

**Agilent Technologies 8960 Series 10 Wireless Communications Test Set**

# **Agilent E6584A Wireless Protocol Advisor Operation Guide**

E6584A Option 001 GSM/GPRS/EGPRS Wireless Protocol Advisor  
E6584A Option 002 cdma2000 Wireless Protocol Advisor  
E6584A Option 003 W-CDMA Wireless Protocol Advisor

Part Number: 1000-1868 (not orderable)

© Copyright Agilent Technologies 2000-2003

**[www.agilent.com/find/8960/](http://www.agilent.com/find/8960/)**



**Agilent Technologies**

---

## Notice

Information contained in this document is subject to change without notice.

All Rights Reserved. Reproduction, adaptation, or translation without prior written permission is prohibited, except as allowed under the copyright laws.

This material may be reproduced by or for the U.S. Government pursuant to the Copyright License under the clause at DFARS 52.227-7013 (APR 1988).

Agilent Technologies, Inc.  
Learning Products Department  
24001 E. Mission  
Liberty Lake, WA 99019-9599  
U.S.A.

---

# Contents

<b>Introduction</b>	<b>5</b>
Conventions used in this Getting Started Guide	6
How to use this Guide	6
<b>Hardware and Software Requirements</b>	<b>8</b>
<b>Installing Wireless Protocol Advisor (WPA) Software on the PC</b>	<b>9</b>
<b>Connecting the PC to the Test Set</b>	<b>10</b>
Direct Connection	10
LAN Connection	16
<b>Protocol Analysis</b>	<b>21</b>
Introduction to WPA	21
WPA Filters	25
WPA Triggers	38
Customizing the Traffic Overview	43
Customizing the Decode View	47
Saving Log Files	50
Exporting and Importing Measurement Setups	53
Working With Multiple Traffic Overviews	54
Tracing Multiple IP Connections (Connection Trace)	58



## Introduction

Last updated: December 9, 2003

### Scope of this guide:

The intent of this guide is to help you quickly learn how to use the Wireless Protocol Advisor software for logging and analyzing the protocol messages transmitted between the test set and your wireless devices under test. It does not cover all features and capabilities of the WPA software. For details, refer to the software online help.

---

**NOTE** The examples in this Getting Started Guide are based on the Agilent Technologies E6584A Option 002 cdma2000 Wireless Protocol Advisor software and the Agilent Technologies E5515C test set with the E6702A/B cdma2000 Lab Application installed. However the basic procedures are the same if you are using WPA options for GPRS or W-CDMA (the product numbers for these are detailed in [Table 1. “Compatibility of Software, Application, and Hardware”](#)).

---

### About the WPA:

The E6584A WPA (Wireless Protocol Advisor) is a software product that assists in analyzing protocol issues that effect communication between a wireless device and base station.

Message decoding is performed on protocol stacks that must be licensed and running on both the WPA and the E5515C test set.

Raw protocol data is captured by the test set at various tap points in the protocol stack as a wireless device communicates with the test set's base station emulator. This data is sent from the test set to the PC running the WPA software. WPA then performs filtering and decoding to display meaningful data.

The WPA software provides controls for formatting the window that displays protocol messages. Detailed information about each message, such as message field contents, is displayed when needed.

Through the use of filters WPA can focus on specific layers in the protocol stack. By “probing” target layers in the protocol stack, the amount of data that is captured can be reduced to only those of interest.

The E6584A Wireless Protocol Advisor (WPA) option 001, 002, or 003 is included with the respective lab or protocol application purchased, as well as being available stand-alone. See [Table 1. “Compatibility of Software, Application, and Hardware”](#) for details.

**Table 1. Compatibility of Software, Application, and Hardware**

Software	Application	Hardware
E6584A Option 001 GSM/GPRS/EGPRS decodes	E6701C GSM/GPRS Lab Application (including E6704A EGPRS Lab Application).	E5515C Wireless Communications Test Set
E6584A Option 002 cdma2000 decodes	E6702A/B cdma2000 Lab Application	E5515C Wireless Communications Test Set
E6584A Option 003 W-CDMA decodes	E6703A/B W-CDMA Lab Application	E5515C Wireless Communications Test Set

**Table 1. Compatibility of Software, Application, and Hardware**

Software	Application	Hardware
E6584A Option 001 GSM/GPRS/EGPRS decodes	E6910A GPRS Protocol Application, revision A.03 or later.	E6900A Wireless Protocol Test Set
E6584A Option 001 GSM/GPRS/EGPRS decodes	E6910B GPRS Protocol Application, revision B.00 or later.	E6900A Wireless Protocol Test Set

## Conventions used in this Getting Started Guide

Throughout this Getting Started Guide, the terms:

- Test set - refers to the *Hardware* with an *Application* installed. See [Table 1. “Compatibility of Software, Application, and Hardware”](#).
- WPA - refers to one of the Agilent Technologies Wireless Protocol Advisors. See [Table 1. “Compatibility of Software, Application, and Hardware”](#).
- Mobile station - refers to any wireless devices specific for your test.

## How to use this Guide

There are many examples provided in this guide to help you understand the features in WPA. You do not need the test equipment or WPA software to learn about WPA, but if you do have the required equipment, this paper can be used as a lab guide.

### As a lab guide (Real Time mode)

See [“Hardware and Software Requirements” on page 8](#) for a listing of the equipment required to use this as a lab guide using the WPA to log data real time. A cdma2000 wireless device is used in the examples found in this guide.

### As a lab guide (Post Capture mode)

If you have access to a PC that has WPA installed but no test equipment is readily available, you can gain experience with WPA by opening one of the many files provided in the “\Program Files\Wireless Protocol Advisor\User Files\Capture Data\Demo Traffic\Cdma” folder and applying the procedures that follow. These demo files contain a collection of call processing operations that were previously captured and included for demonstration purposes.

---

**NOTE** The WPA software can be downloaded from the Internet without a license. You can run WPA in Demo Mode, which allows access to all of the features discussed in this paper. You will find the download links at [www.agilent.com/find/e6584a](http://www.agilent.com/find/e6584a).

---

### For additional documentation

To access comprehensive documentation on the WPA and lab applications available with the Agilent 8960, refer to the online help included in the WPA software and your application’s User’s Guide. This documentation

is available from:

- <http://www.agilent.com/find/8960> (test set)
- <http://www.agilent.com/find/e6701a> (lab application)
- <http://www.agilent.com/find/e6702a> (lab application)
- <http://www.agilent.com/find/e6702b> (lab application)
- <http://www.agilent.com/find/e6703a> (lab application)
- <http://www.agilent.com/find/e6703b> (lab application)
- <http://www.agilent.com/find/e1968a> (test application)
- <http://www.agilent.com/find/e6584a> (WPA)
- the User Documentation CD-ROM shipped with your lab application.

---

## Hardware and Software Requirements

Last updated: December 9, 2003

- Protocol Logging Software: Agilent Technologies Wireless Protocol Advisor (WPA). See [Table 1. “The Compatibility of Software, Application, and Hardware”](#).
- Test Set: Agilent Technologies 8960 Series 10 Wireless Communication test set with a lab or protocol application installed. See [Table 1. “The Compatibility of Software, Application, and Hardware”](#).
- Your Personal Computer (PC) must meet these requirements:
  - Windows® 98, Windows NT® 4.0 (service pack 3 or above), Windows® 2000, or Windows® XP.
  - 300 MHz Pentium or equivalent recommended
  - 128 MB RAM minimum
  - 250 MB available disk space required for installation
  - 100 MB available disk space recommended for storing logged information

---

**NOTE** After installation, WPA requires that at least 5% of the total disk space is available for WPA to begin logging. If WPA is not logging make sure it is connected and the logging mode is Active. If it still is not logging, check disk space and free up space if necessary.

---

- Video resolution minimum 800 by 600 pixels with at least 256 colors
- LAN or WAN connectivity required to connect to the test set
- Wireless Device: any wireless devices under test (for example, a cdma2000 phone)
- Cables:
  - RF Cable: Use an appropriate cable that attaches from your wireless device to the test set's RF IN/OUT port.
  - If you are making a [“Direct Connection” on page 10](#), use the crossover LAN Cable provided, Agilent Part Number 8121-0510. Or, as an alternative, use Black Box® Part No. EVCRB05-0006. This cable is a Category-5 Crossover Cable, 1.8 meters long, with 4-pair RJ-45 connectors (from Black Box Corporation).
  - If you are making a [“LAN Connection” on page 16](#), use standard LAN Cables.





---

## Installing Wireless Protocol Advisor (WPA) Software on the PC

Last updated: December 9, 2003

Follow the procedure below to install the WPA software on your PC. If the software is already installed on your PC, please move on to the [“Using the Wireless Protocol Advisor for Protocol Logging and Analysis” on page 22.](#)

1. Insert CD (shipped with your purchase) to automatically start the installation, or download the software from the web (for example, go to <http://www.agilent.com/find/e6584a>, click "Download Wireless Protocol Advisor Software" under **Highlights** headline, then select the E6584A cdma2000 Wireless Protocol Advisor Software under **Download** headline) and run the  Setup from the downloaded files.
2. Follow the wizard instructions to install the software to the default directories (you can change if desired).
3. After the successful installation, restart your PC, an  icon is shown on your desktop. If no licensed versions of WPA software are detected on your computer, a software utility called Software Option Controller will run first. This allows you to select whether you want to redeem software licenses or run the WPA software in Demo mode.
4. Follow the online help instructions for Loading and Licensing the Wireless Protocol Advisor. If you have not purchased the WPA software, you can still operate it in Demo mode by clicking the Demo Mode button in the Software Option Controller.

---

<b>NOTE</b>	WPA software requires a license file to operate in real time mode, which must be downloaded from the web. The information required to download the license file is found on the Software Entitlement Certificate, which you received when the WPA was purchased.
-------------	--

---

---

## Connecting the PC to the Test Set

Before attempting to make a network connection between your PC and the test set, you must have:

- A licensed WPA software option running on the PC.
- A licensed lab or protocol application running on the test set.

The WPA option must match the application running on the test set. For example, if the CDMA 2000 Lab Application is the current system type running on the test set, WPA option 002 (cdma2000) must be licensed.

To provide a network connection between the Agilent 8960 test set and the PC running the WPA software, you can establish either a:

- [“Direct Connection” on page 10](#) or
- [“LAN Connection” on page 16](#)

### Direct Connection

A direct connection can be made between the test set and the PC running WPA. This method simplifies LAN IP setup requirements by eliminating the need for a system administrator to assign IP addresses for the PC and test set (it is recommended you use the IP addresses given in [“Direct Connection Example IP Settings” on page 11](#)).

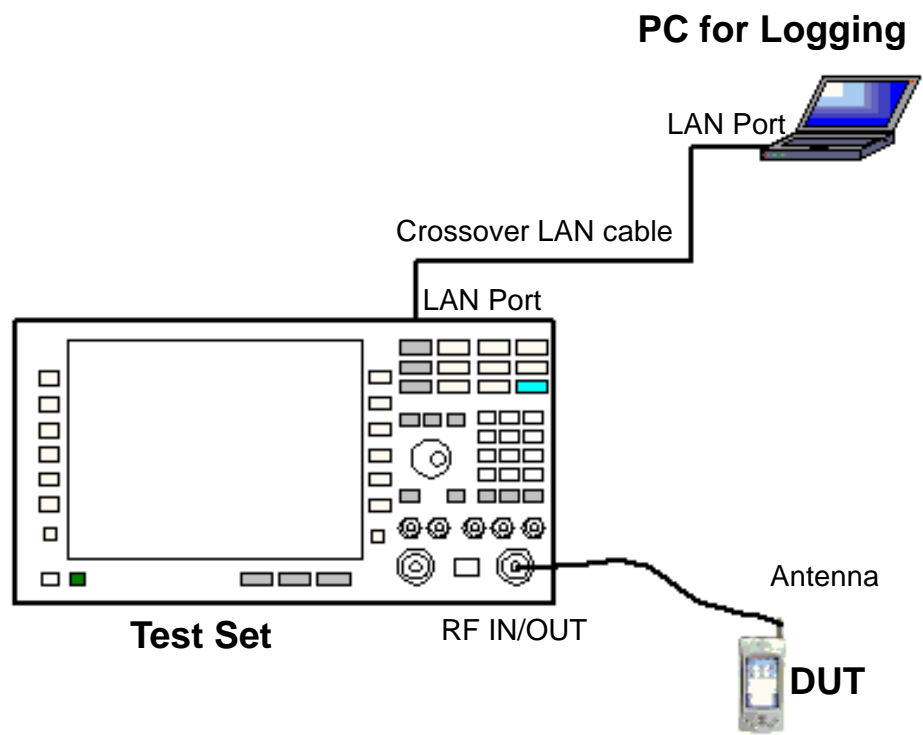
Connect your PC's LAN port to one of the test set's LAN ports using a crossover LAN cable (shipped with the test set). See [Figure 1. on page 11](#).

---

<b>NOTE</b>	There are two LAN ports on the Test Set to provide both front and rear panel data connections. If you are connecting to the test set's front panel DATA port, please verify that the rear panel LAN PORT and ETHERNET TO FRONT PANEL port are connected by a jumper cable (shipped with the test set).
-------------	--

---

**Figure 1. Direct Connection Diagram**



**Direct Connection Setup**

For the direct connection, it is necessary that the PC and test set are on the same subnet, and that the host portion of the IP addresses is unique.

The portion of the IP address that defines the subnet depends on the address class and the Subnet Mask. Refer to [Table 2. on page 11](#) for an example of settings that meet these requirements.

**Table 2. Direct Connection Example IP Settings**

	IP Address	Subnet Mask
Test Set	146.208.241.186	255.255.254.0
PC	146.208.241.26	255.255.254.0

**STEP 1. Enter the Test Set’s IP Address and Subnet Mask.**

1. Turn on the test set. If it is already on, we recommend you reset the test set by pressing the blue **SHIFT** key and then the green **Preset** key.
2. Press the **SYSTEM CONFIG** key.
3. Press the Instrument Setup (**F1**) key, set test set’s LAN IP Address and Subnet Mask using the knob and

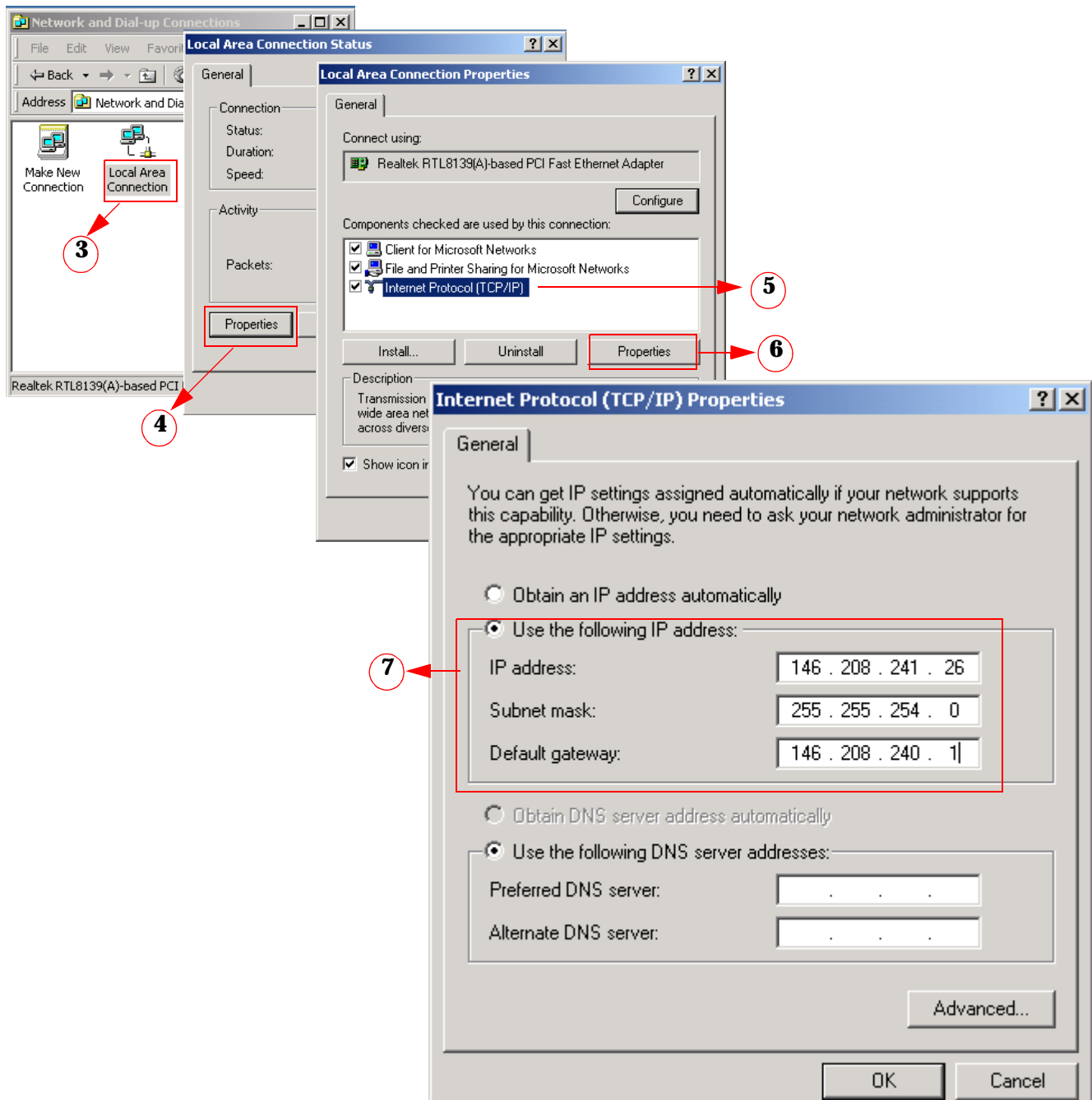
DATA ENTRY Keys. You can set to the values as shown in [Table 2. on page 11](#).

