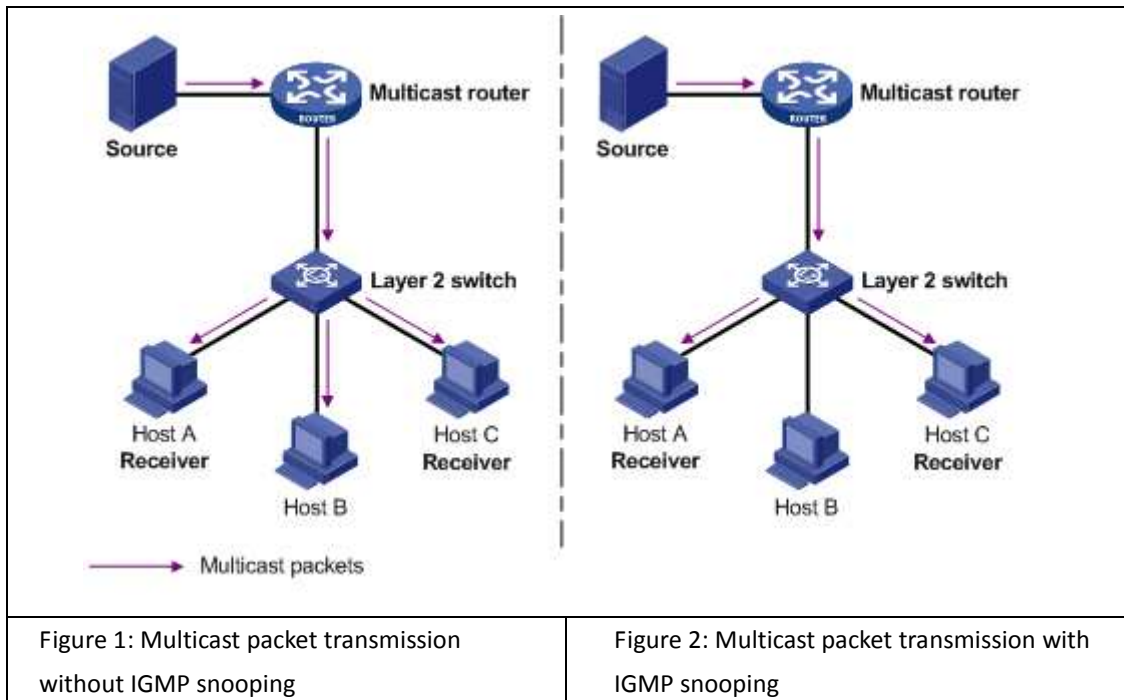
Multicasting data additionally results in better link utilization throughout the system, often removing bottlenecks or allowing the provisioning of smaller, more efficiently used links to save power and reduce the complexity of the board design.

Hereafter, in order to have an efficient video transmission in a surveillance network, Multicast should be used as a communication technology.

How Multicast Works

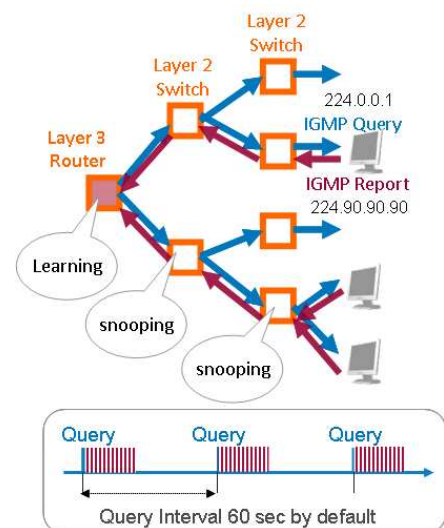
Multicast traffic originates at sources desiring to distribute the same information to multiple recipients. However, typical Ethernet switches flood multicast packets to all ports as broadcast. This means that Ethernet switch needs to learn managing video

traffic of the group; i.e. routers do not forward multicast traffic unless they are multicast capable and have multicast routing protocol enabled. So, when multicast traffic is used in a routed network, the IGMP protocol is used to allow data transmission only to the parts of the network where it is required. It allows hosts to inform routers that they want to receive multicast traffic for a specific multicast group address.



