Roaming Detection

Roaming service is a vital part of every mobile network that represents a major share of overall operating revenue. Network operators need to verify that their systems are handling roaming traffic properly to maintain customer satisfaction and to protect that revenue.

This application note describes how to configure the Tektronix K1205 Protocol Analyzer to detect and monitor roaming traffic. The step-by-step procedure demonstrates how to use pre-recorded sample data to set up the analyzer, edit the setup for a specific network configuration and monitor live traffic. Test results confirm the presence of roaming subscribers and document the amount of roaming traffic that was present during the measurement period.

The techniques used in this example can be applied to the measurement of other network load and traffic properties as well. The K1205 functions described here — *filters, expert mode, triggers* and *statistics* — are powerful general purpose tools for identifying and capturing a wide range of network activities.

The Challenge of Monitoring Roaming Traffic

We want to detect roaming traffic, measure its stability over time and issue an alert when no roamers are connected. At the end of the test, we want to have a report of the number of roaming calls that occurred during each measurement period.

A typical network configuration is shown in *Figure 1*. Roaming traffic uses the MAP (Mobile Application Part) protocol to exchange routing information that is needed to terminate calls. This information is found on the interface between GMSC (Gateway Mobile Switching Center) and HLR (Home Location Register). To capture this information, we will need to define the desired characteristics of a roaming message and set up the K1205 to detect the messages, count them and issue an alert if none occurs within a prescribed time period (indicating the absence of roaming traffic).

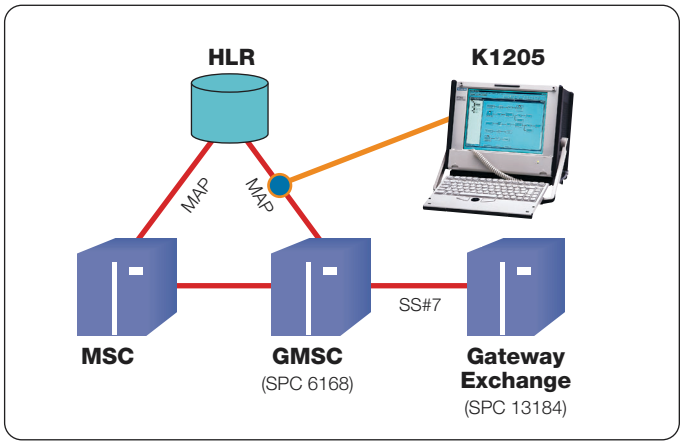


Figure 1. *Measurement Setup*

Tektronix
Enabling Innovation

Meeting the Challenge

Our final objective is to connect the K1205 to the link(s) between GMSC and HLR, configure the test parameters to match the network properties and run tests on live traffic. To accomplish this, we will first test offline with a short sample of pre-recorded data from a file — allowing us to become familiar with the process before we go on to live data.

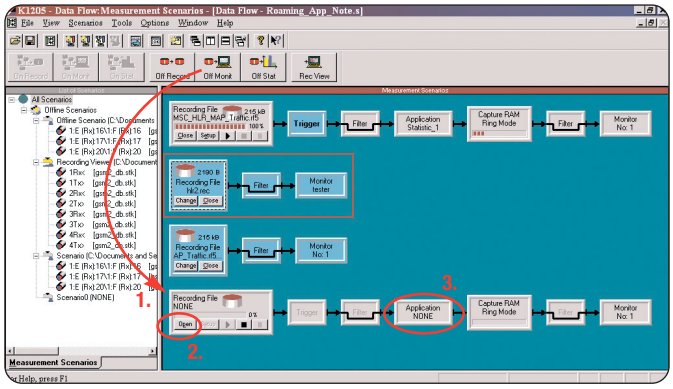
In practice, we recommend a four step approach to live traffic monitoring — even after you have mastered the techniques. This approach helps eliminate setup errors and costly retesting by making sure the equipment is functioning properly before taking data.

