

APPLICATION NOTE

Multicast Routing in K2 Summit

Tony Combs, *Senior Network Analyst*

February 2011

The advantages of using multicast over unicast
for one-to-many media file transfers.

Contents

Understanding and Using Multicast	1
Introduction	1
How Do I Join a Multicast Group? What is IGMP?	1
What Multicast Routing Protocols Are Used Today?	2
Why is DVMRP not Efficient?	2
What Do (*,G) and (S,G) Mean ?	2
What is PIM SM Rendezvous Point (RP)?	2
How Does a Source Send to a Group?	3
Can Multicasting Use TCP?	4
.....	
References	5
How Can I Know Which Multicast IP Addresses To Use?	5
.....	
Appendix	5
.....	

Understanding and Using Multicast

Introduction

The most significant benefit of using multicast over unicast with K2 Summit™ media servers is that you can save significantly on bandwidth. When using unicast, you have to send a source to each destination, causing you to send duplicates. When using multicast, you can send a source to multiple receivers without duplicating the bandwidth to each receiver.

How Do I Join a Multicast Group? What is IGMP?

A computer joins a multicast group by sending an IGMP membership report (IGMP is common to all multicast router protocols). It then sends a join request. IGMP is a communications protocol used to establish multicast group memberships between routers and hosts.

What takes place when an end node requests a channel change or different multicast group?

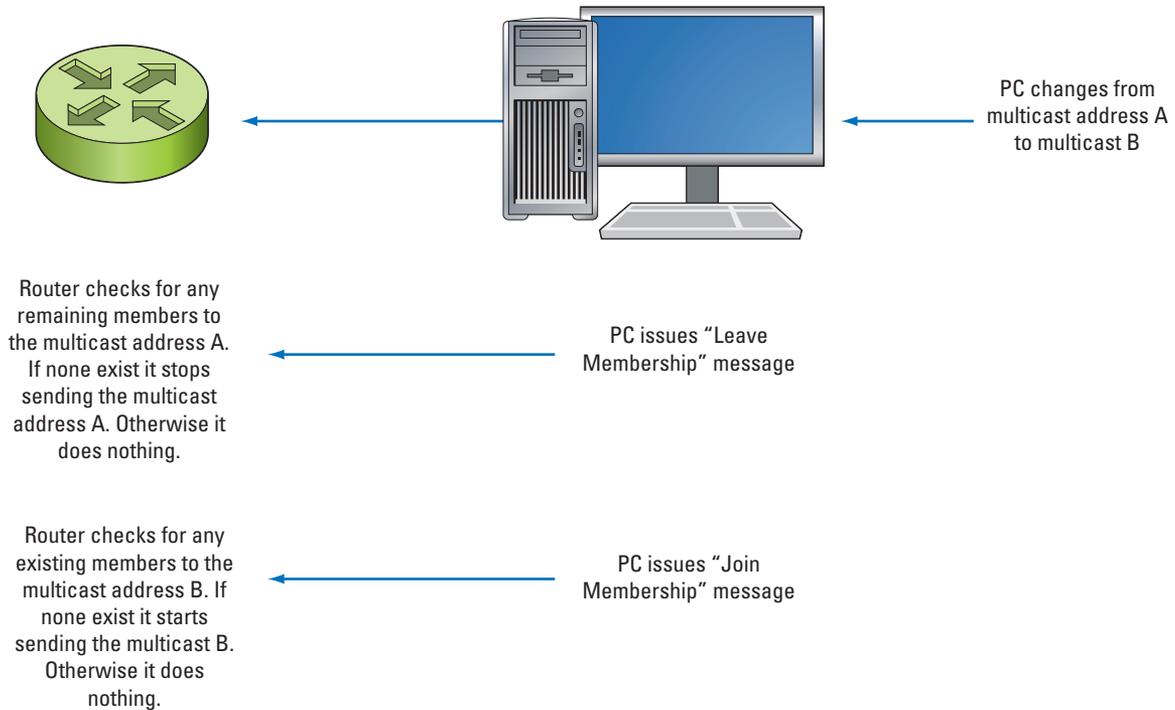


Figure 1 – Node sends an IGMP leave message, membership report, and then a join message.

