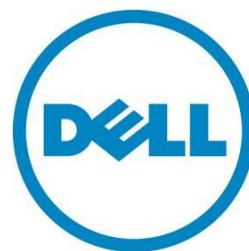# Efficient Video Distribution Networks with Multicast: IGMP Querier and PIM-DM

A Dell technical white paper

Version 1.1

Victor Teeter

Network Solutions Engineer

Contents

Introduction

Dell PowerConnect™ firmware revision 5.1 has added vast improvements in the areas of IGMP (Internet Group Management Protocol) snooping and IP Multicast Failover. Starting with PowerConnect 5.1 firmware, Dell PowerConnect users have a new set of commands to configure IGMP snooping, MLD snooping, MVR (Multicast VLAN Registration), and bridge multicast filtering. This white paper uses several of the new commands to show how an administrator would set up common video distribution networks.

PowerConnect 5.1 firmware is supported on the following Dell PowerConnect devices:

M6220	7024	7048P	8132
M6348	7024F	7048R	8132F
M8024	7024P	8024	8164
M8024k	7048	8024F	8164F

Multicast Overview

Multicast services are used to distribute streaming media, such as audio and video traffic, over the network. These applications typically generate large amounts of traffic taking up network bandwidth. Both *multicast* and *broadcast* allow a network device to send single packets to multiple destinations. The difference is broadcast is designed to forward packets to *all* nodes on the VLAN, whereas multicast is designed to only forward to nodes in a *multicast group*. Multicast is therefore a better solution when trying to conserve network bandwidth. Also, since all nodes must process every frame they receive, multicast saves processing cycles on nodes that do not need to receive the multicast frames.

The multicast model consists of groups, transmitters, and receivers. A typical multicast group contains one transmitter (or sender) and one or more receivers. The receiver sends a "group join" message to network switches and routers via the Internet Group Multicast Protocol (IGMP). The switches and routers then forward multicast traffic only to the receivers that have joined the multicast group.

Dell PowerConnect switches by default will forward multicast frames to all interfaces in a VLAN. No additional configuration is required to pass this traffic; however, the default behavior provides no benefit over using broadcast. To limit unnecessary traffic on the network, an IGMP Querier (layer 2) or PIM router (layer 3) must be seen on the network for multicast to stop broadcasting to all ports. Starting with firmware 5.1.0.0, IGMP snooping is enabled on all switches; however, this does not keep the multicast traffic from broadcasting until the switches can see a Querier or PIM router.

Note: By creating an IGMP Querier or PIM router on the network, switches are able to stop multicast frames from being broadcasted and can forward those frames to transmitters and receivers in a specified multicast group.

Switches can use *IGMP snooping* to automatically collect information about which interfaces are participating in multicast groups. The switches then use this information to direct multicast traffic away from devices that are not interested in the IP multicast traffic.

Switches that are not "multicast aware" can use static multicast groups to manually select the interfaces that will pass multicast traffic.

IGMP snooping and static multicast groups accomplish the same task. One is dynamic; requiring less setup and maintenance, while the other is static; requiring more setup and maintenance time. This paper only discusses how to set up the dynamic IGMP snooping feature with and without a PIM router. If it is desired to set up Static multicast groups, please see the documentation that came with your particular switch for instructions.

Scenarios in this Document

This document provides instructions for setting up two scenarios. In the first scenario, the desire is to keep the multicast network Layer 2 switched only, and therefore the *IGMP snooping querier* is used to perform the query functions of a Layer 3 multicast router.

The second scenario explores PIM and IGMP enabled in a Layer 3 network with IP multicast routing between multiple VLANs. In this case, the IP multicast router acts as the IGMP querier.

Firmware Versions

The firmware used on the PowerConnect 8100 switches in these scenarios was version 5.1.0.0. Only attempt these setups after updating firmware to 5.1.x.x or later on each participating switch. As always, it is best practice to update all BIOS code on computers and use the latest NIC drivers.

