Monitoring and Troubleshooting

This chapter provides an introduction to monitoring and troubleshooting the Cisco Ethernet switches in the Cisco Wireline Video/IPTV Solution, Release 1.1.

The following major topics are presented:

Network Time Protocol (NTP)

It is important to ensure that all devices in the network are accurately synchronized to the same time source. This allows network events to be correlated (for example, for accounting, event logging, fault analysis, security incident response, and network management). The Network Time Protocol (NTP), RFC 1305, synchronizes timekeeping among a set of distributed time servers and clients.

Note There are a number of ways to configure NTP, and describing NTP completely is beyond the scope of this document. A number of resources are available on Cisco.com and the Internet regarding NTP configuration.

At a minimum, the Cisco switches should be configured as NTP clients for a reliable time source, by means of the following commands:

```
clock timezone PST -8
clock summer-time PDT recurring 1 Sun Apr 3:00 last Sun Oct 3:00

clock calendar-valid
ntp server <NTP server IP address>
ntp update-calendar
```

Syslog

Cisco IOS Software has the capability to do UNIX system logging (syslog) to a UNIX syslog server. The Cisco UNIX syslog format is compatible with 4.3 Berkeley Standard Distribution (BSD) UNIX. System logging is useful for monitoring interface status, security alerts, environmental conditions, CPU processes, and many other events on the router can be captured and analyzed by means of UNIX syslog. Management platforms such as Cisco Resource Manager Essentials (RME) and Network Analysis Toolkit (NATKit) make powerful use of syslog information to collect inventory and configuration changes.

The following is a summary and description of the recommended IOS configuration for syslog.

Global Syslog Configuration

Configure the following in global configuration mode:

```
no logging console
no logging monitor
logging buffered 16384
logging trap notifications
logging facility local7
logging host-ip
logging source-interface loopback 0
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
```

Interface Syslog Configuration

Configure the following in interface configuration mode on interfaces of interest:

```
logging event link-status
logging event bundle-status
```

Useful Syslog Commands

The following syslog commands are particularly useful:

- no logging console
- no logging monitor
- logging buffered 16384
- logging trap notifications
- logging facility local7
- logging host
- logging source-interface loopback 0
- service timestamps debug datetime localtime show-timezone msec
- logging event

no logging console

By default, all system messages are sent to the system console. Console logging is a high-priority task in Cisco IOS Software. This function was primarily designed to generate error messages to the system operator prior to a system failure. It is recommended that console logging be disabled in all device configurations to avoid a situation where the router/switch might hang while waiting for a response from a terminal. Console messages can, however, be useful during trouble isolation. In these instances, console logging should be enabled by means of the **logging console level** command, to obtain the desired level of message logging. Logging levels range from 0 to 7.

no logging monitor

This command disables logging for terminal lines other than the system console. If monitor logging is required (by means of **logging monitor debugging** or another command option), it should be enabled at the specific logging level required for the activity (see above).

logging buffered 16384

The **logging buffered** command should be added to log system messages in the internal log buffer. The logging buffer is circular. Once the logging buffer is filled, older entries are overwritten by newer entries. The size of the logging buffer is user-configurable and is specified in bytes. The size of the system buffer varies by platform. 16384 is a good default and should provide adequate logging in most cases.

logging trap notifications

This command provides notification (level 5) messaging to the specified syslog server. The default logging level for all devices (console, monitor, buffer, and traps) is debugging (level 7). Leaving the trap logging level at 7 produces many extraneous messages that are of little or no concern to the health of the network. It is recommended that the default logging level for traps be set to 5.

logging facility local7

This command sets the default logging facility/level for UNIX system logging. The syslog server receiving these messages should be configured for the same facility/level.

logging host

This command sets the IP address of the UNIX syslog server.

logging source-interface loopback 0

This command sets the default IP source address for the syslog messages. Hard coding the logging source address makes it easier to identify the host that sent the message.

service timestamps debug datetime localtime show-timezone msec

By default, log messages are not time stamped. Use this command to enable the time stamping of log messages and configure the time stamping of system debug messages. Time stamping enhances real-time debugging by providing the relative timing of logged events. This information is especially useful when

customers send debugging output to technical support personnel for assistance. To enable the time stamping of system debug messages, use the above command in global configuration mode. This only has an affect when debugging is enabled.

logging event

The **logging event link-status** command enables logging related to link status. The **logging event bundle-status** command enables logging related to bundle status.