- Use a recording file to create and verify a correct set up for the K1205 offline
- Edit the setup parameters offline to match the network to be tested
- Connect the K1205 to the network and verify that it is able to detect the roaming traffic
- Run the final tests to monitor traffic over longer periods of time

Setting Up the K1205 for Offline Test

Load a Recording File:

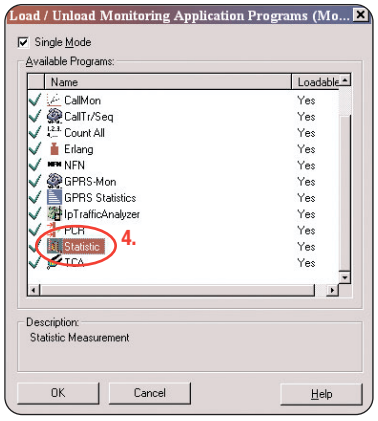
1. Select an empty Offline Monitoring-Pipeline or create a new one (drag from **Off Monit** down to a free area of the *Measurement Scenarios* screen)
2. Click **Open** and select the file that contains the MSC-HLR (Mobile Switching Center-HLR) traffic (MSC_HLR_MAP_Traffic.rf5) and the GSM (Global System for Mobile Communication) protocol stack that includes MAP. The stack in this example *(gsm2p_msc_sms.stk)* is attached to the file and loads automatically (*Figure 2*)



▶ ***Figure 2.*** *Create a Monitoring-Pipeline*

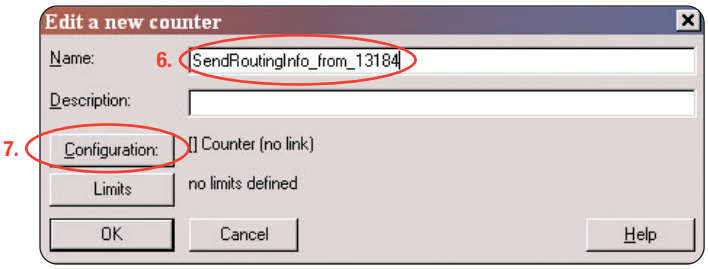
Configure the Statistics

3. Click the **Application** element in the pipeline (*Figure 2*)
4. Select **Statistic** (*Figure 3*)



▶ ***Figure 3.*** *Application Selection Dialog*

5. Right click in the empty area of the statistics window and select **Add Counter**
6. Enter a name for the new counter (**SendRoutingInfo_from_13184**, in this example)
7. Click **Configuration**



▶ ***Figure 4.*** *Edit Counter*

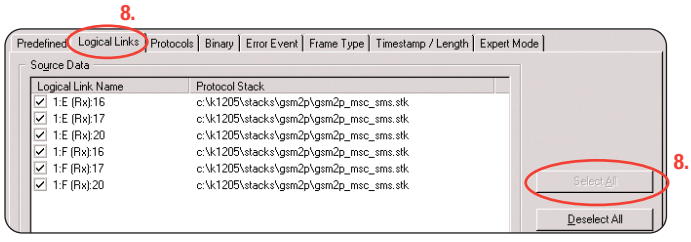
Note: In this example, the GMSC has the SPC (Signaling Point Code) *13184*, so all the traffic originating from there can be detected by filtering for messages that include the OPC (Origination Point Code) *13184*. (In a live environment this value would be set to the pointcode of the actual GMSC in the network.)

Configure the Filter

Roaming traffic can be identified as messages in MAP with the Operation Code *Send Routing Info* in both *BEG* and *END* messages from the GMSC at OPC 13184. To count these messages we will create a filter with the criteria **Send Routing Info AND OPC 13184**. We will use the *Expert Mode* to create the logical AND relationship in the filter.

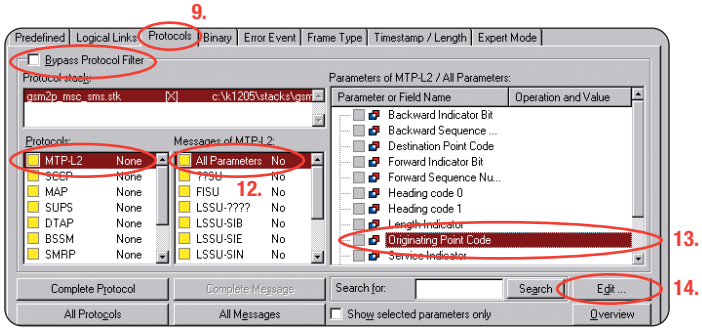
Note: This is only one of many different ways to configure a filter to reach the desired result.

