



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for WildPackets OmniPeek Enterprise with Avaya Aura<sup>™</sup> Communication Manager – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required for WildPackets OmniPeek Enterprise to interoperate with Avaya Aura<sup>™</sup> Communication Manager using Avaya IP Telephones. WildPackets OmniPeek Enterprise provides analysis on the VoIP call signaling and RTP flows from Avaya IP Telephones for monitoring and troubleshooting quality of calls placed across the network.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

# 1. Introduction

These Application Notes describe the configuration steps required for WildPackets OmniPeek Enterprise to interoperate with Avaya Aura<sup>TM</sup> Communication Manager using Avaya IP Telephones. WildPackets OmniPeek Enterprise provides analysis on the VoIP call signaling and RTP flows from Avaya IP Telephones for monitoring and troubleshooting quality of calls placed across the network.

WildPackets OmniPeek Enterprise monitors the Avaya Common Control Messaging Set (CCMS) signaling streams and the H.323 RTP streams from the Avaya IP Telephones, and analyzes the packets to identify voice quality problems. The Avaya CCMS signaling streams are used by WildPackets OmniPeek Enterprise to obtain information such as calling and called party extensions, and to reassemble the call from the captured packets.

## 1.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying WildPackets OmniPeek Enterprise's capture and display of packet streams, and analysis of voice quality from the Avaya IP Telephones. The call scenarios included registration, audio codecs with and without IP media shuffling, encryption, and VoIP impairment.

The serviceability testing focused on verifying the ability of WildPackets OmniPeek Enterprise to recover from adverse conditions, such as disconnecting the Ethernet cable to WildPackets OmniPeek Enterprise.

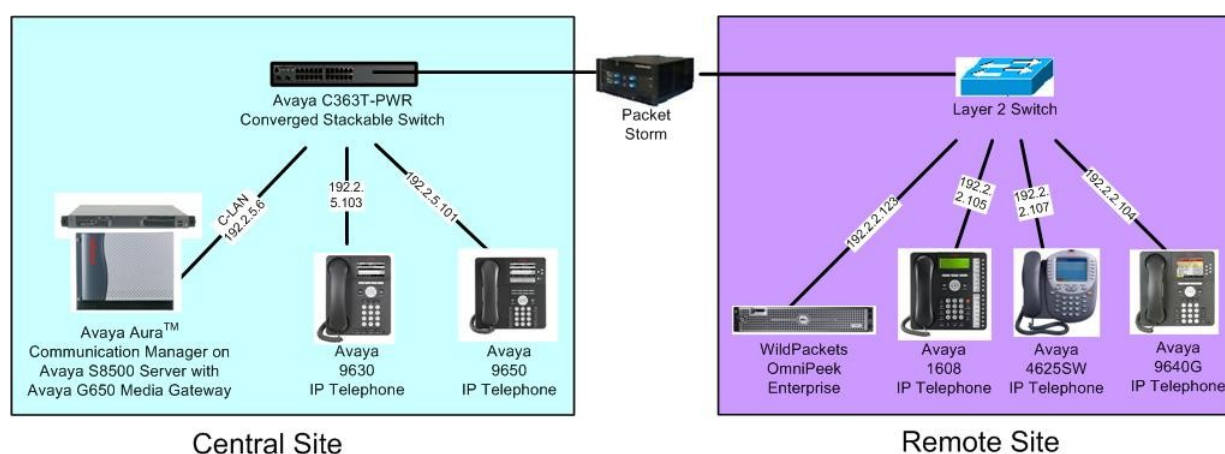
## 1.2. Support

Technical support on WildPackets OmniPeek Enterprise can be requested at [www.wildpackets.com/support/contact](http://www.wildpackets.com/support/contact).

## 2. Reference Configuration

In the test configuration shown below, WildPackets OmniPeek Enterprise monitored the Avaya IP Telephones at the Remote site. The packet streams for the Avaya IP Telephones at the Remote site were mirrored on the local Layer 2 switch, and sent over to WildPackets OmniPeek Enterprise. The Packet Storm was used as a tool to inject VoIP impairments, such as jitter and loss, into the network for calls between the Central and Remote sites.

The Avaya IP Telephony infrastructure is not the focus of these Application Notes and will not be described. Furthermore, the port mirroring on the Remote switch and the VoIP impairment injection on the Packet Storm will also not be described. Note that other network tapping methods, besides port mirroring, may be used for the purpose of packet captures.