Quality of Service (QoS)

The following commands are useful in troubleshooting QoS:

- show class-map
- show policy-map
- show qos maps
- show mls qos maps dscp-cos
- show qos interface
- show queueing interface

show class-map

To verify the class map for QoS classification, use the **show class-map** command.

```
DER# show class-map

 Class Map match-all class_VoIP (id 1)
   Match access-group name acl_VoIP

 Class Map match-any class-default (id 0)
   Match any

 Class Map match-all class_video_VoD_high (id 2)
   Match access-group name acl_video_VoD_high

 Class Map match-all class_video_VoD_low (id 3)
   Match access-group name acl_video_VoD_low

 Class Map match-all class_video_broadcast (id 4)
   Match access-group name acl_video_broadcast

 Class Map match-all class_VoD_signaling (id 5)
   Match access-group name acl_VoD_signaling

 Class Map match-all class_HSD (id 6)
   Match access-group name acl_HSD
```

show policy-map

To verify the policy map for QoS marking, use the **show policy-map** command.

```
DER# show policy-map
```

```
 Policy Map setDSCP
     Description: Mark DSCP values for ingress traffic
   Class class_VoIP
     set dscp ef
   Class class_HSD
     set dscp default
   Class class_VoD_signaling
     set dscp cs3
   Class class_video_broadcast
     set dscp af41
   Class class_video_VoD_high
     set dscp af42
   Class class_video_VoD_low
     set dscp af43
```

show qos maps

On Cisco Catalyst 4500 and Cisco Catalyst 4948-10GE switches, use the **show qos maps** command to verify the DSCP-to-TxQueue and DSCP-to-CoS mappings.

```
AR2# show qos maps

DSCP-TxQueue Mapping Table (dscp = d1d2)
d1 : d2  0  1  2  3  4  5  6  7  8  9
------------------------------------
 0 :    01 01 01 01 01 01 01 01 01 01
 1 :    01 01 01 01 01 01 02 02 02 02
 2 :    02 02 02 02 02 02 02 02 02 02
 3 :    02 02 03 03 03 03 03 03 03 03
 4 :    03 03 03 03 03 03 03 03 04 04
 5 :    04 04 04 04 04 04 04 04 04 04
 6 :    04 04 04 04

<omitted DSCP policing table>

DSCP-CoS Mapping Table (dscp = d1d2)
d1 : d2  0  1  2  3  4  5  6  7  8  9
------------------------------------
 0 :    00 00 00 00 00 00 00 00 01 01
 1 :    01 01 01 01 01 01 02 02 02 02
 2 :    02 02 02 02 03 03 03 03 03 03
 3 :    03 03 04 04 04 04 02 04 01 04
 4 :    05 05 05 05 05 05 05 05 06 06
 5 :    06 06 06 06 06 06 07 07 07 07
 6 :    07 07 07 07

<omitted CoS to DSCP mapping table>
```

show mls qos maps dscp-cos

On the Cisco Catalyst 6500 and Cisco 7600 switches, use the **show mls qos maps dscp-cos** command to verify the DSCP-to-CoS mappings.

```
DER# show mls qos maps dscp-cos

   Dscp-cos map:                                     (dscp= d1d2)
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ------------------------------------
      0 :    00 00 00 00 00 00 00 00 01 01
```

```
1 :    01 01 01 01 01 01 02 02 02 02
2 :    02 02 02 02 03 03 03 03 03 03
3 :    03 03 04 04 04 04 02 04 01 04
4 :    05 05 05 05 05 05 05 05 06 06
5 :    06 06 06 06 06 06 07 07 07 07
6 :    07 07 07 07
```

show qos interface

On the Cisco Catalyst 4500 and Cisco Catalyst 4948-10GE switches, use the **show qos interface** *type slot*/*module* to verify the QoS state, port trust state, queue bandwidth, priority queue, and queue size.

```
AR2# show qos interface tenGigabitEthernet 1/1

QoS is enabled globally
Port QoS is enabled
Administrative Port Trust State: 'dscp'
Operational Port Trust State: 'dscp'
Trust device: none
Default DSCP: 0 Default CoS: 0
Appliance trust: none
Tx-Queue   Bandwidth   ShapeRate   Priority   QueueSize
             (bps)       (bps)               (packets)
  1        1900000000  disabled    N/A        2080
  2        8000000000  disabled    N/A        2080
  3        2500000000  disabled    high       2080
  4        100000000   disabled    N/A        2080
```

