

Mediatrace Used to Isolate Network Impairments

TAC

Document ID: 116033

Contributed by Chidambaram Arunachalam, Cisco TAC Engineer.
Apr 12, 2013

Contents

Introduction

Prerequisites

- Requirements
- Conventions

Network Topology

Configuration

- Central-SW
- Central-WAN
- BR-WAN
- BR-SW

Troubleshooting Methodology

- Step 1
- Step 2
- Step 3
- Step 4

Data Analysis

Common Problems

Frequently Asked Questions

- Q. Is Mediatrace integrated with network management or monitoring systems?
- Q. Do I need to enable Resource Reservation Protocol (RSVP) for the Mediatrace feature?

Related Information

Introduction

This document describes how to use the Mediatrace feature to quickly isolate network impairments, such as packet loss and jitter, that impact Voice and Video Quality.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Mediatrace feature on Cisco Integrated Services Routers (ISR) and ISRG2 platforms – Cisco IOS® Release 15.1(3)T or later
- Mediatrace feature on Cisco 3750 platforms – Cisco IOS Release 12.2(58)SE or later
- Mediatrace feature on the Cisco TelePresence EX90 – Cisco TelePresence Software Release TE 6.0 or later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Network Topology

In this example, the configuration for a video call that experiences packet loss between two EX90 endpoints is explained. The network topology is shown here:



Configuration

The process to configure the Mediatrace initiator and responder is very simple. Refer to these examples for the configuration.

Central-SW

```
interface Vlan201
 ip address 10.2.3.70 255.255.255.0

ip rsvp snooping

mediatrace responder
mediatrace initiator source-ip 10.2.3.70 max-sessions 100
```

Central-WAN

```
interface GigabitEthernet0/0
 description "CE router connected to MPLS PE router"
 ip address 10.16.1.2 255.255.255.252
 ip rsvp source address 10.2.3.65
!
interface GigabitEthernet0/1
 description "Connected to Central-SW"
 ip address 10.2.3.65 255.255.255.0

mediatrace responder
mediatrace initiator source-ip 10.2.3.65 max-sessions 100
```

BR-WAN

```
interface GigabitEthernet0/0
 description "CE router connected to MPLS PE router"
 ip address 10.16.2.2 255.255.255.252
 ip rsvp source address 10.2.4.65
```

```

!
interface GigabitEthernet0/1
  description "Connected to BR3-SW"
  ip address 10.2.4.65 255.255.255.0

mediatrace responder
mediatrace initiator source-ip 10.2.4.65 max-sessions 100

```

BR-SW

```

interface Vlan202
  ip address 10.2.4.70 255.255.255.0

ip rsvp snooping

mediatrace responder
mediatrace initiator source-ip 10.2.4.70 max-sessions 100

```

Troubleshooting Methodology

Cisco recommends that you enable Mediatrace on all applicable nodes in the Enterprise network. It is supported in common switching and routing platforms such as 3750 and ISR-G2.

Step 1

Identify the source and destination IP address / port number of the audio or video Routing Table Protocol (RTP) stream of interest.

EX90

```

xstatus MediaChannels
*s MediaChannels Call 9 IncomingAudioChannel 115 Encryption Status: Off
*s MediaChannels Call 9 IncomingAudioChannel 115 Audio Protocol: AACLD
*s MediaChannels Call 9 IncomingAudioChannel 115 Audio Mute: False
*s MediaChannels Call 9 IncomingAudioChannel 115 Audio Channels: 1
*s MediaChannels Call 9 IncomingAudioChannel 115 Transport RTP Local IpAddress:
  "10.2.3.41"
*s MediaChannels Call 9 IncomingAudioChannel 115 Transport RTP Local Port: 16454
*s MediaChannels Call 9 IncomingAudioChannel 115 Transport RTP Remote IpAddress:
  "10.2.4.5"
*s MediaChannels Call 9 IncomingAudioChannel 115 Transport RTP Remote Port: 16444
*s MediaChannels Call 9 IncomingAudioChannel 115 Transport RTCP Local IpAddress:
  "10.2.3.41"
*s MediaChannels Call 9 IncomingAudioChannel 115 Transport RTCP Local Port: 16455
*s MediaChannels Call 9 IncomingAudioChannel 115 Transport RTCP Remote IpAddress:
  "10.2.4.5"
*s MediaChannels Call 9 IncomingAudioChannel 115 Transport RTCP Remote Port: 16445
*s MediaChannels Call 9 IncomingVideoChannel 118 Encryption Status: Off
*s MediaChannels Call 9 IncomingVideoChannel 118 ChannelRole: Main
*s MediaChannels Call 9 IncomingVideoChannel 118 Video Protocol: H264
*s MediaChannels Call 9 IncomingVideoChannel 118 Video FrameRate: 30
*s MediaChannels Call 9 IncomingVideoChannel 118 Video ResolutionX: 640
*s MediaChannels Call 9 IncomingVideoChannel 118 Video ResolutionY: 360
*s MediaChannels Call 9 IncomingVideoChannel 118 Transport RTP Local IpAddress:
  "10.2.3.41"
*s MediaChannels Call 9 IncomingVideoChannel 118 Transport RTP Local Port: 16456
*s MediaChannels Call 9 IncomingVideoChannel 118 Transport RTP Remote IpAddress:
  "10.2.4.5"
*s MediaChannels Call 9 IncomingVideoChannel 118 Transport RTP Remote Port: 16446
*s MediaChannels Call 9 IncomingVideoChannel 118 Transport RTCP Local IpAddress:
  "10.2.3.41"