## 3. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment	Software
Avaya S8500 Server	Avaya Aura Communication Manager 5.2, R015x.02.0.947.3
Avaya G650 Media Gateway <ul style="list-style-type: none"> <li>TN799DP C-LAN Circuit Pack</li> </ul>	HW01 FW017
Avaya 1600 Series IP Telephones (H.323)	1.02
Avaya 4600 Series IP Telephones (H.323)	2.9
Avaya 9600 Series IP Telephones (H.323)	2.0
Packet Storm	10.5v1
WildPackets OmniPeek Enterprise	6.0.2

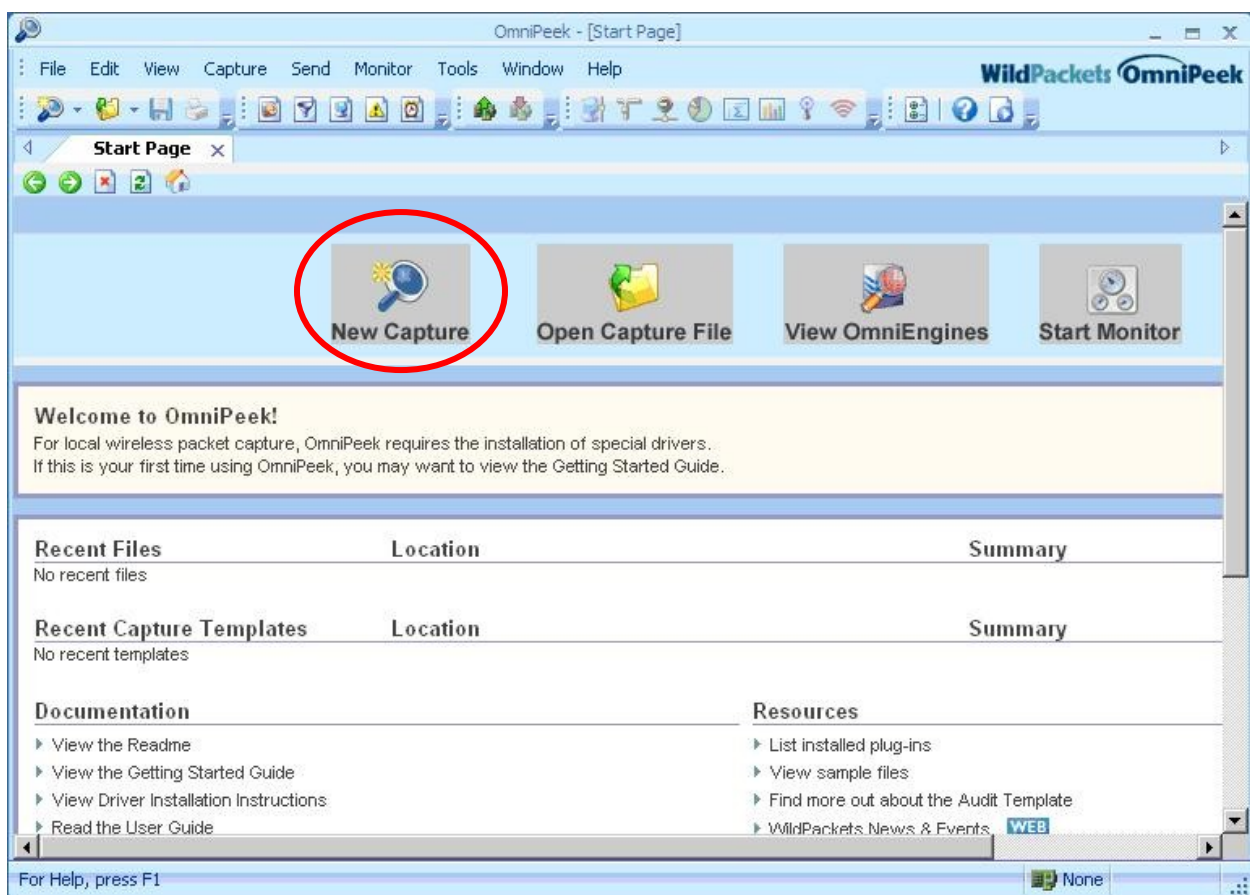
## 4. Configure WildPackets OmniPeek Enterprise

