ROHDE&SCHWARZ

Test and Measurement
Division

User Guide

Application Testing with the R&S® CMU200

1204.5040.52-01

February 2006

Printed in Germany

Contents

1 Introduction

Rohde & Schwarz test instruments are well established in the field of radio communication and protocol testing, but some customers have identified the additional need for testing the actual data functions and applications of mobile phones under clearly defined, and reliably reproduceable, conditions. In essence, emerging technologies have demanded a broadening of the testing focus, as applications are increasingly integrated into mobile devices.

The solution here described facilitates Application Testing on a network simulation of (E)GPRS, CDMA2000, or WCDMA, and requires the relevant options for the R&S CMU200. It also relies on a group of software packages, whose installation and configuration are described in this document.

For all three network options, installation of the Application Test Environment (ATE) software makes available various application enablers and testcases: for example, an MMS server, with which sending and receiving MMS messages can be tested.

Although the option of a live internet connection is supported for each of the network simulations, this document describes a test setup which, instead, uses a "Server PC" to provide the various required services within the simulated network.

In the chapters that follow, some familiarity with IP addressing and TCP Ports is assumed, but an overview of these topics is provided in Appendix A.

General guidelines are given for the whole process, from installation through to running the actual tests, and more specific guidance is given for some of the required settings (especially those which are less intuitively accessible). However, for fuller coverage, please refer to the relevant document for the product you are using.

Although the current document is particularly directed towards the Universal Radio Communication Tester, i.e. the R&S CMU200, the test procedures it describes apply equally well, overall, to R&S CRTU Protocol Testers that support the same network simulations.

Hardware and Software Requirements

Application Testing is carried out in a special test environment which simulates a radio network and offers access to various IP Data based services (e.g. servers for file and message transfers, and for video streaming). There are specific hardware and software requirements for the R&S CMU and the Server PC, as follows:

R&S CMU200

Network Support	R&S CMU Options
(E)GPRS	R&S CMU-K92
CDMA2000	R&S CMU-B87, R&S CMU-K87
WCDMA	R&S CMU-K96

For full details, please refer to Appendix C - Mandatory R&S CMU200 HW/SW Configuration

Server PC

For Application Testing over (E)GPRS, you must use a PC that has an available Ethernet port (at least 100 Mbps) and is running either Windows XP or Windows 2000.

For Application Testing over WCDMA or CDMA2000, a free Ethernet port (at least 100 Mbps) is required, but no particular platform is necessary, as long as the various IP Data based facilities are supported. Of course, if you wish to install any of the specific IP Data based packages described in this document then the Windows requirement still applies.

Client PC

Application Testing when the phone is being used as a modem needs a Client PC attached to the phone. There are no particular requirements for this PC, except that it can provide the relevant IP Data based support as required.

Configuration

1. A consistent set of IP addresses and TCP Ports is required on the R&S CMU, in the software installed on the Server PC (and Client PC), and in the mobile phone under test. The IP addresses and ports used throughout this document are not mandatory, but if you use different values you are advised to comply with IANA guidelines for non-routable addresses and port numbers.

2. Mobile phones are usually supplied with preset factory settings, typically relating to a particular network operator. During MMS testing, for example, it is important to make sure that the message centre address is changed to that of the MMS server within the test environment.

The configuration steps are described below, but for the mobile phone it is not possible to provide exact instructions: there is no universal manufacturer agreement on naming conventions, or on menu layout. It is common to find significant differences even between different models from the same manufacturer. However, the guidelines that *are* given should be enough to locate and set the relevant values.

General System Arrangement

The layout of equipment and software is largely the same for all of the tests described later, but the exact setup depends on the chosen network environment and whether the mobile phone is being used standalone or as a modem for the Client PC.

The general system arrangement for Application Testing is shown in Figure 1. All tests require a PC to be attached to the R&S CMU, and this is referred to as the "Server PC". A second PC, attached to the phone and called the "Client PC", is needed for tests that just use the phone as a modem, such as the FTP session.
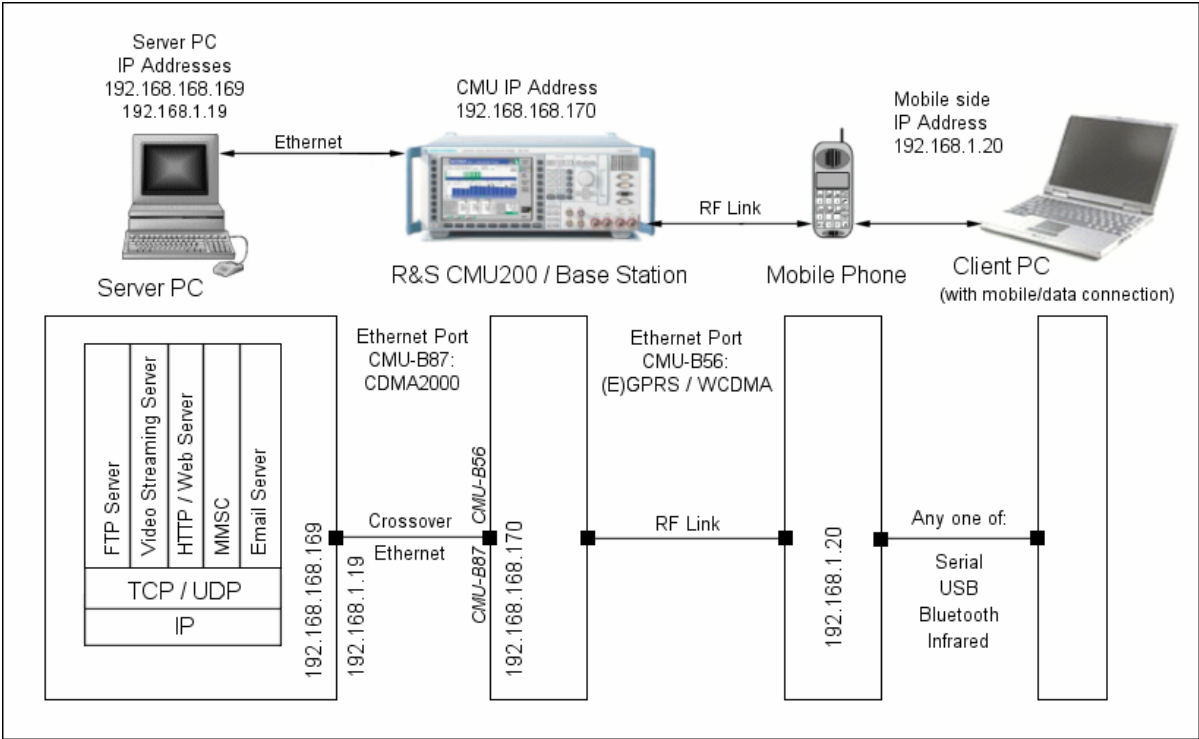
Figure 1 General system arrangement for application testing