Scenario 1: Layer 2 Video Distribution on a Single VLAN (Using IGMP Querier)

The first scenario for this paper consists of three PowerConnect switches, a video server, and multiple clients to receive the streaming video. The particular setup for generating this document contains a Dell PowerEdge R815 (Video Server), three Dell PowerConnect 8132 switches, and three Dell laptops for use as multicast receivers (Figure 2). VLC Media Player is used on a Windows server and Windows clients to generate and receive the multicast stream. The server is Windows Server 2008 R2 Enterprise, and clients include both Windows 7 and Windows XP.

This white paper includes instructions on how to set up and configure the hardware, how to download and install the VLC Media Player, and then how to test the entire setup using VLC.

Figure 1.   Single VLAN Video Distribution Using IGMP Querier
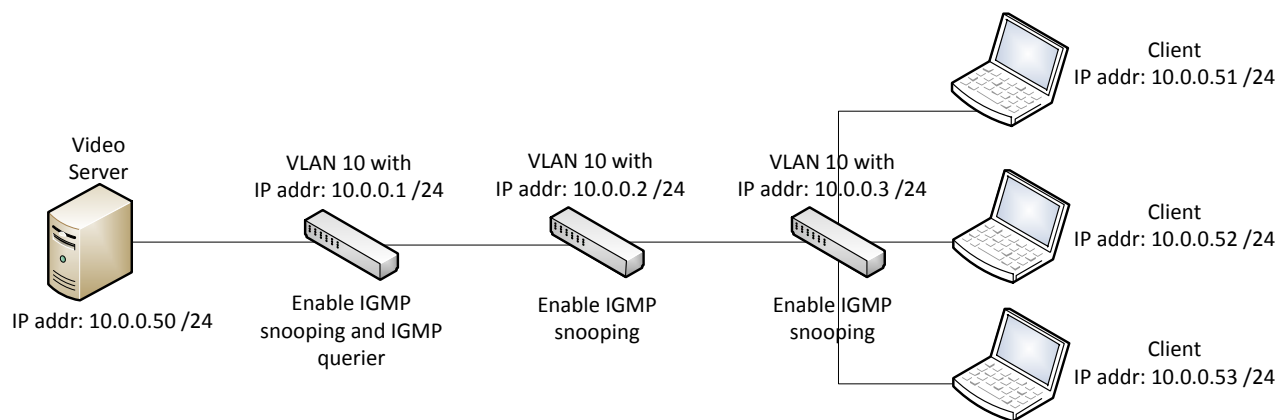
Without IGMP snooping, multicast packets are broadcast throughout the network, causing unnecessary traffic. This impedes the efficiency of both the network and every system on the network that has to process and drop multicast packets they were not expecting. For example, all three laptops in Figure 2 would receive the traffic although only one or two of them may desire to.

Follow the steps below to set up and test the Multicast topology shown in Figure 2.

Multicast Using IGMP Querier Setup (CLI commands are given below)

Note: Best practice, particularly in a production environment, is to configure new switches before connecting them into the existing network. In an isolated test network such as this, it is okay to connect the switches together in the first step, provided they have no significant configuration other than for management. This will allow the administrator to telnet to each switch for configuring. Otherwise, use a console cable to each switch for configuring, and make cabling the switches together the last step.

1. Bring up all three switches and connect them together in a daisy chain with a LAG or single cable between switches as shown in Figure 2.

2. On all three switches, create VLAN 10. Assign VLAN 10 an IP address *on each switch* so that each switch's VLAN 10 is on the same subnet.

   Note: Non-querier switches such as the second and third switch here, do not require a VLAN IP address, but it is nice to have for management and troubleshooting purposes.

3. For each trunk port (going from one switch to another switch), configure the port in *trunk* mode and assign it to VLAN 10.

4. Plug in the server at one end of the network and the clients at the opposite end as shown in Figure 2.

5. On the two end switches, for each access port (going to a video server or client), configure the port in *access* mode and assign them VLAN 10.

6. Provide the server and each client an IP address within the same subnet as VLAN 10. For this example we gave the video server an IP address of 10.0.0.50, and we gave the clients IP addresses 10.0.0.51 through 10.0.0.53.

7. From a client, ping the server and all three VLAN IP addresses on the three switches to ensure the network is configured correctly.

