



Avaya Solution & Interoperability Test Lab

Application Notes for WildPackets OmniEngine Enterprise with Avaya Aura[™] Communication Manager – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for WildPackets OmniEngine Enterprise to interoperate with Avaya Aura[™] Communication Manager using Avaya IP Telephones. WildPackets OmniEngine 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 OmniEngine Enterprise to interoperate with Avaya Aura[™] Communication Manager using Avaya IP Telephones. WildPackets OmniEngine 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 OmniEngine 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 OmniEngine Enterprise to obtain information such as calling and called party extensions, and to reassemble the call from the captured packets.

WildPackets OmniEngine Enterprise is typically deployed to remote sites within a distributed enterprise network, and uses the WildPackets OmniPeek Enterprise user interface for displaying captured packets and analyzed reports.

1.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying WildPackets OmniEngine Enterprise's capture of packet streams, and analysis of voice quality from the Avaya IP Telephones. The captured packets and analyzed reports were viewed from the user interface provided by WildPackets OmniPeek Enterprise. 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 OmniEngine Enterprise to recover from adverse conditions, such as disconnecting the Ethernet cable to WildPackets OmniEngine Enterprise.

1.2. Support

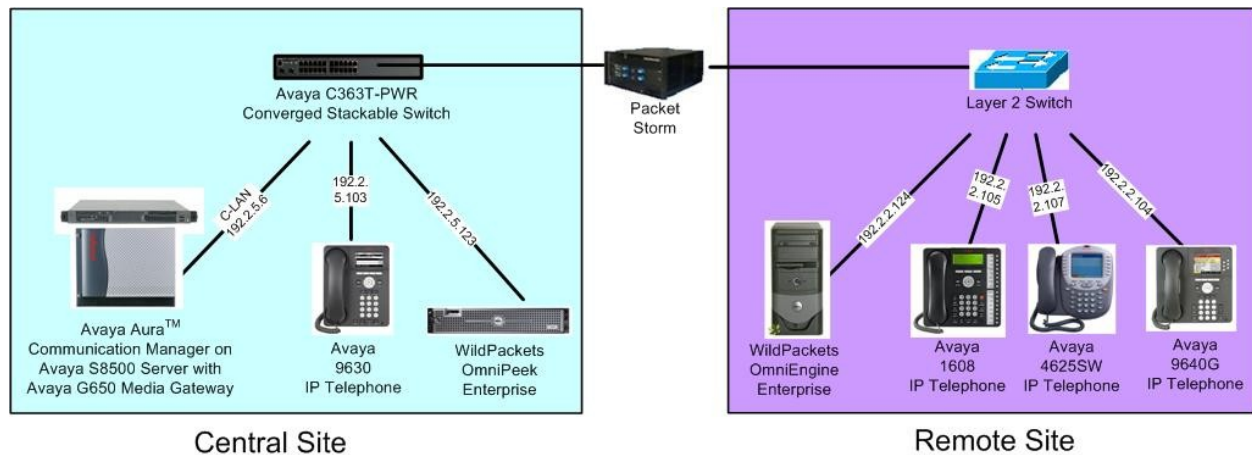
Technical support on WildPackets OmniEngine Enterprise can be requested at www.wildpackets.com/support/contact.

2. Reference Configuration

In the test configuration shown below, WildPackets OmniEngine Enterprise monitored the Avaya IP Telephones at the Remote site, and WildPackets OmniPeek Enterprise monitored the Avaya IP Telephone at the Central site. The WildPackets OmniPeek Enterprise was also used as a software console for the WildPackets OmniEngine Enterprise.