Instrument Setup	Value
GPIB Address	14
LAN IP Address	146.208.241.186
Subnet Mask	255.255.254.0
Default Gateway	146.208.240.1
Display Mode	Track
Display Brightness	High
Beeper State	Off
Date (yyyy.mm.dd)	2000.01.01

4. Press the Close Menu (**F6**) key.
5. Verify that the desired lab application is active. If not, switch applications.

**STEP 2. Set Up Your PC** This procedure assumes you are using a standalone PC (not connected to a network) using the Microsoft® Windows 2000 operating system. Other PC operating systems may use slightly different setups.

1. Click **Start**, highlight **Settings**, then click the **Control Panel**.
2. Click **Network and Dial-up Connections** icon, then perform the following procedure (see [Figure 2. on page 13](#)):
3. Select the **Local Area Connection** icon,
4. Click **Properties**,
5. Highlight **Internet Protocol (TCP/IP)** item,
6. Click **Properties**,
7. Check the box labeled **Use the following IP Address**, then enter the IP address and Subnet Mask for the PC. Refer to [Table 2. on page 11](#) for an example of IP Address settings.
8. Select **OK**, then **OK** again to exit the Network and Dial-up Connections settings.

**Figure 2. Set the PC's IP Address****STEP 3. Attempt to make a connection between the PC and the test set .**

1. Double-click the WPA icon. The WPA main menu will be displayed

Figure 3. WPA Main Menu

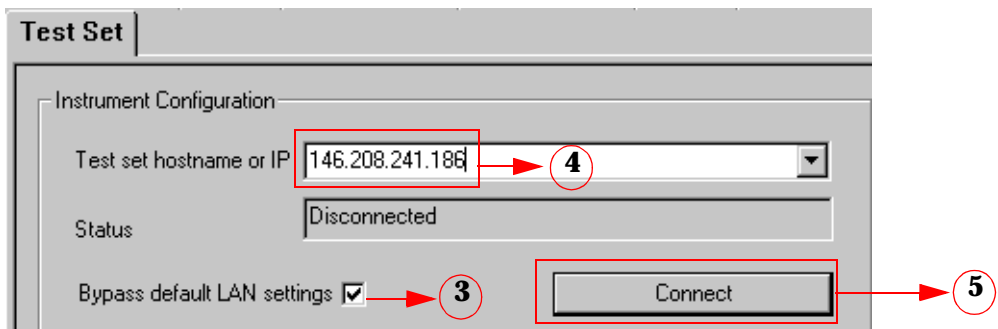


2. Click the Real Time button.

**NOTE** When Real Time is selected, WPA will automatically display the Configuration window if it detects that there has not been a test set IP address entered.

If a test set IP address has been entered in a prior session, WPA will automatically attempt to connect with the test set. If it is successful, WPA will display the Traffic Overview and you are ready to begin logging. If the connection attempt is unsuccessful, the Configuration window will be displayed.

Figure 4. Configuration Window

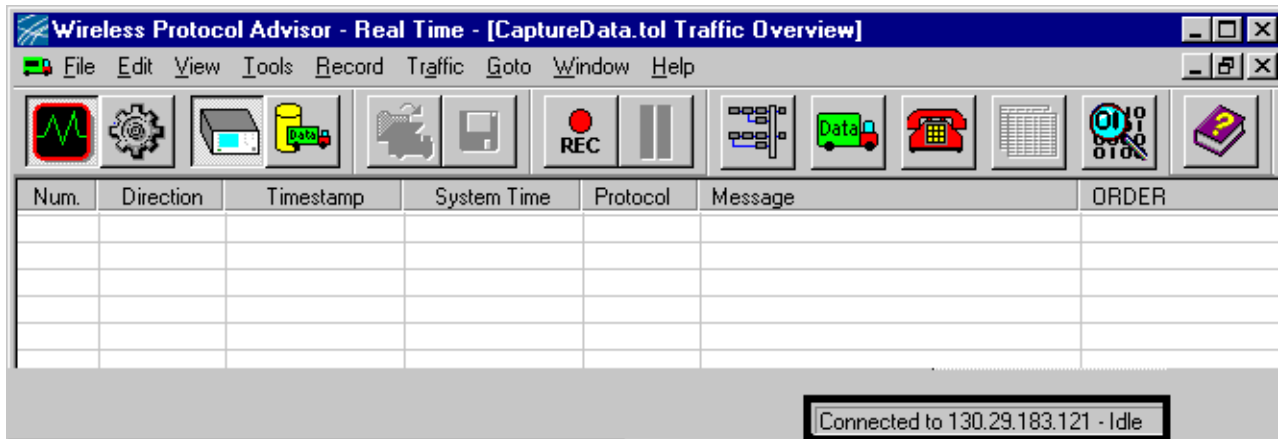


3. Select the Bypass default LAN settings box.

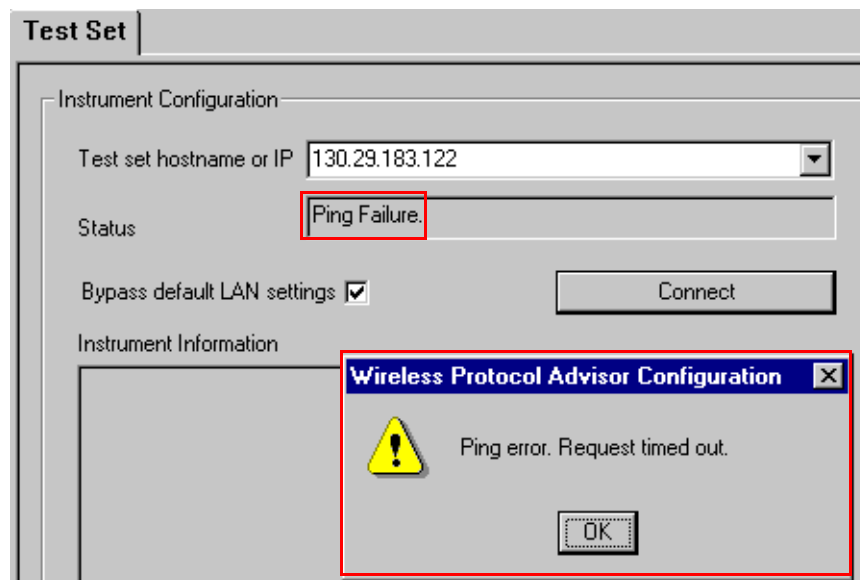
4. Enter the test set's IP address.
5. Click on the Connect button.

The WPA will attempt to establish a network connection with the test set. If successful, the Traffic Overview window will be displayed:

When a connection is successful, the WPA Traffic Overview will be displayed with the status message "Connected to <host> - Idle". The test set will display "Logging:Idle" on the front panel display.



If the connection is not successful, the Instrument Configuration window will display an error message:



### Troubleshooting:

- Check the IP addresses on both the PC and the test set's System Config screen
- Make sure the check box Bypass default LAN settings is checked.

## LAN Connection

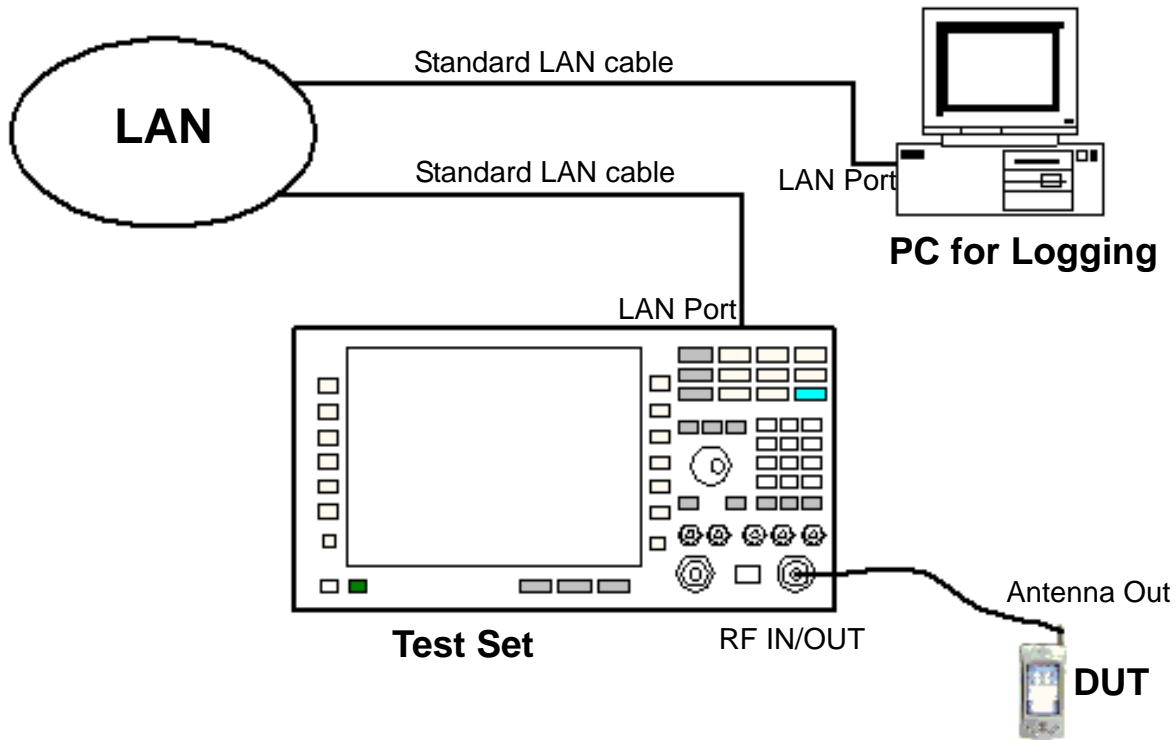
This procedure assumes that your PC is connected to a LAN. Connect one of the test set's LAN ports to your network using a standard LAN cable. See [Figure 5. on page 16](#).

---

**NOTE** There are two LAN ports on the Test Set to provide both front and rear panel data connections. If you are connecting to the test set's front panel DATA port, please verify that the rear panel LAN PORT and ETHERNET TO FRONT PANEL ports are connected by a jumper cable (shipped with the test set).

---

**Figure 5. LAN Connection Diagram**





## LAN Connection Setup

Before a connection between the test set and a PC can be established through the LAN, the test set and PC must be assigned valid IP addresses. IP addresses are typically obtained through a network administrator, and in the case of the PC are typically entered into the PC automatically through a network protocol called DHCP.

You can find out your PC's IP address by entering `ipconfig` on the MS DOS command line, then pressing the Enter key. The displayed results vary depending upon your PC's configuration (see the example in the following figure).

If multiple Ethernet adapters are displayed, locate your active Ethernet LAN adapter by its title and record the Ethernet adapter IP Address (this is the IP address assigned to your PC)

```

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : 
    IP Address. . . . . : 146.208.241.26
    Subnet Mask . . . . . : 255.255.254.0
    Default Gateway . . . . . : 146.208.240.1

C:\>_

```

If the PC is not currently configured for LAN connectivity, contact your system administrator to have an IP address assigned to the PC.

The test set must also be assigned an IP address with a unique host number. Since the test set does not recognize DHCP, it must have its assigned IP address entered manually.

If it provides additional convenience, record your test set and PC IP address information in [Table 3. on page 17](#)

**Table 3. LAN Connection IP Address Settings**

	IP Address	Subnet Mask
Test Set		
PC		

### STEP 1. Enter the Test Set's IP Address .

1. Turn on the test set. If the test set is already on, we recommend you reset the test set by pressing the blue **SHIFT** key and then the green **Preset** key.
2. Press the **SYSTEM CONFIG** key.

## Connecting the PC to the Test Set

3. Press the **Instrument Setup (F1)** key, set test set's LAN IP Address, Subnet Mask, and Default Gateway using the knob and DATA ENTRY Keys.
4. Press the **Close Menu (F6)** key.
5. Verify that the desired lab application is active. If not, switch applications.

### STEP 2. Attempt to make a connection between the PC and the test set .

1. Double-click the WPA icon. The WPA main menu will be displayed

**Figure 6. WPA Main Menu**



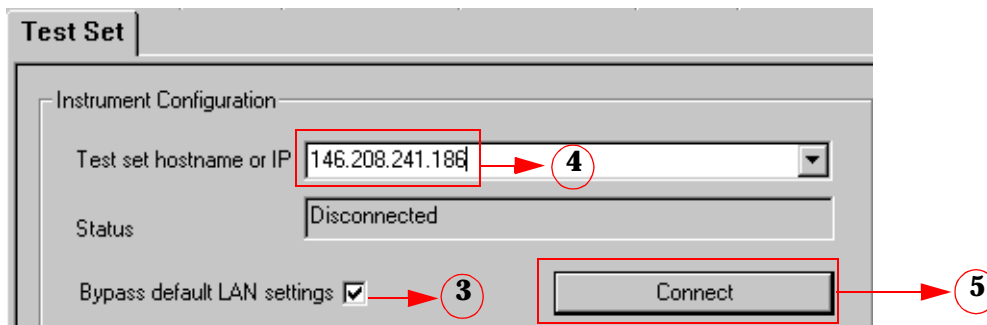
2. Click the Real Time button.

---

**NOTE** When Real Time is selected, WPA will automatically display the Configuration window if it detects that there has not been a test set IP address entered.

If a test set IP address has been entered in a prior session, WPA will automatically attempt to connect with the test set. If it is successful, WPA will display the Traffic Overview and you are ready to begin logging. If the connection attempt is unsuccessful, the Configuration window will be displayed with an error message.

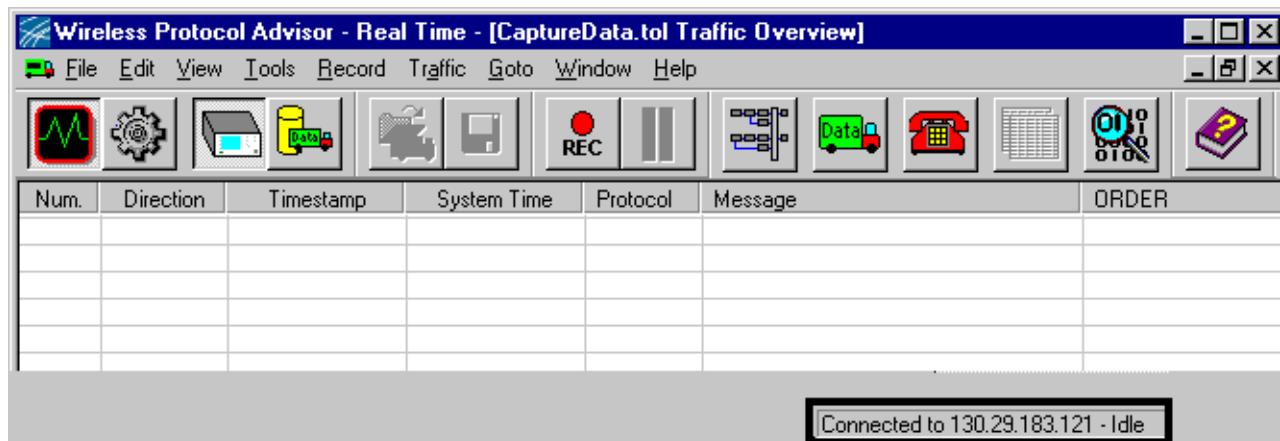
---

**Figure 7. Configuration Window**

3. Select the Bypass default LAN settings box.
4. Enter the test set's IP address.
5. Click on the Connect button.

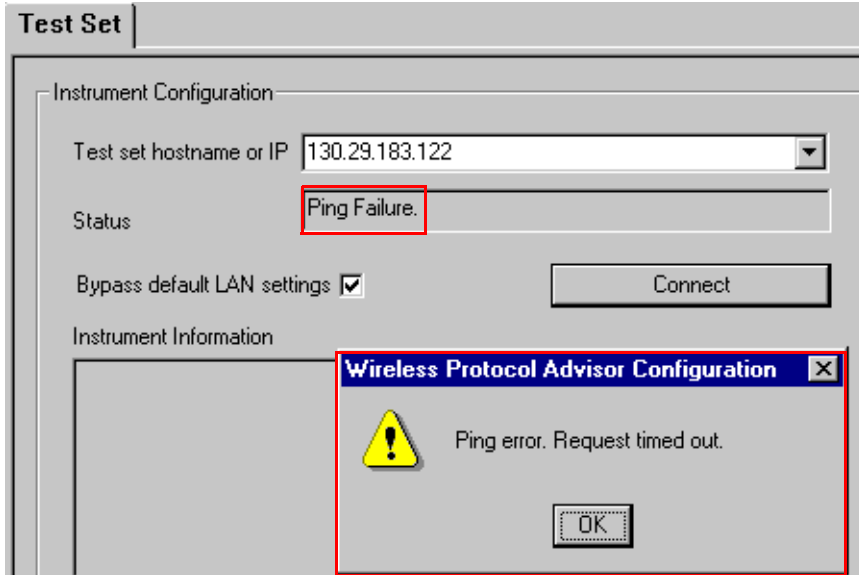
The WPA will attempt to establish a network connection with the test set. If successful, the Traffic Overview window will be displayed:

When a connection is successful, the WPA Traffic Overview will be displayed with the status message "Connected to <host> - Idle". The test set will display "Logging:Idle" on the front panel display.



If the connection is not successful, the Instrument Configuration window will display an error message:

## Connecting the PC to the Test Set



### Troubleshooting:

- Check the IP addresses on both the PC and the test set's System Config screen
- Make sure the check box labeled Bypass default LAN settings is checked.

---

## Protocol Analysis

This section describes the basic features in WPA, the Agilent Technologies E6584A Wireless Protocol Advisor. The examples shown in this section pertain to the cdma2000 application but the concepts presented here can easily be applied to other applications.