Layer 3 Router sends IGMP Query periodically to the viewers, which respond with IGMP report. Hence, Layer 3 Router learns how to send multicast video on demand. To learn how to forward multicast traffic effectively, Layer 2 switch must be IGMP aware, it means it should have IGMP Snooping.

But how does IGMP Snooping work? Generally, Ethernet switch snoops for IGMP Report messages. It learns from which port the viewer is and saves the group and/or port entry in MAC table. After it the switch can forward the multicast videos only to the ports with viewers. However, unknown multicast is still flooded to all ports as broadcast.



Hence, to provide an efficient video stream transmission when there is a lot of multicast data on the network, a switch with IGMP protocols is required

Optimized IGMP for IP Surveillance

Usually, IGMP Query is only supported by multicast enabled Layer 3 Routers, which are very costly. Besides, most Layer 2 switches do not support IGMP snooping, these means that they do not have the capacity to handle a large table of IGMP Multicast traffic, so the multicast will flood everywhere when IGMP snooping is absent. As a result, the bandwidth utilization will be poor and the video quality very low. This is critical for IP surveillance system.

Therefore, to solve all these issues Korenix introduced the optimized IGMP protocol for ensuring a reliable and high performance video transmission in IP surveillance network.

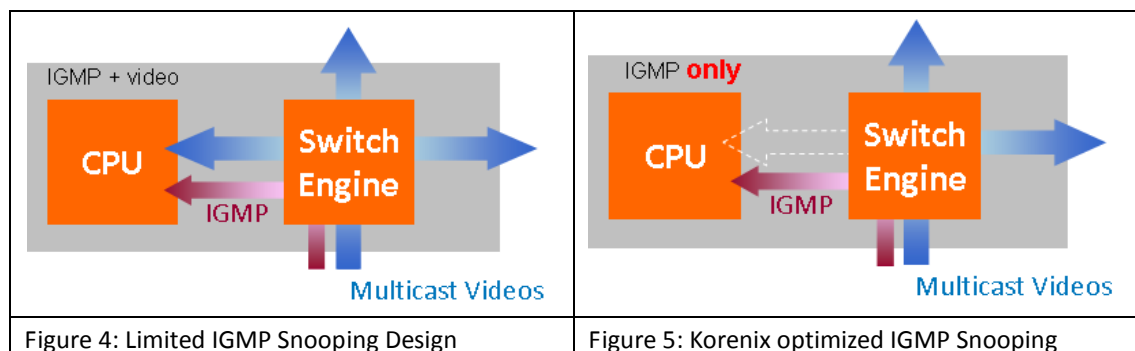
Complete Multicast Support

To ensure an efficient video image transmission Korenix Layer 2 switches support both IGMP Query and IGMP Snooping. With IGMP Query protocol, Korenix replaces traditional expensive L3 switches with its cost-effective L2 switches. Besides, Korenix L2 switches, which support IGMP Snooping, can provide high quality of video transmission. Hence, a single Layer 2 switch solves all the problems of network communication by providing a complete, end-to-end multicast management.



Optimized Performance

Normal switches have limited IGMP Snooping design. This means that when a CPU snoops for IGMP, it does get video data, so it is overwhelmed by Multicast videos and can be too busy to manage the traffic. This results in poor bandwidth management, so the switch is not capable of supporting large scale surveillance systems.



Opposite to this, Korenix Layer 2 switches are specifically designed for providing an optimized IP surveillance solution with optimized IGMP technology. Here CPU snoops IGMP only and doesn't get multicast videos along with the IGMP. Therefore it will not lose time on managing multicast video traffic and will effectively manage the bandwidth and provide scalable and high video quality.

Seamless Restoration

To protect against network failure and to ensure the reliable video transmission, legacy IP surveillance networks use redundant technology. However, in the redundant network the topology change is inevitable. A topology change alters data flowing paths and requires IGMP snooping to relearn forwarding multicast traffics correctly. Before regaining correct multicast group information, multicast traffic is either lost or flooded everywhere, which prolongs system downtime and downgrades the quality of network service. The convergence procedure starts from next IGMP Report which can take up to one more IGMP query interval. This is not acceptable for mission-critical IP surveillance applications.