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 OmniEngine Enterprise for analysis. 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 and the integration between WildPackets OmniPeek Enterprise with Avaya Aura Communication Manager are 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">• TN799DP C-LAN Circuit Pack	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
WildPackets OmniEngine Enterprise	6.0.2

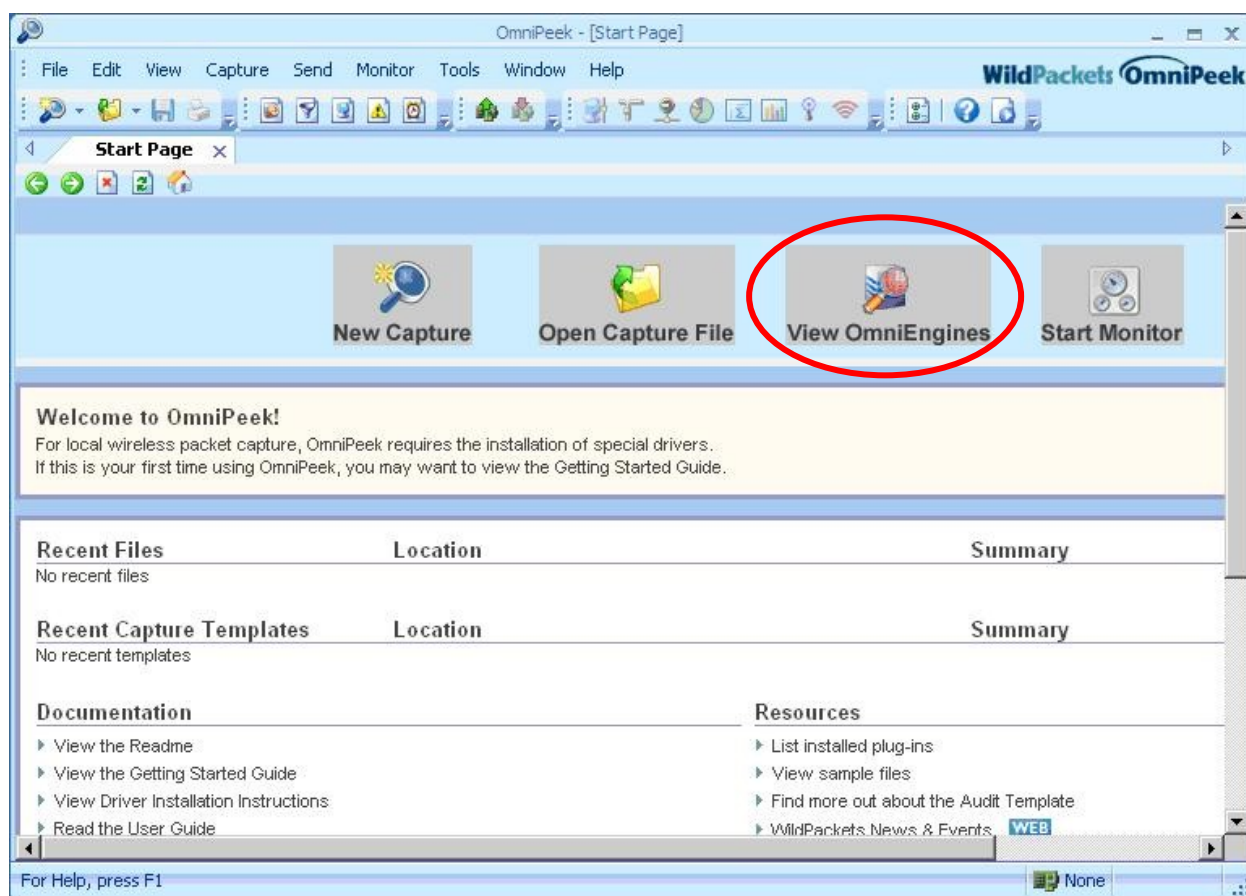
4. Configure WildPackets OmniEngine Enterprise