Understanding and Using Multicast (cont.)

What Multicast Routing Protocols Are Used Today?

For some time, the original multicast routing protocol was “dense mode.” PIM-DM makes an assumption that all receivers want to initially receive all multicast traffic. All traffic is flooded throughout the network until the receiver sends a “leave” message to stop receiving all traffic and “prunes” that traffic back. DVMRP, otherwise known as Distance Vector Multicast Routing Protocol, is the oldest multicast routing protocol and is similar to PIM-DM

The most recent multicast routing protocol is “sparse mode” or PIM-SM. It assumed that no receiver wanted multicast traffic until it asked for it. There is no flooding with sparse mode.

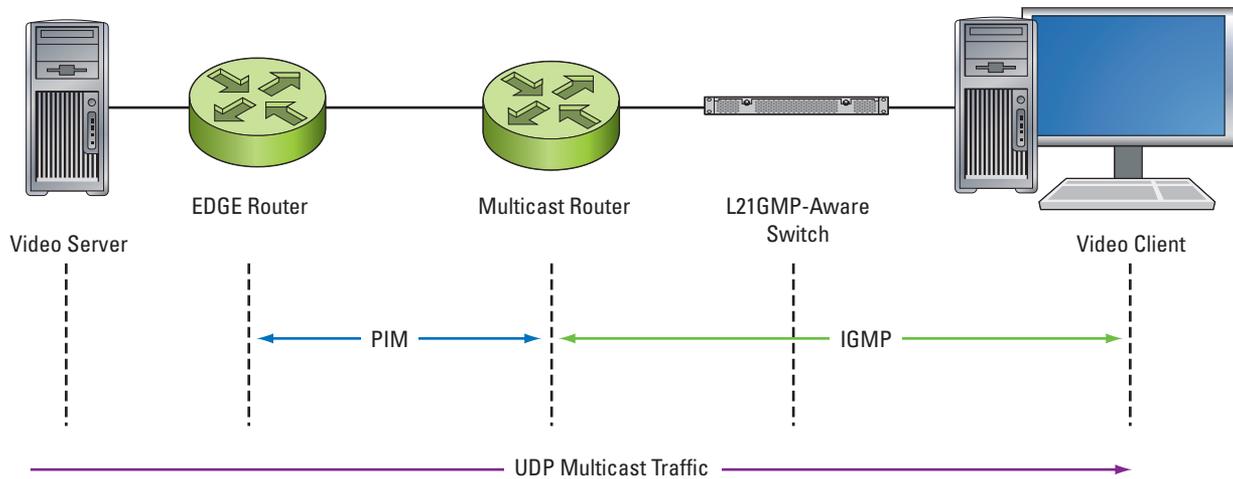


Figure 2 – Video server streams out multicast video to the EDGE router and Multicast router.

Why is DVMRP not Efficient?

DVMRP constructs its own routing tables independent of the unicast routing tables. This is not an efficient process. It also tends to flood frequently and does not know how to prune messages efficiently. PIM is more efficient because it references the unicast routing table to route multicast.

What Do (*,G) and (S,G) Mean ?

Any multicast transmission has a multicast group address (G). Each group can have more than one source (S) and each source would have a Class: A, B, or C or a CIDR address. When we say (S,G) we mean a particular source and group.

What is PIM SM Rendezvous Point (RP)?

Think of this as being domain oriented and within that domain the RP’s address is distributed throughout the domain. When the end node or receiver wants to join a multicast group, it sends a membership report to the router, which sends a G message to the route processor. In this case, you may have multiple routers and one of them will be deemed the DR or designated router. When a node wants to transmit multicast, the DR unicasts the multicast data to the RP, which strips off the encapsulation data and multicasts it to the group members.

Understanding and Using Multicast (cont.)

How Does a Source Send to a Group?

The source node sends packets to the appropriate Class D group address. The packets are then captured by the DR. If there is more than one hop, the packets are encapsulated and unicast to the RP. After the initial transmission is established, the RP sends S and G join messages to the source. When the source packets are received by the DR, the encapsulation is stopped and the native multicast packets of the sources output are sent to the RP.