2 Connection Configuration and Settings

The following sections describe the steps necessary for correct configuration and setting of connections between the R&S CMU200, Server PC, Mobile Phone and, when required, the Client PC.

Note: The IP Addresses used throughout this document form a consistent set that is recommended for your own test setup, but their use is not mandatory. However, if you choose different IP addresses, it is recommended that you follow IANA guidelines, especially in terms of assigned non-routable addresses (i.e. "private IP addresses").

Server PC - R&S CMU200 Connection

Server PC

(1)   Setup the Ethernet adapter:

On the Server PC, open the *Control Panel*.

Double-click the *Network Connections* Icon.

Double-click the icon for the Ethernet Adapter you will use with the R&S CMU200.

Click on **Properties** Tab.

Double-click on *Internet Protocol (TC/IP)*.

Click the Radio button *Use the following IP Address*.

Enter *192.168.168.169* in the IP address field.

Enter *255.255.0.0* for the Subnet mask.

Click **OK** twice.

Note: the Ethernet card must support speeds of at least 100 Mbps.
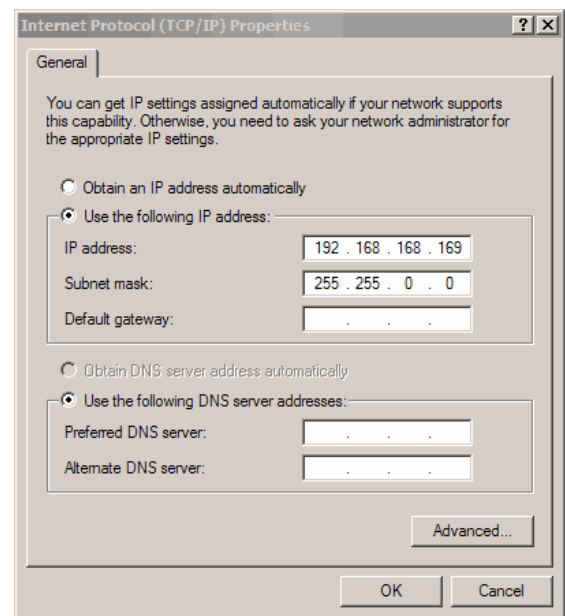
Figure 2 TCP/IP Properties

(2)   *Only for (E)GPRS Application Testing*, a special PC-based software package called the Data Applications Test Suite (DATS) is required. For correct DATS configuration, the following IP addresses have to be set on the Server PC:

Open the file *prostacklink.ini* in the *C:\OPSW\<version>\CR02P2P* folder.

```
[Config]
CMU_IP_ADDRESS=192.168.168.170
WS_IP_ADDRESS=192.168.168.169
IP_PORT=3000
[Log]
ENABLE_LOG=0
```

Note: In addition to setting the IP addresses, make sure that the Port number is set to 3000.

(3)   *Only for (E)GPRS Application Testing*, configure the IP addresses for incoming connections:

Open **Network Connections**.

Click *Incoming Connections*.

On the Networking tab, under **This connection uses the following items**, click *Internet Protocol (TCP/IP)*,

Click *Properties*.

Select *Allow callers to access my local area network*.

Click *Specify TCP/IP addresses*.

In **From**, type the starting IP address.

In **To**, type the ending IP address.