8. On the Logical Links tab of the Filter Setup screen choose Select All (to evaluate the traffic from all logical links in the file or the online source)



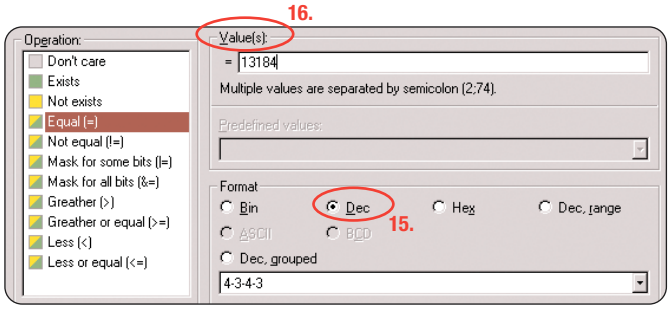
▶ ***Figure 5.*** *Select all logical links*

9. Click the **Protocols** tab
10. Uncheck box next to **Bypass Protocol Filter**
11. Select **MTP-L2** (Message Transfer Part-L2) from *Protocols* list
12. Select **All Parameters** from *Messages of MTP-L2* list
13. Select **Originating Point Code** from Parameter or Field Name list
14. Click **Edit**



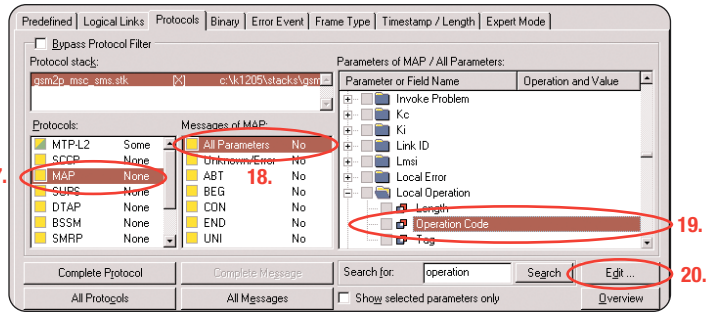
▶ ***Figure 6.*** *Select OPC 13184 (1)*

15. Click **Dec** in the *Format* section
16. Enter "**13184**" into *Value(s)*



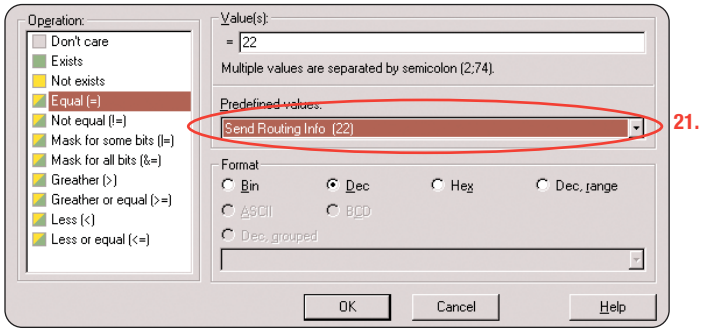
▶ ***Figure 7.*** *Select OPC (2)*

17. Select **MAP** from *Protocols* list
18. Select **All Parameters** from *Messages* list
19. Select **Operation Code** in *Local Operation* folder in *Parameter or Field Name* list
20. Click **Edit**



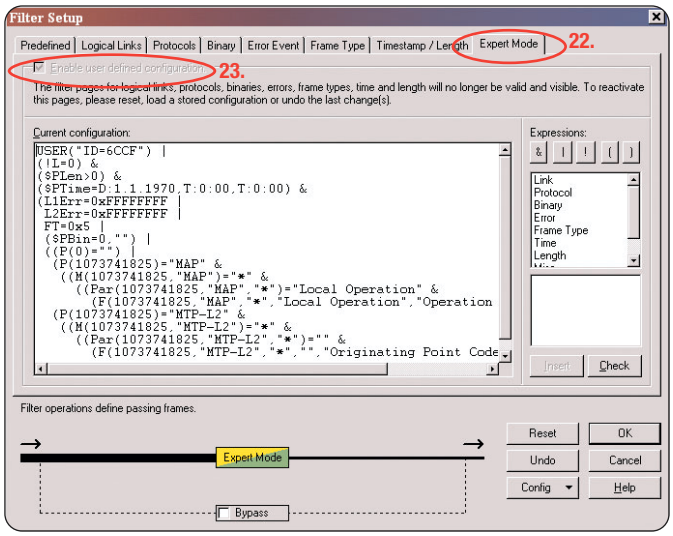
▶ ***Figure 8.*** *Select Operation Code (1)*