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

- Launch OmniPeek
- Insert engine
- Administer new capture
- Start capture

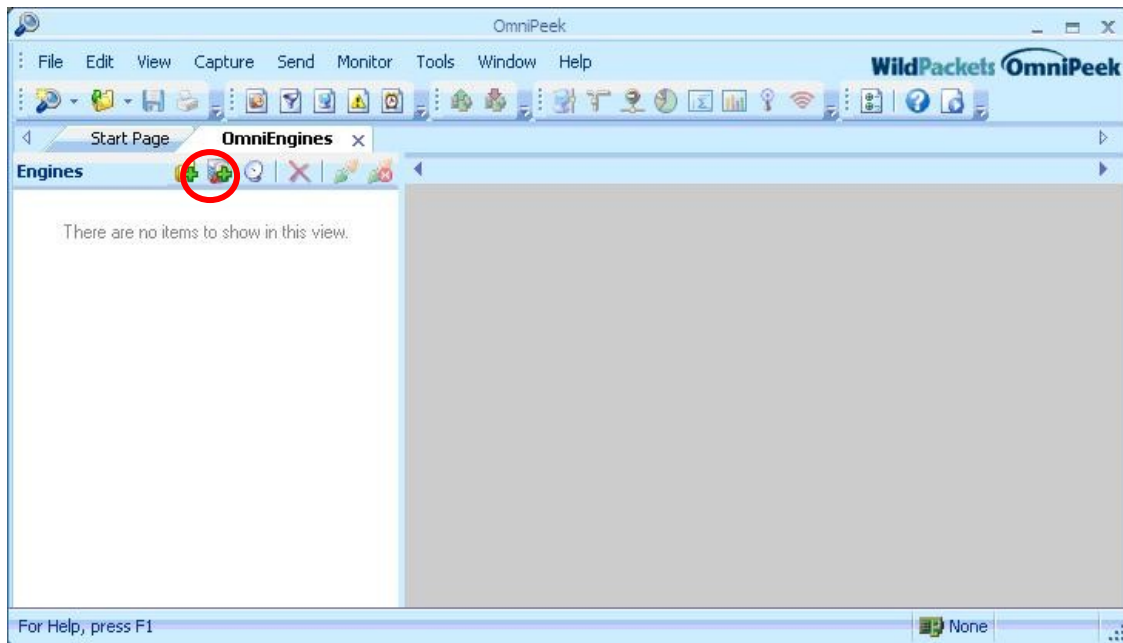
4.1. Launch OmniPeek

The user interface for OmniEngine is provided by OmniPeek. Therefore, from the OmniPeek Enterprise server, select **Start > All Programs > WildPackets OmniPeek**. The **OmniPeek – [Start Page]** screen is displayed, as shown below. Select **View OmniEngines**.



4.2. Insert Engine

The **OmniPeek** screen is updated with an **OmniEngines** tab, as shown below. Click on the Insert Engine icon circled below to add an OmniEngine.

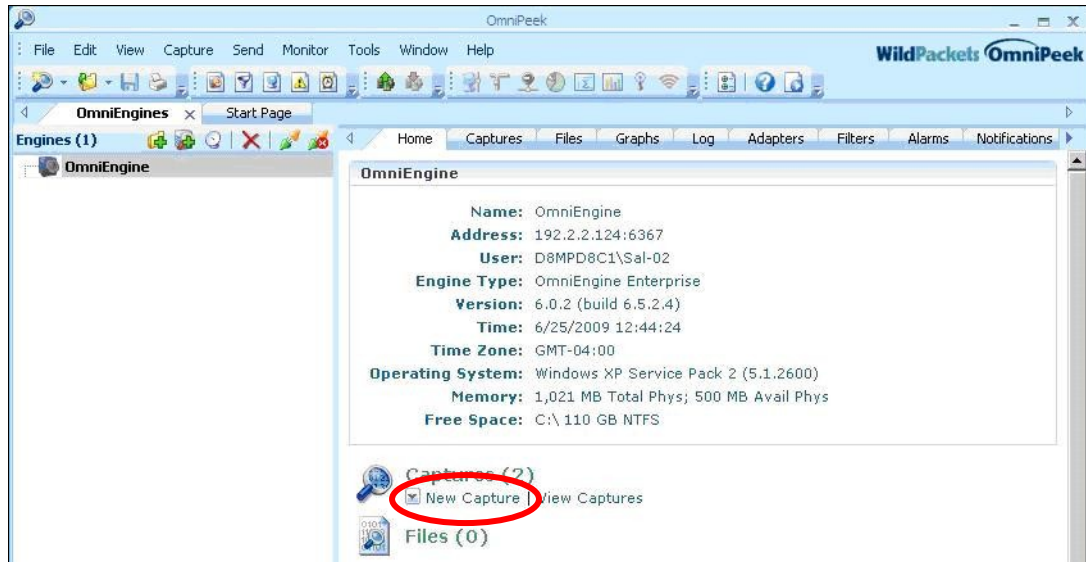


The **Insert Engine** screen is displayed. Enter the IP address of the OmniPeek Engine in the **Host** field, and enter the administrator credentials for the OmniPeek Engine machine in the **Username** and **Password** fields. Retain the default values in the remaining fields, and click **Connect**.