Select *Allow calling computer to specify its own IP address*.
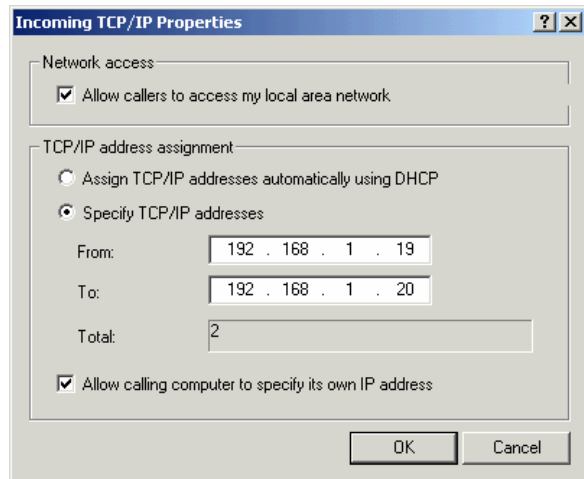
Figure 3 Configure incoming connections

R&S CMU200

IP addresses are set in the R&S CMU as follows:

(a) (E)GPRS

Press **Setup** key on the front panel.

Press **TCP/IP** tab.

Select the *CMU-B21* and expand item.

Set the IP address to *192.168.168.170*. This is the IP address for the link handler R&S CMU-B21.

Set Subnet Mask to *255.255.0.0.*

Set Default Gateway to *192.168.0.1*. This is the IP address for the Ethernet network adapter on the Server PC.

Figure 4 Set IP Addresses for R&S CMU

Press **Connect/Control** tab.

Press **1-2** tab.

Press **Misc** tab.

Set IP Address Server PC to *192.168.168.169.*

Press **1-2 tab** to return to connection screen.

Figure 5 Set IP Address for Server PC

(b) WCDMA

Press **Setup** key on the front panel.
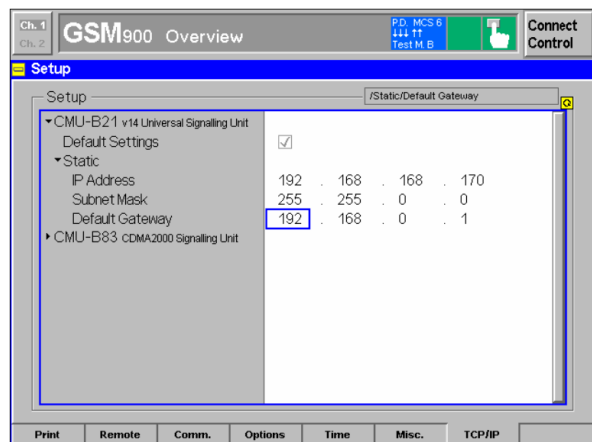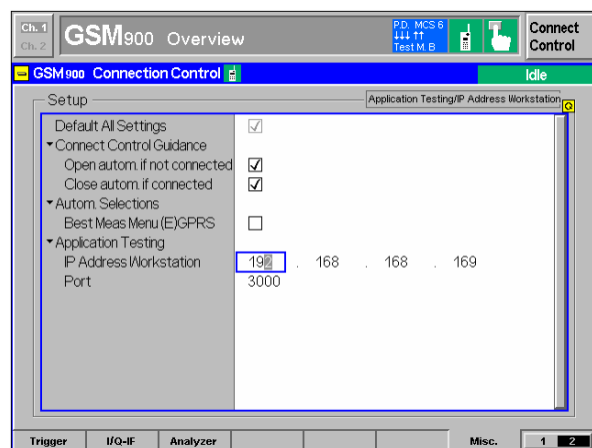
Press **TCP/IP** tab.

Select the **CMU-B21** and expand item.

Set the IP address to *192.168.168.170*. This is the IP address for the link handler R&S CMU-B21.

Set Subnet Mask to *255.255.0.0.*

Set Default Gateway to *192.168.0.1*. This is the IP address for the Ethernet network adapter on the Server PC.
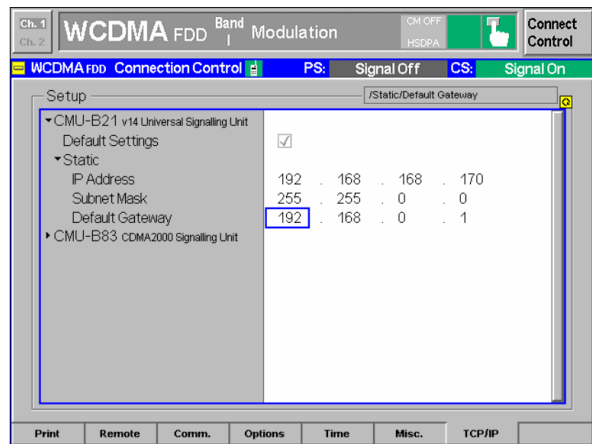
Figure 6 Set IP Addresses for R&S CMU

Set the IP address for the Mobile Phone:

Press *1-2* tab.

Press *Misc* tab.

Enter the *Virtual IP address.*

The default is *192.168.1.19.*

Enter the *UE IP address*. This is the Mobile Phone address during the PPP connection.

The default is *192.168.1.20.*

Press *1-2* tab.
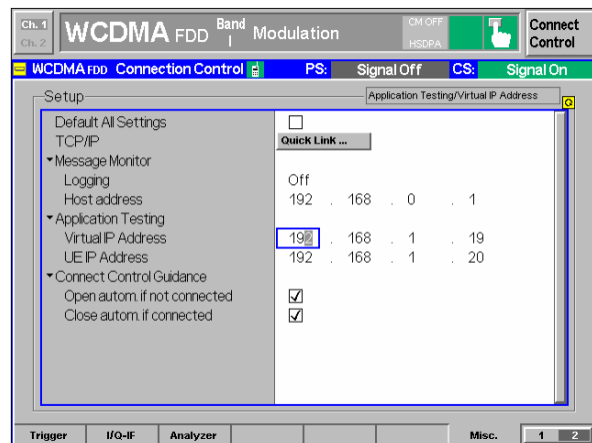
Figure 7 Set IP address for mobile phone

(c) CDMA2000

Press **SETUP** key on front panel.