show queueing interface

On the Cisco Catalyst 6500 and Cisco 7600 switches, use the **show queueing interface** *type slot*/*module* command to verify the queueing strategy, priority queue, WRR bandwidths, queue sizes, thresholds, CoS-to-queue mappings, and queue drops.

```
DER# show queueing interface tenGigabitEthernet 7/1

Interface TenGigabitEthernet7/1 queueing strategy:  Weighted Round-Robin
  Port QoS is enabled
  Trust state: trust DSCP
  Extend trust state: not trusted [COS = 0]
  Default COS is 0
    Queueing Mode In Tx direction: mode-cos
    Transmit queues [type = 1p7q8t]:
    Queue Id    Scheduling  Num of thresholds
    -----------------------------------------
       01         WRR                 08
       02         WRR                 08
       03         WRR                 08
       04         WRR                 08
       05         WRR                 08
       06         WRR                 08
       07         WRR                 08
       08         Priority            01

    WRR bandwidth ratios:   64[queue 1] 255[queue 2]   0[queue 3]   0[queue 4]   0[queue
5]   0[queu
e 6]   0[queue 7]
    queue-limit ratios:     40[queue 1]  50[queue 2]   0[queue 3]   0[queue 4]   0[queue
5]   0[queu
```

```
e 6]   0[queue 7]

    queue tail-drop-thresholds
    --------------------------
    1     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    2     45[1] 85[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    3     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    4     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    5     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    6     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    7     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]

    queue random-detect-min-thresholds
    ----------------------------------
      1    75[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
      2    40[1] 70[2] 70[3] 70[4] 70[5] 70[6] 70[7] 70[8]
      3    70[1] 70[2] 70[3] 70[4] 70[5] 70[6] 70[7] 70[8]
      4    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
      5    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
      6    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
      7    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]

    queue random-detect-max-thresholds
    ----------------------------------
      1    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
      2    70[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
      3    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
      4    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
      5    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
      6    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
      7    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]

    WRED disabled queues:      2  4  5  6  7

    queue thresh cos-map
    ---------------------------------------
    1     1      0
    1     2
    1     3
    1     4
    1     5
    1     6
    1     7
    1     8
    2     1      1
    2     2      2
    2     3      3 4 6 7
    2     4
    2     5
    2     6
    2     7
    2     8
    3     1
    3     2
    3     3
    3     4
    3     5
    3     6
    3     7
    3     8
    4     1
    4     2
    4     3
    4     4
```

```
    4     5
    4     6
    4     7
    4     8
    5     1
    5     2
    5     3
    5     4
    5     5
    5     6
    5     7
    5     8
    6     1
    6     2
    6     3
    6     4
    6     5
    6     6
    6     7
    6     8
    7     1
    7     2
    7     3
    7     4
    7     5
    7     6
    7     7
    7     8
    8     1      5

    Queueing Mode In Rx direction: mode-cos
    Receive queues [type = 8q8t]:
    Queue Id    Scheduling  Num of thresholds
    -----------------------------------------
       01         WRR                 08
       02         WRR                 08
       03         WRR                 08
       04         WRR                 08
       05         WRR                 08
       06         WRR                 08
       07         WRR                 08
       08         WRR                 08

    WRR bandwidth ratios:  100[queue 1]   0[queue 2]   0[queue 3]   0[queue 4]   0[queue
5]   0[queu
e 6]   0[queue 7]   0[queue 8]
    queue-limit ratios:    100[queue 1]   0[queue 2]   0[queue 3]   0[queue 4]   0[queue
5]   0[queu
e 6]   0[queue 7]   0[queue 8]

    queue tail-drop-thresholds
    --------------------------
    1     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    2     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    3     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    4     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    5     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    6     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    7     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    8     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]

    queue random-detect-min-thresholds
    ----------------------------------
      1    40[1] 40[2] 50[3] 50[4] 50[5] 50[6] 50[7] 50[8]
```

```
  2    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
  3    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
  4    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
  5    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
  6    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
  7    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
  8    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]

queue random-detect-max-thresholds
----------------------------------
  1    70[1] 80[2] 90[3] 100[4] 100[5] 100[6] 100[7] 100[8]
  2    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
  3    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
  4    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
  5    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
  6    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
  7    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
  8    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]

WRED disabled queues:      1  2  3  4  5  6  7  8

queue thresh cos-map
---------------------------------------
1     1      0 1 2 3 4 5 6 7
1     2
1     3
1     4
1     5
1     6
1     7
1     8
2     1
2     2
2     3
2     4
2     5
2     6
2     7
2     8
3     1
3     2
3     3
3     4
3     5
3     6
3     7
3     8
4     1
4     2
4     3
4     4
4     5
4     6
4     7
4     8
5     1
5     2
5     3
5     4
5     5
5     6
5     7
5     8
6     1
```

```
  6     2
  6     3
  6     4
  6     5
  6     6
  6     7
  6     8
  7     1
  7     2
  7     3
  7     4
  7     5
  7     6
  7     7
  7     8
  8     1
  8     2
  8     3
  8     4
  8     5
  8     6
  8     7
  8     8


Packets dropped on Transmit:

  queue     dropped  [cos-map]
  ---------------------------------------------
  1               0  [0 ]
  2               0  [1 2 3 4 6 7 ]
  3               0  []
  4               0  []
  5               0  []
  6               0  []
  7               0  []
  8               0  [5 ]

Packets dropped on Receive:

  queue     dropped  [cos-map]
  ---------------------------------------------
  1               0  [0 1 2 3 4 5 6 7 ]
  2               0  []
  3               0  []
  4               0  []
  5               0  []
  6               0  []
  7               0  []
  8               0  []
```