21. Select **Send Routing Info (22)** from Predefined Values list



▶ ***Figure 9.*** *Select Operation Code (2)*

22. Click the **Expert Mode** tab of the Filter Setup screen
23. Check **Enable user defined configuration** to invoke the *Expert Mode*



▶ ***Figure 10.*** *Filter Expert Mode*

Note: In Figure 11, the **brown** text describes **general filter settings**
the **blue** text describes the settings for **Send Routing Info (22)**
the **green** text describes the settings for **OPC 13184**
the **purple** text describes the setting for **error message handling**
The symbol "|" represents logical OR
The symbol "&" represents logical AND

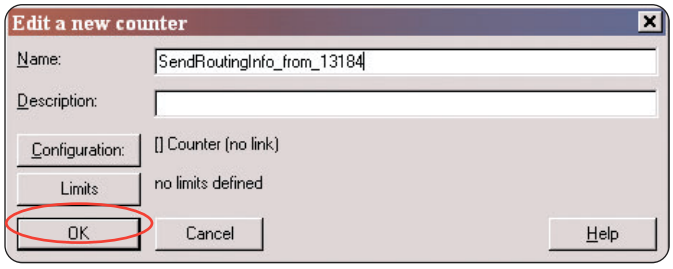
24. Go to the circled area of the code window (*see Figure 11*) and replace the "|" with an "&", establishing the logical AND operation

```
 USER("ID=6CCF") |
(!L=0) & ($PLen>0) &
($PTime=D:1.1.1970,T:0:00,T:0:00) & (L1Err=0xFFFFFFFF
|
L2Err=0xFFFFFFFF |
FT=0x5 | ($PBin=0,"") |
 ((P(0)="") |
  (P(1073741825)="MAP" &
   ((M(1073741825,"MAP")="*" &
    ((Par(1073741825,"MAP","*")="Local Operation" &
      (F(1073741825,"MAP","*","Local
Operation","Operation Code")=22)))))) | 24.
 (P(1073741825)="MTP-L2" &
  ((M(1073741825,"MTP-L2")="*" &
   ((Par(1073741825,"MTP-L2","*")="" &
     (F(1073741825,"MTP-L2","*","","Originating Point
Code")=13184))))))) |
DecErr=0x0)
```

▶ ***Figure 11.*** *Filter Code*

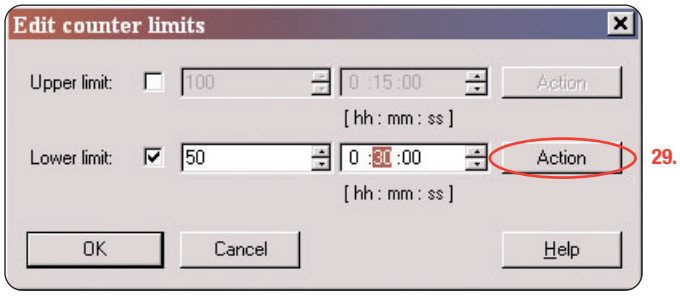
Configure the Trigger and Limits

25. Click the **Application Statistic_1** element in the monitoring pipeline
26. Select the counter **SendRoutingInfo_from_13184**
27. Click **Limits**

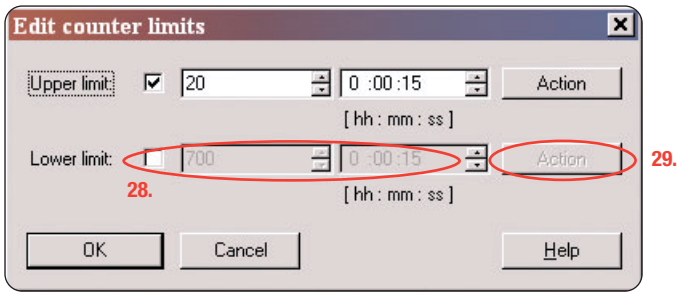


▶ ***Figure 12.*** *Edit Counter*

28. Define a lower limit for the counter. The screen in *Figure 13* shows 30 minutes, which might be an appropriate value for live monitoring. However, because the recorded sample is extremely short, set the **Lower limit** to 15 seconds and set the **Upper limit** to 15 seconds to trigger a result (*see Figure 14*)