This section provides the procedures for configuring WildPackets OmniPeek Enterprise. The procedures fall into the following areas:

- Launch OmniPeek
- Administer new capture
- Start capture

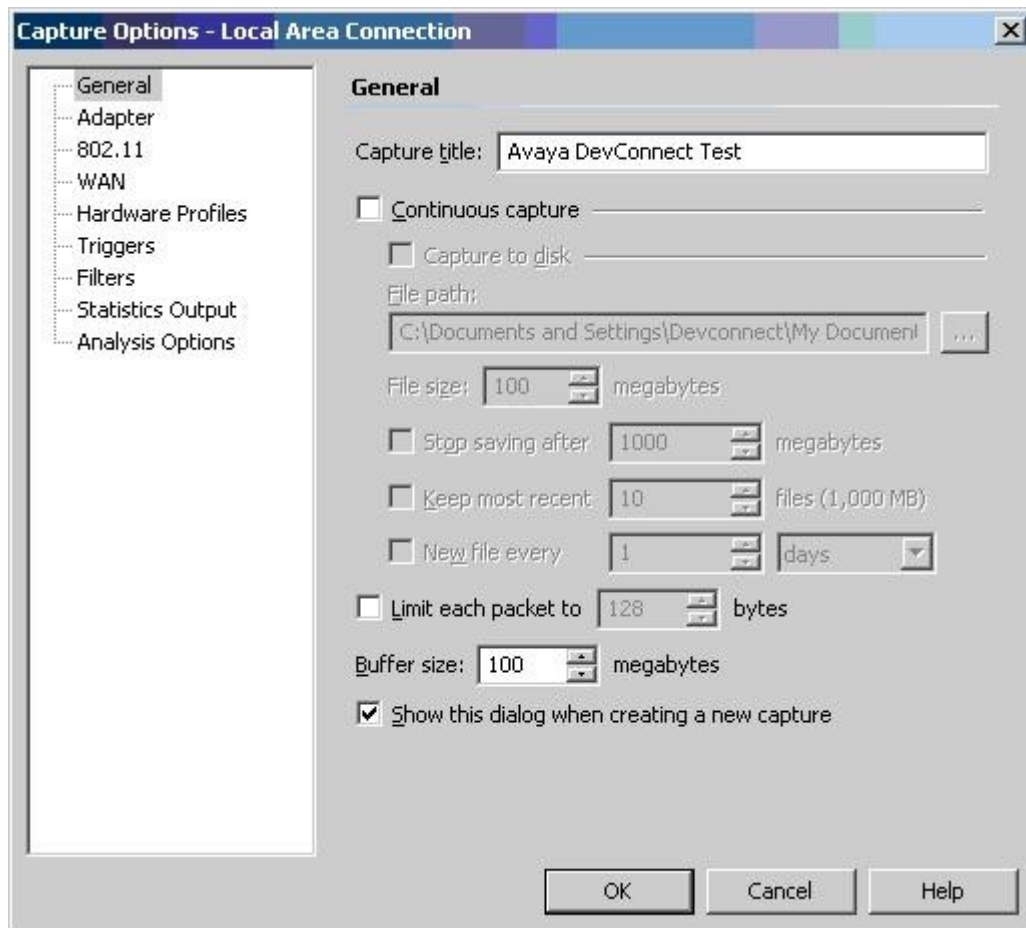
### 4.1. Launch OmniPeek

From the OmniPeek Enterprise server, select **Start > All Programs > WildPackets OmniPeek**. The **OmniPeek – [Start Page]** screen is displayed, as shown below. Select **New Capture**.