### Introduction to WPA

[“Fundamental Operating Modes” on page 21](#)

[“Capturing and Stopping Protocol Message Logs” on page 21](#)

[“The Decode View” on page 24](#)

### Fundamental Operating Modes

The WPA software runs in one of two fundamental operating modes:

- Real Time Operating Mode




In real time mode, logging data is acquired by the PC running WPA software as a call is in progress. Logging data is transferred between the test set and the PC by way of a TCP/IP connection.

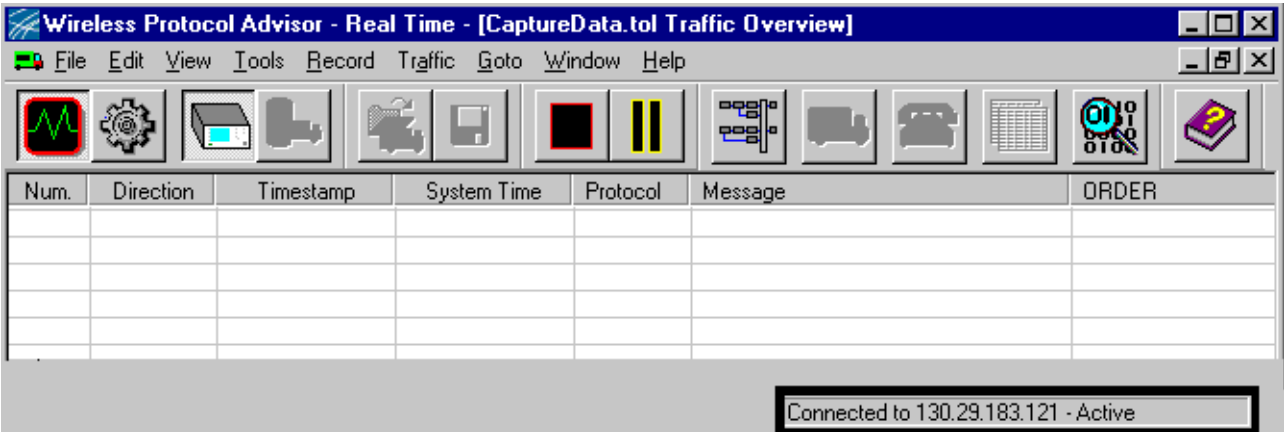
- Post Capture Operating Mode



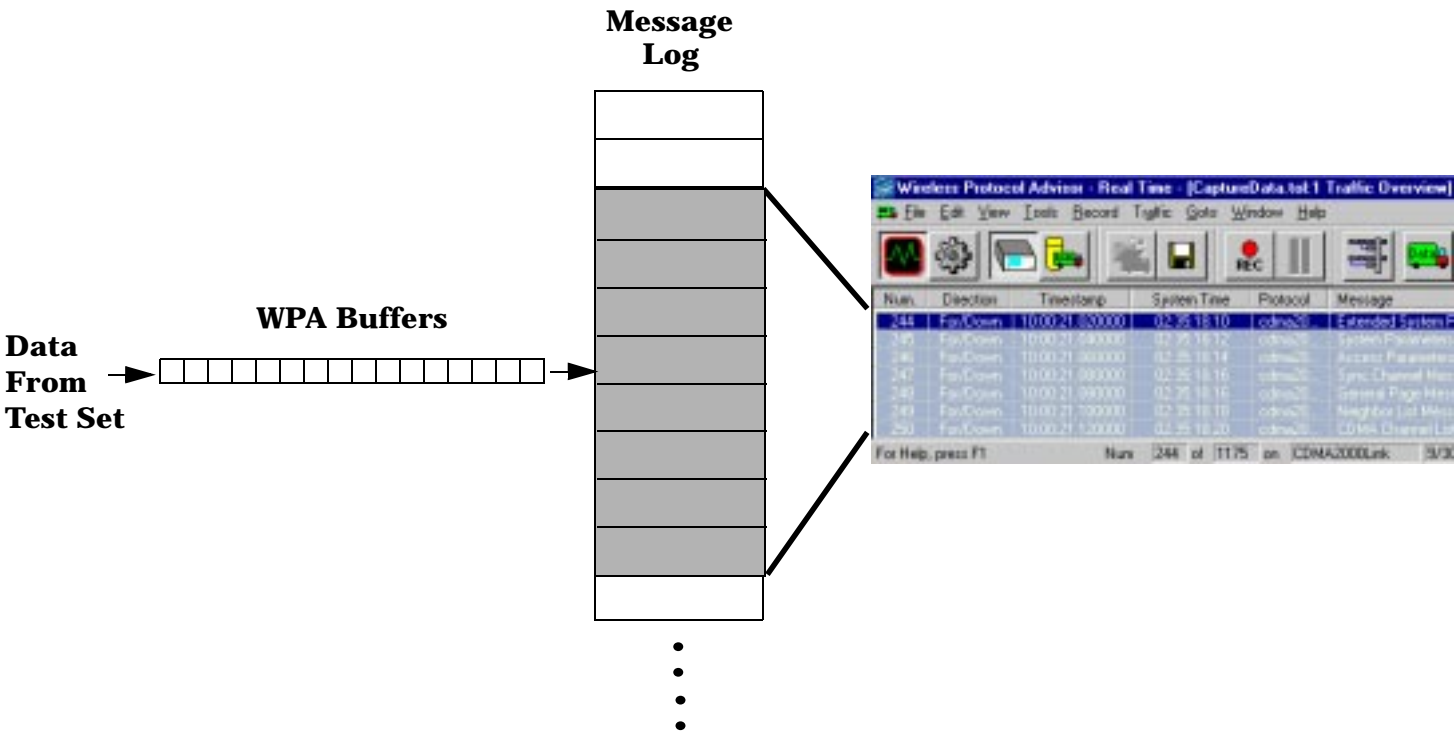
In post capture mode, previously logged data can be analyzed by a PC that without a connection to the test set.

### Capturing and Stopping Protocol Message Logs

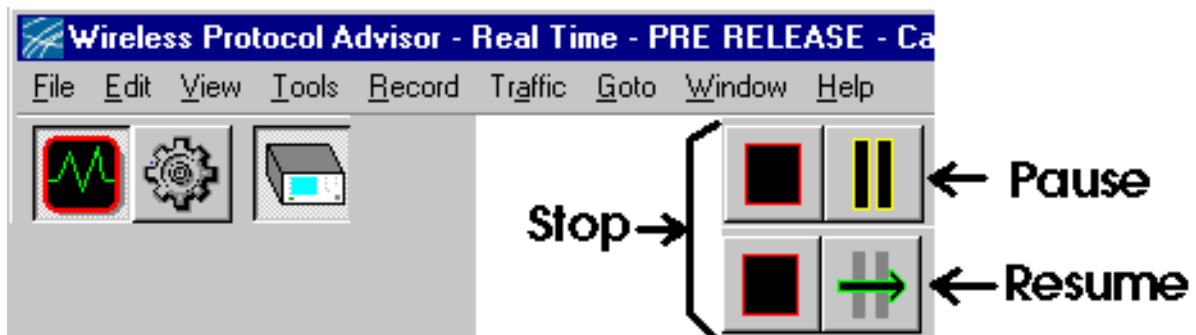
In Real Time mode, once the WPA software displays the Traffic Overview window it is possible to begin logging messages. Click on the REC(ord) button  and WPA will display “Active” in the status window.



At this point the WPA begins accepting protocol data from the test set. Protocol data is stored in buffers as WPA logs messages and enters the results into a file. The Traffic Overview provides a “window” into the log file.



Press the Stop or the Pause button to stop messages from being logged.



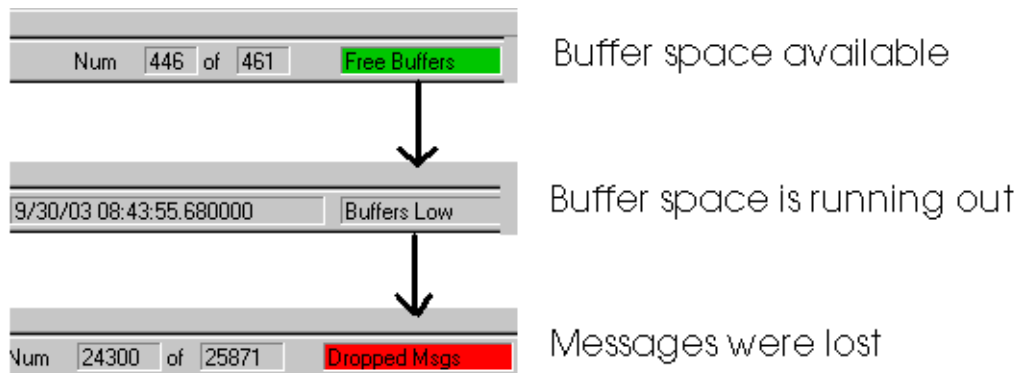
The difference between Stop and Pause is:

- Clicking the Stop button stops data transfer over the LAN connection. As soon as the WPA buffers are cleared, no further logging is performed until another session is started.
- Clicking the Pause button allows WPA to continue buffering messages while you scroll through the Traffic Overview window. As soon as you press Resume, buffered messages will be added to the message log.


---

**NOTE** There are limits to the number of messages buffered by WPA. When paused, the buffers can fill up and eventually lose messages, especially if filter settings are allowing a large number of messages to be sent from the test set to WPA. An indicator is provided to warn when this condition is developing, and to alert the user when messages were dropped during a pause.


---



Pressing the Resume button after a pause will cause WPA to transfer the backlog of messages from buffer space to the log as it continues to buffer new data. The status window will display “Num <message currently highlighted in Traffic Overview> of <total number of messages in the message log>”. You will notice that messages scroll more quickly down the display until the message highlighted in the Traffic Overview window is closely synchronized with the total number of messages in the message log.

Similarly, pressing the Stop button after a pause will cause WPA to transfer messages from buffer space to the log. During this time, the Stop button will display an hourglass icon . If you want to stop the logging session immediately, click on the hourglass icon.

The Decode View

Pressing the Decode View icon  will display details of the message currently highlighted in the Traffic Overview.

The E5515C test set includes a proprietary protocol layer known as the MTAL (Mobile Test Adaptation Layer). When messages are displayed, the MTAL layer provides additional information about each message that is very useful for troubleshooting. The information provided by MTAL is color coded and appears as the first set of octets in the decode view

octet	MSB	Bin	LSB	Hex	Description
Message 4 of 14 on CDMA2000Link (Test Set (Test Set to DUT))					
1	00000100			04	CDMA System Time=Apr 12 1992 20:11:17.70
2	10000001			81	
3	11000111			c7	
4	11110010			f2	
5	11011101			dd	
6	00000000			00	Protocol=cdma2000
	00000000				MTAL Event Type=PDU
7	00000011			03	Channel Type=f-dsch
8	00001000			08	MSG_LENGTH=8(dec)
9	00000001			01	f-dsch MSG_TYPE=Order Message
10	11100010			e2	ACK_SEQ=7
	11100010				MSG_SEQ=0
	11100010				ACK_REQ=Acknowledgment required
	11100010				ENCRYPTION=0
11	00000000			00	
	00000000				USE_TIME=No explicit action time is specified
	00000000				ACTION_TIME=0(dec)
12	01000000			40	f-csch/f-dsch ORDER=Base Station Acknowledgment Order
	01000000				ADD_RECORD_LEN=0
13	00000000			00	
	00000000				PADDING=0
14	00110010			32	CRC=32b2(hex)
15	10110010			b2	

The MTAL layer provides:

- System Time.
- Protocol stack description.
- Event type (PDU, SDU, etc).



## WPA Filters

[“WPA Filter Stages” on page 25](#)

[“The Test Set Filter” on page 26](#)

[“Test Set Filter Setup” on page 26](#)

[“The Log Filter” on page 29](#)

[“Log Filter Initialization” on page 30](#)

[“Setting Up a Message Match” on page 31](#)

[“Setting Up a Time Filter” on page 34](#)

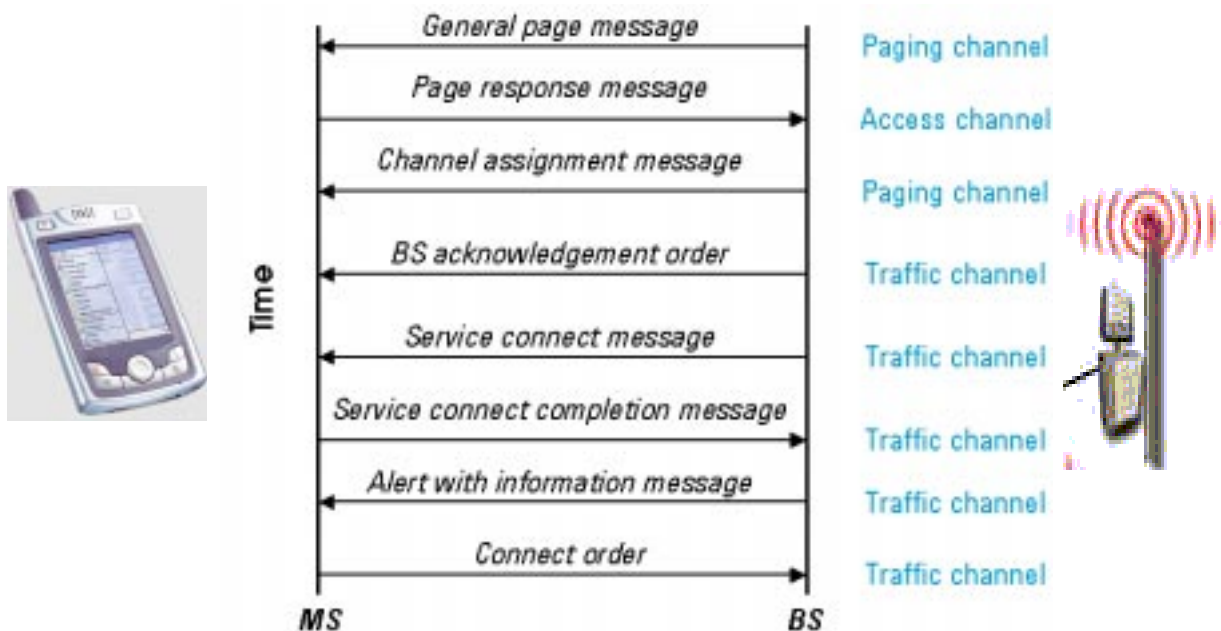
[“Setting Up a Text Search Filter” on page 35](#)

[“The View Filter” on page 37](#)

Call processing generates many messages at each layer in a given protocol stack. WPA is designed to help you troubleshoot protocol problems by focusing analysis on specific events, message types, or message fields. Filtering limits the scope of the traffic overview, allowing you to more quickly recognize problems.

Some examples based on the following ladder diagram will help illustrate the use of filters.

A ladder diagram shows the sequence of messages and the direction of message flow during call processing. The following diagram is from an Annex in the cdma2000 standard. It shows the messages that flow between mobile station and base station during a base station originated voice call.



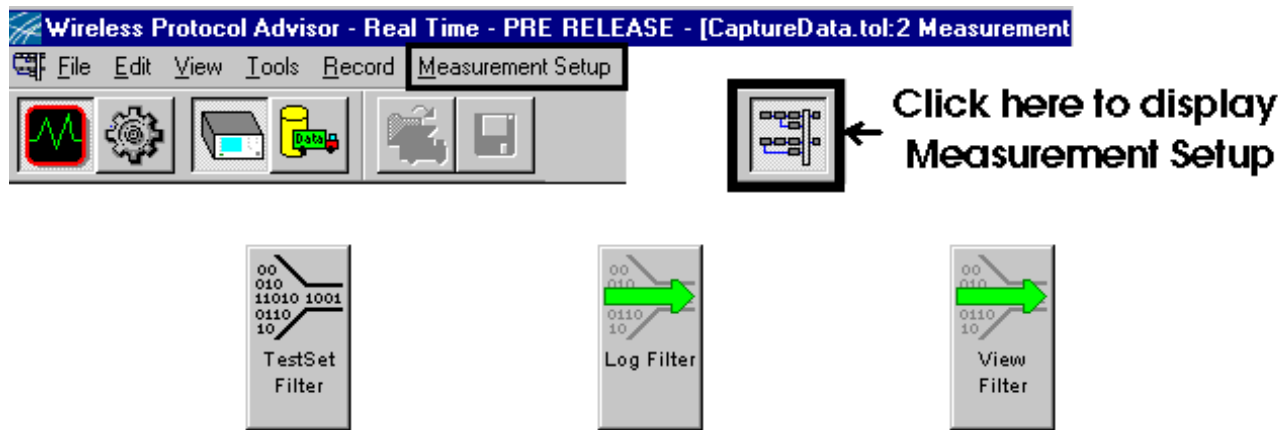
## WPA Filter Stages

There are three stages of filtering that you can use to determine which messages are decoded and displayed:

### 1. The Test Set Filter

- 2. The Log Filter
- 3. The View Filter


When setting up filters, it is recommended that you begin by considering which messages to include with the first stage of filtering, the Test Set Filter. Single clicking on the Measurement Setup icon (it resembles a flow diagram) brings up the Measurement Setup view.



**The Test Set Filter**

During a logging session, the test set will send raw message data to the PC. Test set filter settings determine how much logging data from the test set will transfer to WPA Buffers (see [“Capturing and Stopping Protocol Message Logs” on page 21](#)) when call processing events occur. Filtering at the test set filter reduces LAN traffic and reduces processing overhead for both the test set and PC.