8. Enable IGMP snooping on VLAN 10 on all three switches.

   Note: With PowerConnect 5.1 and later firmware, IGMP snooping is enabled globally and on all VLANs by default. The *vlan* parameter is used to enable IGMP snooping on a specific VLAN, and the *no* parameter is used to remove IGMP snooping from a particular VLAN.

9. Remove IGMP snooping on VLAN 1.

10. Enable IGMP querier on the switch closest to the video server.

On a layer 2 network with a single VLAN, IGMP snooping must be enabled on all switches in the multicast route. With PowerConnect 5.1, IGMP snooping is enabled by default. A PIM router is not required for Multicast Routing to occur on a layer 2 network with one VLAN.

CLI Commands

Switch 1. Enter or cut and paste the following on the first switch (closest to the Video Server):

```
configure
vlan database
    vlan 10
    exit
interface vlan 10
    ip address 10.0.0.1 255.255.255.0
    exit
no ip igmp snooping vlan 1
ip igmp snooping querier
ip igmp snooping querier query-interval 20      ← set to 20 to speed up test (see CLI
ip igmp snooping querier vlan 10                            guide for more details)
interface Te1/0/23                              ← connected to Video Server
    switchport access vlan 10
    switchport mode access
    exit
interface Te1/0/24                              ← connected to second switch
    switchport mode trunk
    switchport trunk allowed vlan 10
    switchport trunk native vlan 10
    exit
```

Switch 2. Enter or cut and paste the following on the middle switch:

```
configure
vlan database
    vlan 10
    exit
interface vlan 10
    ip address 10.0.0.2 255.255.255.0
    exit
no ip igmp snooping vlan 1
interface Te1/0/23                              ← connected to first switch
    switchport mode trunk
    switchport trunk native vlan 10
    switchport trunk allowed vlan 10
    exit
interface Te1/0/24                              ← connected to third switch
    switchport mode trunk
    switchport trunk native vlan 10
    switchport trunk allowed vlan 10
    exit
```

7

Switch 3. Enter or cut and paste the following on the third switch (closest to clients):

```
configure
vlan database
    vlan 10
    exit
interface vlan 10
    ip address 10.0.0.3 255.255.255.0
    exit
no ip igmp snooping vlan 1
interface range Te1/0/21-23          ← 3 ports connected to 3 clients
    switchport access vlan 10
    switchport mode access
    exit
interface Te1/0/24                    ← connected to middle switch
    switchport mode trunk
    switchport trunk native vlan 10
    switchport trunk allowed vlan 10
    exit
```

Server and Client Setup

1. Download VLC Media Player for Windows:
    http://www.videolan.org/vlc/download-windows.html

    Note: In writing this paper, version 2.0.5 was used for the server and versions 2.0.3 and 2.0.5 were used for the clients. Version 1.1.9 was also used as both sender and receiver and found to be just as stable. All were tested and may be used for either role. VLC *Media Player* software is also used as the steaming server software on the Video Server.

2. Install VLC to the server and all clients that you want to receive streaming video; taking all defaults during the install process.

Create a Multicast Video

From the Dell PowerEdge R815 Multicast Server (Sender):

1. Start VLC Media Player.

2. Select **Media -> Streaming… -> Add.**

3. Browse to a video file (we used MP4 and WMA/WMV files for streaming). Click **Open**.

4. Click **Stream** at the bottom of the window.

5. At the **Stream Output** window, click **Next**.

6. Under **Destinations**, select **RTP/MPEG Transport Stream** from the pull-down menu.

7. Check the **Display Locally** box, and click **Add.**

8. In the **Address** field, enter a valid IPv4 multicast group address (we used **239.0.0.25**).

    ⚠️ **Caution: Some multicast addresses in the multicast range are reserved. It is best to use an address of 239.X.Y.Z, where X is _not_ 0, 128, 144, 160, _OR_ Y is not 0, _OR_ Z is not 1, 2, 3, or 4, or 13. Using a reserved address will impede you network's efficiency. Table 1 provides some examples:**

Table 1.   Examples of Multicast Addresses

Good (non-reserved) multicast addresses			Bad (reserved) multicast addresses		
239.0.0.5	239.0.0.6	239.0.100.99	239.0.0.1	239.0.0.2	239.0.0.13
239.1.0.2	239.3.0.1	239.0.1.1	239.128.0.4	239.144.0.1	239.0.0.3

9. Base Port must be **5004**.

    Note: Port 5004 is assigned to RTP media data only. See http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml for more information about port assignments.