Press *TCP/IP* tab.

Expand the R&S CMU-B83 *CDMA2000 signaling unit* item.

Expand *Static* item.

Enter **192.168.168.170** for *IP Address*. This is the IP address of the R&S CMU during the packet data connection.

Enter Subnet Mask: **255.255.0.0.**

Enter *Default Gateway* Address **192.168.0.1.** This is the address of the Server PC.

Press *Escape* and then *Connect Control* tab.

Figure 8 Set IP address for R&S CMU and Server PC

Now the setting for the Mobile Phone:

Scroll down and expand **Protocol** item.

Expand **Mobile IP** item.

Set **Mobile Node Home IP Addr** to *192.168.0.10*.
This is the IP address allocated to the phone during
the packet data session.

Scroll Down and expand PPP item.

Expand **IP Address** item.

Expand **Static** item.

Set **MS PPP IP Address** to *192.168.1.20.*

Set **BS PPP IP Address** to *192.168.1.19.*
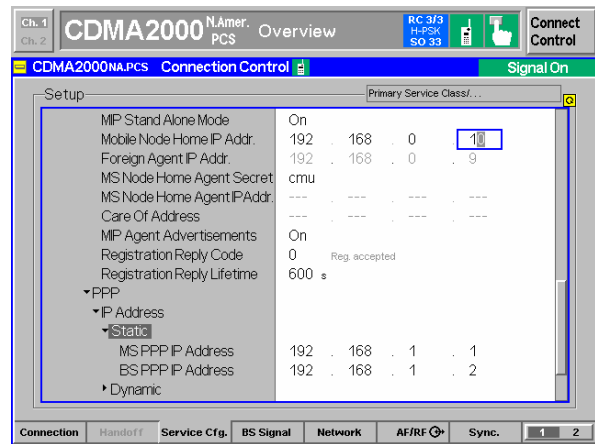
Figure 9 Set IP address for mobile phone

Connection Check

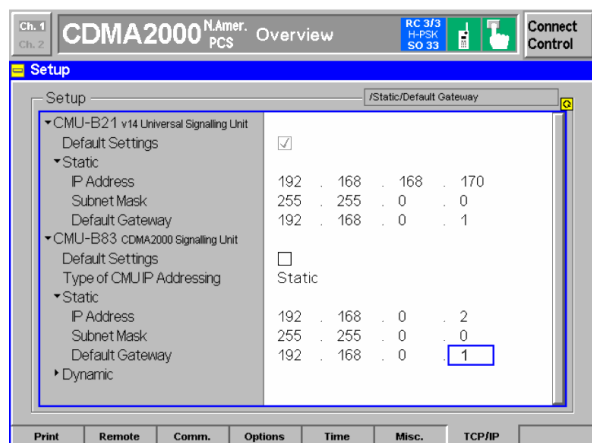With all settings made for the connection between Server PC and R&S CMU, we can now check that
the connection works:

First make the physical connection between the R&S CMU and the Server PC using a crossover
Ethernet cable (Cat 5/RJ-45). Note that the R&S CMU has two Ethernet ports:

  a) The upper port is labeled Ethernet B-87 and should be used for CDMA2000

  b) The lower port is labeled Ethernet B-56 and should be used for (E)GPRS and WCDMA.

Open a Command Prompt window (**Start|Run|cmd**) and type: `ping 192.168.168.170`   **<Enter>**

If the two devices are properly connected, the system confirms a response from the R&S CMU and
reports the time taken for the "round trip". If there is a problem with the physical connection, you will see
a message that the Ping has timed out. If the IP address setup is wrong, the system reports that the
Host cannot be found.

Ping is a very useful command, and perhaps the easiest way to confirm "mutual reachability" across a
connection. For details of the command options, type "`ping /?`".

R&S CMU200 - Mobile Phone Connection

(E)GPRS

Press **Menu Select** on the R&S CMU front panel.

Scroll Down and select *GSM Mobile Station.*

Expand the GSM application and select (for example) the *GSM900* function group.

Launch the application.

Note: Make sure the selected GSM band is correct for the phone you are using.
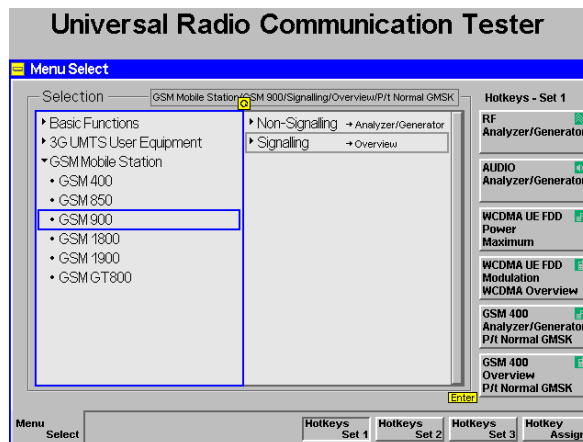
Figure 10 Setup GSM application

Configure the AF/RF settings as follows:

Press **RF Output** and select the RF port.