**Example 1. Test Set Filter Setup**

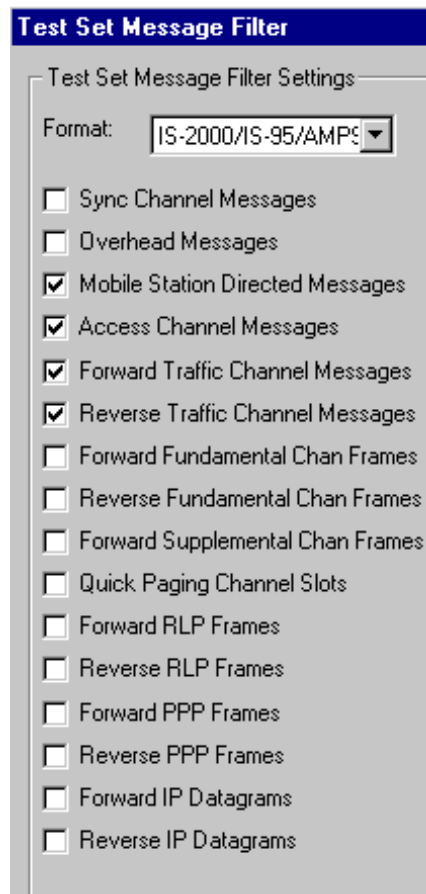
- 1. From the Measurement Setup screen, double click on the Test Set Filter icon  .

---

**NOTE** To bring up any of the filter menus, the status of WPA logging must be Idle. If the status is Active, click on the Stop button to return the WPA logging status to Idle.


---

2. Click on all of the four check boxes shown below to select test set filter settings, then click on OK.



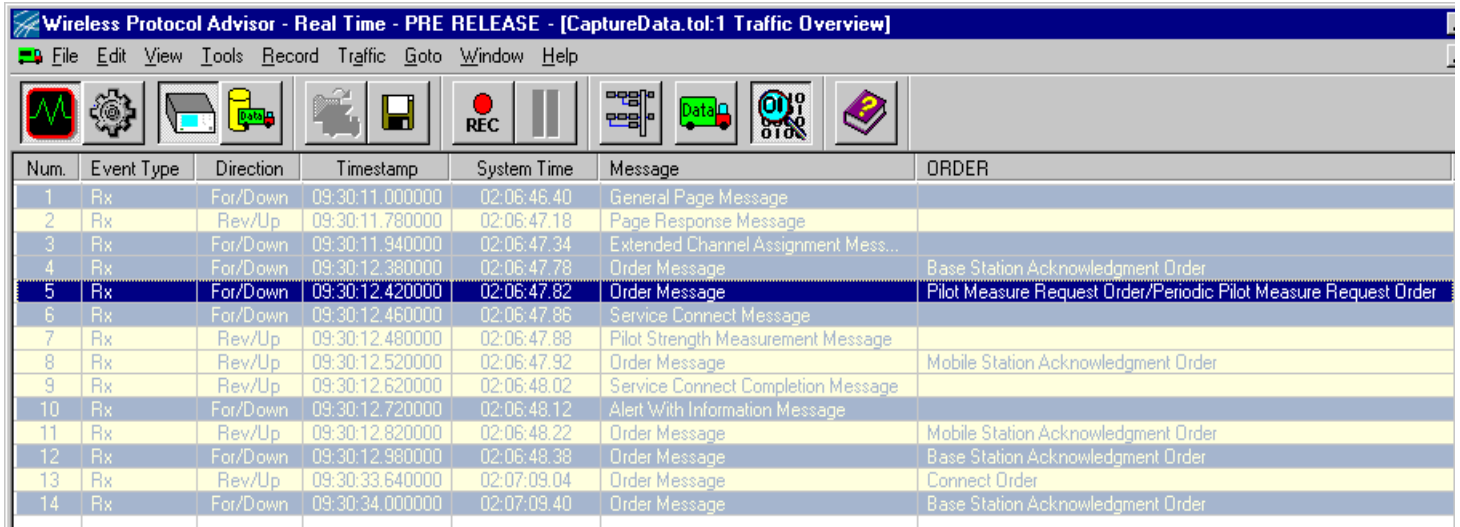
Placing a check mark in these selections configures the test set to send only messages that are included in the cdma2000 voice call ladder diagram shown above.

The list of selections available in the Test Set Message Filter menu vary depending on the lab application and firmware revision currently running on the test set.

3. Click again on the Measurement Setup icon  to return to the traffic overview

After connecting a mobile station to the test set and making an SO3 voice call the Traffic Overview will display the following messages:

## Protocol Analysis




The screenshot shows the 'Wireless Protocol Advisor - Real Time - PRE RELEASE - [CaptureData.tol:1 Traffic Overview]' window. It features a menu bar (File, Edit, View, Tools, Record, Traffic, Goto, Window, Help) and a toolbar with icons for signal analysis, settings, capture, and help. Below the toolbar is a table with 14 rows of protocol data. The table columns are: Num., Event Type, Direction, Timestamp, System Time, Message, and ORDER. The messages include General Page Message, Page Response Message, Extended Channel Assignment Message, Order Message, Service Connect Message, Pilot Strength Measurement Message, and various Acknowledgment and Completion messages.

Num.	Event Type	Direction	Timestamp	System Time	Message	ORDER
1	Rx	For/Down	09:30:11.000000	02:06:46.40	General Page Message	
2	Rx	Rev/Up	09:30:11.780000	02:06:47.18	Page Response Message	
3	Rx	For/Down	09:30:11.940000	02:06:47.34	Extended Channel Assignment Mess...	
4	Rx	For/Down	09:30:12.380000	02:06:47.78	Order Message	Base Station Acknowledgment Order
5	Rx	For/Down	09:30:12.420000	02:06:47.82	Order Message	Pilot Measure Request Order/Periodic Pilot Measure Request Order
6	Rx	For/Down	09:30:12.460000	02:06:47.86	Service Connect Message	
7	Rx	Rev/Up	09:30:12.480000	02:06:47.88	Pilot Strength Measurement Message	
8	Rx	Rev/Up	09:30:12.520000	02:06:47.92	Order Message	Mobile Station Acknowledgment Order
9	Rx	Rev/Up	09:30:12.620000	02:06:48.02	Service Connect Completion Message	
10	Rx	For/Down	09:30:12.720000	02:06:48.12	Alert With Information Message	
11	Rx	Rev/Up	09:30:12.820000	02:06:48.22	Order Message	Mobile Station Acknowledgment Order
12	Rx	For/Down	09:30:12.980000	02:06:48.38	Order Message	Base Station Acknowledgment Order
13	Rx	Rev/Up	09:30:33.640000	02:07:09.04	Order Message	Connect Order
14	Rx	For/Down	09:30:34.000000	02:07:09.40	Order Message	Base Station Acknowledgment Order

If you compare the ladder diagram with this message log you will see that a Pilot Measurement Request Order was sent from the base station and the mobile station responded with a Pilot Strength Measurement Message. These messages are not part of the call flow sequence outlined in the ladder diagram. They occurred because the test set is programmed to send the Pilot Measurement Request Order every time a call is made. This is the way the test set obtains the data it needs to enter pilot channel levels into the Mobile Station Reported Pilot Level Information window located on the Soft Handoff Information screen.

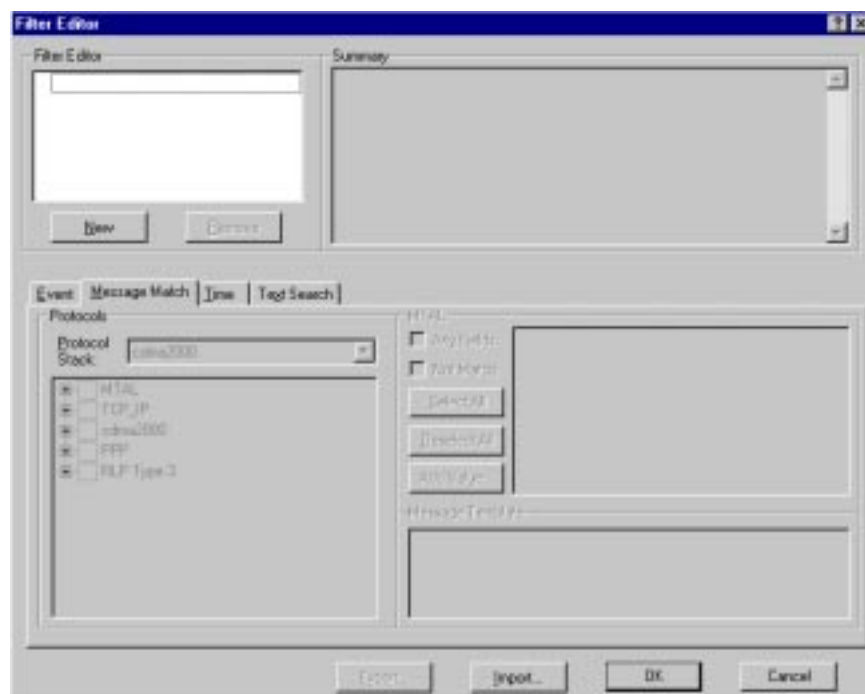
## The Log Filter

The Log Filter determines the logging data that goes into the WPA Buffers (see [“Capturing and Stopping Protocol Message Logs” on page 21](#)).

Click on the Measurement Setup icon  to return to the Measurement Setup view, and double click on the

Log Filter icon  .

The screen shown below will be displayed:



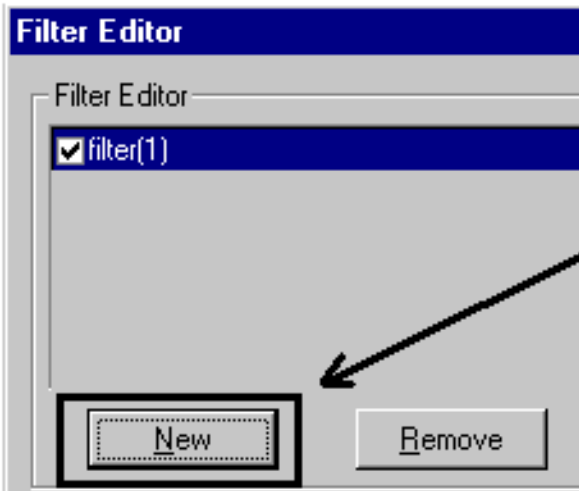
Initially, the Filter Editor will not have any filter controls enabled. This is because no filters have been selected yet. To enable filter controls you must either select:

- Import (to select a filter), or
- New (to create a new filter)

When a filter (or filters) have been created, they can be Exported to a file folder. WPA sets up a default folder in the following path:

“Program Files\Wireless Protocol Advisor\User Files\Triggers and Filters”

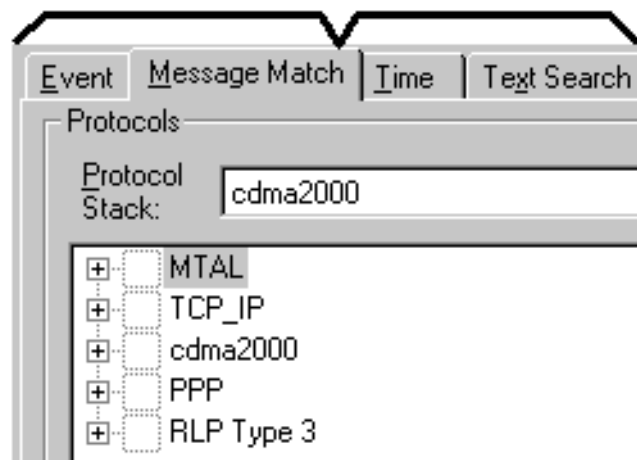
Selecting New will create a filter, named “filter(1)” by default. At this point, all controls for assigning settings to filters become enabled and you can begin defining the filter settings for filter(1).



Select New to create a new filter and enable filter settings

Filter settings are located under tabs in the lower portion of the Filter Editor window.

Filter settings are grouped under these tabs



Each tab provides a different type of filtering:

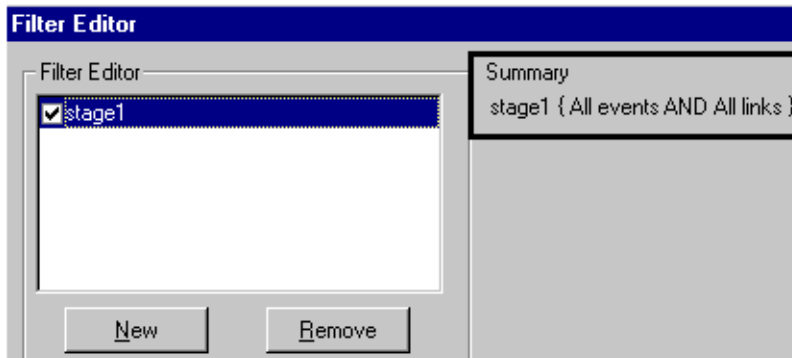
- Event (reserved for future use)
- Message Match (specifies protocol messages)
- Time (filters on timestamps)
- Text Search (filters on text strings)

### Example 2. Log Filter Initialization

1. From the Measurement Setup screen, double click on the Log Filter icon.

- Click on the New button.

Double-click on the name “filter(1)” and change the name to “stage1” so the window appears like this:



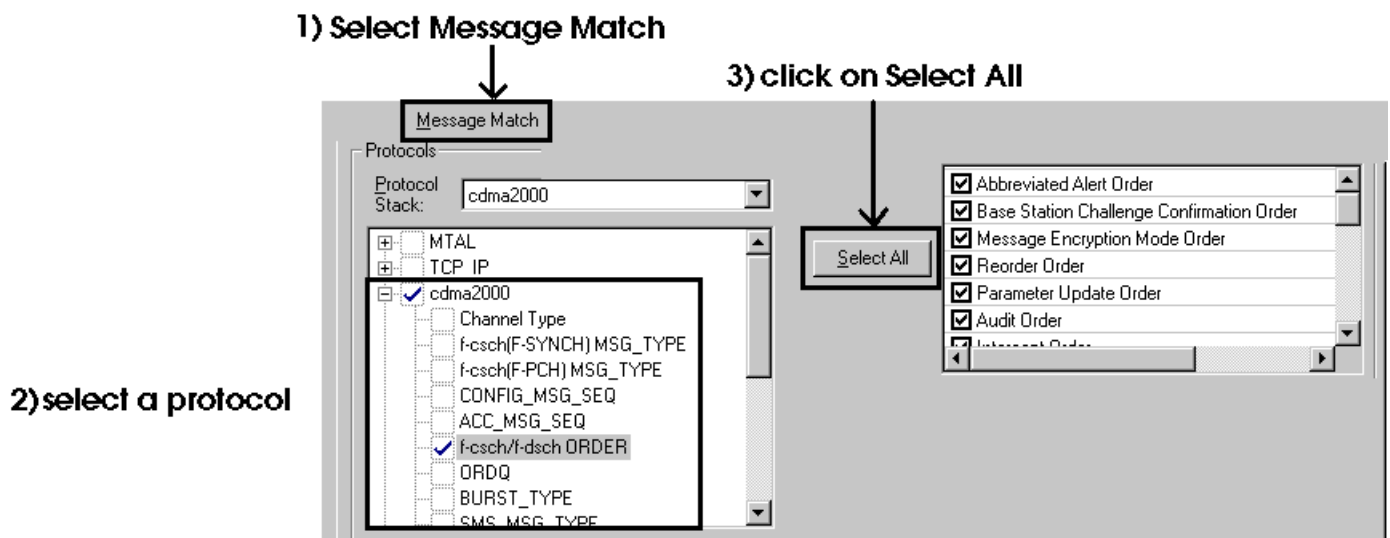
**Default filter summary  
for stage1**

Note that the default filter file setting for “stage1” in the Summary window includes {All events AND All links}.

### Example 3. Setting Up a Message Match

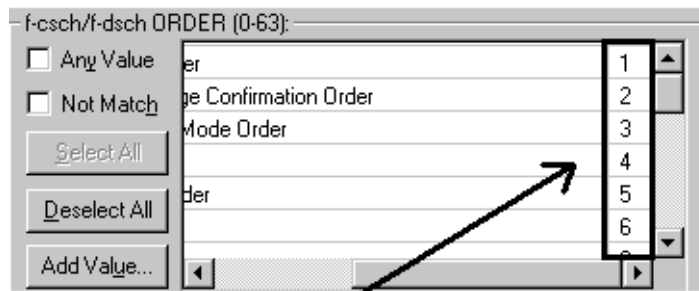
If you want to log ORDER messages only, you would perform the following steps.

- Click on the Message Match tab.
- Double-click on cdma2000 in the Protocol directory (this will expand the cdma2000 choices) and click on the “f-csch/f-dsch ORDER” box.
- Click on the button labeled Select All. This will place check marks next to all f-csch/f-dsch ORDER messages. It will also place check marks in the cdma2000 and f-csch/f-dsch ORDER boxes.



If you scroll to the right of the messages next to the Select All button, you will see values assigned to each

message. These are defined by the cdma2000 standard.



**Scroll to display ORDER codes**

By clicking on the Select All button, you instruct WPA to log only the f-csch/f-dsch ORDER messages identified by names and numbers.