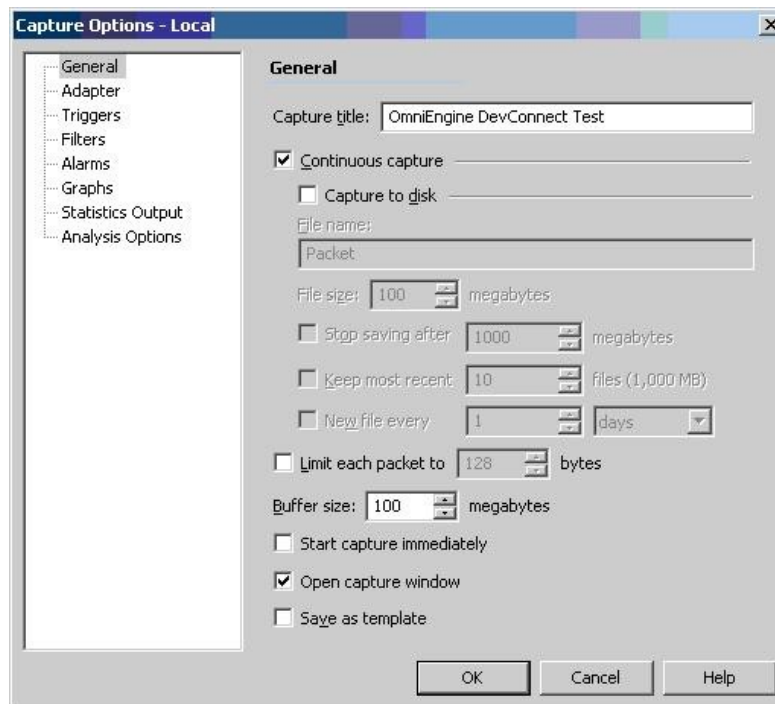
The screenshot shows the "Insert Engine" dialog box. It has a title bar with the text "Insert Engine" and a close button. The dialog is divided into two sections: "Engine" and "Credentials". In the "Engine" section, there is a "Host" field with the value "192.2.2.124" and a "Port" field with the value "6367". In the "Credentials" section, there is an "Authentication" dropdown menu set to "Default", a "Domain" field, a "Username" field with the value "xxx", and a "Password" field with three dots. There is also a checkbox labeled "Save my password" which is unchecked. At the bottom of the dialog, there are three buttons: "Connect", "Cancel", and "Help".