PIM-SM will switch from the Shared Tree to the Shortest Path Tree (SPT). A receiver's first hop router, or DR, will issue an S and G join message to the source. This join message travels up the Shared Tree until it finds the source, or a router with an S and G state that is already receiving from the source. At this point, multicast traffic starts flowing down the SPT to the receiver. At the router—where the Shared Tree and the SPT diverge—traffic will be received from both trees. That router will then issue a prune towards the RP, stopping the traffic flowing down that branch of the Shared Tree. Eventually, a steady state may be reached, where all traffic is flowing down the SPT, and when the RP can cease transmissions.

PIM builds an S and G entry in a Source-Rooted Tree (SRT). When multiple routers are connected to a multi-access network, one router becomes the designated router. The designated router receives data from the source on interface 1/0 and multicasts the data to its downstream neighbors on interfaces 1/1, 2/0, and 2/1. In the designated router routing table, the entry for this operation lists the source as the IP address of the source and the group as the IP address of the multicast group.

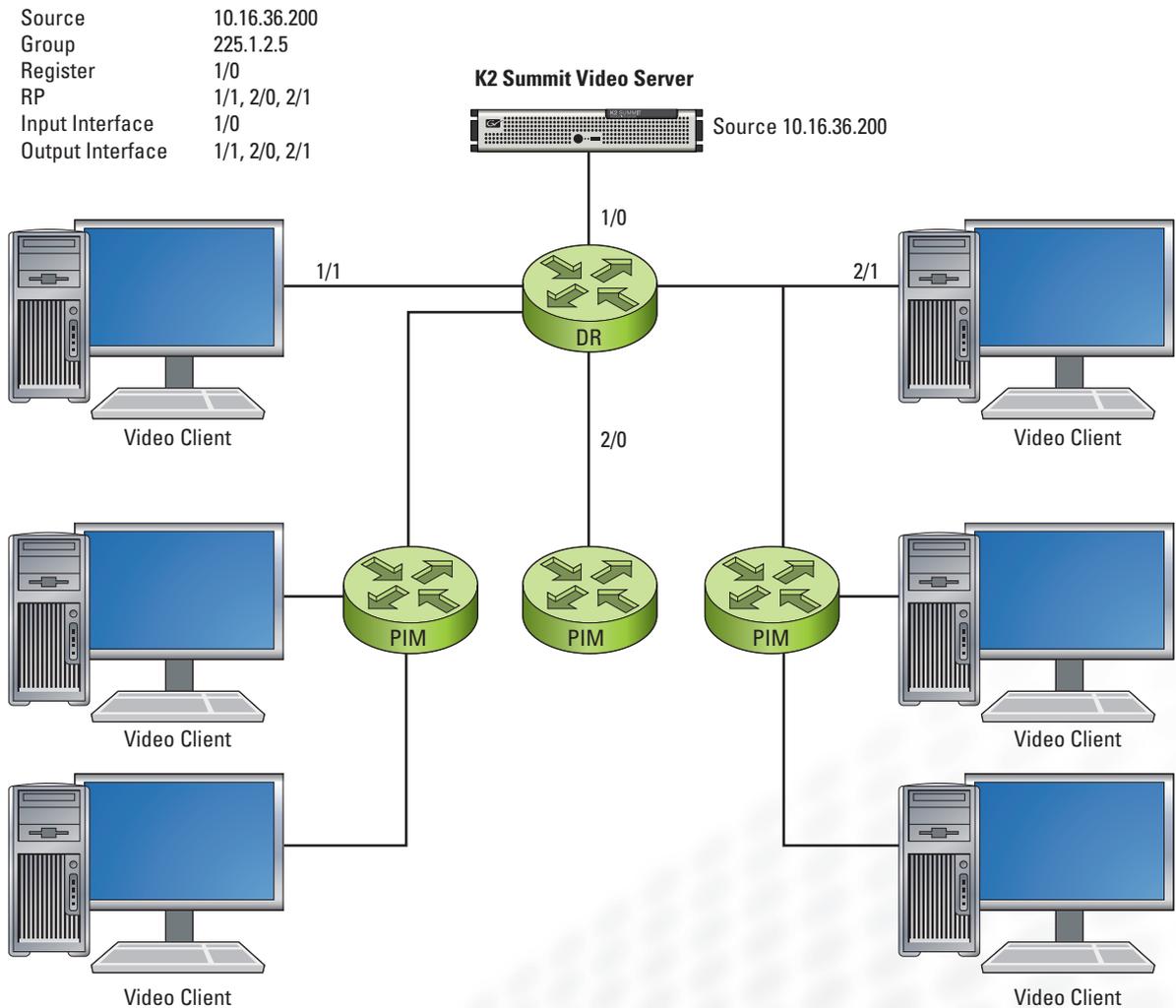


Figure 3 – Source multicast stream is registered on the router input I/O port.

Understanding and Using Multicast (cont.)

Can Multicasting Use TCP?

No, multicast uses UDP. TCP transmits ACK packets between the receiver and transmitter to determine if the packets have arrived.

Open Systems Interconnection Model

Layer	Description	Protocols
Application Layer (7)	This layer represents the application making use of communication services / It is responsible for the semantics of the data being exchanged by the application	FTP File Transfer Protocol HTTP Hypertext Transfer Protocol IMAP4 Internet Message Access Protocol rev 4 IMPPpre/IMPPmes Instant Messaging and Presence Protocols IPDC IP Device Control IRC Internet Relay Chat Protocol NTP Network Time Protocol POP3 Post Office Protocol version 3 Radius Remote Authentication Dial-In User Service RLOGIN Remote Login RTSP Real-time Streaming Protocol SCTP Stream Control Transmission Protocol S-HTTP Secure Hypertext Transfer Protocol SLP Service Location Protocol SMTP Simple Mail Transfer Protocol SNMP Simple Network Management Protocol SOCKS Socket Secure (Server) TACACS+ Terminal Access Controller Access Control System TELNET TCP/IP Terminal Emulation Protocol TFTP Trivial File Transfer Protocol WCCP Web Cache Coordination Protocol X-Window X Window