10. Make sure there is a check in the **Activate Transcoding** checkbox.

11. If using an MP4 file, set the **Profile** pull-down menu to either MP4 profile:

    a. **Video – H.264 + ACC (MP4),** or
    b. **Video – H.264 + MP3 (MP4)**

    If using a WMA/WMV file, use Profile: **Video – WMV + WMA**

12. Click **Stream**. A multicast group is now created for others to join.

    Note: Allow a few seconds for the video to begin playing locally on the Video Server. At that point, the video is also being transmitted to the multicast stream.

    Note: Some MP4 files will only display the first video frame locally on the server, but are still being streamed to the network, which is seen by the progress bar below the display. To get around this issue, stream WMV/WMA or other files.

13. Pressing the Loop button at the bottom of the VLC screen will keep the file playing in a continuous loop.   This is very helpful when setting up clients for testing.

From a Multicast Client (Receiver):

1. Start VLC Player.

2. Select **Media -> Open Network Stream...**

3. Enter the Network URL**: RTP://239.0.0.25:5004**   (same address from steps 8 and 9 above).

4.   Click **Play.**

⚠️   **CAUTION: Seeing the video playing on the client does not ensure multicast is working, because it may be receiving a broadcast stream if multicast is not set up correctly. Be sure to test the multicast setup as instructed in the next section.**

The client port has now joined the multicast group. Allow a few seconds for the video to begin playing. When the Loop button on the server is pressed in, the video will repeat on the clients as well.

5.   Repeat these steps on other receiver clients on the network who want to join the multicast group and view the video.

Testing the Multicast Setup

To check the Multicast IGMP setup on each switch, run the show commands for IGMP and multicast.

Table 2.   Show Commands for IGMP and Multicast

Show Commands	Description
show statistics tengigabitethernet <port> | include Multicast	Shows number of multicast packets sent/received on port specified.
show ip igmp snooping groups	Run on IGMP snooping switches to show ports that have joined the group. This command can be used seconds after joining or leaving a group to verify the ports have in fact joined or left the group. For this example, look for the group with an IP ending in 0.0.1. This can be run on any switch, but only IGMP switches will show entries.
show ip igmp snooping mrouter	Run on IGMP snooping switches to show the port that knows where the server is. This can be run on any IGMP snooping switches. Other switches will not show any entries.

Use Wireshark on each client to see the UDP protocol frames being received at the client once it joins a multicast group (hint: the UDP packet's destination address will be 239.0.0.1). Upon leaving the group (using the stop button on the VLC player), you should notice the UDP protocol frames in Wireshark will stop being received on the client/receiver port on the switch. If pressing the Stop button on the VLC player doesn't stop the UDP packets from coming to the client (usually within a few seconds), then Multicast is not working and the client ports are receiving video broadcasts. Recheck your settings and also see *Troubleshooting Tips* below.

Visit http://www.wireshark.org/download.html to download the latest Wireshark.

Troubleshooting Tips

If you are receiving video at the clients but no ports are showing up under 0.0.1 from the **show ip igmp snooping groups** command, then Multicast is not working. They are receiving video because the traffic is still being broadcasted to all ports (this is the default behavior of the switches). Recheck settings on all switches.

If VLC on the client is stopped (you must press the Stop button to leave the multicast group), but Wireshark is showing UDP traffic from 239.0.0.1, then the video is being broadcasted to all ports and Multicast is not working. Check settings on all switches. Keep in mind that when the VLC client sends a "leave group" message, that it takes a few seconds before the UDP frames stop.

Each time you want to leave the multicast group, be sure to do so by pressing the Stop button at the *bottom* of the VLC media player or by closing the window using the X button. Pressing *pause* within the player will *not* leave the group.

If the UDP frames are not making it to the receiver port and no video is seen at the receiver, the time to live (TTL) value may need to be increased when starting the stream from the server. To do this, in step 12 above, instead of clicking **Stream**, click **Next**, and set the TTL to 16. Then click **Stream** to continue. This is only necessary on a routed network and does not apply to a "layer 2 only" network.