Press **Ext. Att. Output** and enter the compensation.

Press **RF Input** and select the RF port.

Press **Ext Att Input** and enter the compensation.

RF Connection Check:

With settings completed, we now check the RF connection (see section 0).

Figure 11 Configure AF/RF settings

WCDMA

Set the frequency band and RF parameters:

Press the *Band Select* tab.

Select the band in which the mobile operates.

Press *RF Chn Downlink* or *Uplink Chn* tab and set the channel or the corresponding frequency.

Set the correct levels for Uplink and Downlink power.

Figure 12 Set frequency band and RF parameters

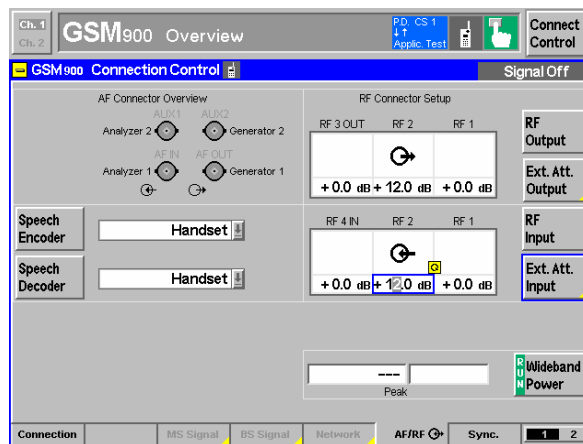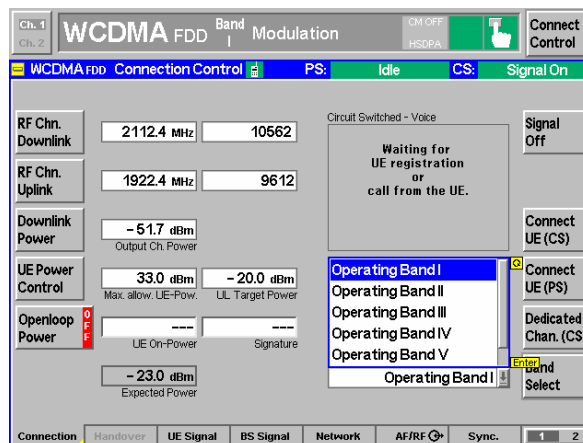Configure the RF Path:

Press the *AF/RF* tab.

Press *RF Ouput* and select the RF Outport port.

Press *Ext Att Output* and enter a compensation value in dB.

Repeat this process for the RF Input port.

RF Connection Check:

The band and RF settings are now complete, so we check the RF connection (see section 0).
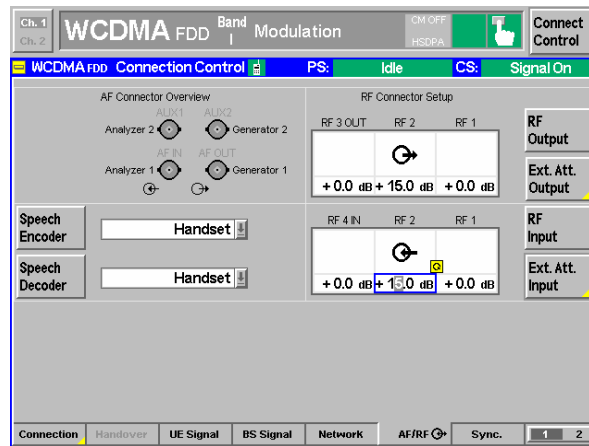
Figure 13 Configure the RF path

CDMA2000

Press **Menu select**.

Select the **IMT2000 Mobile Station** function group.

Select the **CDMA2000 PCS** frequency band.

Select **Signaling –> Overview** mode.

Press the knob to start CDMA2000 PCS mode.

RF Connection Check:

These settings are now complete, so we check the RF connection (see section 0).
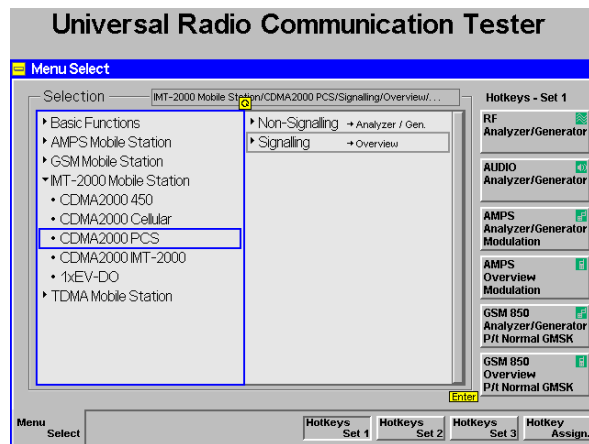
Figure 14 Configure the CDMA2000 settings

R&S CMU - Mobile Phone RF Connection Check

Run a simple test to confirm that the RF connection between R&S CMU and phone is working correctly:

Set up a link between the R&S CMU and the mobile phone by means of a simple RF measurement, with the settings just entered for frequency and power level, and additional channel configuration and coding.

Mobile Phone - Client PC

For Application Testing when the mobile is being used simply as a modem, a second PC is included in the setup. This is termed the "Client PC" and is attached to the mobile phone.