Multicast

The following commands are useful in troubleshooting multicast:

- show ip mroute
- show ip mroute ssm
- show ip mroute active
- show ip pim neighbor
- show ip igmp snooping
- show ip igmp groups
- show ip igmp ssm-mapping
- show ip igmp membership
- debug ip igmp
- debug ip pim
- debug domain

show ip mroute

To see the details of the multicast routing table, use the **show ip mroute** command. The output of this command also shows the legend for the flags.

```
AR3# show ip mroute

IP Multicast Routing Table

Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, 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 - Candidate for MSDP Advertisement,

U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel

Y - Joined MDT-data group, y - Sending to MDT-data group

Outgoing interface flags: H - Hardware switched, A - Assert winner

Timers: Uptime/Expires

Interface state: Interface, Next-Hop or VCD, State/Mode

(192.168.70.101, 232.1.5.220), 1w4d/stopped, flags: sTI

Incoming interface: Null, RPF nbr 0.0.0.0

Outgoing interface list:

Vlan130, Forward/Sparse, 1w1d/00:01:46, H

(192.168.70.101, 232.1.5.221), 1w4d/stopped, flags: sTI

Incoming interface: Null, RPF nbr 0.0.0.0
```

```
Outgoing interface list:

Vlan130, Forward/Sparse, 1w1d/00:01:46, H

(192.168.70.101, 232.1.5.222), 1w4d/stopped, flags: sTI

Incoming interface: Null, RPF nbr 0.0.0.0

Outgoing interface list:

Vlan130, Forward/Sparse, 1w1d/00:01:46, H

(192.168.70.101, 232.1.5.223), 1w4d/stopped, flags: sTI

Incoming interface: Null, RPF nbr 0.0.0.0

Outgoing interface list:
```

show ip mroute ssm

To verify the source-specific multicast (SSM) mapping of multicast groups to multicast sources, use the **show ip mroute ssm** command. With this command, you can also verify the path of the multicast ingress and egress interface(s).

Tip To see the legend for the flags field, you must use the **show ip mroute** command.

```
AR2# show ip mroute ssm

(192.168.70.101, 232.1.5.220), 1w4d/stopped, flags: sTI

Incoming interface: Null, RPF nbr 0.0.0.0

Outgoing interface list:

Vlan130, Forward/Sparse, 1w1d/00:01:40, H

(192.168.70.101, 232.1.5.221), 1w4d/stopped, flags: sTI

Incoming interface: Null, RPF nbr 0.0.0.0

Outgoing interface list:

Vlan130, Forward/Sparse, 1w1d/00:01:40, H

(192.168.70.101, 232.1.5.222), 1w4d/stopped, flags: sTI

Incoming interface: Null, RPF nbr 0.0.0.0

Outgoing interface list:

Vlan130, Forward/Sparse, 1w1d/00:01:40, H

(192.168.70.101, 232.1.5.223), 1w4d/stopped, flags: sTI

Incoming interface: Null, RPF nbr 0.0.0.0

Outgoing interface list:
```

```
Vlan130, Forward/Sparse, 1w1d/00:01:40, H

(192.168.70.101, 232.1.5.216), 1w4d/stopped, flags: sTI

Incoming interface: Null, RPF nbr 0.0.0.0

Outgoing interface list:
```