Some MP4 files will only display the first video frame locally on the VLC Video server, but are still being streamed to the clients, which can be verified by the progress bar below the display. To get around this issue, stream WMV/WMA or other files.

If you see traffic flooding on all ports of VLAN 10, make sure the snooping switch has learned an mrouter port by using the command **show ip igmp snooping mrouter**.

Scenario 2: Layer 3 Video Distribution with Multiple VLANs (Using PIM-DM)

The second scenario consists of two switches, two video servers and multiple clients to receive the streaming videos. The particular setup for generating this document contains two Dell PowerEdge R815 (Video Servers), two Dell PowerConnect 8132 switches, and three Dell laptops for use as multicast receivers (Figure 2Figure 2). VLC Media Player is used on a Windows server and Windows clients to generate and receive the multicast stream. The servers have Windows Server 2008 R2 Enterprise installed, and clients include both Windows 7 and Windows XP.

This white paper includes instructions on how to set up and configure the hardware, how to download and install the VLC Media Player, and then how to test the entire setup using VLC. Static routes are used for this demonstration, though OSPF or RIP will also work.

Figure 2.   Multiple VLAN Video Distribution Using PIM-DM
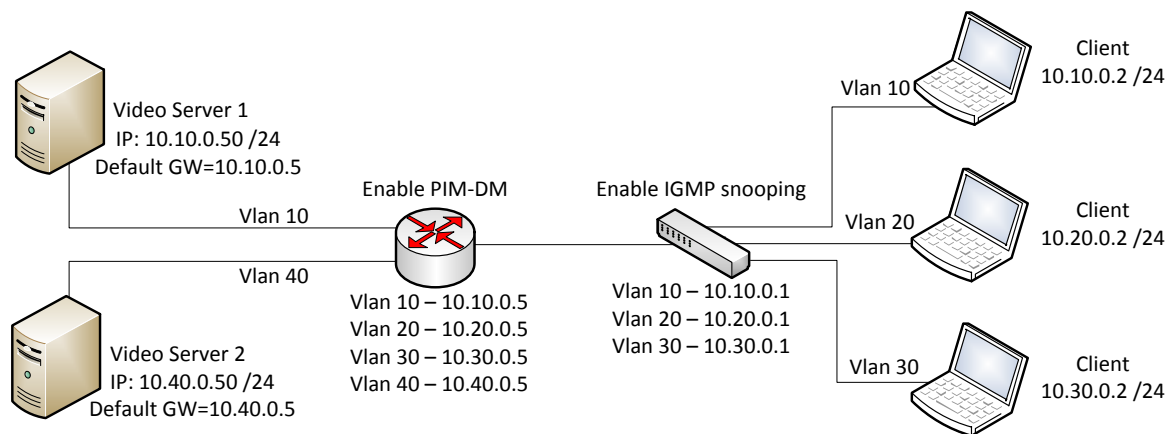
This scenario enables PIM on a switch to show how it routes multicast frames between VLANs. Enabling PIM causes an IP routing switch to become a Multicast Router (or PIM Router). The Multicast PIM router performs the same function in the Layer 3 network as the IGMP querier does in the Layer 2 network as seen in Scenario 1.

Follow the steps below to set up and test the Layer 3 Multicast topology shown in Figure 2.

Multicast Using PIM-DM Setup (CLI commands are below)

Note: Best practice, particularly in a production environment, is to configure new switches before connecting them into the existing network. In an isolated test network such as this, it is okay to connect the switches together in the first step provided they have no significant configuration other than for management. This will allow the administrator to telnet to each switch for configuring. Otherwise, use a console cable to each switch for configuring and make cabling the switches together the last step.

1. Bring up two PowerConnect 8100 switches and connect them together with a LAG or single cable between switches as shown in Figure 2.