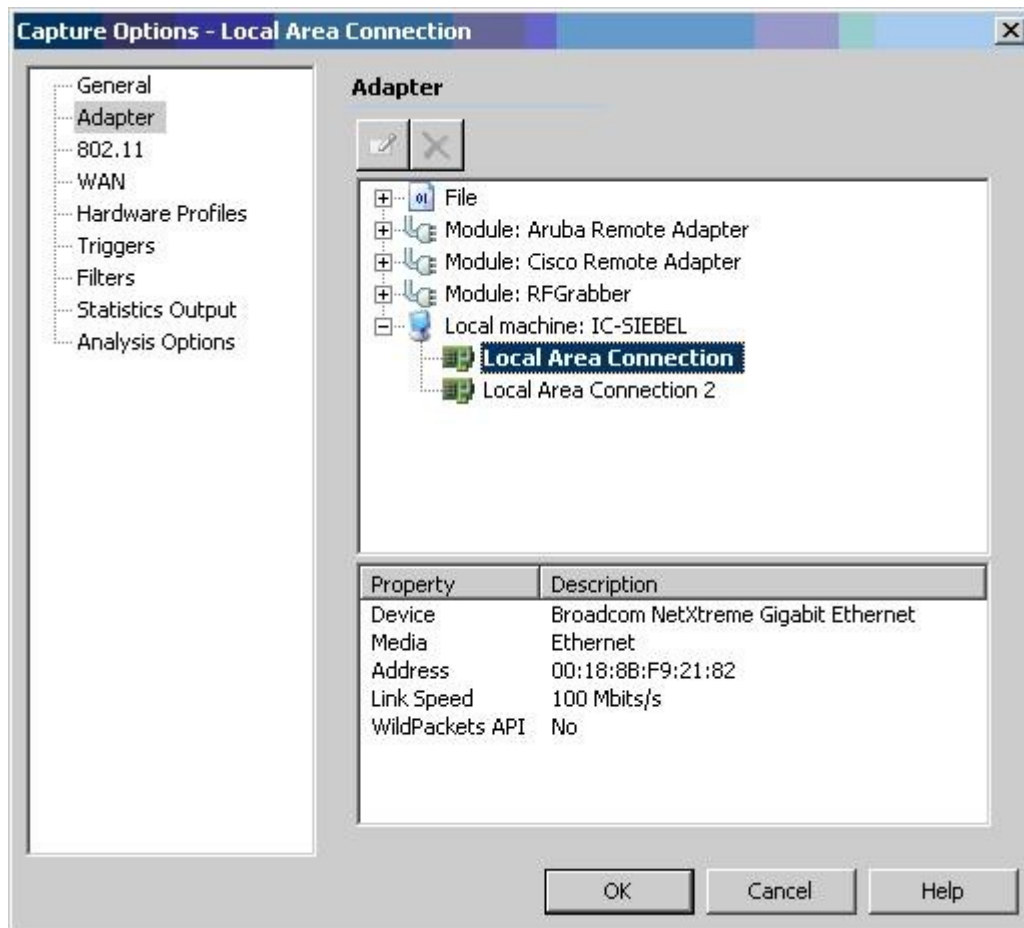


## 4.2. Administer New Capture

The **Capture Options** screen is displayed. Select **General** from the left pane. In the **Capture title** field, enter a descriptive name for the capture. The remaining fields may be modified as needed. For the compliance testing, all default values were retained, which allows the capture to continue until the buffer is filled with 100 megabytes of data.