4.3. Administer New Capture

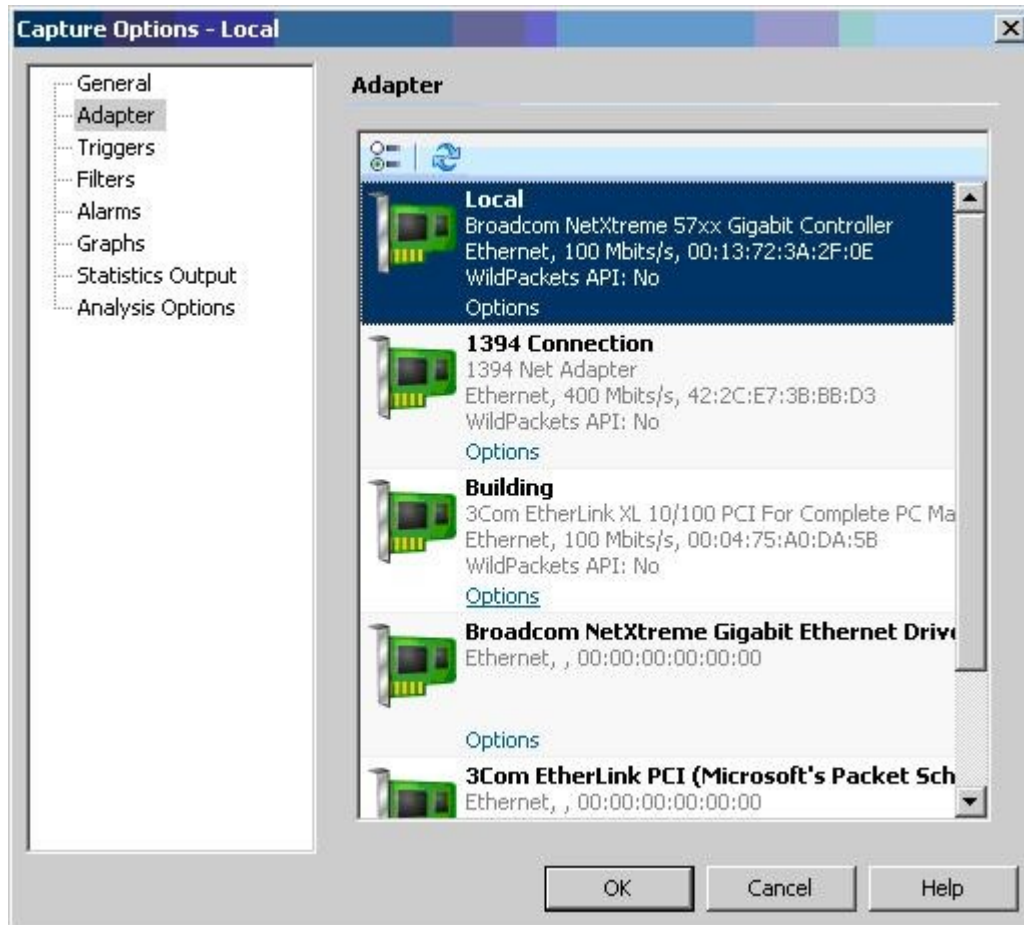
The **OmniPeek** screen is updated with information for the connected OmniEngine, as shown below. Click **New Capture**.



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.