2. On the first switch (closest to the Video Servers), create VLANs 10, 20, 30, and 40. Assign IP address to each VLAN.

3. Enable routing, which will set up static routing on the first switch to route between VLANs.

4. Enable PIM-DM on the first switch. PIM must be set globally as well as on each VLAN.

5. Disable IGMP snooping on the first switch. Enable IGMP globally and on each VLAN.

6. Create VLANs 10, 20, and 30 on the second switch, assigning each an IP address.

Note: Layer 2 switches do not require an IP address on each VLAN, but assigning them could come in handy for troubleshooting connectivity.

7. Enable IGMP snooping on the second switch (this is enabled by default starting with firmware 5.1.x.x).

8. On both switches, for each trunk port (going from one switch to another switch), configure the port in trunk mode, allowing VLANs 10, 20, and 30 on each trunk port.

9. On both switches, for each access port (going to a video server or client), configure the port in access mode and assign them to a VLAN. For this scenario, Video Server 1 is on VLAN 10 and Video Server 2 is on VLAN 40. The first client is on VLAN 10, the second on VLAN 20, and the third on VLAN 30.

10. Plug in the server at one end of the network and the clients at the opposite end as shown in Figure 2.   Connect one client to each VLAN. Set IP addresses on clients and servers as required, and within the same subnet of the VLAN where they are attached.

11. Set the default gateway on each computer to point toward the router. For this example, each computer will have the default gateway of 10.xx.0.5, where xx is the VLAN the computer is connected to.

CLI Commands
Switch 1. Enter or cut and paste the following into the first switch (routing switch):

```
configure
vlan database
    vlan 10,20,30,40
    exit
ip routing
interface vlan 10
    ip address 10.10.0.5 255.255.255.0
    ip igmp
    ip pim
    exit
interface vlan 20
    ip address 10.20.0.5 255.255.255.0
    ip igmp
    ip pim
    exit
interface vlan 30
    ip address 10.30.0.5 255.255.255.0
    ip igmp
    ip pim
    exit
interface vlan 40
    ip address 10.40.0.5 255.255.255.0
    ip igmp
    ip pim
    exit
ip multicast
ip igmp
ip pim dense
interface Te1/0/22                          ← connected to Video Server 1 on vlan 10
    switchport access vlan 10
    exit
interface Te1/0/23                          ← connected to Video Server 2 on vlan 40
    switchport access vlan 40
    exit
interface Te1/0/24                          ← connected to second switch
    switchport mode trunk
    switchport trunk native vlan 10
    switchport trunk allowed vlan 10,20,30
    exit
```

Switch 2. Enter or cut and paste the following into the second switch:

```
configure
vlan database
    vlan 10,20,30
    exit
ip default-gateway 10.10.0.5
interface vlan 10
    ip address 10.10.0.1 255.255.255.0
    exit
interface vlan 20
    ip address 10.20.0.1 255.255.255.0
    exit
interface vlan 30
    ip address 10.30.0.1 255.255.255.0
    exit
no ip igmp snooping vlan 1
ip multicast
interface Te1/0/21                          ← connected to client on vlan 10
    switchport access vlan 10
    exit
interface Te1/0/22                          ← connected to client on vlan 20
    switchport access vlan 20
    exit
interface Te1/0/23                          ← connected to client on vlan 30
    switchport access vlan 30
    exit
interface Te1/0/24                          ← connected to first switch
    switchport mode trunk
    switchport trunk native vlan 10
    switchport trunk allowed vlan 10,20,30
    exit
```

Server and Client Setup

1. Download VLC Media Player for Windows:
   http://www.videolan.org/vlc/download-windows.html

   Note: In writing this paper, version 2.0.5 was used for the server and 2.0.3 for the client. Version 1.1.9 was also used as both sender and receiver and found to be very stable. All were tested and may be used for either role. VLC Media Player software is also used as the steaming server software on the Video Server.

2. Install VLC to the server and all clients you wish to receive streaming video, taking all defaults during the install process.

Create a Multicast Video

From a Dell PowerEdge R815 Multicast Server (Sender):

1. Start VLC Media Player.

2. Select Media -> Streaming... -> Add.

3. Browse to a video file (we used MP4 and WMA/WMV files for streaming). Click Open.

4. Click Stream at the bottom of the window.

5. In the **Stream Output** window, click Next.

6. Under **Destinations**, select RTP/MPEG Transport Stream from the pull-down menu.

7. Check the **Display Locally** box, and click Add.

8. In the **Address** field, enter a valid IPv4 multicast group address (we used 239.0.0.25 on Video Server 1 and 239.0.0.26 on Video Server 2).