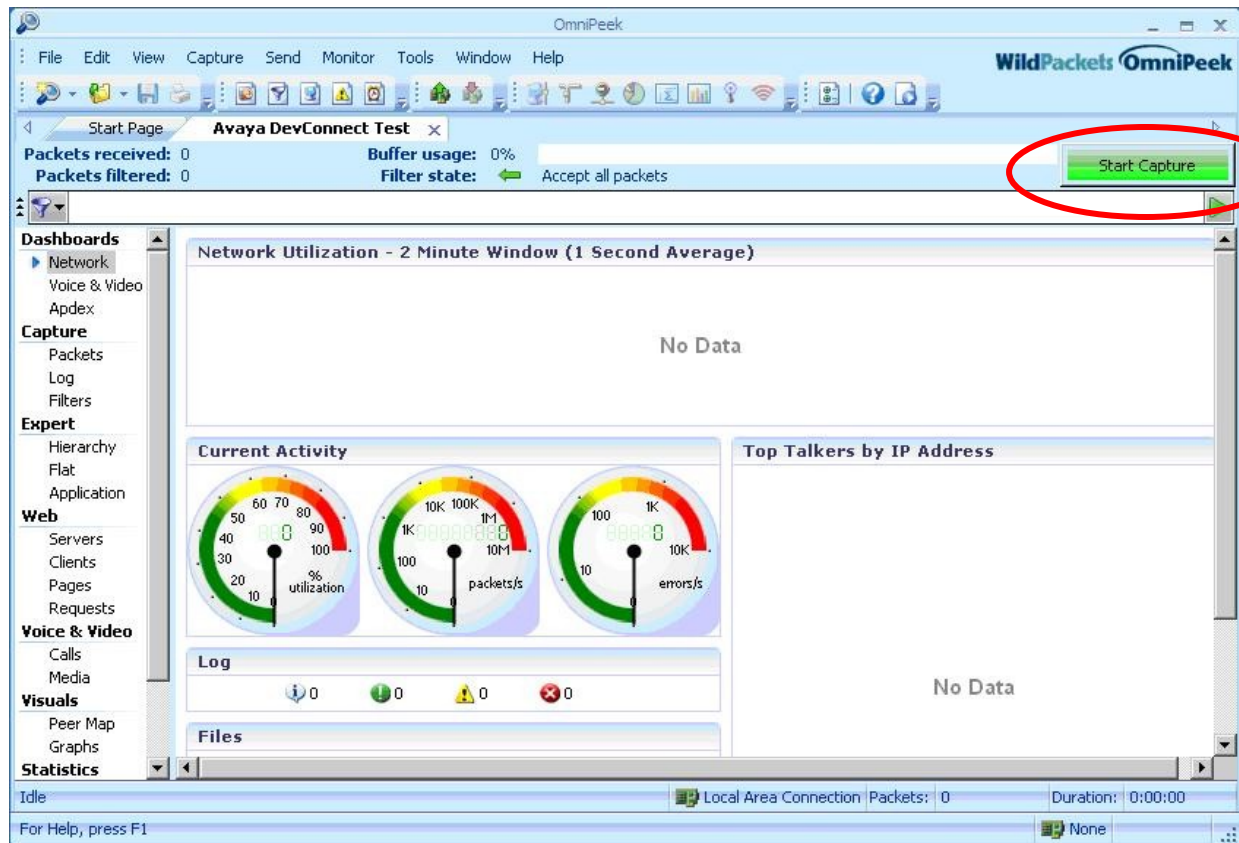


Select **Adapter** from the left pane. Expand the **Local machine** directory in the right pane, and select an appropriate network adapter to use for the testing. Note that the local machine and adapter names may vary. For the compliance testing, the **Local Area Connection** Ethernet adapter was used. For network configurations involving WAN or wireless, a different type of adapter will need to be installed and selected. Click **OK**.



### 4.3. Start Capture

The **OmniPeek** screen is displayed next, as shown below. Click **Start Capture** to start the data capture.



## 5. General Test Approach and Test Results

All tests were performed manually. The Packet Storm was used to inject VoIP impairments, such as jitter and loss, into the network for calls between the two sites.

The serviceability test cases were performed manually by disconnecting and reconnecting the LAN cable to WildPackets OmniPeek Enterprise.

The verification of all tests included proper display of captured data at the WildPackets OmniPeek Enterprise server. The reported VoIP impairments from OmniPeek Enterprise were compared with the impairment injections from the Packet Storm, and with the network audio quality data reported on the Avaya IP Telephones.

All test cases were executed and passed.