show ip mroute active

To verify the bitrate of a multicast group, use the **show ip mroute active** command.

```
AR2# show ip mroute active

Active IP Multicast Sources - sending >= 4 kbps

Group: 232.255.0.1, (?)
   Source: 192.168.71.105 (1.0.255.232.coronado.net)
     Rate: 334 pps/3517 kbps(1sec), 2829 kbps(last 30 secs), 2703 kbps(life avg)

<rest of the output omitted>
```

show ip pim neighbor

To verify the protocol-independent multicast (PIM) neighbors, use the **show ip pim neighbor** command.

```
AR2# show ip pim neighbor

PIM Neighbor Table
Neighbor          Interface               Uptime/Expires    Ver   DR
Address                                                           Prio/Mode
192.168.254.9     Vlan908                 1d16h/00:01:34    v2    1 / S
192.168.254.18    Vlan916                 1d16h/00:01:24    v2    1 / DR S
```

show ip igmp snooping

To verify IGMP snooping on the switch and interfaces, use the **show ip igmp snooping** command.

```
AR2# show ip igmp snooping

Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping             : Enabled
IGMPv3 snooping           : Enabled
Report suppression        : Enabled
TCN solicit query         : Disabled
TCN flood query count     : 2

Vlan 1:
--------
IGMP snooping                       : Enabled
IGMPv2 immediate leave              : Disabled
Explicit host tracking              : Enabled
Multicast router learning mode      : pim-dvmrp
CGMP interoperability mode          : IGMP_ONLY

Vlan 70:
--------
```

```
IGMP snooping                        : Enabled
IGMPv2 immediate leave               : Disabled
Explicit host tracking               : Enabled
Multicast router learning mode       : pim-dvmrp
CGMP interoperability mode           : IGMP_ONLY

<rest of output omitted>
```

show ip igmp groups

To verify IGMP group membership on a switch, use the **show ip igmp groups** command.

```
AR2# show ip igmp groups

IGMP Connected Group Membership
Group Address    Interface                Uptime    Expires   Last Reporter
232.255.0.1      Vlan120                  1d17h     stopped   0.0.0.0
232.255.0.2      Vlan120                  1d17h     stopped   0.0.0.0
232.255.0.3      Vlan120                  1d17h     stopped   0.0.0.0
232.255.0.5      Vlan120                  1d17h     stopped   0.0.0.0
232.255.0.12     Vlan120                  1d17h     stopped   0.0.0.0
224.0.1.40       Vlan120                  1d16h     00:02:56  192.168.120.1
```

show ip igmp ssm-mapping

To verify the SSM mapping configuration on the switch, use the **show ip igmp ssm-mapping** command.

```
AR3# show ip igmp ssm-mapping

SSM Mapping  : Enabled
DNS Lookup   : Enabled
Mcast domain : coronado.net
Name servers : 192.168.11.101
```

show ip igmp membership

Another command to verify IGMP group membership, which provides some additional information compared to the previous command, is the **show ip igmp membership** command.

```
AR2# show ip igmp membership

Flags: A  - aggregate, T - tracked
       L  - Local, S - static, V - virtual, R - Reported through v3
       I - v3lite, U - Urd, M - SSM (S,G) channel
       1,2,3 - The version of IGMP, the group is in
Channel/Group-Flags:
       / - Filtering entry (Exclude mode (S,G), Include mode (G))
Reporter:
       <mac-or-ip-address> - last reporter if group is not explicitly tracked
       <n>/<m>      - <n> reporter in include mode, <m> reporter in exclude

 Channel/Group                 Reporter        Uptime   Exp.  Flags  Interface
/*,232.255.0.1                 0.0.0.0         1d17h    stop  2MA    Vl120
 192.168.71.105,232.255.0.1                    1d17h    stop  SA     Vl120
/*,232.255.0.2                 0.0.0.0         1d17h    stop  2MA    Vl120
 192.168.71.105,232.255.0.2                    1d17h    stop  SA     Vl120
/*,232.255.0.3                 0.0.0.0         1d17h    stop  2MA    Vl120
 192.168.71.105,232.255.0.3                    1d17h    stop  SA     Vl120
```

```
/*,232.255.0.5                  0.0.0.0         1d17h    stop  2MA    Vl120
 192.168.71.105,232.255.0.5                     1d17h    stop  SA     Vl120
/*,232.255.0.12                 0.0.0.0         1d17h    stop  2MA    Vl120
 192.168.71.105,232.255.0.12                    1d17h    stop  SA     Vl120
 *,224.0.1.40                   192.168.120.1   1d16h    02:22 2LA    Vl120
```