   Note: Each multicast stream must have a unique multicast group address.

   Caution: Some multicast addresses in the multicast range are reserved. It is best to use an address of 239.X.Y.Z, where X is _not_ 0, 128, 144, 160, _OR_ Y is not 0, _OR_ Z is not 1, 2, 3, or 4, or 13. Using a reserved address will impede you network's efficiency.

Table 3 provides some examples of good and bad multicast addresses.

Table 3.   Examples of Multicast Addresses

Good (non-reserved) multicast addresses			Bad (reserved) multicast addresses		
239.0.0.5	239.0.0.6	239.0.100.99	239.0.0.1	239.0.0.2	239.0.0.13
239.1.0.2	239.3.0.1	239.0.1.1	239.128.0.4	239.144.0.1	239.0.0.3

9. Base Port should be 5004. Port 5004 is assigned to RTP media data only. See http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml for more information.

10. Make sure there is a check in the **Activate Transcoding** checkbox.

11. If using an MP4 file, set the **Profile** pull-down menu to either MP4 profile:

    a. **Video – H.264 + ACC (MP4),** or
    b. **Video – H.264 + MP3 (MP4)**

    If using a WMA/WMV file, use Profile: **Video – WMV + WMA.**

12. Click Next. Increase the TTL (time to live) value to 16. Depending on the number of routers in the network, this value may be raised or lowered at a later time.

13. Click Stream. A multicast group is now created for clients to join.

Note: Allow a few seconds for the video to begin playing locally on the Video Server. At that point, the video is also being transmitted to the multicast stream.

Note: Some MP4 files will only display the first video frame locally on the server, but are still being streamed to the clients, which is seen by the progress bar below the display. To get around this issue, stream WMV/WMA or other files.

14. Pressing the Loop button at the bottom of the VLC screen will keep the file playing in a continuous loop. This is optional but is very helpful when setting up clients for testing.

From a Multicast Client (Receiver):

1. Start VLC Player.

2. Select Media **->** Open Network Stream...

3. Enter the Network URL: RTP://239.0.0.xx:5004   (an address from steps 8 and 9 above).

4. Click Play.

⚠ **CAUTION: Seeing the video playing on the client does not ensure multicast is working, because it may be receiving a broadcast stream if multicast is not set up correctly. Be sure to test the multicast setup as instructed in the next section.**

The client port has now joined the multicast group. Allow a few seconds for the video to begin playing. When the Loop button on the server is pressed in, the video will repeat on the clients as well.

Repeat the Sender and Receiver steps on the other sender (server) and receivers (clients) on the network to create multiple multicasts groups and clients viewing multiple videos.

Testing the Multicast Setup

To check the Multicast IGMP setup on each switch, run the show commands for IGMP and multicast and run Wireshark to capture and analyze the traffic.

Table 4.   Show Commands for IGMP and Multicast

Show Commands	Description
show statistics tengigabitethernet \<port\> | include Multicast	Shows number of multicast packets sent/received on port specified.
show ip igmp snooping groups	Run from a IGMP snooping switch to show ports that have joined the group. This command can be used seconds after joining or leaving a group to verify the ports have in fact joined or left the group. For this example, look for the group with an IP ending in 0.0.1. This can be run on an IGMP snooping switch. Other switches will not show any entries.

Show Commands	Description
show ip igmp snooping mrouter	Run from an IGMP snooping switch to show the port that knows where the server is. This can be run on any IGMP snooping switches. Other switches will not show any entries.
show ip igmp membership	Run from the PIM router to see what VLANs and IP interfaces have joined the multicast group.
show ip igmp groups	Shows the Querier status (routers only), IP address, and vlan interface for each group.

Use Wireshark on each client to see the UDP protocol frames being received at the client once it joins a multicast group (hint: the UDP packets destination address will be 239.0.0.x). Upon leaving the group (using the stop button on the VLC player), you should notice the UDP protocol frames in Wireshark will stop being received on the client/receiver port on the switch.   If pressing the stop button on the VLC player doesn't stop the UDP packets from coming to the client (usually within 30 seconds), then multicast is not working and the client ports are receiving video broadcasts. Recheck your settings and also see *Troubleshooting Tips* below.