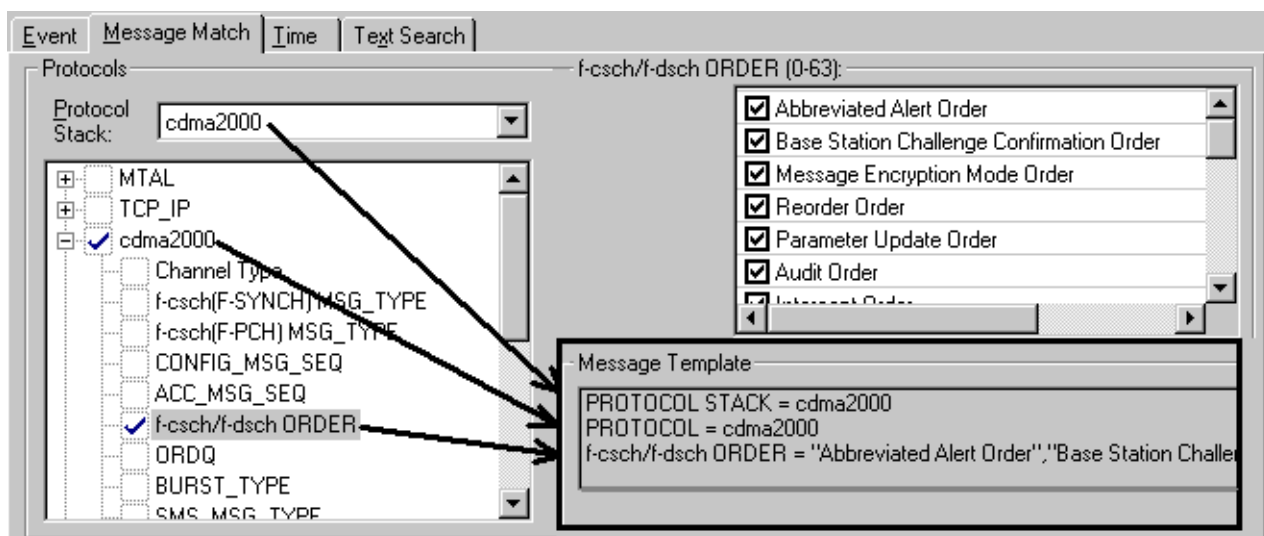
If you want to log all messages that WPA determined to be f-csch/f-dsch ORDER messages, including those with ORDER codes that do not match any in the window, you can place a check mark in the Any Value check box. Checking this box will cause WPA to log f-csch/f-dsch ORDER messages even if the message field does not match any numbers in this list.

If you want WPA to log only specific f-csch/f-dsch ORDER messages that are identified by numbers in this list, choose Deselect All and place a check mark in the boxes next to the messages you want included.

If you want WPA to log only specific f-csch/f-dsch ORDER messages that are not currently identified by numbers in this list, you can click on the Add Value button. WPA will prompt you for a number, check to see if it is within the allowable range, and add a check box so you can select and deselect it.

If you want WPA to exclude selected messages you can click on the Not Match button. When the Not Match box has a check mark, any messages that have check marks next to them will not be logged.

The Message Template window shown in the lower portion of the filter editor describes the current log filter settings.



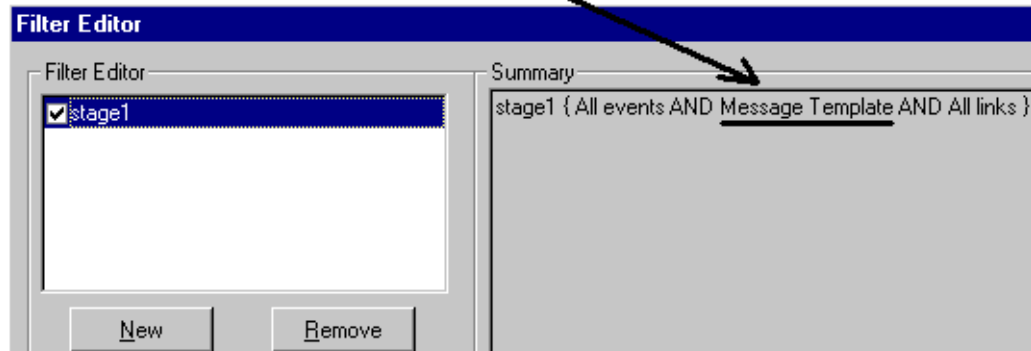
In this example the interpretation of the Message Template would be:



- Look for messages in PROTOCOL STACK = cdma2000
- Out of these messages, look for messages in the cdma2000 network layer.
- Out of the remaining messages, look for the selected f-csch/f-dsch ORDER messages: “Abbreviated Alert Order”, Base Station Challenge Order,...etc.

Note that the Message Template is now included in the Summary window

### Message Template has been added to Summary



If the voice call represented by the ladder diagram were made again with this setting, WPA would filter out all but the forward dedicated signaling channel ORDER messages:

Wireless Protocol Advisor - Real Time - PRE RELEASE - [CaptureData.tol:1 Traffic Overview]						
File Edit View Tools Record Traffic Goto Window Help						
Num.	Direction	Timestamp	Protocol	Message	ORDER	Channel Type
1	For/Down	14:09:27.300000	cdma20...	Order Message	Base Station Acknowledgment Order	f-dsch
2	For/Down	14:09:27.340000	cdma20...	Order Message	Pilot Measure Request Order/Periodic Pilot Measure Request Order	f-dsch
3	For/Down	14:09:27.900000	cdma20...	Order Message	Base Station Acknowledgment Order	f-dsch
4	For/Down	14:09:32.740000	cdma20...	Order Message	Base Station Acknowledgment Order	f-dsch

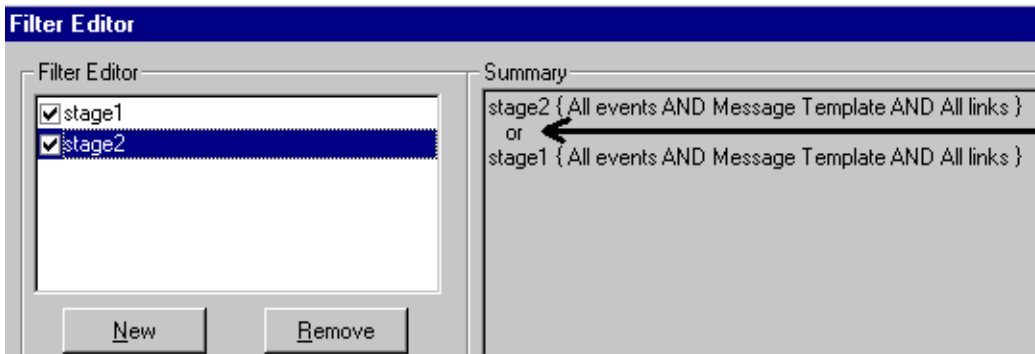
4. Click on the New button again.

The filter editor will display another filter. Name it “stage2”.

Each time you click on New, another filter is added with a corresponding check box.

5. For the stage2 filter, select all order messages associated with r-csch/r-dsch ORDER. (Repeat steps 2 and 3, selecting r-csch/r-dsch ORDER messages).

When new filters are added, WPA OR's any newly-included messages to those already defined by existing filters. The Summary window to the right will automatically update the description of the currently selected filters and which types of filtering are active.



Summary showing  
stage1 OR'd with  
stage2

If the voice call represented by the ladder diagram were made again with this setting, WPA would filter out all but the forward OR reverse dedicated signaling channel ORDER messages:

Wireless Protocol Advisor - Real Time - PRE RELEASE - [CaptureData.tol:1 Traffic Overview]						
File Edit View Tools Record Traffic Goto Window Help						
Num.	Direction	Timestamp	Protocol	Message	ORDER	Channel Type
1	For/Down	14:04:55.300000	cdma20...	Order Message	Base Station Acknowledgment Order	f-dsch
2	For/Down	14:04:55.340000	cdma20...	Order Message	Pilot Measure Request Order/Periodic Pilot Measure Request Order	f-dsch
3	Rev/Up	14:04:55.440000	cdma20...	Order Message	Mobile Station Acknowledgment Order	r-dsch
4	Rev/Up	14:04:55.740000	cdma20...	Order Message	Mobile Station Acknowledgment Order	r-dsch
5	For/Down	14:04:55.900000	cdma20...	Order Message	Base Station Acknowledgment Order	f-dsch
6	Rev/Up	14:04:59.900000	cdma20...	Order Message	Connect Order	r-dsch
7	For/Down	14:05:00.260000	cdma20...	Order Message	Base Station Acknowledgment Order	f-dsch

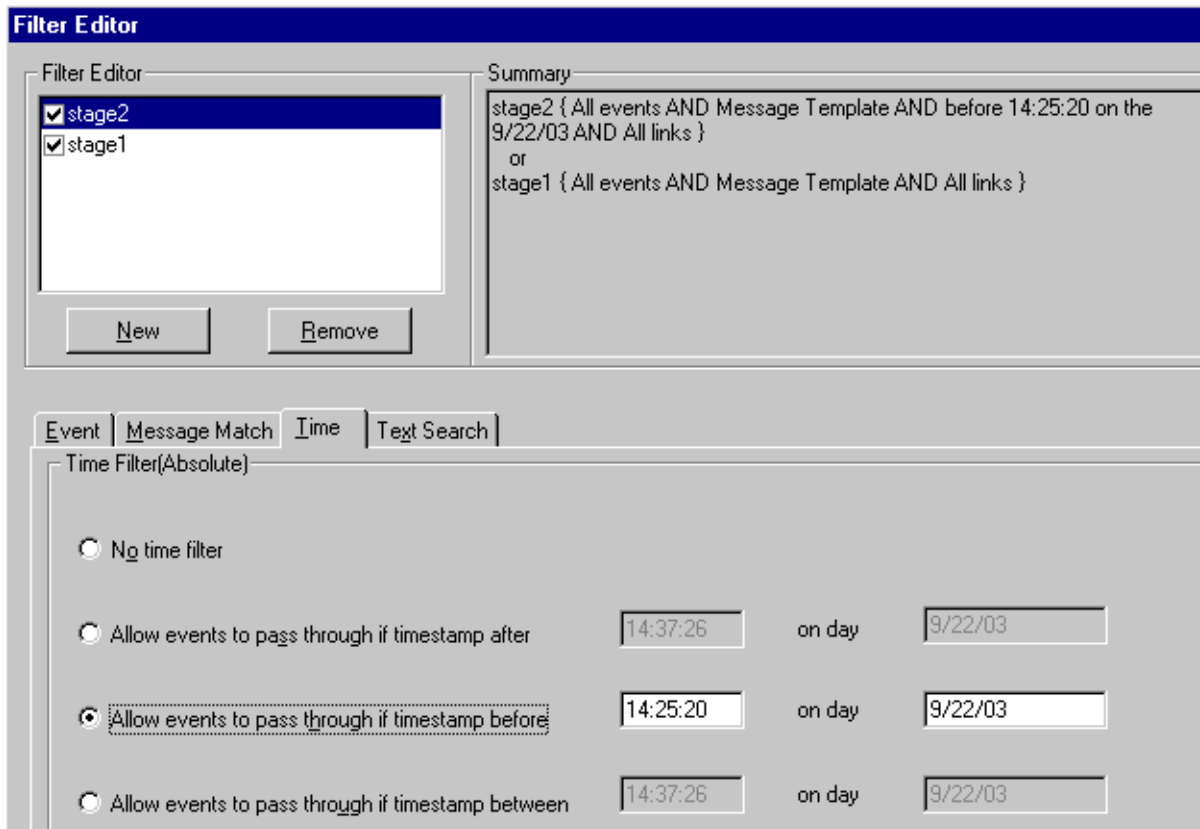
- From the Filter Editor, click on **Export** to save the filter file. The save utility will ask you if you want all of the filters (i.e. stage1, stage2). This provides you a chance to specify only those filters that you will consider using when the filter file is **Imported** later. Keep in mind that you can always check or uncheck filters in the filter editor.

The default directory that WPA uses is called Triggers and Filters. Name the file "order\_msg1".

#### Example 4. Setting Up a Time Filter

The time filter allows time limits to be applied to message logging. Based on the PC clock, you can set up WPA to display only those messages which occurred before, after, or within a time specified.

- Click on the **Time** tab.
- Highlight the stage2 filter (do not uncheck the box).
- Click on the third radial button in the list, "Allow events to pass through if timestamped before"
- Enter a time value that is a minute or two later than the time currently displayed.



By highlighting “stage2”, you were specifying that time limits will apply to the reverse dedicated signaling channel messages.

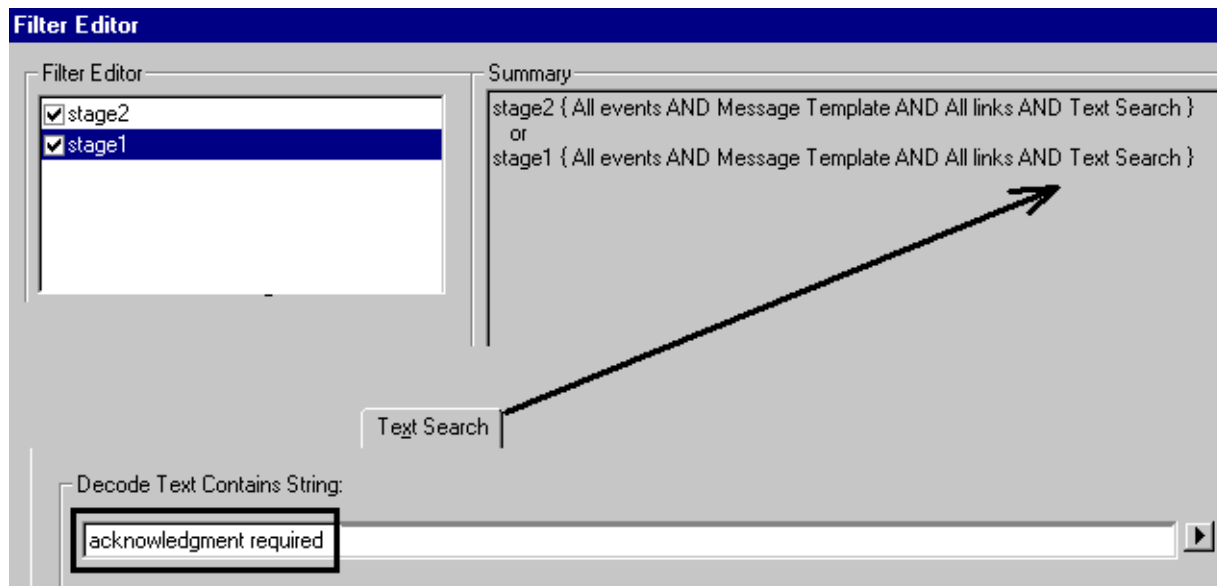
If the voice call shown in the ladder diagram is made before the time you entered arrives, all ORDER messages will display.

If you wait a minute or two and make the call again, only the stage1 filter messages (the forward dedicated signaling channel ORDER messages), will be displayed.

### Example 5. Setting Up a Text Search Filter

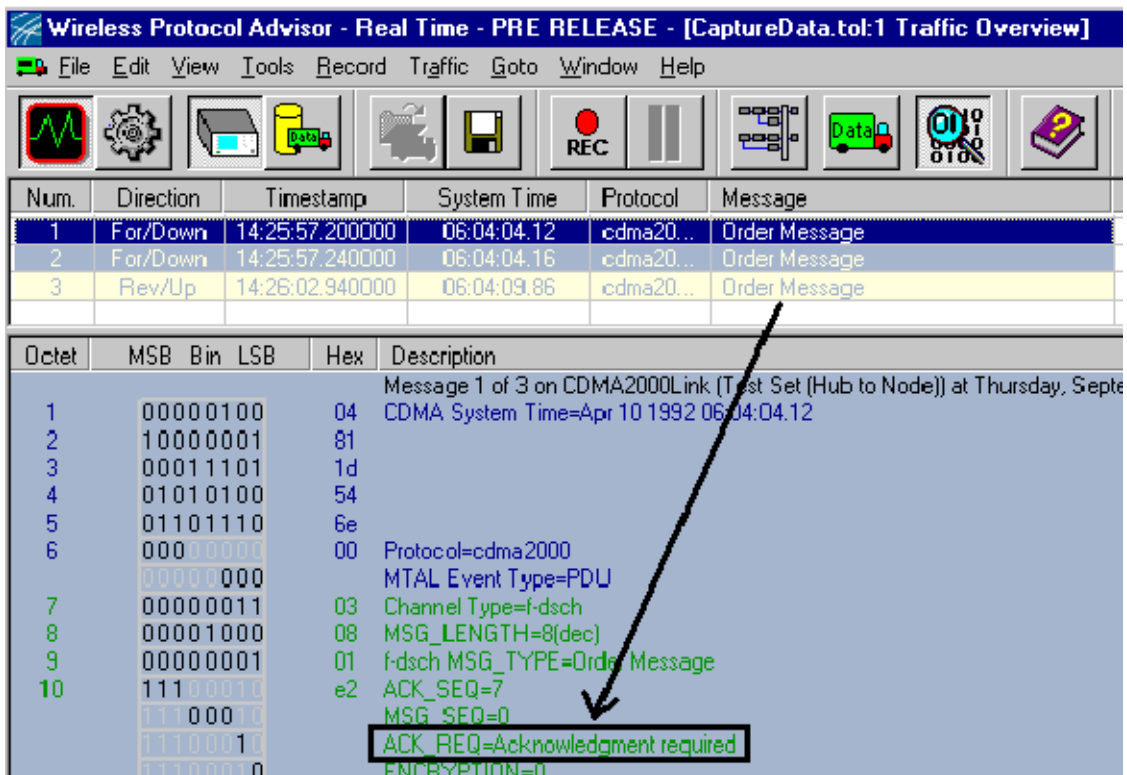
The WPA provides a text search feature for finding text strings within decoded protocol messages.

1. Click on the **Text Search** tab.
2. Click on the “stage1” filter.
3. Enter the string “acknowledgment required” (no quotes necessary).
4. Click on the “stage2” filter.
5. Enter the string “acknowledgment required” (the same as the stage1 text search string).



**Messages that contain "acknowledgment required" will be logged**

If the voice call shown in the ladder diagram is made with these settings, only the ORDER messages requiring acknowledgement will be logged.