```

```
*s MediaChannels Call 9 IncomingVideoChannel 118 Transport RTCP Local Port: 16457
*s MediaChannels Call 9 IncomingVideoChannel 118 Transport RTCP Remote IpAddress:
"10.2.4.5"
*s MediaChannels Call 9 IncomingVideoChannel 118 Transport RTCP Remote Port: 16447
*s MediaChannels Call 9 IncomingVideoChannel 121 Encryption Status: Off
```

Step 2

Identify the switch to which the origination endpoint is connected. This switch can be identified with the Cisco Discovery Protocol (CDP) *show* commands.

EX90

xstatus Network

```
*s Network 1 Ethernet MacAddress: "FF:FF:FF:70:E6:B6"
*s Network 1 Ethernet Speed: 100full
*s Network 1 IPv4 Address: "10.2.3.41"
*s Network 1 IPv4 SubnetMask: "255.255.255.0"
*s Network 1 IPv4 Gateway: "10.2.3.65"
*s Network 1 IPv4 DNS Domain Name: ""
*s Network 1 IPv4 DNS Server 1 Address: ""
*s Network 1 IPv4 DNS Server 2 Address: ""
*s Network 1 IPv4 DNS Server 3 Address: ""
*s Network 1 IPv4 DNS Server 4 Address: ""
*s Network 1 IPv4 DNS Server 5 Address: ""
*s Network 1 IPv6 Address: ""
*s Network 1 IPv6 Gateway: ""
*s Network 1 MTU: 1500
*s Network 1 VLAN Voice VlanId: "201"
*s Network 1 VLAN Native VlanId: "202"
*s Network 1 CDP Platform: "cisco WS-C3750V2-24TS"
*s Network 1 CDP Version: "Cisco IOS Software, C3750 Software
(C3750-IPSERVICESK9-M), Version 12.2(58)SE2, RELEASE SOFTWARE (fc1)
*Technical Support: http://www.cisco.com/techsupport*Copyright (c)
1986-2011 by Cisco Systems, Inc.*Compiled Thu 21-Jul-11 01:53 by
prod_rel_team"
*s Network 1 CDP Capabilities: "0x0028"
*s Network 1 CDP DeviceID: "Central-SW"
*s Network 1 CDP PortID: "FastEthernet1/0/23"
*s Network 1 CDP Duplex: "Full"
*s Network 1 CDP VTPMgmtDomain: ""
*s Network 1 CDP Address: "10.2.3.70"
*s Network 1 CDP PrimaryMgmtAddress: "10.2.3.70"
*s Network 1 CDP SysName: ""
*s Network 1 CDP SysObjectID: ""
*s Network 1 CDP VoIPApplianceVlanID: "201"
** end
```

Step 3

Log in to the first-hop switch and configure a flow specifier to uniquely identify the RTP stream. This flow specifier is used in the *mediatrace poll* command.

```
mediatrace flow-specifier RTP
source-ip 10.2.3.41 source-port 16456
dest-ip 10.2.4.5 dest-port 16446
```

Step 4

Enter the *mediatrace poll* command.

- Source value – IP address of origination UC endpoint
- Destination value – IP address of destination UC endpoint
- Flow specifier – Name of the flow specifier that contains the 4 value tuple to identify RTP stream

```
#mediatrace poll path-specifier source 10.2.3.41 destination 10.2.4.5
  perf-monitor flow-specifier RTP
```

Started the data fetch operation.

Waiting for data from hops.

This may take several seconds to complete...

Data received for hop 1

Data received for hop 2

Data received for hop 3

Data received for hop 4

Data fetch complete.

Results:

Data Collection Summary:

Request Timestamp: 11:00:54.302 EST Sun Mar 10 2013

Request Status: Completed

Number of hops responded (includes success/error/no-record): 4

Number of hops with valid data report: 4

Number of hops with error report: 0

Number of hops with no data record: 0

Detailed Report of collected data:

Number of Mediatrace hops in the path: 4

Mediatrace Hop Number: 1 (**host=Central-Wan**, ttl=254)

Metrics Collection Status: Success

Reachability Address: 10.2.3.65

Ingress Interface: Gi0/1

Egress Interface: Gi0/0

Metrics Collected:

Flow Sampling Start Timestamp: 10:26:48

Loss of measurement confidence: FALSE

Media Stop Event Occurred: FALSE

IP Packet Drop Count (pkts): 0

IP Byte Count (Bytes): 191965

IP Packet Count (pkts): 402

IP Byte Rate (Bps): 15996

Packet Drop Reason: 64

IP DSCP: 32

IP TTL: 63

IP Protocol: 0

Media Byte Rate Average (Bps): 15058

Media Byte Count (Bytes): 180709

Media Packet Count (pkts): 402

RTP Interarrival Jitter Average (usec): 155

RTP Packets Lost (pkts): 0

RTP Packets Expected (pkts): 397

RTP Packet Lost Event Count: 0

RTP Loss Percent (%): 0.00

Mediatrace Hop Number: 2 (**host=BR-Wan**, ttl=251)

Metrics Collection Status: Success

Reachability Address: 10.16.2.2

Ingress Interface: Gi0/0

Egress Interface: Gi0/1

Metrics Collected:

Flow Sampling Start Timestamp: 09:58:40

Loss of measurement confidence: FALSE

Media Stop Event Occurred: FALSE

IP Packet Drop Count (pkts): 0

IP Byte Count (Bytes): 331523

IP Packet Count (pkts): 694

IP Byte Rate (Bps): 16576

Packet Drop Reason: 64

IP DSCP: 32
IP TTL: 60
IP Protocol: 0
Media Byte Rate Average (Bps): 15604
Media Byte Count (Bytes): 312091
Media Packet Count (pkts): 694
RTP Interarrival Jitter Average (usec): 1648
RTP Packets Lost (pkts): 14
RTP Packets Expected (pkts): 708
RTP Packet Lost Event Count: 13
RTP Loss Percent (%): 1.97

Mediatrace Hop Number: 3 (**host=BR-SW**, ttl=251)

Metrics Collection Status: Success

Reachability Address: 10.2.4.70

Ingress Interface: Fa1/0/22

Egress Interface: Fa1/0/24

Metrics Collected:

Flow Sampling Start Timestamp: 22:50:37
Loss of measurement confidence: FALSE
Media Stop Event Occurred: FALSE
IP Packet Drop Count (pkts): 0
IP Byte Count (Bytes): 505526
IP Packet Count (pkts): 1059
IP Byte Rate (Bps): 16850
Packet Drop Reason: 0
IP DSCP: 32
IP TTL: 60
IP Protocol: 17
Media Byte Rate Average (Bps): 16144
Media Byte Count (Bytes): 484346
Media Packet Count (pkts): 1059
RTP Interarrival Jitter Average (usec): 1511
RTP Packets Lost (pkts): 22
RTP Packets Expected (pkts): 1075
RTP Packet Lost Event Count: 21
RTP Loss Percent (%): 2.04

Mediatrace Hop Number: 4 (**host=BR-EX90**, ttl=251)

Metrics Collection Status: Success

Reachability Address: 10.2.4.5

Ingress Interface: eth0

Egress Interface: None

Metrics Collected:

Flow Sampling Start Timestamp: 11:02:00
Loss of measurement confidence: FALSE
Media Stop Event Occurred: FALSE
IP Packet Drop Count (pkts): 0
IP Byte Count (Bytes): 0
IP Packet Count (pkts): 0
IP Byte Rate (Bps): 0
Packet Drop Reason: 0
IP DSCP: 0
IP TTL: 0
IP Protocol: 17
Media Byte Rate Average (Bps): 16000
Media Byte Count (Bytes): 478219
Media Packet Count (pkts): 1056
RTP Interarrival Jitter Average (usec): 4953
RTP Packets Lost (pkts): 17
RTP Packets Expected (pkts): 1073
RTP Packet Lost Event Count: 6
RTP Loss Percent (%): 0.04

Central-SW#

Data Analysis

These observations can be made from *mediatrace poll* command output :

1. The network path of RTP flow contains 4 Mediatrace enabled devices from Central-SW:
 - ◆ Central-WAN
 - ◆ BR-WAN
 - ◆ BR-SW
 - ◆ BR-EX90
2. No packet loss is observed at the Central-WAN router.
3. Packet loss is observed at BR-WAN, BR-SW, and BR-EX90.
4. The conclusion is that packet loss is introduced between Central-WAN and BR-WAN.

Common Problems

The typical factors that contribute to packet loss are:

1. Incorrect Differentiated Services Code Point (DSCP) value.
2. Policer within the service provider network to limit bandwidth utilization.
3. Layer 2 errors, such as duplex mismatches and controller errors.

Frequently Asked Questions

Q. Is Mediatrace integrated with network management or monitoring systems?

A. Yes, Cisco Prime Collaboration enables administrators to troubleshoot video calls with the use of Mediatrace in a single click and displays the results in graphical format.

Q. Do I need to enable Resource Reservation Protocol (RSVP) for the Mediatrace feature?

A. No, Mediatrace uses RSVP-TP which is enabled automatically when the Mediatrace initiator or responder is configured. There is no need to enter the *ip rsvp bandwidth* command.

Related Information

- *Technical Support & Documentation – Cisco Systems*