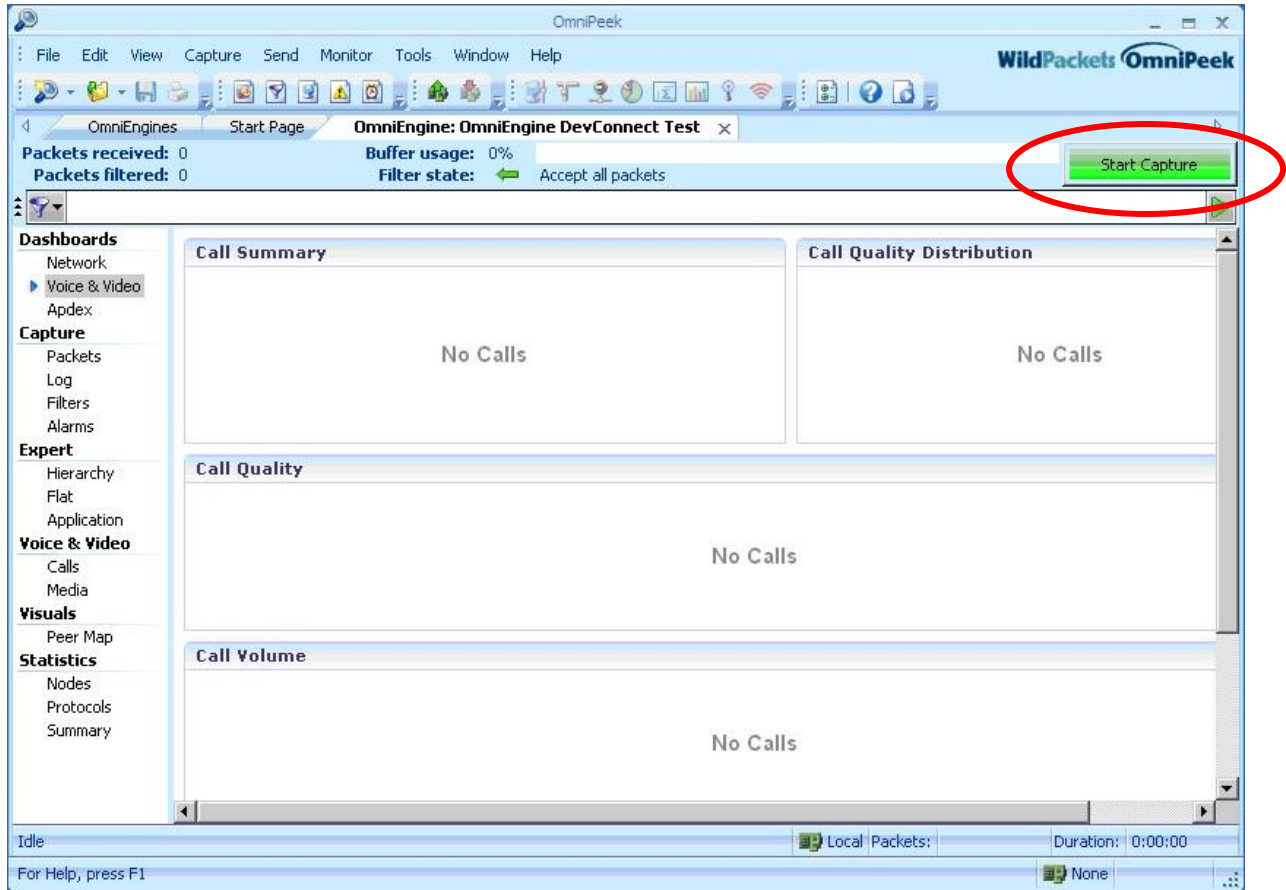


Select **Adapter** from the left pane to display a list of available adapters for the OmniEngine. Select an appropriate network adapter to use for the testing. Click **OK**.



4.4. Start Capture

The **OmniPeek** screen is displayed again, 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 OmniEngine Enterprise.

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

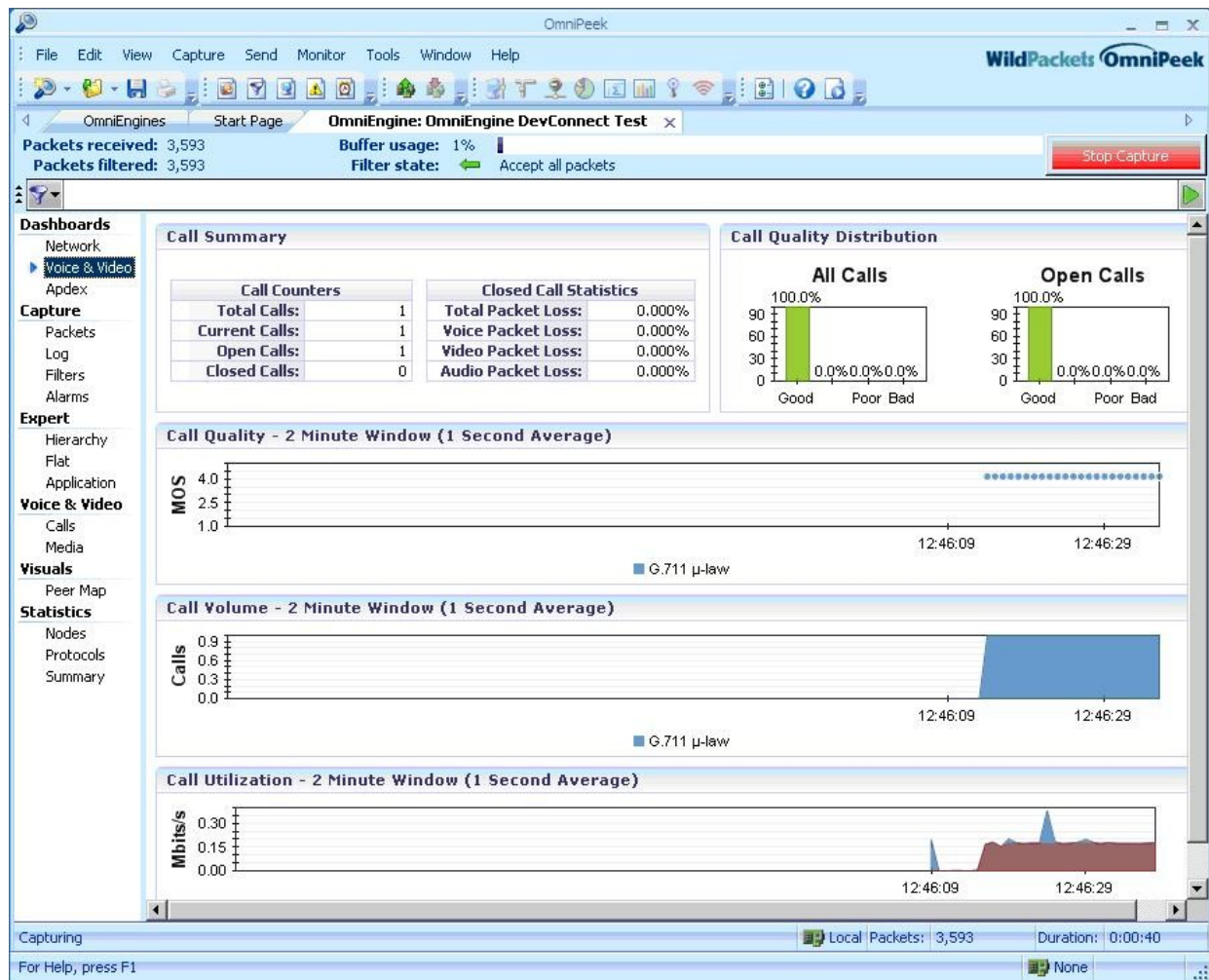
All test cases were executed and passed.

