NETGEAR®
Connect with Innovation™

7000 Series - Configuring IGMP Snooping (Multicasting)

The aim of this document is to describe the steps to setup and test IGMP Snooping

The purpose Internet Group Management Protocol (IGMP) snooping is to restrain multicast traffic in a switched network. By default, a LAN switch floods multicast traffic within the broadcast domain and this can consume a lot of bandwidth if many multicast servers are sending streams to the segment.

Multicast IP addresses are Class D IP addresses. Therefore, all IP addresses from 224.0.0.0 to 239.255.255.255 are multicast IP addresses.

IGMP Snooping can be very effective in network environments where Multicast applications like Video/Audio streaming are being used.

Table of Contents

Software **2**

Physical Setup **2**

Logical Setup **2**

Network Diagram **2**

CONFIGURATION – Management IP address and IGMP **3**

Set the Management IP address 3

IGMP snooping implementation **3**

Enable IGMP Snooping (CLI) on VLAN 1 3

Enable IGMP snooping on any VLAN 3

TESTING - Multicast **4**

Software

Native VLAN:	1
Multicast software:	VLC version 0.8.6d (supports IGMP v1,v2,v3)
Multicast stream:	700 Mb AVI File
Netgear Switch:	GSM7312 FW 6.0.0.15, 6.1.0.9 and 6.2.0.14
Multicast Sender:	WinXP 192.168.0.2
Multicast Receiver:	WinXP 192.168.0.10 and 192.168.0.20
Multicast address:	239.255.0.1

Packet capturing software: Wireshark 0.99

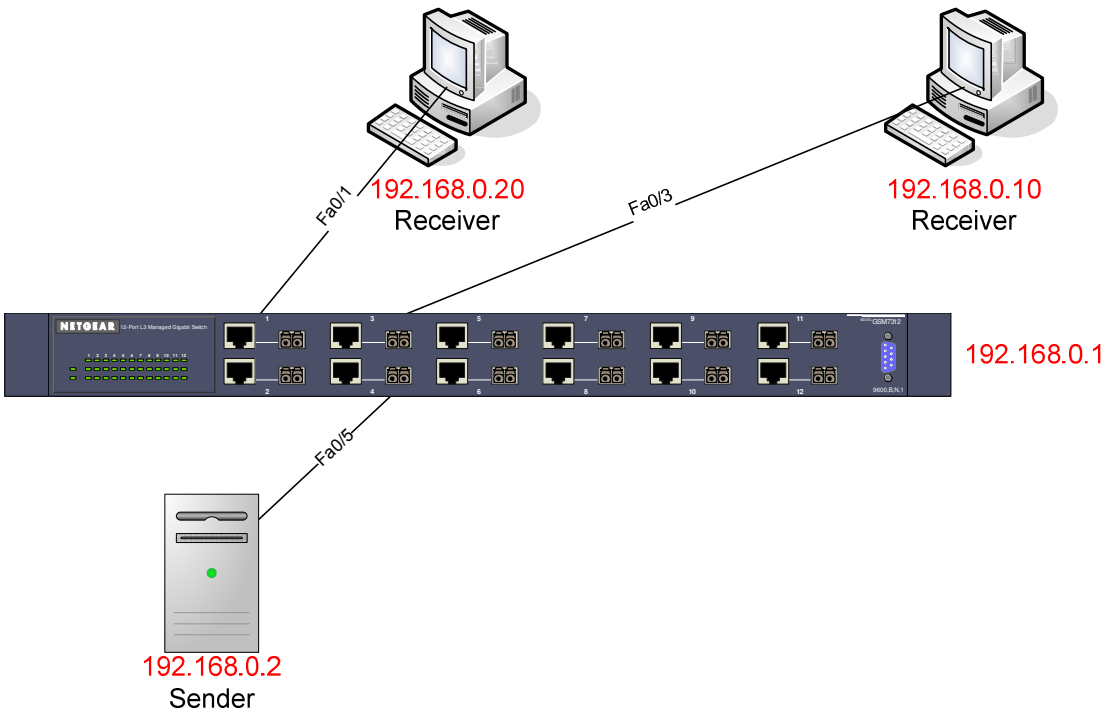
Physical Setup

1x GSM7312 Prosafe Layer 3 Managed switch
3x Windows XP Computers

Logical Setup

Sender:	192.168.0.2
Receiver:	192.168.0.10
	192.168.0.20

Network Diagram



CONFIGURATION – Management IP address and IGMP

Set the Management IP address

1) Plugged the console cable to the Serial port of the switch and the serial port on the PC
2) Open a new Hyper Terminal session (connecting via the COM port) – settings 9600, 8 , None , 1, None
3) Power Cycle the switch
4) Upon POST the User: prompt will appear
5) Username is **admin** , password "**blank"**
6) Type **Enable** to access the privileged mode (password "**blank"**)
7) Type **network protocol none** to reset the network settings
8) Type **network parms <<Management IP>> <<Subnet Mask>> <<Default Gateway IP>>**. For example **network parms 192.168.0.2 255.255.255.0 192.168.0.1**
9) User **copy system:running-config nvram:startup-config** to save the configuration
10) Check with **show network** if the settings are correct