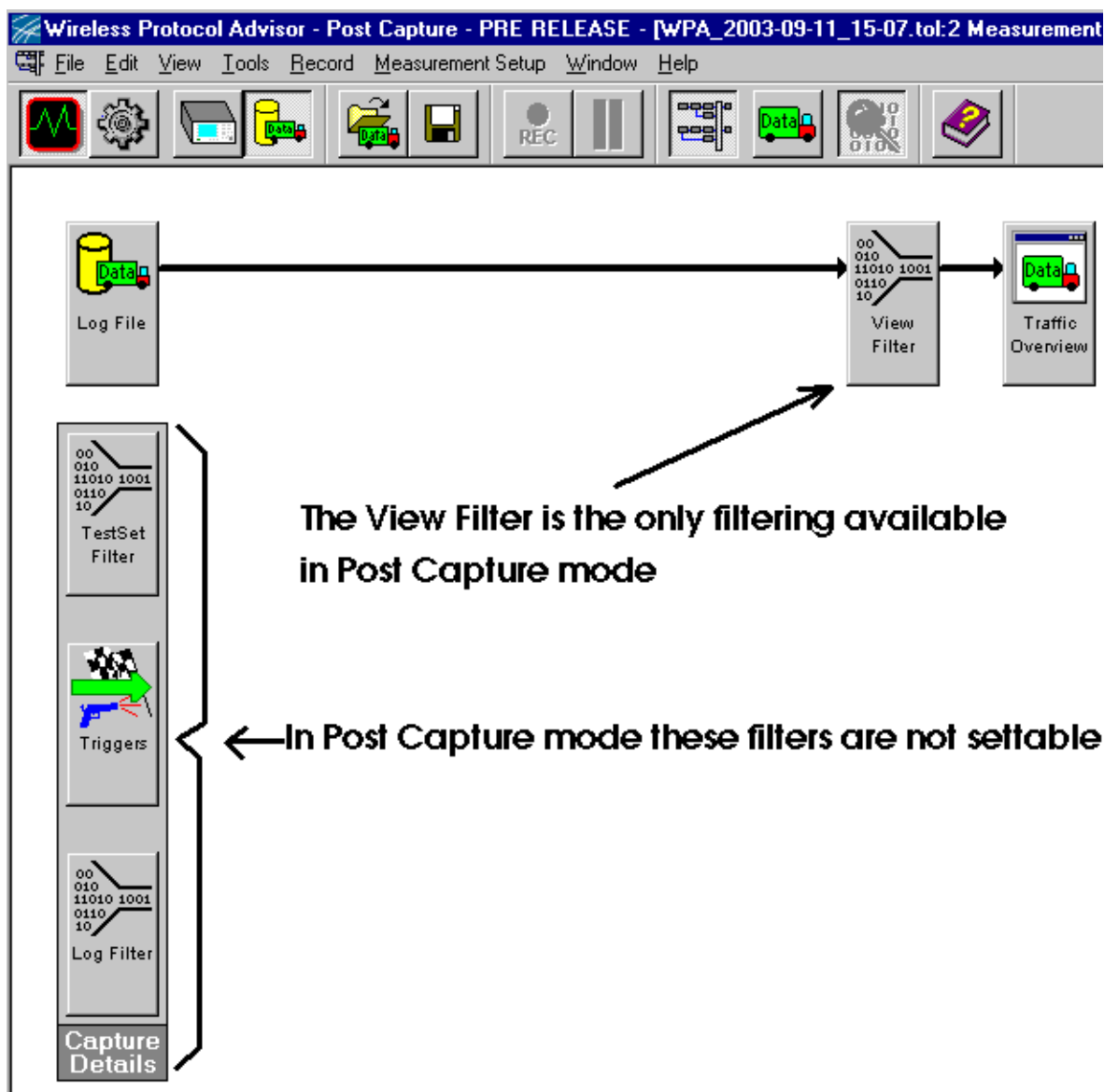


**NOTE** Including a Text Search as part of a logging filter or trigger setup may slow protocol logging significantly. (Performance will vary depending on the PC system WPA is running on.). Refer to the WPA on line help for a detailed description of Text Search and how to avoid performance problems.

## The View Filter

The View Filter determines what is visible in the Message Log (see [“Capturing and Stopping Protocol Message Logs” on page 21](#)). Its controls are almost identical to the Log Filter. The significant differences are:

- The View Filter does not affect the amount of LAN traffic resulting from message logging.
- The View Filter settings can be changed in both post capture mode and real time mode.




## WPA Triggers

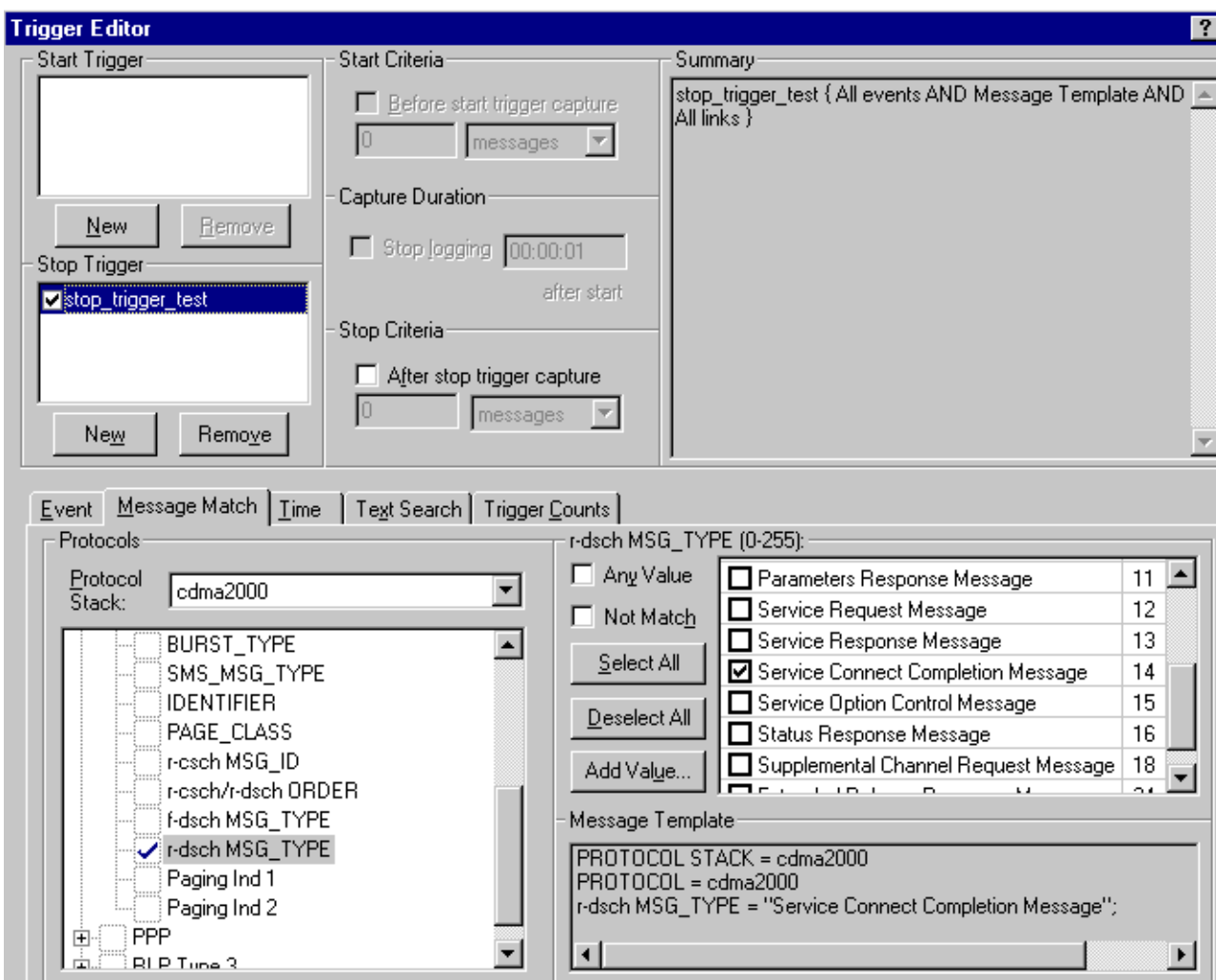
[“Setting up a Start Trigger On a Message Match” on page 40](#)

[“Setting up a Pre-trigger on a Message Match” on page 42](#)

Setting up start and stop triggers provides additional control over the messages that are decoded and displayed by the WPA. Triggering is based on the same types of protocol events that can be selected for filtering.

### Example 6. Setting up a Stop Trigger On a Message Match

1. From the Measurement Setup screen, double click on the Triggers  icon.
2. Click on the New button in the Stop Trigger window. Name the Trigger “stop\_trigger\_test”.
3. Select the Message Match tab.
4. Double click on cdma2000 in the Protocol directory. Scroll down the list of message types and select “r-dsch MSG\_TYPE”.
5. In the message window place a check mark in the Service Connect Completion Message box.



If the voice call represented by the ladder diagram were made now, the logging would end with a Stop Trigger event immediately following the Service Connect Completion Message.

---


**NOTE** The traffic overview window was modified for this example to include a column labeled Event Type. This was added by right clicking in the traffic overview window and placing a check mark in the Event Type check box.

---

Wireless Protocol Advisor - Real Time - [CaptureData.tol:1 Traffic Overview]						
File Edit View Tools Record Traffic Goto Window Help						
Num.	Event Type	Direction	Timestamp	System Time	Protocol	Message
1	Rx	For/Down	11:35:48.000000	03:10:20.80	cdma20...	General Page Message
2	Rx	Rev/Up	11:35:48.700000	03:10:21.50	cdma20...	Page Response Message
3	Rx	For/Down	11:35:48.860000	03:10:21.66	cdma20...	Extended Channel Assignment Mess...
4	Rx	For/Down	11:35:49.380000	03:10:22.18	cdma20...	Order Message
5	Rx	For/Down	11:35:49.420000	03:10:22.22	cdma20...	Order Message
6	Rx	For/Down	11:35:49.460000	03:10:22.26	cdma20...	Service Connect Message
7	Rx	Rev/Up	11:35:49.460000	03:10:22.26	cdma20...	Pilot Strength Measurement Message
8	Rx	Rev/Up	11:35:49.520000	03:10:22.32	cdma20...	Order Message
9	Rx	Rev/Up	11:35:49.620000	03:10:22.42	cdma20...	Service Connect Completion Message
10	Stop Trigger	Rev/Up	11:35:49.620000			

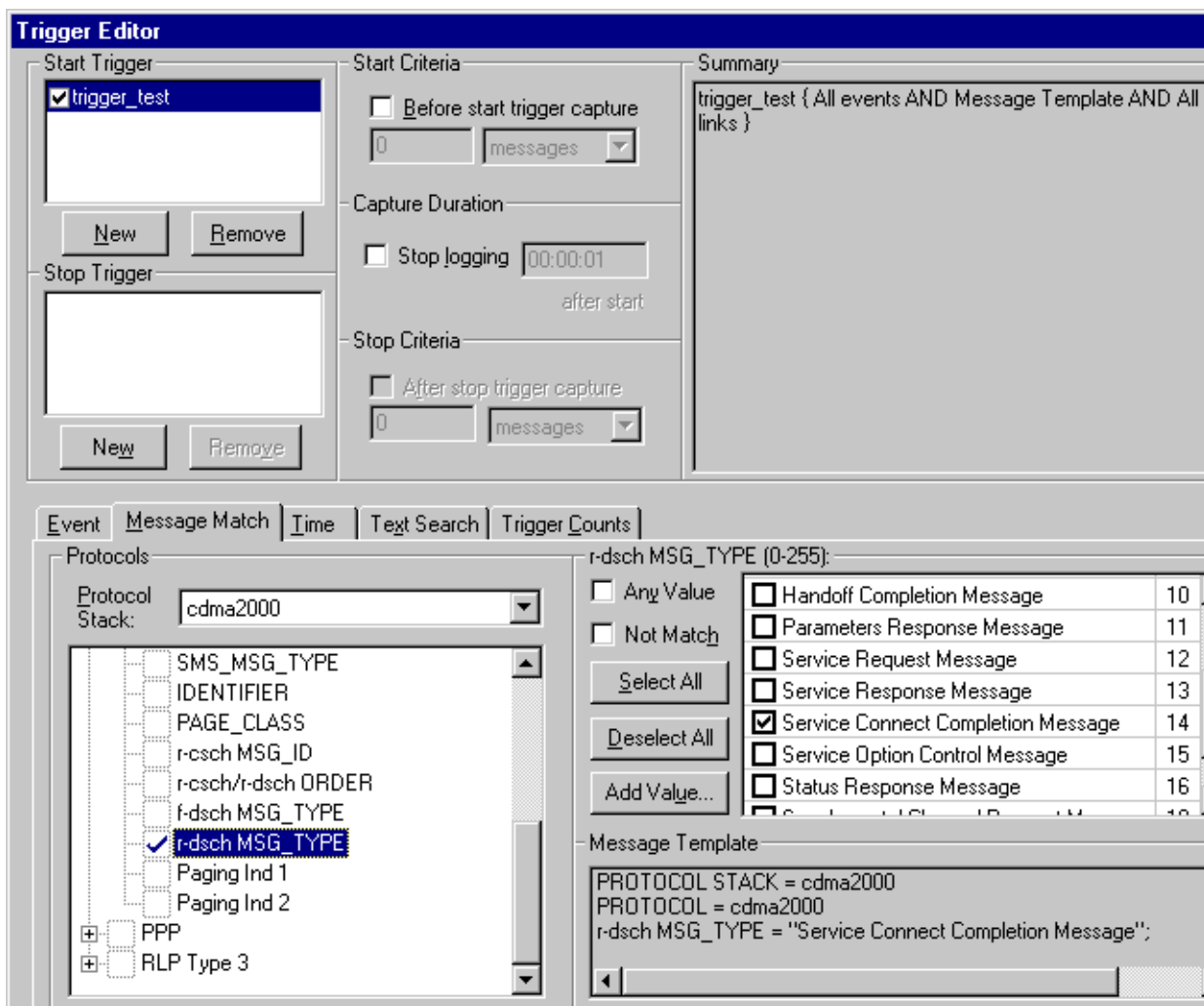
Example 7. Setting up a Start Trigger On a Message Match

1. From the Measurement Setup screen, double click on the Triggers



icon.
2. Click on the New button in the Start Trigger window. Name the Trigger “start\_trigger\_test”.
3. Select the Message Match tab.
4. Double click on cdma2000 in the Protocol directory. Scroll down the list of message types and select “r-dsch MSG\_TYPE”.
5. In the message window place a check mark in the Service Connect Completion Message box.



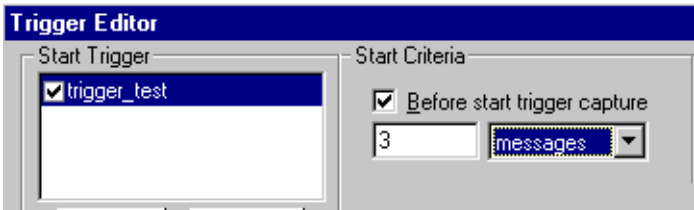


If the voice call represented by the ladder diagram were made now, the logging would begin with a Start Trigger message (see line number one), followed by the Service Connect Completion Message.

Wireless Protocol Advisor - Real Time - PRE RELEASE - [CaptureData.tol:1 Traffic Overview]						
File Edit View Tools Record Traffic Goto Window Help						
Num.	Event Type	Direction	Timestamp	Protocol	Message	Channel Type
1	Start Trigger	Rev/Up	07:43:57.280000			
2	Rx	Rev/Up	07:43:57.280000	cdma20...	Service Connect Completion Message	r-dsch
3	Rx	For/Down	07:43:57.380000	cdma20...	Alert With Information Message	f-dsch
4	Rx	Rev/Up	07:43:57.480000	cdma20...	Order Message	r-dsch
5	Rx	For/Down	07:43:57.640000	cdma20...	Order Message	f-dsch
6	Rx	Rev/Up	07:44:03.120000	cdma20...	Order Message	r-dsch
7	Rx	For/Down	07:44:03.480000	cdma20...	Order Message	f-dsch

**Example 8. Setting up a Pre-trigger on a Message Match**

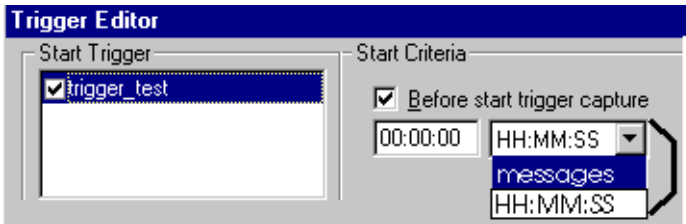
- 1. Perform the same steps as in “Setting up a Start Trigger On a Message Match” .
- 2. From the Trigger Editor, place a check mark in the Before start trigger capture box.
- 3. From the Trigger Editor, place a check mark in the Before start trigger capture box. Enter the number 3 in the field below the check box to indicate you want a trigger to occur three messages before the trigger message.



If the voice call represented by the ladder diagram were made now, the log would display three messages prior to a message indicating that a logging trigger occurred, followed by the Service Connect Completion Message. If less than three messages occur before a message match, WPA will still trigger.

Wireless Protocol Advisor - Real Time - PRE RELEASE - [CaptureData.tol:1 Traffic Overview]						
File Edit View Tools Record Traffic Goto Window Help						
Num.	Event Type	Direction	Timestamp	System Time	Protocol	Message
1	Rx	For/Down	10:24:19.380000	01:41:19.46	cdma20...	Service Connect Message
2	Rx	Rev/Up	10:24:19.380000	01:41:19.46	cdma20...	Pilot Strength Measurement Message
3	Rx	Rev/Up	10:24:19.440000	01:41:19.52	cdma20...	Order Message
4	Start Trigger	Rev/Up	10:24:19.540000			
5	Rx	Rev/Up	10:24:19.540000	01:41:19.62	cdma20...	Service Connect Completion Message
6	Rx	For/Down	10:24:19.640000	01:41:19.72	cdma20...	Alert With Information Message
7	Rx	Rev/Up	10:24:19.740000	01:41:19.82	cdma20...	Order Message
8	Rx	For/Down	10:24:19.900000	01:41:19.98	cdma20...	Order Message

**NOTE** Clicking on the drop down menu below the Before start trigger capture check box (shown below) will bring up a field that allows pre-triggering based on system time.