Mobile Phone

Arrange a suitable connection between the mobile phone and the Client PC: a serial cable link, or a connection that uses either Bluetooth or infra-red. Consult the phone's operating manual for guidance.

Client PC

The objective in this section is to create dial-up networking on the Client PC. However, before you can do that you must install the relevant driver for the mobile phone to which the PC is connected. The software for that, along with instructions for installing it, are usually available for download from the manufacturer's website. Once the relevant driver is installed, you then create the dial-up-networking so you may then setup a packet connection from the Client PC, using the mobile phone as a modem:

Open the **Network Connections** window, click *New Connection Wizard*.
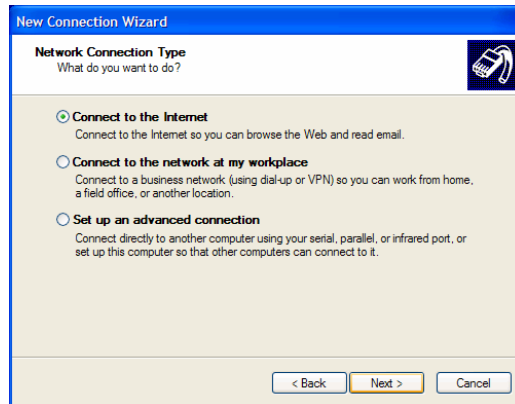
Click *Next* Click *Connect to the Internet*, click *Next.*
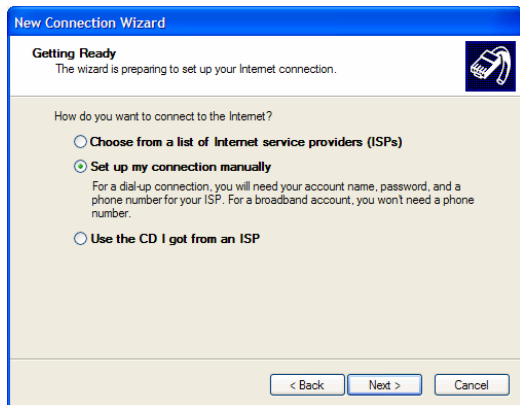
Click *Set up my connection manually*, click *Next.* Click *Connect using dial-up modem*, click *Next*.
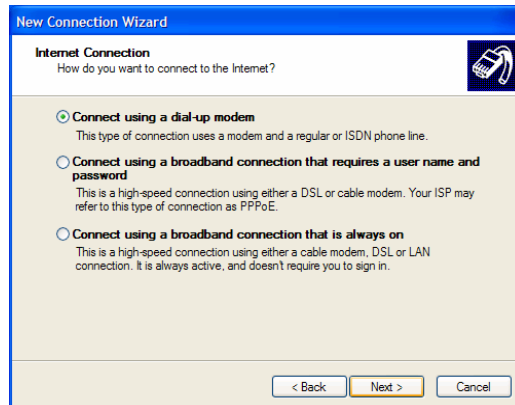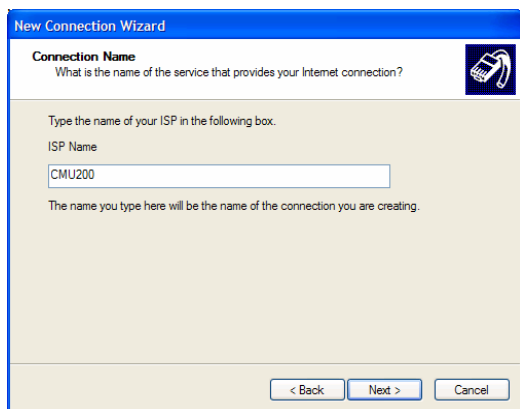
Select the modem for your phone, click *Next.*
Enter *CMU200* as ISP Name, click *Next*.
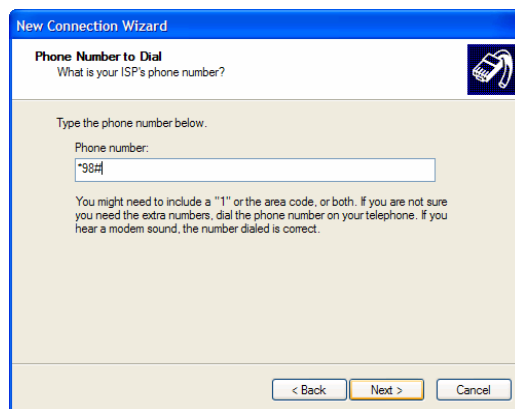
Enter **99#* for WCDMA/(E)GPRS packet data, or *#777* for CDMA2000 packet data, click *Next.*
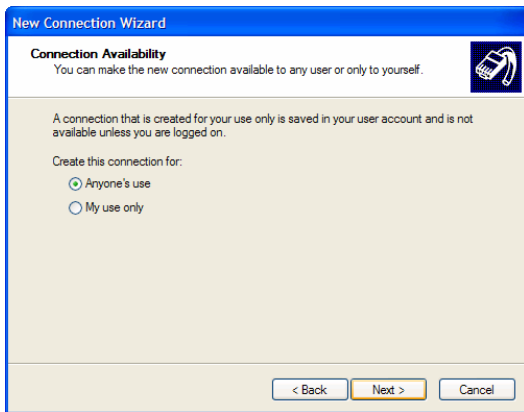
Click the radio button *Anyone's use*, click *Next.*   Enter the *Username* and *Password*, click *Next.*

Click *Finish*.