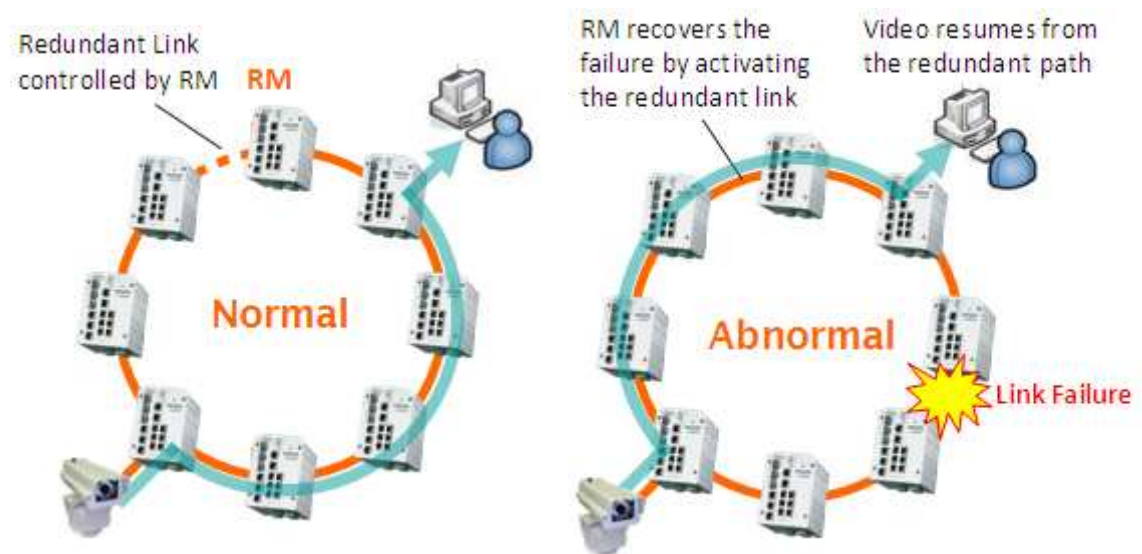


Figure 6: Topology Change Alters Data Flowing Path

Korenix Layer 2 Switches have an error-free restoration procedure, Seamless Restoration, which provides fast convergence from topology change. Here IGMP relearning process starts immediately once the topology is changed. By fast reacting to topology change, the convergence time is down to within a few seconds and multicast traffic can soon find its way to destination. The patented mechanism shortens the system downtime, eliminates any unstable status and guarantees the best quality and smooth video delivery.

Advanced Multicast Control

In addition to all these benefits, Korenix Layer 2 switches provide also unknown multicast filtering. This means that multicast traffic without IGMP report is not identified by the switch and it will not be forwarded unless it is recognized by the switches. The unknown multicast filtering also prevents the degradation of the network transmission as well as prevents from malicious attacks providing a secure surveillance network connection.

Besides IGMP snooping, Korenix switches support static multicast filtering. These two mechanisms can enable and work with each other simultaneously.

IGMP snooping learns multicast group membership dynamically; however, it cannot join a device without IGMP support which requires multicast traffic. Static multicast filtering provides a method for user to configure multicast group memberships manually.

Thus, with static multicast filtering it is possible to control the multicast traffic precisely.

Summary

Korenix Ethernet switches run IGMP technology to provide a complete, end-to-end multicast management from the IP cameras to the monitoring center. The optimized IGMP Query and Snooping implementation in Korenix switches makes possible to have a cost-effective and high quality video multicasting and exactly match the requirements of surveillance markets such as airport and harbor surveillance, city and bank surveillance, transit and retail surveillance, etc.

About Korenix

Korenix Technology, a Beijer Electronics Group company is a World leader in IP Surveillance Networking, dedicated in providing the most reliable and high quality PoE and High Power PoE switches, Video-optimized Gigabit Ethernet and Waterproof Ethernet switches, Wireless outdoor APs and embedded programmable PoE routing computers for IP video surveillance anytime, anywhere and for any purposes.

Copyright © 2010 by Korenix Technology Co., Ltd

All rights are reserved. Any redistribution or reproduction of materials herein is prohibited without the permission from Korenix Technology Co., Ltd.