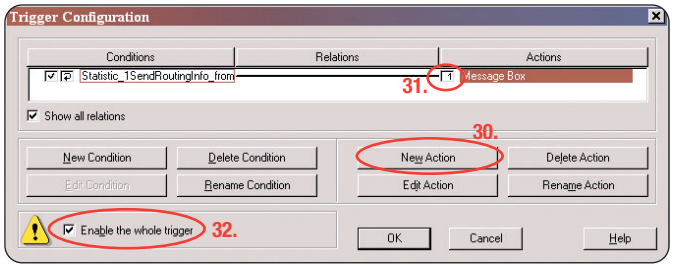


▶ ***Figure 13.*** *Edit Counter Limits*



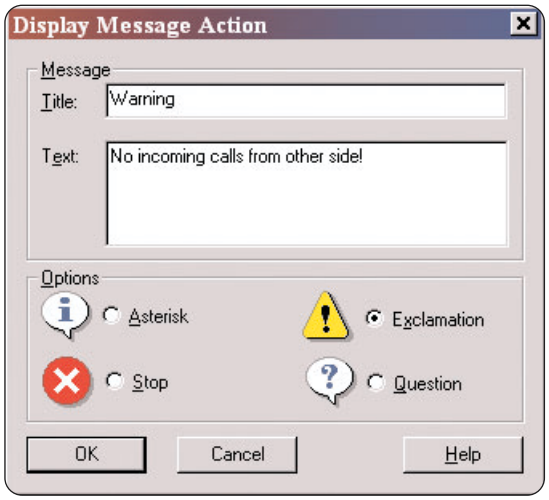
▶ ***Figure 14.*** *Example Limit Settings*

29. Click **Action** to define the trigger action that should be executed after the limit is reached
30. Click **New Action** and choose **Display Message Box**
31. Connect the Condition and the Action by clicking into the empty box in front of **Message Box**
32. Make sure that **Enable whole trigger** is checked



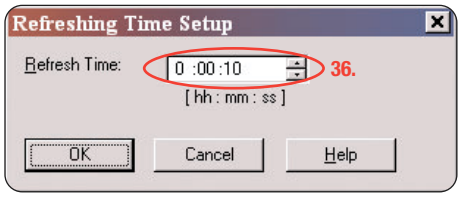
▶ ***Figure 15.*** *Trigger Configuration*

33. Define the *Title, Text* and icon *Option* for the message box, as in *Figure 16*



▶ ***Figure 16.*** *Message Box Definition*

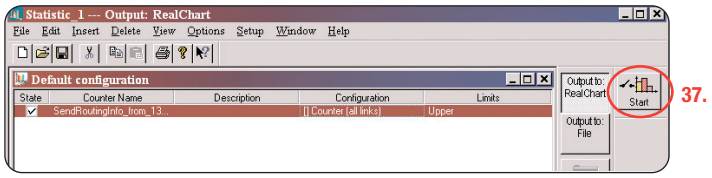
34. After confirming all of these settings the *Statistic_1* window should look like *Figure 18*
35. **Right click** in the empty area in the *Statistic_1* window and choose **Refreshing Time Setup**
36. Set the *Refresh Time* to **10 sec**. for this example as in *Figure 17* (for real traffic, 30 min. might be more appropriate)



▶ ***Figure 17.*** *Refresh Time Setup*

Running the Test on Recorded Data

37. Click **Start** to activate the statistics together with the defined trigger

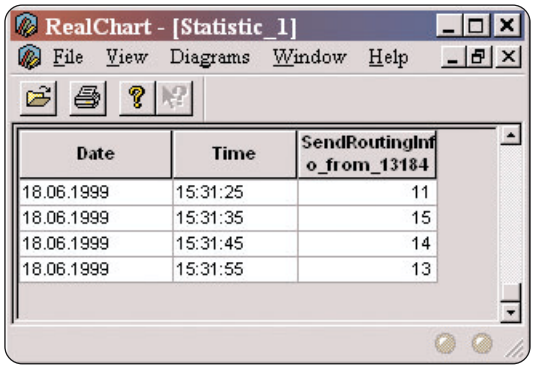


▶ ***Figure 18.*** *Statistic Configuration*

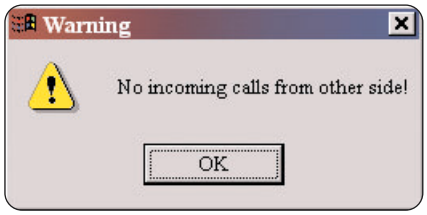
38. Start the playback of the recording file (click on__)

▶ ***Figure 19.*** *Playback Pipeline*

39. The counter results will be displayed in a RealChart window *(see Figure 20)* and a message box *(Figure 21)* will appear after the limit is reached for this example configuration



▶ ***Figure 20.*** *RealChart display of the counter results*



▶ ***Figure 21.*** *Message Box*

Editing Test Values to Monitor Live Traffic

Once the K1205 has successfully measured the test data, this instrument can be easily reconfigured to monitor live data on an actual network. Connect the K1205 to the link(s) between GMSC and HLR, set up the logical links with desired timeslots (TS16 in most cases) and use a GSM-stack that includes MAP (*gsm2p_msc_sms.stk* in this example).