Presentation Layer (6)	This layer is responsible for the syntax of the data being exchanged by the application. If two applications apply different syntax to the same piece of data this layer is responsible for "mapping" the data to/from the different syntax formats	RDP Remote Desktop Protocol ASCII Network Data Representation External Data Representation
Session Layer (5)	This layer is responsible for the managing the connection between two or more communicating applications	BGMP Border Gateway Multicast Protocol DNS Domain Name iSCSI Small Computer Systems Interface LDAP Lightweight Directory Access Protocol NetBIOS/IP NetBIOS/IP for TCP/IP Environment
Transport Layer (4)	This layer performs data transfers for tasks such as flow control (acknowledged data transfers) and fragmentation/reassembly	TCP Transmission Control Protocol UDP User Datagram Protocol
Network Layer (3)	This layer is responsible for address management and the routing of packets through the network	DHCP Dynamic Host Configuration Protocol DVMRP Distance Vector Multicast Routing Protocol ICMP/ICMPv6 Internet Control Message Protocol IGMP Internet Group Management Protocol IP Internet Protocol version 4 IPv6 Internet Protocol version 6 MARS Multicast Address Resolution Server PIM Protocol Independent Multicast-Sparse Mode (PIM-SM) RIP2 Routing Information Protocol VRRP Virtual Router Redundancy Protocol
Data Link Layer (2)	This layers performs transmission media access control (MAC) functions. It will govern the transmission of data provided by the upper layers and, when necessary, execute error recovery strategies	ARP/RARP Address Resolution Protocol/Reverse Address DCAP Data Link Switching Client Access Protocol
Physical Layer (1)	This layer performs tasks such as: encoding/decoding bits on the physical transmission media, sensing the idle status of the media, and sensing error conditions on the media (e.g., collisions)	CAT5/6 Fiber

References

How Can I Know Which Multicast IP Addresses To Use?