## Customizing the Traffic Overview

[“Adding a Column to the Traffic Overview” on page 43](#)

[“Setting the colors in the traffic overview” on page 45](#)

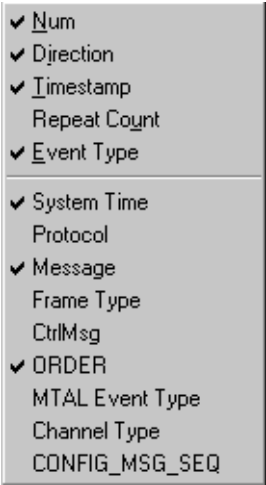
The traffic overview lists each decoded message with a row of information about the message. The number of columns and order they are presented can be selected. Also, color coding is used to show which messages are coming from the mobile station and which messages are coming from the base station. These colors can be changed.

### Example 9. Adding a Column to the Traffic Overview

1. From the Traffic Overview screen, right click anywhere in the traffic overview window.
2. Select Columns.



A selected list of columns is displayed with the check mark next to the columns currently displayed in the traffic overview.



This list is divided into two parts, information that WPA provides in addition to the protocol (the upper group) and protocol dependant choices (the lower group).

You can add a column to the display by placing a check mark next to it.

---

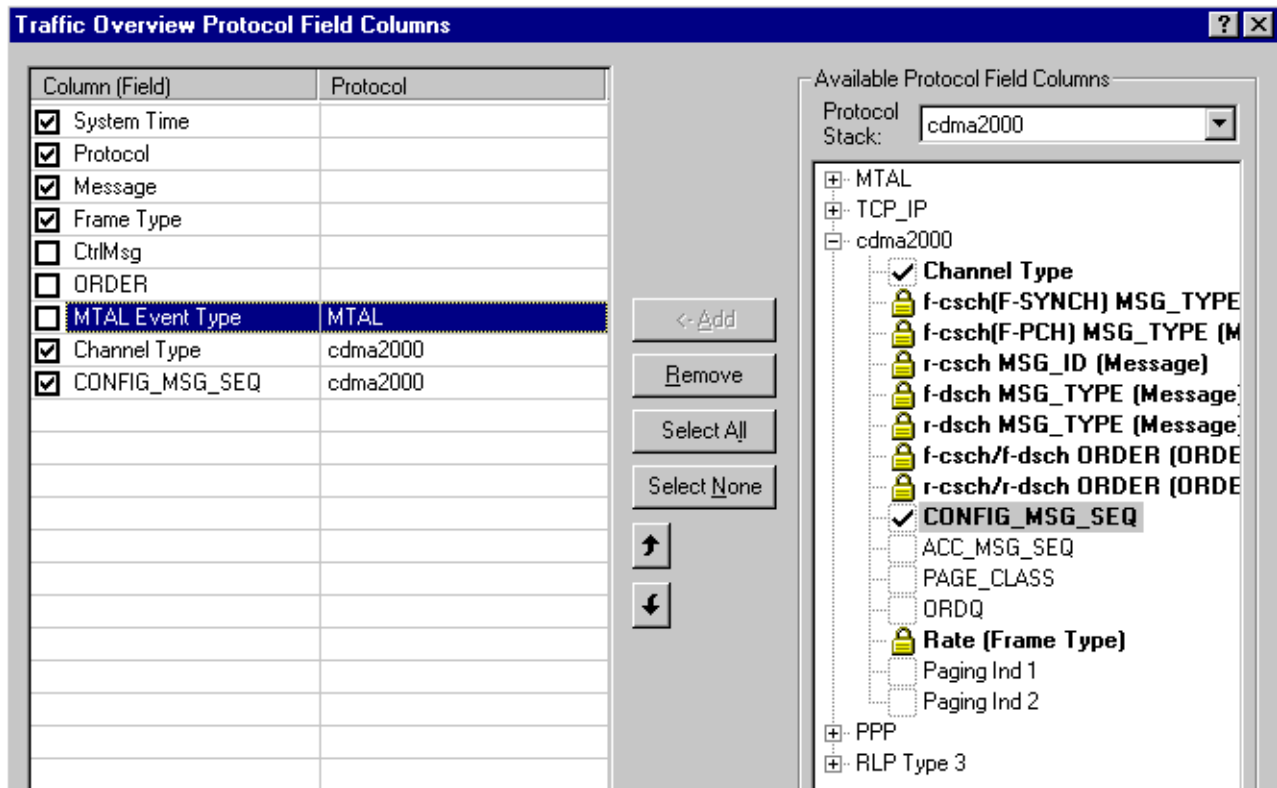
**IMPORTANT** This list only shows selections that are on the list by default or that have been added by the user. You can add to this list from the full list of column choices by continuing with step 3.

---

- 3. From the Traffic Overview screen, right click anywhere in the traffic overview window.
- 4. Select Column Setup.



The complete set of choices for columns is displayed with a padlock icon designating those protocol entities that are displayed in another column. The expression in parenthesis (e.g. (Message)) describes which column is associated with a padlocked protocol entity.



On the left window, the columns currently displayed on the traffic overview will have a check mark next to them. (This list is the same list that appears on the bottom portion of the window displayed in step 2.)

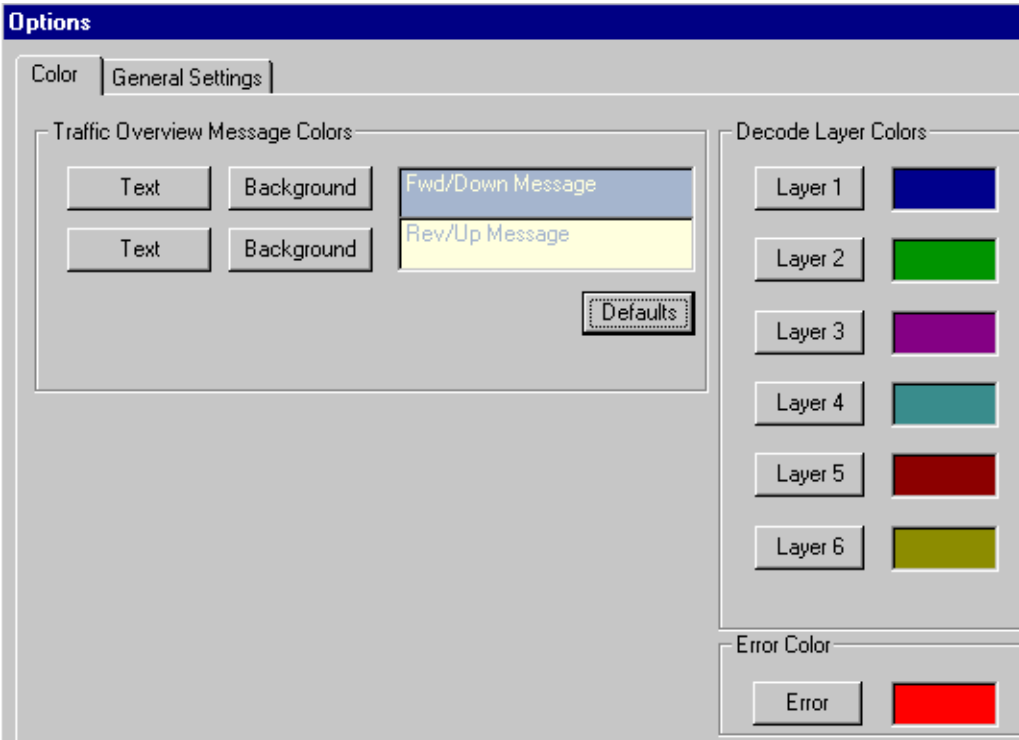
On the right window, a directory of protocol message choices (Available Protocol Field Columns) is displayed. Double click on a choice to add it to the left window. Selections you make will be displayed in the traffic overview and will become part of the list that you select from when you select Columns as in step 2.

### Example 10. Setting the colors in the traffic overview

Colors are used by WPA to make it easier to differentiate the direction of message flow

1. From the Traffic Overview screen, select Tools, Options.

A menu is displayed for changing background or text colors for the Traffic Overview screen and layer colors in the Decode screen.




## Customizing the Decode View

[“Setting Up Columns in the Decode View” on page 47](#)

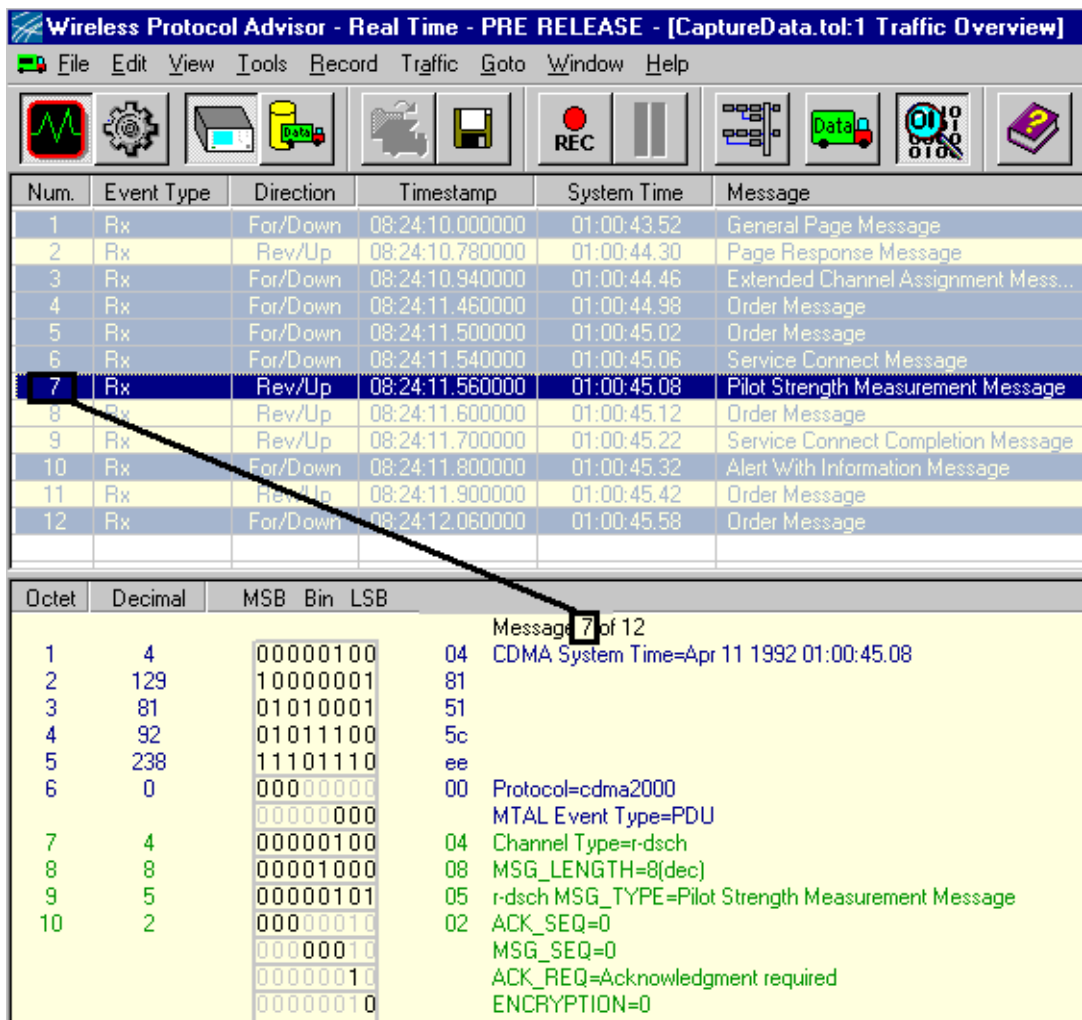
[“Setting Up Rows in the Decode View” on page 48](#)

The Decode View is displayed below the Traffic Overview when selected. The Decode View displays detailed message information including bit-by-bit decodes and field labeling.

### Example 11. Setting Up Columns in the Decode View

1. From the Traffic Overview screen, select the Decode View  .

2. Click on a message in the Traffic Overview screen.



The screenshot shows the 'Wireless Protocol Advisor - Real Time - PRE RELEASE - [CaptureData.tol:1 Traffic Overview]' window. The 'Traffic Overview' table lists 12 messages. Message 7, 'Pilot Strength Measurement Message', is selected. A callout box points to this message with the text 'Click on a message to display decodes'. Below the table, the 'Decode View' is displayed, showing MTAL data followed by decodes message data. The MTAL data includes fields like 'CDMA System Time=Apr 11 1992 01:00:45.08', 'Protocol=cdma2000', 'MTAL Event Type=PDU', 'Channel Type=r-dsch', 'MSG\_LENGTH=8(dec)', 'r-dsch MSG\_TYPE=Pilot Strength Measurement Message', 'ACK\_SEQ=0', 'MSG\_SEQ=0', 'ACK\_REQ=Acknowledgment required', and 'ENCRYPTION=0'.

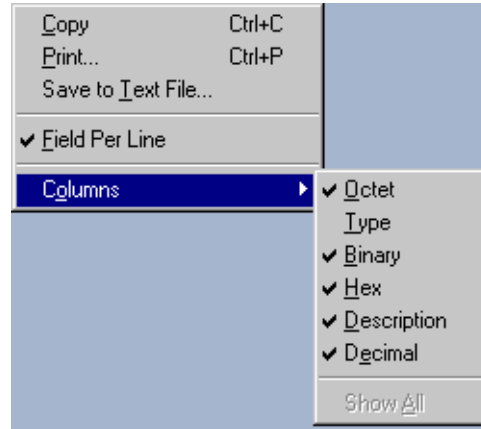
Num.	Event Type	Direction	Timestamp	System Time	Message
1	Rx	For/Down	08:24:10.000000	01:00:43.52	General Page Message
2	Rx	Rev/Up	08:24:10.780000	01:00:44.30	Page Response Message
3	Rx	For/Down	08:24:10.940000	01:00:44.46	Extended Channel Assignment Mess...
4	Rx	For/Down	08:24:11.460000	01:00:44.98	Order Message
5	Rx	For/Down	08:24:11.500000	01:00:45.02	Order Message
6	Rx	For/Down	08:24:11.540000	01:00:45.06	Service Connect Message
7	Rx	Rev/Up	08:24:11.560000	01:00:45.08	Pilot Strength Measurement Message
8	Rx	Rev/Up	08:24:11.600000	01:00:45.12	Order Message
9	Rx	Rev/Up	08:24:11.700000	01:00:45.22	Service Connect Completion Message
10	Rx	For/Down	08:24:11.800000	01:00:45.32	Alert With Information Message
11	Rx	Rev/Up	08:24:11.900000	01:00:45.42	Order Message
12	Rx	For/Down	08:24:12.060000	01:00:45.58	Order Message

Octet	Decimal	MSB	Bin	LSB	
1	4	00000100	04		Message 7 of 12
2	129	10000001	81		CDMA System Time=Apr 11 1992 01:00:45.08
3	81	01010001	51		
4	92	01011100	5c		
5	238	11101110	ee		
6	0	00000000	00		Protocol=cdma2000
		00000000			MTAL Event Type=PDU
7	4	00000100	04		Channel Type=r-dsch
8	8	00001000	08		MSG_LENGTH=8(dec)
9	5	00000101	05		r-dsch MSG_TYPE=Pilot Strength Measurement Message
10	2	00000010	02		ACK_SEQ=0
		00000010			MSG_SEQ=0
		00000010			ACK_REQ=Acknowledgment required
		00000010			ENCRYPTION=0

Click on  
a message  
to display  
decodes

The Decode View screen will display MTAL data followed by decodes message data.

3. Right click anywhere in the Decode View screen.
4. Select Columns.
5. Place a check mark next to the columns you would like displayed in the Decode View window.



### Example 12. Setting Up Rows in the Decode View

1. With the Decode View displayed and a message highlighted, right click anywhere in the Decode View screen.
2. Select or deselect the Field Per Line selection.

This selection determines the amount of information which will be displayed on each line.

Without Field Per Line check marked, all of the bits are displayed one octet per line. More than one message field may be displayed on one line.

With Field Per Line check marked, bits are divided so that there is one message field per line.



Octet	Decimal	MSB Bin LSB	Hex	Description
				Message 7 of 12
1	4	00000100	04	CDMA System Time=Apr 11 1992 01:00:45.08
2	129	10000001	81	
3	81	01010001	51	
4	92	01011100	5c	
5	238	11101110	ee	
6	0	00000000	00	MTAL Event Type=PDU; Protocol=cdma2000
7	4	00000100	04	Channel Type=r-dsch
8	8	00001000	08	MSG_LENGTH=8(dec)
9	5	00000101	05	r-dsch MSG_TYPE=Pilot Strength Measurement Message
10	2	00000010	02	ACK_SEQ=0; MSG_SEQ=0; ACK_REQ=Acknowledgment required; ENCRYPTION=0
11	3	00000011	03	REF_PN=12(dec)
12	14	00001110	0e	PILOT_STRENGTH=14(dec)
13	128	10000000	80	KEEP=1; PADDING=0
14	217	11011001	d9	CRC=d945(hex)
15	69	01000101	45	

**Without  
Field Per Line**

Octet	Decimal	MSB Bin LSB	Hex	Description
				Message 7 of 12
1	4	00000100	04	CDMA System Time=Apr 11 1992 01:00:45.08
2	129	10000001	81	
3	81	01010001	51	
4	92	01011100	5c	
5	238	11101110	ee	
6	0	00000000	00	Protocol=cdma2000
		00000000		MTAL Event Type=PDU
7	4	00000100	04	Channel Type=r-dsch
8	8	00001000	08	MSG_LENGTH=8(dec)
9	5	00000101	05	r-dsch MSG_TYPE=Pilot Strength Measurement Message
10	2	00000010	02	ACK_SEQ=0
		00000010		MSG_SEQ=0
		00000010		ACK_REQ=Acknowledgment required
		00000010		ENCRYPTION=0
11	3	00000011	03	REF_PN=12(dec)
12	14	00001110	0e	

**With  
Field Per Line**

## Saving Log Files

[“Saving a Logging Session to a .tol File” on page 50](#)

[“Saving the Traffic Overview to a .csv file” on page 50](#)

[“Saving the Decode View to a .txt file” on page 51](#)

WPA log files can save messages in three different formats:

- .tol
- .csv
- .txt

If you want to save a logging session for post capture analysis using WPA, you would save as a .tol file.