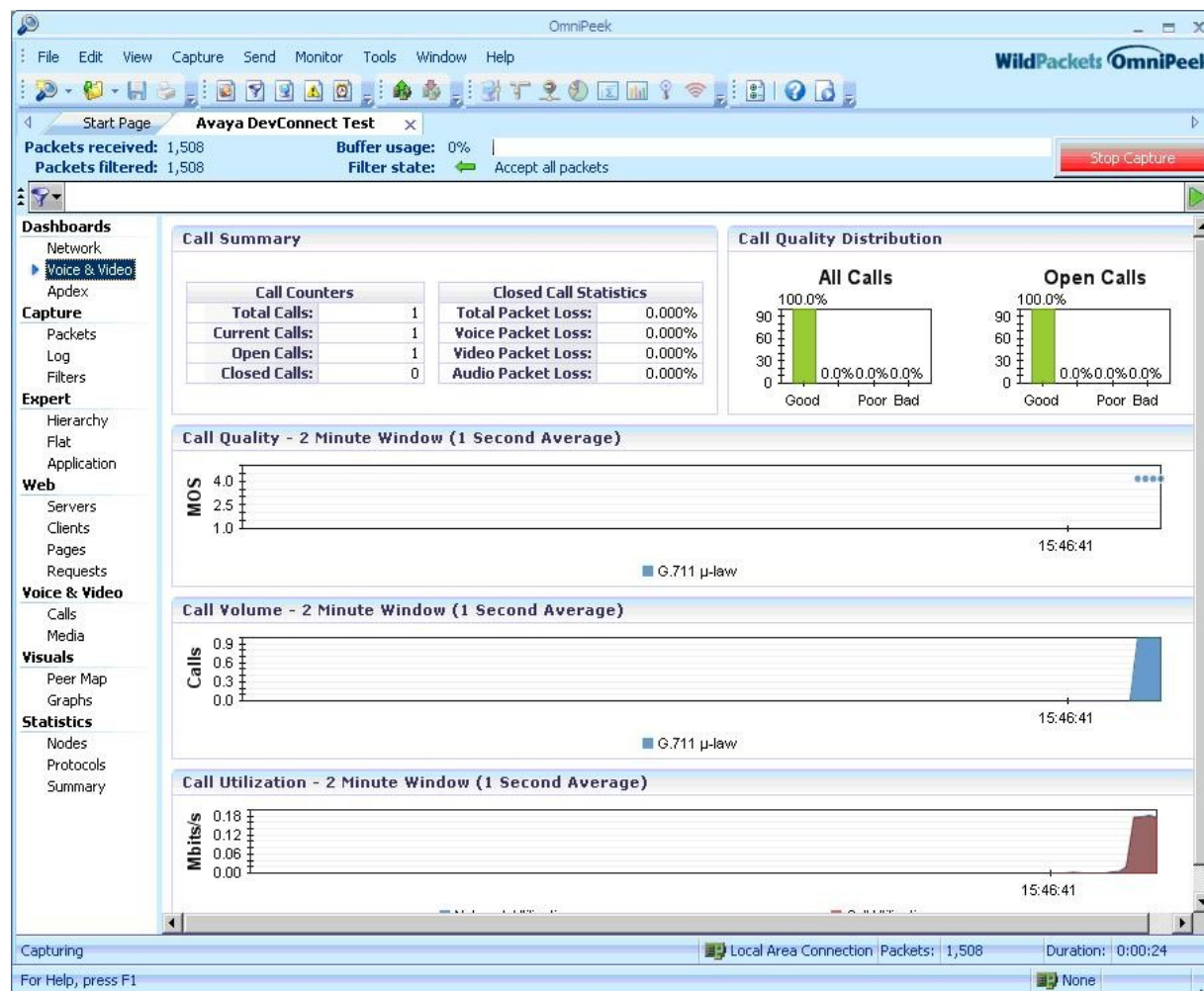
There were three observations from the compliance testing. First, the extension associated with the non-monitored user is not always updated in the call and media entries. Second, when a monitored user ends one call and makes another one immediately, there is a race condition that may result in the reporting of the new call as continuation of the previous call. Third, the reported delay value appears to be twice of what was injected.



## 6. Verification Steps

This section provides the tests that can be performed to verify proper configuration of WildPackets OmniPeek Enterprise. Prior to verification, establish a call between the Central and Remote sites.

In the **OmniPeek** screen, select **Dashboards > Voice & Video** from the left pane. Verify that a visual display of **Call Summary**, **Call Quality**, **Call Volume**, and **Call Utilization** is presented, as shown below.



Select **Voice & Video > Calls** from the left pane. Verify that a call entry is displayed in the top pane for the active call. Note that the IP address 192.2.5.7 denotes the IP Media Processor board in the compliance testing. Select the call entry, and verify that the lower pane is updated with the call detail information. Double click on the call entry in the top pane to launch the Voice & Video Expert.