The switch should now be accessible patching a CAT5 Straight-through cable. The PC NIC must be configured with an IP address within the same subnet used to configure the management IP of the switch (Example: 192.168.0.2 255.255.255.0

IGMP snooping implementation

Enable IGMP Snooping (CLI) on VLAN 1

(GSM7312)# config
(GSM7312) (config) #ip igmpsnooping
(GSM7312) (config) #ip igmpsnooping unknown-multicast filter
(GSM7312) (config) #ip igmpsnooping interfacemode
(GSM7312) (config) #exit

(GSM7312)# vlan database

This command activate IGMP on all the ports in VLAN 1
(GSM7312) (vlan) #ip igmp 1

This command activate the Querier to be the VLAN address (In this case 192.168.0.1)
(GSM7312) (vlan) #ip igmpsnooping querier 1

(GSM7312) (vlan) #exit

Enable IGMP snooping on any VLAN

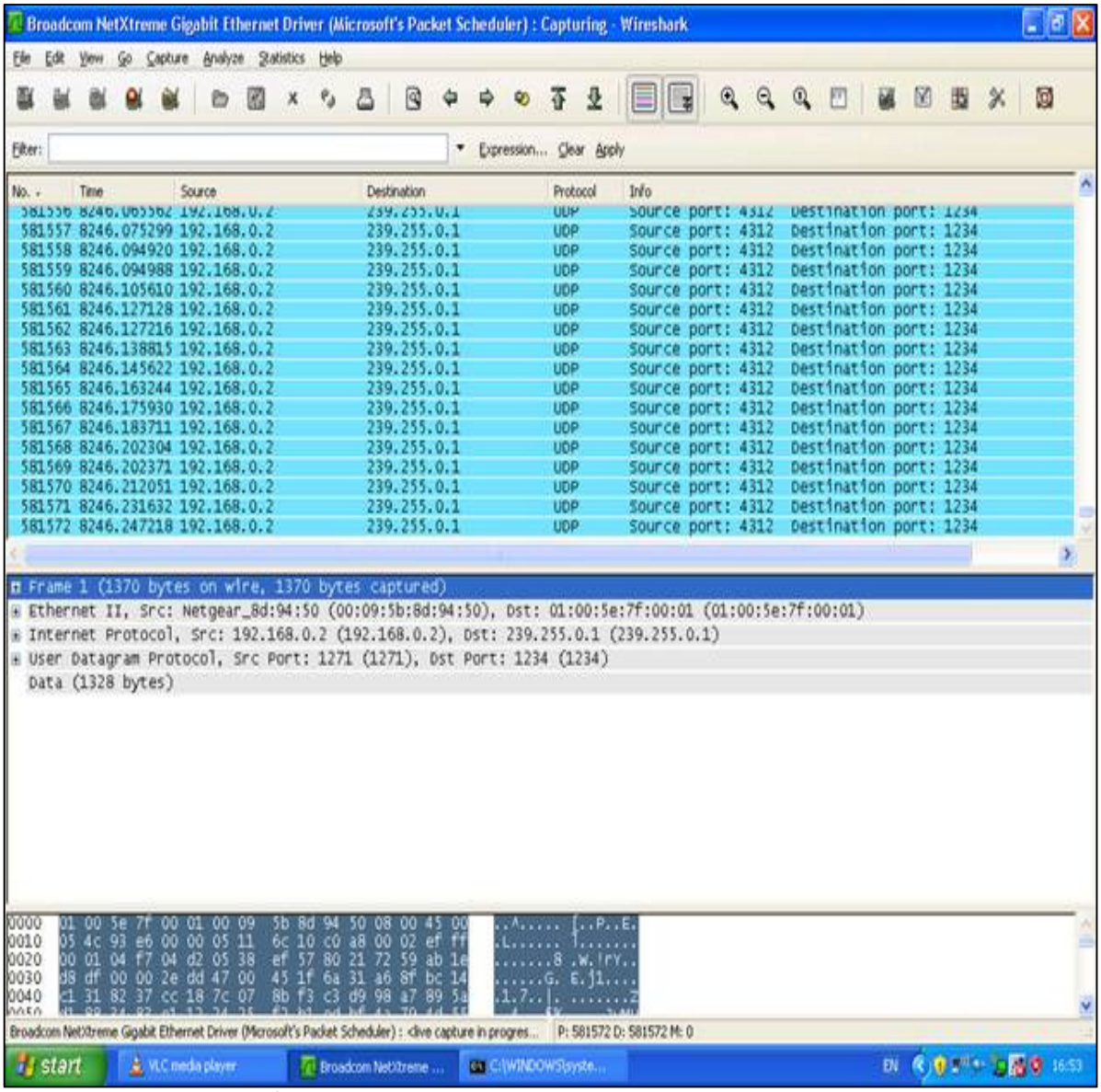
In order to activate IGMP on any other VLAN the following list of commands must be modified replacing <VLAN-ID> with the VLANID number:

GSM7312)# vlan database
(GSM7312) (vlan) #ip igmp <VLAN-ID>
(GSM7312) (vlan) #ip igmpsnooping querier <VLAN-ID>
(GSM7312) (vlan) #exit

TESTING - Multicast

1- Activated Wireshark on the Receivers to filter Multicast traffic

2- Activated VLC on the Sender, to send Multicast to 239.255.0.1, Source File a 700 MB AVI



3- Activated VLC on the Receivers , to listen to Multicast for the address 239.255.0.1

Fig.1

Both receivers would display the output in Fig.1 and receive the Multicast AVI transmission on the VLC viewer

4- Closed VLC on one of the Receiver

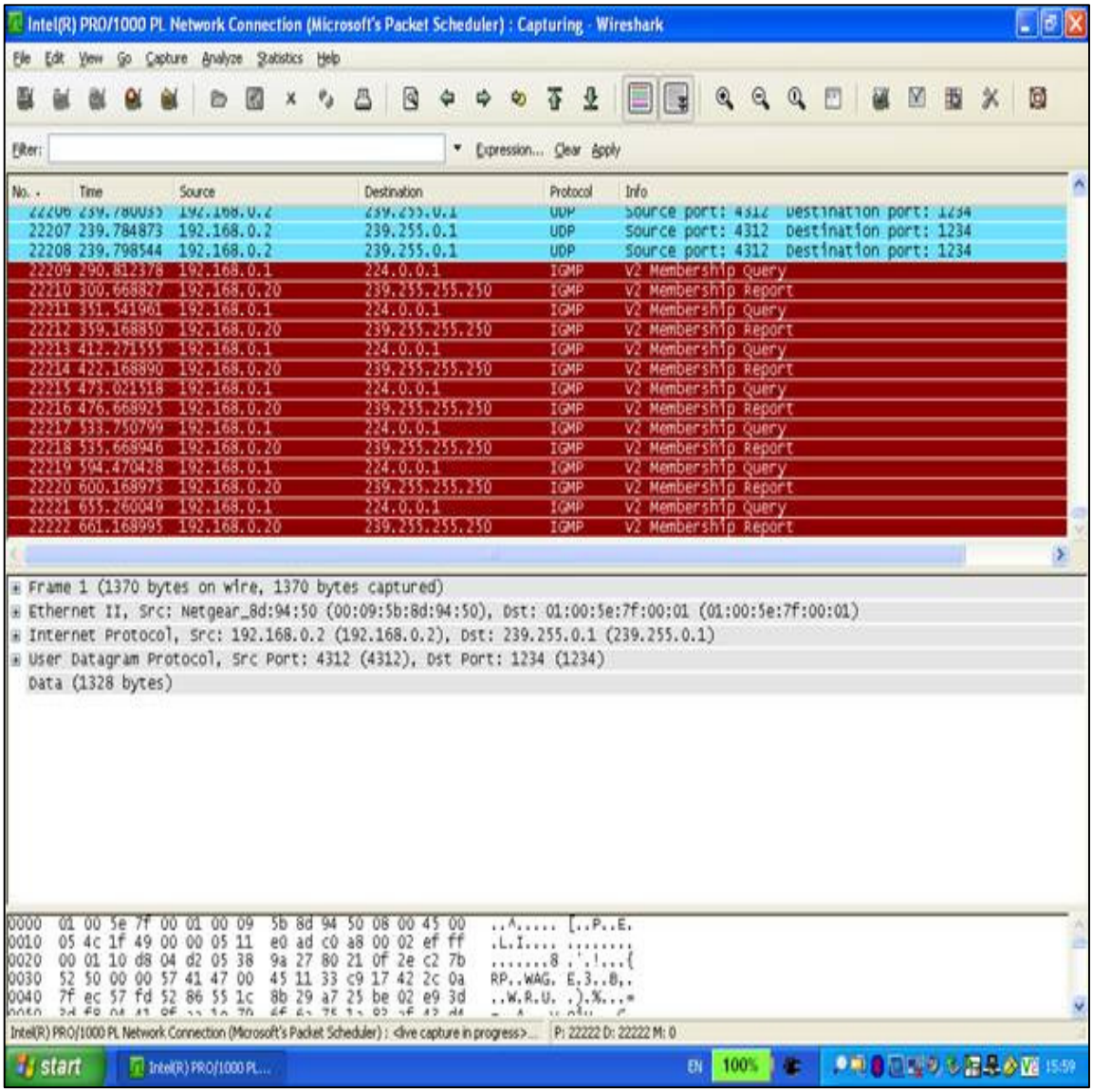


Fig.2

Fig.2 show the output on one of the clients once the Client stops claiming Multicast membership