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 OmniEngine 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. 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 application window. The top menu bar includes File, Edit, View, Capture, Send, Monitor, Tools, Window, and Help. Below the menu bar is a toolbar with various icons. The main window is titled "OmniPeek" and "WildPackets OmniPeek". The status bar at the top shows "Packets received: 7,927", "Packets filtered: 7,927", "Buffer usage: 2%", and "Filter state: Accept all packets". A "Stop Capture" button is visible on the right.

The left pane contains a tree view with the following categories:

- Dashboards**
 - Network
 - Voice & Video
 - Apdex
- Capture**
 - Packets
 - Log
 - Filters
 - Alarms
- Expert**
 - Hierarchy
 - Flat
 - Application
 - Voice & Video**
 - Calls** (selected)
 - Media
 - Visuals**
 - Peer Map
 - Statistics**
 - Nodes
 - Protocols
 - Summary

The main pane displays call information. At the top, it shows "Total Calls: 1" and "Current Calls: 1". Below this is a table with the following columns: Call Number, Name, Call Status, End Cause, Codec, and Media Type. The table contains one entry:

Call Number	Name	Call Status	End Cause	Codec	Media Type
1	66007-->66003	Open		G.711 μ-law	Voice

Below the table is a "Details" tab with a sub-tab "Event Summary". The "Event Summary" tab displays a list of call details:

Name	Value
Call Number	1
Caller Address	192.2.2.107
Caller Port	
Callee Address	192.2.5.103
Callee Port	
Gatekeeper Address	192.2.5.6
Gatekeeper Port	61441
Media Flows	5
Media Packets	8226
Media Frames	329040
Control Flows	4
Control Packets	38
Signaling Flows	1
Signaling Packets	18
Packets	8282

The bottom status bar shows "Capturing" and "Local" with "Packets: 7,927" and "Duration: 0:01:21".

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

Packet	Message	192.2.2.107	192.2.5.6	192.2.5.103	192.2.5.7	Call Number	Flow Index
35	1	H.225/Q.931 Info: CCMS Off-Hook				1	1
36	2	H.225/Q.931 Info: CCMS Embedded DCP: Ringer Off, Display update				1	1
37	3	H.225/Q.931 Info: CCMS Embedded DCP: Lamp update, Lamp update				1	1
38	4	H.225/Q.931 Info: CCMS Embedded DCP: Display update, Lamp update, Lamp update				1	1
41	5	H.225/Q.931 Facility (FastStart #25, PCMU/8000/192.2.5.7:26060)				1	1
43				RTP/RTCP (G.711 µ-law)		1	2
58				RTP (G.711 µ-law)		1	4
71	6	H.225/Q.931 Info: CCMS Keypad press: 6				1	1
72				RTP/RTCP (G.711 µ-law)		1	2
74				RTP (G.711 µ-law)		1	4
100	7	H.225/Q.931 Info: CCMS Keypad press: 6				1	1
103		92 R Factor CQ (92-92) .0ms Jitter (0-0ms)				1	2

Signaling

For Help, press F1

Select **Voice & Video > Media** from the left pane. Verify that media entries are displayed for the active call. Select a media entry, and verify that the lower pane is updated with the media detail information, including audio quality parameters.