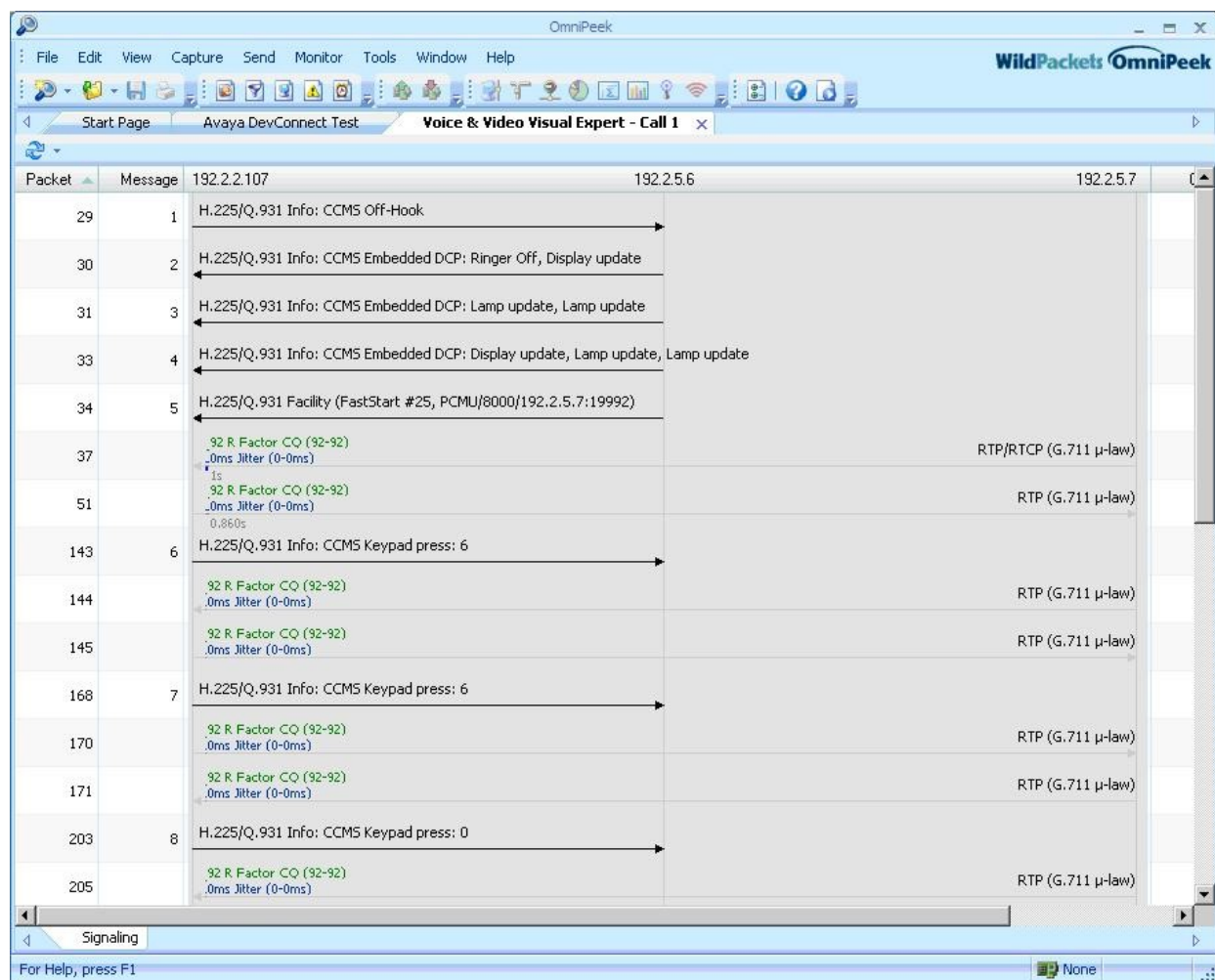
The screenshot shows the OmniPeek software interface. The top menu bar includes File, Edit, View, Capture, Send, Monitor, Tools, Window, and Help. The toolbar contains various icons for file operations and network analysis. The dashboard on the left has sections for Dashboards (Network, Voice & Video, Apdex), Capture (Packets, Log, Filters), Expert (Hierarchy, Flat, Application), Web (Servers, Clients, Pages, Requests), Voice & Video (Calls, Media), Visuals (Peer Map, Graphs), and Statistics (Nodes, Protocols, Summary).

The main display area shows a call entry for 66007-->192.2.5.7. The call status is Open, and the media type is Voice. The event summary table below provides detailed information about the call.