Setup a new **Online** *Monitoring Pipeline and Statistics* in the same manner as in steps 1-7, substituting the appropriate MAP stack and the pointcode for the actual GMSC in the network. The same filter design as in steps 8-24 can be used by substituting the proper pointcode everywhere the value “13184” appears.

Choose counter and trigger values to suit the anticipated traffic situations and desired measurement time periods (as in steps 25-33). Select an appropriate condition to alert for absense of roaming traffic, to create a warning message and to set up a refresh time (steps 35-36).

NOTE: It is good practice to make a trial run using very short measurement time settings to confirm the configuration. This will ensure that roaming traffic is being properly detected before the final tests are run over much longer periods.

Conclusion

We have seen how to configure the Tektronix K1205 Protocol Analyzer to detect and monitor roaming traffic. The step-by-step procedure used pre-recorded sample data to set up the analyzer, edited the setup to suit a specific network configuration and connected the analyzer to monitor live traffic. Test results confirmed the presence of roaming subscribers and documented the amount of roaming traffic that was present during the measurement period.

The K1205 functions used in this example – *filters, expert mode, triggers* and *statistics* – are powerful general purpose tools for identifying and capturing a wide range of other network load and traffic properties, as well. These same functions are also available in the Tektronix K1297 G20 protocol monitoring application package.

Please direct your comments and questions to mpt.hotline@tek.com or contact us at the Tektronix locations listed on page 8.

Abbreviations

DPC	Destination Point Code
GMSC	Gateway Mobile Switching Center
GSM	Global System for Mobile Communication
HLR	Home Location Register
MAP	Mobile Application Part
MSC	Mobile Switching Center
MTP	Message Transfer Part
OPC	Origination Point Code
SPC	Signaling Point Code
SS#7	Signaling System No. 7
TS	Timeslot

Files used in this example

Recording-file containing MAP traffic: MSC_HLR_MAP_Traffic.rf5

Filter configuration: SendRoutingInfo_13184.flt

Statistics configuration: Roaming_App_Note.sts

File "Roaming_AppNote.zip" can be downloaded here:

http://us-wv-a26.wv.tek.com/CSBU/ITG/Patchwork/Main.fwx in section "K1205"

Contact Tektronix:

ASEAN Countries & Pakistan (65) 6356 3900

Australia & New Zealand (65) 6356 3900

Austria +43 2236 8092 262

Belgium +32 (2) 715 89 70

Brazil & South America 55 (11) 3741-8360

Canada 1 (800) 661-5625

Central Europe & Greece +43 2236 8092 301

Denmark +45 44 850 700

Finland +358 (9) 4783 400

France & North Africa +33 (0) 1 69 86 80 34

Germany +49 (221) 94 77 400

Hong Kong (852) 2585-6688

India (91) 80-2275577

Italy +39 (02) 25086 1

Japan (Sony/Tektronix Corporation) 81 (3) 3448-3111

Mexico, Central America & Caribbean 52 (55) 56666-333

The Netherlands +31 (0) 23 569 5555

Norway +47 22 07 07 00

People's Republic of China 86 (10) 6235 1230

Poland +48 (0) 22 521 53 40

Republic of Korea 82 (2) 528-5299

Russia, CIS & The Baltics +358 (9) 4783 400

South Africa +27 11 254 8360

Spain +34 (91) 372 6055

Sweden +46 8 477 6503/4

Taiwan 886 (2) 2722-9622

United Kingdom & Eire +44 (0) 1344 392400

USA 1 (800) 426-2200

For other areas contact Tektronix, Inc. at: 1 (503) 627-7111

Updated 8 February 2002

For Further Information

Tektronix maintains a comprehensive, constantly expanding collection of application notes, technical briefs and other resources to help engineers working on the cutting edge of technology. Please visit **www.tektronix.com**

2FW-15386-0

Tektronix
Enabling Innovation