Wireless Network Card

An alternative to the Clent PC/Phone combination is to use a wireless network card (plugged into the Client PC). A typical setup procedure for installing the software is as follows, but consult the installation documentation that is supplied with the card:.

1.   Insert the installation CD and start the installation procedure.

2.   Follow the installer instructions to complete the software installation.

3.   When prompted to do so, insert the card into the PCMCIA slot on the Client PC.

Note: Do not plug in the card before you start the installation.

3   Service Installation and Configuration

Web Server Lite

From the R&S CMU-K92/R&S CMU-K96 installation CD copy the contents of Freeware\HTTP_Server to the folder C:\HTTP_Server on the Server PC (the default web page and some images for download are included).

The software can also be downloaded from the Gloris CMU Customer Web.

On the desktop, create a shortcut to WebServerLite.exe.

On the Server PC, ensure that the file Index.html is in the folder C:\http_server. This is the default page that will be downloaded to the mobile phone when the packet connection is established via the phone's browser.

Copy into the C:\http_server folder any other files that you want to use for your Web session.

Video Streaming Server

A video streaming server allows you to stream media to clients across the Internet using the industry standard RTP and RTSP protocols. Darwin Streaming Server (DSS) is the open source version of Apple's QuickTime Streaming Server, and can be downloaded from:

http://developer.apple.com/darwin/projects/streaming.

Download the files and follow the installation instructions.

The following sample movies, in 3gp format, are available on the installation CD, and can also be downloaded from the Gloris CMU Customer Web:

> RS1-50kbps.3gp
>
> RS2-50kbps.3gp
>
> RS2-100kbps.3gp

Copy the sample movies into the folder ***c:\Program Files\Darwin Streaming Server\Movies***.

The files can be viewed with any suitable media player/viewer, such as Quicktime from Apple (http://www.apple.com/quicktime/download/win.html).

Configure the DSS Service

By default, DSS is installed to start automatically when the computer boots. If you prefer manual starting, configure the service as follows, with reference to Figure 15:

(1)   Open the Control Panel and double-click ***Administrative Tools***.

(2)   Double-click ***Services*** for a list of all installed services.

(3)   Double-click ***Darwin Streaming Server*** to display the DSS Properties screen.

(4)   Click on the down-arrow in "Startup type" and then click ***Manual***.

(5)   Click ***OK***.
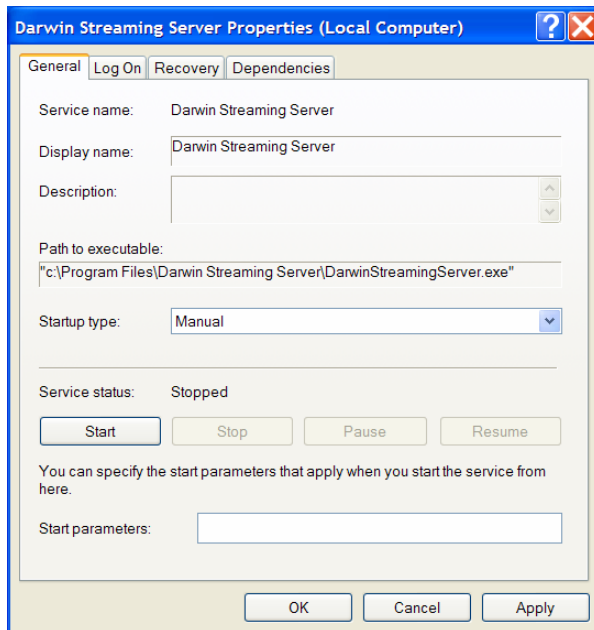
Figure 15 Properties page for DSS

FTP Server

An FTP server is supplied in the folder "Freeware" on the CD for K92 and K96, and can also be downloaded from the [Gloris](#) CMU Customer Web.

Copy the program file, Ftpserv.exe, to folder **c:\FTP_Server**. For easy startup later, create a shortcut to Ftpserve.exe on the Server PC desktop.

MMS

Server PC

MMS support is provided as an extension (R&S CRTU-AA01) of ATE: the Application Test Environment software package (R&S CRTU-AP01). You first do a base installation of R&S CRTU-AP01, and then install R&S CRTU-AA01. For detailed information on installation the ATE Desktop software and the MMS plug-in, please refer to the following Manuals:

1204.0003.02   Application Test Environment   R&S CRTU-AP01

1166.0958.02   Application Test Environment   R&S CRTU-AA01

Preconditions for ATE installation: note that a hardware "Dongle" and software licensing are required for access to the full range of features of the software.

The MMS server, combined with the MMS composer/viewer enables the user to parse, compose, edit, send and receive Multimedia Messages.

The MMS server communicates directly with the mobile phone over the defined (OMA) MMS Interface.