<http://www.iana.org/assignments/multicast-addresses/multicast-addresses.xml>

Class D Subnet Range

224.0.0.0 - 239.255.255.255

Appendix

Vendor	Hardware Platforms	Software	Protocols Supported	Port Speed
Cisco	CAT 3750-X	IP Base Software	RFC2365 Multicast Routing RFC4601 PIM-SM RFC4541 IGMP Snooping	10/100/1000
Cisco	CAT 3560-X	IP Base Software	RFC2365 Multicast Routing RFC4601 PIM-SM RFC4541 IGMP Snooping	10/100/1000
Cisco	CAT 3750-E	IP Base Software	RFC2365 Multicast Routing RFC4601 PIM-SM RFC4541 IGMP Snooping	10/100/1000
Cisco	CAT6500	IP Base Software	RFC2365 Multicast Routing RFC4601 PIM-SM RFC4541 IGMP Snooping	10/100/1000
Cisco	CAT7600	IP Base Software	RFC2365 Multicast Routing RFC4601 PIM-SM RFC4541 IGMP Snooping	10/100/1000
Cisco	CAT4500	IP Base Software	RFC2365 Multicast Routing RFC4601 PIM-SM RFC4541 IGMP Snooping	10/100/1000

Appendix (cont.)

Building a VLAN on the Switch

1. Login to the switch
2. Put the switch in enable mode by typing "enable" and <enter>
3. Enter into configuration mode by typing "config t" and <enter>
4. Create a VLAN by typing "interface vlan 20" and <enter>
 - a. Within the VLAN put an IP Address on the VLAN by typing "ip address 192.168.1.1 255.255.255.0" and <enter>

Adding Ports to a VLAN

1. Login to the switch
2. Put the switch in enable mode by typing "enable" and <enter>
3. Enter into configuration mode by typing "config t" and <enter>
4. Select a port to add to a VLAN. Enter the command "interface gi1/0/1" <enter>
 - a. Make the ports and switch port and add it to a VLAN by typing "switchport" <enter> and then "switchport access vlan 20" <enter>

Configuring Routing for Standard IP Traffic and Multicast Traffic

1. Login to the switch
2. Put the switch in enable mode by typing "enable" and <enter>
3. Enter into configuration mode by typing "config t" and <enter>
4. To enable IP routing type "ip routing" <enter>
5. To enable Multicast Routing globally type "ip multicast-routing distributed" <enter>

Configuring Multicast Routing on a VLAN (to enable a VLAN to process multicast traffic)

Note: This will need to be done on a per VLAN basis if you want multicast traffic to be available on that VLAN.

1. Login to the switch
2. Put the switch in enable mode by typing "enable" and <enter>
3. Enter into configuration mode by typing "config t" and <enter>
4. You now need to decide which VLAN's you will pass multicast traffic on. Select the VLAN by typing "interface vlan 20" <enter>. This will put you into the VLAN configuration.
 - a. If you want VLAN 20 to route multicast traffic you need to enter the command "ip pim sparse-mode" <enter>

Appendix (cont.)

Troubleshooting

Checking the S and G Entries

show ip igmp groups

```
IGMP Connected Group Membership
Group Address Interface Uptime Expires Last Reporter
239.255.0.1 Ethernet1 00:10:54 00:01:10 192.168.9.1
224.0.1.40 Ethernet0 01:36:27 00:02:45 192.168.10.2
224.0.1.40 Ethernet1 01:48:15 never 192.168.9.3
```

Checking the PIM Configuration

show ip pim interface

```
Address Interface Version/Mode Nbr Query DR
Count Intvl
192.168.10.1 Ethernet0 v2/Sparse-Dense 1 30 192.168.10.2
192.168.9.3 Ethernet1 v2/Sparse-Dense 1 30 192.168.9.5
```

Checking the Multicast Route Summary

show ip mroute summary

```
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT
M - MSDP created entry, X - Proxy Join Timer Running
A - Advertised via MSDP
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode
```

Appendix (cont.)