debug ip igmp

To troubleshoot IGMP issues, use the **debug ip igmp** command. The debug output indicates IGMP membership queries, membership responses, and the conversion of IGMPv2 to IGMPv3 through DNS lookup.

```
AR2# debug ip igmp

IGMP debugging is on
AR2#
*Aug  8 14:20:53.039: IGMP(0): Received v2 Query on Vlan908 from 192.168.254.9
AR2#
*Aug  8 14:21:16.880: IGMP(0): Send v2 general Query on Vlan120
*Aug  8 14:21:16.880: IGMP(0): Set report delay time to 8.4 seconds for 224.0.1.40 on
Vlan120
*Aug  8 14:21:16.880: IGMP(0): Send v2 general Query on Vlan916
AR2#
*Aug  8 14:21:25.881: IGMP(0): Send v2 Report for 224.0.1.40 on Vlan120
*Aug  8 14:21:25.881: IGMP(0): Received v2 Report on Vlan120 from 192.168.120.1 for
224.0.1.40
*Aug  8 14:21:25.881: IGMP(0): Received Group record for group 224.0.1.40, mode 2 from
192.168.120.1
 for 0 sources
*Aug  8 14:21:25.881: IGMP(0): Updating EXCLUDE group timer for 224.0.1.40
*Aug  8 14:21:25.881: IGMP(0): MRT Add/Update Vlan120 for (*,224.0.1.40) by 0
AR2#
*Aug  8 14:21:39.089: IGMP(0): Convert IGMPv2 static (*, 232.255.0.1) to IGMPv3 with 1
source(s) using DNS
*Aug  8 14:21:39.089: IGMP(0): Convert IGMPv2 static (*, 232.255.0.2) to IGMPv3 with 1
source(s) using DNS
*Aug  8 14:21:39.089: IGMP(0): Convert IGMPv2 static (*, 232.255.0.3) to IGMPv3 with 1
source(s) using DNS
*Aug  8 14:21:39.089: IGMP(0): Convert IGMPv2 static (*, 232.255.0.5) to IGMPv3 with 1
source(s) using DNS
*Aug  8 14:21:39.089: IGMP(0): Convert IGMPv2 static (*, 232.255.0.12) to IGMPv3 with 1
source(s) using DNS
```

debug ip pim

To troubleshoot PIM issues, use the **debug ip pim** command. The output indicates join and prune messages for PIM.

```
AR2# debug ip pim

PIM debugging is on
AR2#
*Aug  8 14:23:04.149: PIM(0): Building Periodic Join/Prune message for 232.255.0.1
*Aug  8 14:23:04.149: PIM(0): Insert (192.168.71.105,232.255.0.1) join in nbr
192.168.254.18's queue
*Aug  8 14:23:04.149: PIM(0): Building Join/Prune packet for nbr 192.168.254.18
*Aug  8 14:23:04.149: PIM(0): Adding v2 (192.168.71.105/32, 232.255.0.1), S-bit Join
*Aug  8 14:23:04.149: PIM(0): Send v2 join/prune to 192.168.254.18 (Vlan916)
```

debug domain

To troubleshoot domain name server (DNS) lookup issues, use the **debug domain** command.

```
AR2# debug domain

Aug  8 21:28:34.274: Domain: query for 1.0.255.232.coronado.net type 1 to 192.168.11.101
Aug  8 21:28:34.274: DOM: dom2cache: hostname is 1.0.255.232.coronado.net, RR type=1,
class=1, ttl=43200, n=4
Reply received ok
```

References

The following documents provide practical tips on configuring the switches used in the solution.

- *Best Practices for Catalyst 6500/6000 Series and Catalyst 4500/4000 Series Switches Running Cisco IOS Software*, at the following URL:

  http://www.cisco.com/en/US/partner/products/hw/switches/ps700/products_white_paper09186a00801b49a4.shtml#cg24

- *Cisco ISP Essentials: Essential IOS Features Every ISP Should Consider*, by Barry Green and Philip Smith, at the following URL:

  http://wwwin-cons.cisco.com/~philsmit/isp/workshop/afnog2004/inet2000/adv-bgp/iosess29.pdf

Note A Cisco Connection Online (CCO) password may be required to access these documents.