Name	Value	Name	Value
Call Number	1	Name	66007-->192.2.5.7
Caller Address	192.2.2.107	From	ext66007@192.2.2.107:57862
Caller Port		To	gwp@192.2.5.7
Callee Address	192.2.5.7	Call ID	000000000000100000000000C002026B
Callee Port		Call Status	Open
Gatekeeper Address	192.2.5.6	End Cause	
Gatekeeper Port	61441	Signaling	Avaya CCMS/DCP
Media Flows	2	Codec	G.711 µ-law
Media Packets	7535	Bit Rate	64000
Media Frames	301400	Media Type	Voice
Control Flows	2	Setup Time	PDD
Control Packets	36	Start	6/23/2009 15:46:51
Signaling Flows	1	Finish	6/23/2009 15:48:07
Signaling Packets	15	Duration	0:01:15.518589
Packets	7586	MOS-Low	4.17

The bottom status bar shows the capture status: Capturing, Local Area Connection, Packets: 8,125, Duration: 0:01:29. A footer bar indicates 'For Help, press F1' and 'None'.

The **OmniPeek** screen is updated with a **Voice & Video Visual Expert** tab, along with a graphical view of every packet captured for the call.



Select **Voice & Video > Media** from the left pane. Verify that media entries are displayed for the active call. Note that a voice call usually has two media flows, with one flow for each direction. Select a media entry, and verify that the lower pane is updated with the media detail information, including audio quality parameters.

**OmniPeek** WildPackets OmniPeek

File Edit View Capture Send Monitor Tools Window Help

Start Page **Avaya DevConnect Test**

Packets received: 12,451 Buffer usage: 3%  
Packets filtered: 12,451 Filter state: Accept all packets Stop Capture

**Dashboards**  
Network  
Voice & Video  
Apdex  
**Capture**  
Packets  
Log  
Filters  
**Expert**  
Hierarchy  
Flat  
Application  
**Web**  
Servers  
Clients  
Pages  
Requests  
**Voice & Video**  
Calls  
**Media**  
**Visuals**  
Peer Map  
Graphs  
**Statistics**  
Nodes  
Protocols  
Summary

**Current Calls: 1**  
**Media flows: 2**

Call Number	SSRC	Name	End Cause	Codec	Media Type
1	79DC43FD	G.711 192.2.2.107:57862<--192.2.5.7:19992		G.711 µ-law	Voice
1	64576748	G.711 192.2.2.107:57862-->192.2.5.7:19992		G.711 µ-law	Voice

**Details** Event Summary Event Log

Name	Value	Name	Value
Call Number	1	Name	G.711 192.2.2.107:57862<--192.2.5.7:19992
Flow Index	3	From	ext66007@192.2.2.107:57862
SSRC	79DC43FD	To	gwp@192.2.5.7
Flow ID	7	Call ID	0000000000010000000000C002026B
Caller Address	192.2.2.107	End Cause	
Caller Port	57862	Signaling	Avaya CCMS/DCP
Callee Address	192.2.5.7	Protocol	G.711
Callee Port	19992	Codec	G.711 µ-law
Gatekeeper Address	192.2.5.6	Bit Rate	64000
Gatekeeper Port	61441	Media Type	Voice
Source Addr	192.2.5.7	Setup Time	
Source Port	19992	PDD	
Dest Addr	192.2.2.107	Start	6/23/2009 15:46:51
Dest Port	57862	Finish	6/23/2009 15:48:47
Media Packets	5783	Duration	0:01:55.640934
Media Frames	231320	One-Way Delay	0.055000
R Factor Listening	93	Packet Loss %	0
R Factor Conversational	92	Jitter	0.000337
R Factor G.107	92	MOS-LQ	4.19
R Factor Nominal	93	MOS-CQ	4.17
VS-AQ		MOS-PQ	4.44
VS-MQ		MOS-Nom	4.19
VS-PQ		MOS-A	
VS-TQ		MOS-AV	
		MOS-V	

Capturing Local Area Connection Packets: 12,451 Duration: 0:02:11  
For Help, press F1 None

## 7. Conclusion

These Application Notes describe the configuration steps required for WildPackets OmniPeek Enterprise 6.0.2 to interoperate with Avaya Aura Communication Manager via Avaya IP Telephones. All feature and serviceability test cases were completed successfully.

## 8. Additional References

This section references the product documentation relevant to these Application Notes.

1. *Administering Avaya Aura<sup>TM</sup> Communication Manager*, Document 03-300509, Issue 5.0, Release 5.2, May 2009, available at <http://support.avaya.com>.
2. *WildPackets OmniPeek Getting Started Guide*, available on OmniPeek Enterprise installation CD.
3. *WildPackets OmniPeek User Guide*, available on OmniPeek Enterprise installation CD.

---

**©2009 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).