This format saves all data from a logging session, including the test set filter settings, log filter settings, and trigger settings that were in use during the logging session. Knowing these settings helps in analyzing the purpose of the logging session and makes it possible to repeat a session under the same circumstances, if necessary.

### Example 13. Saving a Logging Session to a .tol File

1. With WPA in real time mode, stop logging (status will be Idle).
2. Select File, Save As.
3. Save the file as “voice\_call.tol”.

Switch WPA to post capture mode and open the log file (File, Open Log File). This file can be opened and analyzed by another user without requiring connection to a test set.

If you want to display the traffic view in a spreadsheet, you would save as a .csv file

### Example 14. Saving the Traffic Overview to a .csv file

---

<b>NOTE</b>	The Decode View cannot be saved as a .csv file.
-------------	---

---

1. With WPA in real time mode, stop logging (status will be Idle).
2. Right click in the Traffic Overview window.
3. Select Save to CSV Log File.
4. Save the file as “voice\_call.csv”

Open the .csv file in a spreadsheet application. The messages will be displayed in spreadsheet format.

	A	B	C	D	E	F	G	H	I	J
1	Num.	Event Type	Direction	Timestamp	System Time	Protocol	Message			
2	1	Rx	For/Down	01:19.0	18:05.4	cdma2000	General Page Message			
3	2	Rx	Rev/Up	01:19.8	18:06.2	cdma2000	Page Response Message			
4	3	Rx	For/Down	01:19.9	18:06.4	cdma2000	Extended Channel Assignment Message			
5	4	Rx	For/Down	01:20.5	18:06.9	cdma2000	Order Message			
6	5	Rx	For/Down	01:20.5	18:06.9	cdma2000	Order Message			
7	6	Rx	For/Down	01:20.5	18:07.0	cdma2000	Service Connect Message			
8	7	Rx	Rev/Up	01:20.5	18:07.0	cdma2000	Pilot Strength Measurement Message			
9	8	Rx	Rev/Up	01:20.6	18:07.0	cdma2000	Order Message			
10	9	Rx	Rev/Up	01:20.7	18:07.1	cdma2000	Service Connect Completion Message			
11	10	Rx	For/Down	01:20.8	18:07.2	cdma2000	Alert With Information Message			
12	11	Rx	Rev/Up	01:20.9	18:07.3	cdma2000	Order Message			
13	12	Rx	For/Down	01:21.1	18:07.5	cdma2000	Order Message			
14	13	Rx	Rev/Up	01:25.1	18:11.6	cdma2000	Order Message			
15	14	Rx	For/Down	01:25.5	18:11.9	cdma2000	Order Message			

If you want to display the Decode view of a message or messages in a text editor, you would save as a .txt file.

---

**NOTE** The Traffic Overview cannot be saved as a .txt file.

---

#### Example 15. Saving the Decode View to a .txt file

1. With WPA in real time mode, stop logging (status will be Idle).
2. In the Traffic Overview window, highlight the message or messages you want to save. You can use the Shift key to highlight a block of messages, or the Ctrl key to select messages at random.
3. Right click in the Decode View window.
4. Select Save to Text File.
5. Save the file as "voice\_call.txt".

Open the .txt file in a text editor. Messages decodes will be formatted as plain text.

## Protocol Analysis

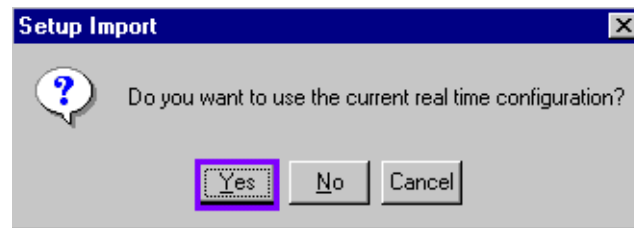
Octet	Decimal	Binary	Hex	Description
Message 1 of 14 on CDMA2000Link (Test Set (Hub to Node)) at Wednesday, September 17, 2003				
1	4	00000100	04	CDMA System Time=Apr 10 1992 21:18:05.44
2	129	10000001	81	
3	71	01000111	47	
4	43	00101011	2b	
5	160	10100000	a0	
6	0	00000000	00	MTAL Event Type=PDU; Protocol=cdma2000
7	1	00000001	01	Channel Type=f-csch (F-PCH)
8	16	00010000	10	MSG_LENGTH=16(dec)
9	17	00010001	11	f-csch(F-PCH) MSG_TYPE=General Page Message
10	92	01011100	5c	CONFIG_MSG_SEQ=23; ACC_MSG_SEQ=8
11	142	10001110	8e	CLASS_0_DONE=1; CLASS_1_DONE=1; TMSI_DONE=1; ORDERED_TMSIS=0
12	128	10000000	80	BROADCAST_DONE=1; RESERVED=0; ADD_LENGTH=0
13	5	00000101	05	PAGE_CLASS=Class 0, IMSI_S included; MSG_SEQ=2; IMSI_S= 0000000643
14	243	11110011	f3	
15	252	11111100	fc	
16	245	11110101	f5	
17	10	00001010	0a	
18	64	01000000	40	SDU_INCLUDED=1; SERVICE_OPTION=3(dec)=Enhanced Variable Rate Voice Service (8 kbps)
19	0	00000000	00	
20	195	11000011	c3	CRC=36ed9ad(hex)
21	110	01101110	6e	
22	217	11011001	d9	
23	173	10101101	ad	

## Exporting and Importing Measurement Setups

If you have a measurement setup that you want to be able to reuse later, or if you have a .tol file saved and would like to perform a real time logging session with the same settings, you can use the Export/Import Setup feature.

### Example 16. Reusing a Measurement Setup

1. With the WPA in Post Capture mode click on File, Open Log File.
2. Open the “voice\_call.tol” file.
3. Click on File, Export Setup. Name the file “voice\_call.msf”.
4. Switch to Real Time mode, and create a new log filter (see [“Log Filter Initialization” on page 30](#)). Name the filter “temp”.
5. Click on File, Import Setup. Select “voice\_call.msf”. When the dialog box shown below appears, click on Yes.



6. Return to the Log Filter Editor and you will see that the filter settings have reverted to the same settings used in the voice call log file.

## Working With Multiple Traffic Overviews

Comparing two or more different log files is performed by saving logging data to separate .tol files, opening the files, and arranging the windows as needed.

---

**NOTE** This example assumes that there are two .tol files available for comparison

---


### Example 17. Comparing Two Log Files

1. With the WPA in post capture mode click on File, Open Log File.
2. Open the first .tol file
3. Repeat steps 1 and 2 to open the second file.
4. Click on Window, Tile.

### Analyzing Copies of the Same Log File

The WPA allows replication of log files to simultaneously provide more than one view, possibly using different filters, triggers, or display configurations.

### Example 18. Adding Traffic Overviews

1. In post capture mode, open the “voice\_call.tol” file if it is not already open. Click on Window and, if there are any other files, open close them.
2. Click on the Add a Traffic Overview icon  .

A “copy” of the traffic overview window will be displayed on the right side of the display. It will be named “voice\_call.tol:2”.

Both windows will be sized to fit the display

3. Click anywhere in the “voice\_call.tol:1” window and display the Decode View if it is not already displayed. The decode view should appear only for “voice\_call.tol:1”.

4. Right click anywhere in the “voice\_call.tol:2” window and select View Filter

This step is a short cut to the View Filter.

5. In post capture mode, open the “voice\_call.tol” file if it is not already open. Click on Window and, if there are any other files, open close them.
6. Create a New view filter and name it “copy1”.
7. In the Message Match folder, select cdma2000.

Select Channel Type and check the box labeled “f-csch(F-PCH)”.

This step will filter out all messages except for the forward paging channel messages.

8. Click on OK.

The display will look like this:

Wireless Protocol Advisor - Real Time - PRE RELEASE - voice\_call.tol

File Edit View Tools Record Traffic Goto Window Help

voice\_call.tol:1 Traffic Overview

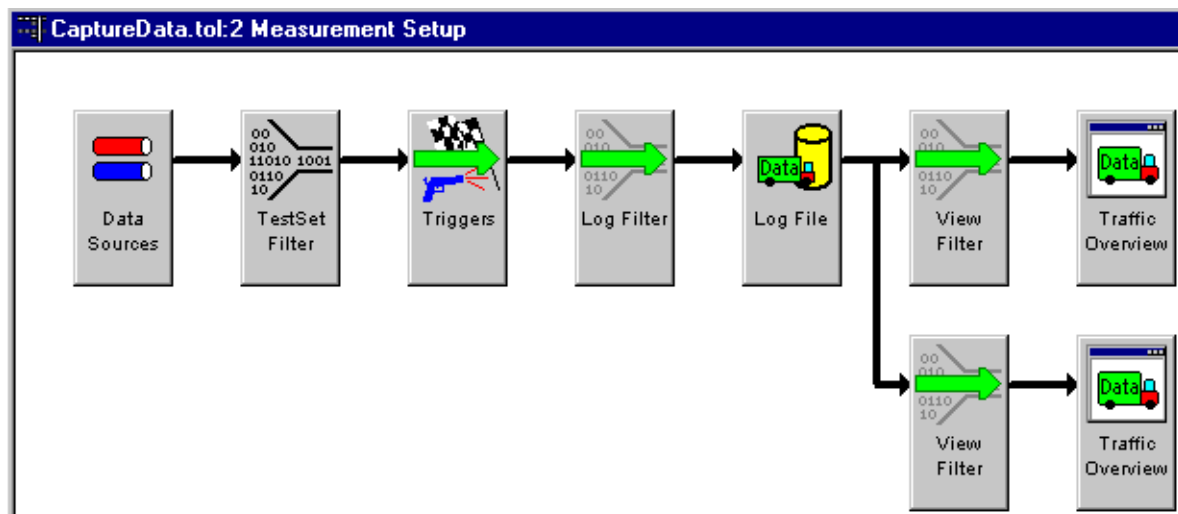
Nu...	Direction	Timestamp	Protocol	Message
1	For/Down	09:54:28.00...	cdma20...	General Page Message
2	Rev/Up	09:54:28.58...	cdma20...	Page Response Message
3	For/Down	09:54:28.74...	cdma20...	Extended Channel Assignment Message
4	For/Down	09:54:29.22...	cdma20...	Order Message
5	For/Down	09:54:29.26...	cdma20...	Order Message
6	For/Down	09:54:29.30...	cdma20...	Service Connect Message
7	Rev/Up	09:54:29.30...	cdma20...	Pilot Strength Measurement Message
8	Rev/Up	09:54:29.36...	cdma20...	Order Message
9	Rev/Up	09:54:29.46...	cdma20...	Service Connect Completion Message
10	For/Down	09:54:29.56...	cdma20...	Alert With Information Message
11	Rev/Up	09:54:29.66...	cdma20...	Order Message
12	For/Down	09:54:29.82...	cdma20...	Order Message
13	Rev/Up	09:54:32.00...	cdma20...	Order Message
14	For/Down	09:54:32.36...	cdma20...	Order Message

voice\_call.tol:2 Traffic Overview (Filtered)

Num.	Direction	Timestamp	Protocol	Message
1	For/Down	09:54:28.000000	cdma20...	General Page Message
3	For/Down	09:54:28.740000	cdma20...	Extended Channel Assignment Message

9. Click on the measurement setup view icon  .

Selecting the measurement setup view will bring up a diagram that shows there are now two paths for measurement setup.



10. Right click on the View Filter icon shown in the upper path.

The window should show a check mark indicating the View Filter is Enabled.

11. Close the Measurement View

12. Click on Traffic, Synchrondize Views.



**Synchronize Views  
locks messages  
in multiple  
windows**

13. Select any message in the “voice\_call.tol:2” window.

If you select a message in either traffic overview with Synchronize Views enabled, WPA will automatically display the same message in the corresponding log.

### **Example 19. Displaying the Decode View Beside the Traffic Overview**

If you would like to see the Decode View at the side of the Traffic Overview (instead of below it), you can add a Traffic Overview and then maximize the Decode View in the copy.

1. In post capture mode, open the “voice\_call.tol” file if it is not already open. Click on Window and, if there are any other files open close them.
2. Click on the Add a Traffic Overview icon.

A “copy” of the traffic overview window will be displayed on the right side of the display. It will be named “voice\_call.tol:2”.

Both windows will be sized to fit the display

3. Click anywhere in the “voice\_cal.tol:2” window and click on the Decode View icon.
4. Resize the Decode View so that it occupies the entire “voice\_cal.tol:2” window.

The display will show the Traffic Overview on the left and the Decode View on the right.



Wireless Protocol Advisor - Post Capture - PRE RELEASE - voice\_call.tol

File Edit View Tools Record Traffic Goto Window Help

voice\_call.tol:1 Traffic Overview

Num.	Direction	Timestamp	Protocol	Message
1	For/Down	09:54:28.000000	cdma20...	General Page Message
2	Rev/Up	09:54:28.580000	cdma20...	Page Response Message
3	For/Down	09:54:28.740000	cdma20...	Extended Channel Assignment Message
4	For/Down	09:54:29.220000	cdma20...	Order Message
5	For/Down	09:54:29.260000	cdma20...	Order Message
6	For/Down	09:54:29.300000	cdma20...	Service Connect Message
7	Rev/Up	09:54:29.300000	cdma20...	Pilot Strength Measurement Message
8	Rev/Up	09:54:29.360000	cdma20...	Order Message
9	Rev/Up	09:54:29.460000	cdma20...	Service Connect Completion Message
10	For/Down	09:54:29.560000	cdma20...	Alert With Information Message
11	Rev/Up	09:54:29.660000	cdma20...	Order Message
12	For/Down	09:54:29.820000	cdma20...	Order Message
13	Rev/Up	09:54:32.000000	cdma20...	Order Message
14	For/Down	09:54:32.360000	cdma20...	Order Message

voice\_call.tol:2 Traffic Overview

Num.	Direction	Timestamp	Protocol	Message
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				

Octet Decimal MSB Bin LSB Hex Description

1	4	00000100	04	Message 7 of 14 on CDMA2000Link
2	129	10000001	81	CDMA System Time=Apr 12 1992 20:11:17.78
3	199	11000111	c7	
4	242	11110010	f2	
5	225	11100001	e1	
6	0	00000000	00	MTAL Event Type=PDU; Protocol=cdma2000
7	4	00000100	04	Channel Type=r-dsch
8	8	00001000	08	MSG_LENGTH=8(dec)
9	5	00000101	05	r-dsch MSG_TYPE=Pilot Strength Measurement t
10	2	00000010	02	ACK_SEQ=0; MSG_SEQ=0; ACK_REQ=Acknow
11	3	00000011	03	REF_PN=12(dec)
12	15	00001111	0f	PILOT_STRENGTH=15(dec)
13	128	10000000	80	KEEP=1; PADDING=0
14	234	11101010	ea	CRC=ea74(hex)
15	116	01110100	74	

##### 5. Click on Traffic, Synchronize Views

When you select any message in the left window, the Decode View in the right window will display that message.

## Tracing Multiple IP Connections (Connection Trace)

Connection Trace is a feature of the WPA (Wireless Protocol Advisor) that mirrors the behavior of a network connection within the WPA for the purpose of tracking and performing measurements on IP connections. This feature only applies to TCP/IP connections, such as web page downloading.


If you have a wireless device that is capable of Internet connectivity (e.g. has a web browser or functions as a modem for a PC with a web browser) you will be able to analyze real time TCP/IP connections.

If you do not have a wireless device that is capable of Internet connectivity, you can go into post capture mode or demo mode and access the `connection_trace.tol` file for demonstration purposes.

### Example 20. Group Messages by Connection

1. If you are operating WPA in Real Time mode:
  - a. Go to the Test Set filter and check the box that is labeled TCP/IP (or IP).
  - b. Remove all Log Filters and View Filters.
  - c. Activate logging and browse the Internet, accessing multiple web sites.
  - d. Stop logging.

If you are operating WPA in Post Capture mode, open the log file `connection_trace.tol`

2. Select the Connection Trace icon. 
3. In the Connection Trace Configuration window, click on OK.

The Connection Trace View will open.

connection_trace.tol:3 Connection Trace: TCP						
Conn. Id	Duration	Status	DUT Address	DUT Port	Network Ad...	Network Port
0	23.03		130.29.182.230	1069	130.29.152.194	80
1	13.72		130.29.182.230	1071	130.29.154.58	80
2	21.51		130.29.182.230	1072	130.29.154.58	80
3	34.31		130.29.182.230	1073	130.29.154.58	80
4	1:00.21		130.29.182.230	1074	130.29.154.58	80
5	47.11		130.29.182.230	1075	130.29.154.58	80

4. Double-click the first connection (Conn Id = 0).

The Traffic Overview window will now display only those messages that were part of the connection between the DUT and Network hosts identified by Connection Id 0.

5. Click on the Group icon. 

This action UNGrouped the Traffic Overview.

6. Right-click in the Connection Trace View. Select Summary View from the menu.

A Summary View window will open that provides a connection count

Total Connections	Active Connections	Terminated Connecti...
28	16	12

7. Double-click on any message in the Traffic Overview window.

This action re-grouped all messages that were part of the selected message's connection.