The screenshot shows the OmniPeek application window. The top menu bar includes File, Edit, View, Capture, Send, Monitor, Tools, Window, and Help. The status bar at the top indicates 'Packets received: 28,238', 'Packets filtered: 28,238', 'Buffer usage: 8%', and 'Filter state: Accept all packets'. A 'Stop Capture' button is visible on the right.

The left sidebar contains a tree view with the following categories: Dashboards, Network, Voice & Video, Apex, Capture, Packets, Log, Filters, Alarms, Expert, Hierarchy, Flat, Application, Voice & Video, Calls, Media (selected), Visuals, Peer Map, Statistics, Nodes, Protocols, and Summary.

The main window displays a table of media flows. The table has columns: Call Number, SSRC, Name, End Cause, Codec, Media ..., Start, and Duration. The selected row is:

Call Number	SSRC	Name	End Cause	Codec	Media ...	Start	Duration
1	32FD615F	G.711 192.2.2.107:57862<--192.2.5.7:26060		G.711 μ-law	Voice	6/25/2009 12:46:16	2.099956
1	6F7D6188	G.711 192.2.2.107:57862-->192.2.5.7:26060		G.711 μ-law	Voice	6/25/2009 12:46:16	2.059678
1	236E5F17	G.711 192.2.2.107:57862<--192.2.5.103:6...		G.711 μ-law	Voice	6/25/2009 12:46:18	0.040034
1	108ESD1B	G.711 192.2.2.107:57862<--192.2.5.103:6...		G.711 μ-law	Voice	6/25/2009 12:46:18	0:04:10.877714
1	33C33D73	G.711 192.2.2.107:57862-->192.2.5.103:6...		G.711 μ-law	Voice	6/25/2009 12:46:18	0:04:10.693020

The bottom pane shows the details of the selected media flow. It is divided into two sections: 'Details' and 'Event Summary'. The 'Details' section lists various parameters:

Name	Value
Call Number	1
Flow Index	7
SSRC	33C33D73
Flow ID	9
Caller Address	192.2.2.107
Caller Port	57862
Callee Address	192.2.5.103
Callee Port	62332
Gatekeeper Address	192.2.5.6
Gatekeeper Port	61441
Source Addr	192.2.2.107
Source Port	57862
Dest Addr	192.2.5.103
Dest Port	62332
Media Packets	12536
Media Frames	501440
R Factor Listening	93
R Factor Conversational	92
R Factor G.107	92
R Factor Nominal	93
V5-AQ	
V5-MQ	

The 'Event Summary' section lists various parameters:

Name	Value
Name	G.711 192.2.2.107:57862-->192.2.5.103:62332
From	ext66007@192.2.2.107:57862
To	ext66003@192.2.5.103:62332
Call ID	000000000000100000000000C002026B
End Cause	
Signaling	Avaya CCMS/DCP
Protocol	G.711
Codec	G.711 μ-law
Bit Rate	64000
Media Type	Voice
Setup Time	0.822782
PDD	0.060816
Start	6/25/2009 12:46:18
Finish	6/25/2009 12:50:29
Duration	0:04:10.693020
One-Way Delay	0.054000
Packet Loss %	0
Jitter	0.000226
MOS-LQ	4.19
MOS-CQ	4.17
MOS-PQ	4.44
MOS-Nom	4.19
MOS-A	

The bottom status bar shows 'Capturing' status, 'Local' source, 'Packets: 28,238', 'Duration: 0:04:24', and a 'None' button.

7. Conclusion

These Application Notes describe the configuration steps required for WildPackets OmniEngine 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 AuraTM Communication Manager*, Document 03-300509, Issue 5.0, Release 5.2, May 2009, available at <http://support.avaya.com>.
2. *WildPackets OmniEngine Getting Started Guide*, available on OmniEngine 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.