Visit http://www.wireshark.org/download.html to download the latest Wireshark.

Troubleshooting Tips

If you are receiving video at the clients but no ports are showing up under 0.0.1 or 0.0.2 from the **show ip igmp snooping groups** command, then Multicast is not working. They are receiving video because the traffic is still being broadcasted to all ports (this is the default behavior of the switches). Recheck settings on all switches. Also read *Testing the Multicast Setup*.

If VLC on the client is stopped (you must press the stop button to leave the multicast group), but Wireshark is showing UDP traffic from 239.0.0.x, then the video is being broadcasted to all ports and multicast is not working. Check settings on all switches. Keep in mind that when the VLC client sends a "leave group" message, that it takes a few seconds before the UDP frames stop. Also read *Testing the Multicast Setup.*

Each time you want to leave the multicast group, be sure to do so by pressing the stop button at the *bottom* of the VLC media player or by closing the window using the X button. Pressing *pause* within the player will *not* leave the group.

If the UDP frames are not making it to the receiver port and no video is seen at the receiver, the time to live (TTL) value may need to be increased when starting the stream from the server.   To do this, return to step 12 above and increase the TTL value. Then click Stream to continue.

Some MP4 files will only display the first video frame locally on the VLC Video server, but are still being streamed to the clients, which can be verified by the progress bar below the display. To get around this issue, stream WMV/WMA or other files.

Keep in mind these general rules:

➢ PIM does not route. Routing must be working for it to work.
➢ No more than 3 hops should be used between the transmitter and receiver when multicast is used. This does not include a Rendezvous Point when using PIM-SM, but only refers to the shortest path that is taken after pruning.
➢ Rendezvous Points (first and redundant) when using PIM-SM need to be as close to the center of the network as much as possible.

Multicast Frames Explained

Multicast IP addresses fall in the range of 224.0.0.1 and 239.255.255.255. These multicast addresses are only used as a destination, never as a source address. The destination addresses given to multicast traffic is a combination of the number 01:00:5E and the last 23 bits of the multicast IP address (ignoring the first 9 bits). Since the first octet of the MAC address has a value of 1 (01:xx:xx:xx:xx:xx), it denotes it as a multicast MAC address and is therefore handled differently in the switch than a unicast MAC address.

For example, the IP address 239.0.0.1 has a destination address of 01:00:5E:00:00:01, and the multicast IP address of 239.0.0.2 has a destination address of 01:00:5E:00:00:02. These multicast destination addresses will be seen in every multicast UDP packet captured in Wireshark.

Bandwidth Considerations

Video Streaming in high quantity or high quality takes considerable network bandwidth. Test and fine-tune your equipment thoroughly using the User Guide and CLI Reference Guide for your particular switches. LAGs used on access ports and trunks can also provide additional bandwidth to allow the network and servers to handle the traffic. When using PIM-SM (not covered in this document), place the RP in a strategic location that is most beneficial for efficient video distribution. More information about PIM-SM, including an example, can be found in the User Guide.

Useful Links

Table 5.   Reference Links

VLC Media Player	http://www.videolan.org/vlc/download-windows.html
WireShark	http://www.wireshark.org/download.html
IPv4 Multicast Address Assignments	https://tools.ietf.org/html/rfc5771
Internet Group Management Protocol, Version 3	https://tools.ietf.org/html/rfc3376
Protocol Independent Multicast - Dense Mode (PIM-DM)	https://tools.ietf.org/html/rfc3973
Protocol Independent Multicast - Sparse Mode (PIM-SM)	https://tools.ietf.org/html/rfc4601
IPv4 Multicast Address Space Registry	http://www.iana.org/assignments/multicast-addresses/multicast-addresses.xml
Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches	http://tools.ietf.org/html/rfc4541

About Dell

Dell is a leading technology provider to commercial and public enterprises around the world. For more information on Dell PowerConnect products and features, visit www.dell.com/powerconnect.