Showing the IP Multicast Route

show ip mroute

```
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
      R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT
      M - MSDP created entry, X - Proxy Join Timer Running
      A - Advertised via MSDP
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode
```

```
(* , 239.255.0.1), 01:55:27/00:02:59, RP 192.168.7.2, flags: SJCF
  Incoming interface: Ethernet0, RPF nbr 192.168.10.2
  Outgoing interface list:
    Ethernet1, Forward/Sparse, 01:55:27/00:02:52
```

```
(133.33.33.32, 239.255.0.1), 01:54:43/00:02:59, flags: CJT
  Incoming interface: Ethernet0, RPF nbr 192.168.10.2
  Outgoing interface list:
    Ethernet1, Forward/Sparse, 01:54:43/00:02:52
```

```
(192.168.9.1, 239.255.0.1), 01:55:30/00:03:26, flags: CFT
  Incoming interface: Ethernet1, RPF nbr 0.0.0.0
  Outgoing interface list:
    Ethernet0, Forward/Sparse, 01:55:30/00:03:12
```

```
(* , 224.0.1.40), 1d00h/00:00:00, RP 192.168.7.2, flags: SJPCL
  Incoming interface: Ethernet0, RPF nbr 192.168.10.2
  Outgoing interface list: Null
```

Showing Which IP Multicasts are Active

show ip mroute active

```
Active IP Multicast Sources - sending >= 4 kbps

Group: 239.255.0.1, (?)
  Source: 133.33.33.32 (?)
  Rate: 10 pps/115 kbps(1sec), 235 kbps(last 23 secs), 87 kbps(life avg)
```

Appendix (cont.)

Showing Multicast Reverse Path Forwarding

```
ip rpf 133.33.33.32
```

```
RPF information for ? (133.33.33.32)
RPF interface: Ethernet0
RPF neighbor: ? (192.168.10.2)
RPF route/mask: 133.33.0.0/16
RPF type: unicast (eigrp 1)
RPF recursion count: 0
Doing distance-preferred lookups across tables
```

Debugging the IP Multicast Fast Switching Cache

```
show ip mcache
```

```
IP Multicast Fast-Switching Cache
(133.33.33.32/32, 239.255.0.1), Ethernet0, Last used: 00:00:00
Ethernet1 MAC Header: 01005E7F000100000C13DBA90800
(192.168.9.1/32, 239.255.0.1), Ethernet1, Last used: 00:00:00
Ethernet0 MAC Header: 01005E7F000100000C13DBA80800
```

Checking the IP Route in the Unicast Table and the Reverse Path Forwarding Failures in the Multicast Routing Table

```
show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set
D 192.168.9.0/24 [90/307200] via 192.168.10.1, 00:59:45, Ethernet0
C 192.168.10.0/24 is directly connected, Ethernet0
D 192.168.4.0/24 [90/11040000] via 192.168.7.1, 23:21:00, Serial0
D 192.168.5.0/24 [90/11023872] via 192.168.7.1, 23:21:02, Serial0
C 192.168.7.0/24 is directly connected, Serial0
D 133.33.0.0/16 [90/2195456] via 192.168.7.1, 1d23h, Serial0
D 192.168.1.0/24 [90/11552000] via 192.168.7.1, 22:41:27, Serial0
```

Appendix (cont.)

If you are having problems receiving and transmitting PIM packets, you can use the debug command to look at messages. When there are multiple routers on the network, you may need to run the following command on all routers involved:

debug ip pim

debug ip pim

```
PIM: Send v2 Hello on Ethernet0
PIM: Send v2 Hello on Ethernet1
PIM: Received v2 Hello on Ethernet0 from 192.168.10.2
PIM: Send v2 Hello on Ethernet0
PIM: Send v2 Hello on Ethernet1
PIM: Building Join/Prune message for 239.255.0.1
PIM: v2, for RP, Join-list: 192.168.7.2/32, RP-bit, WC-bit, S-bit
PIM: Send v2 periodic Join/Prune to RP via 192.168.10.2 (Ethernet0)
PIM: Received RP-Reachable on Ethernet0 from 192.168.7.2 for group 239.255.0.1
PIM: Update RP expiration timer (270 sec) for 239.255.0.1
```

SALES

Local and regional sales contacts can be found by visiting
www.grassvalley.com/sales

SUPPORT

Local and regional support contacts can be found by visiting
www.grassvalley.com/support