After installing R&S CRTU-AA01, the MMS icon and window are available in the ATE Desktop as shown below, in Figure 16:
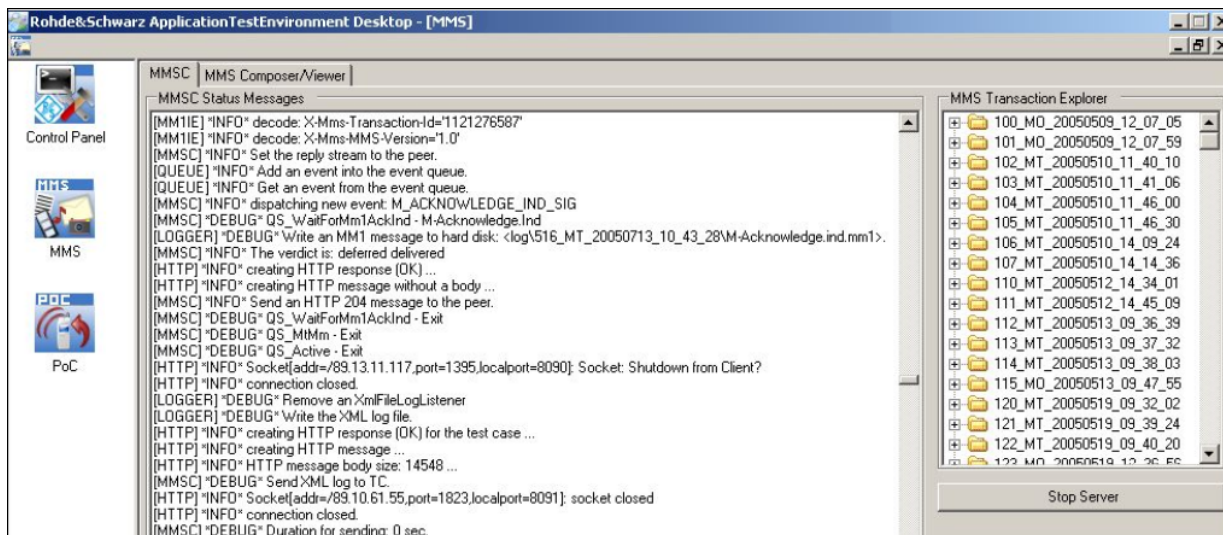
Figure 16 MMS on the ATE Desktop

The "Serving Scenario" IP address has to match the IP address assigned in the network simulation, i.e. to the Server PC (192.168.168.169). The Port for the Serving Scenario must be 8080. These values are configured as follows:

(1)   Double-click the Control Panel icon on the ATE Desktop.

(2)   Click the Configuration tab, and expand the left hand column (+).

(3)   Click **MMSC** to open the configuration parameters pane.

(4)   Double-click the parameter you wish to change.

(5)   The parameter dialogue box is displayed, as in Figure 17:
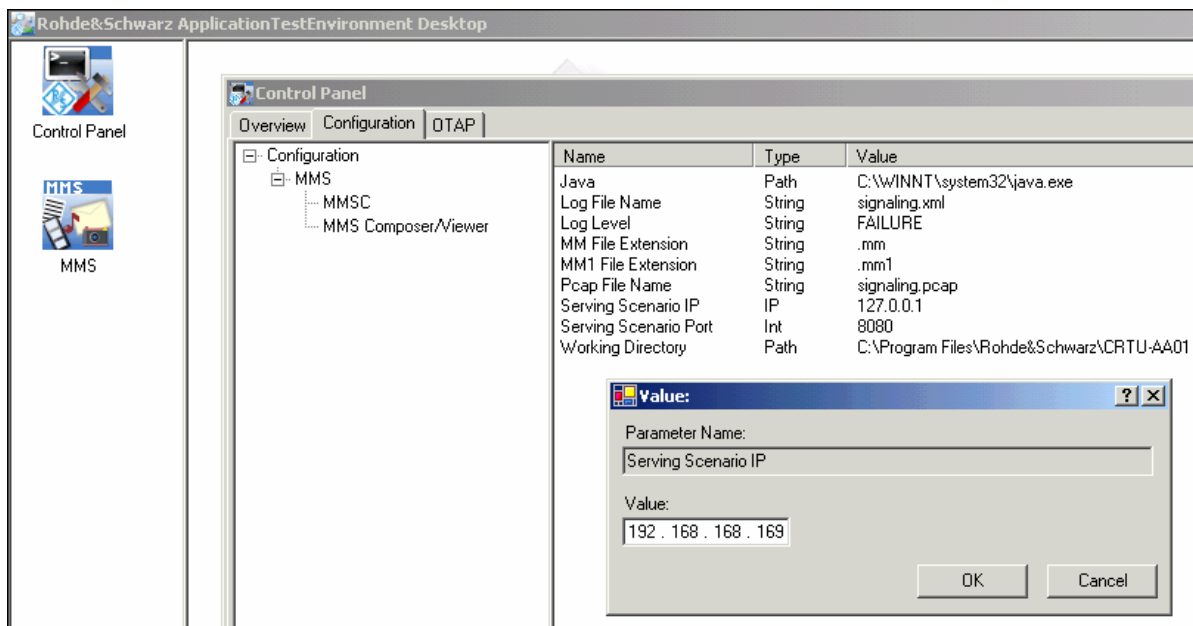
Figure 17 MMSC Configuration

```
WebServerLite.ini - Notepad
File  Edit  Format  Help
[General]
Directories=2
Port=8080
DNSLookup=0
ThreadPoolSize=10

[Dir0]
Alias=/
Path=c:\GD03_INET
DefaultFile=index.html
DirectoryListing=0
Writable=0
Script=0

[Dir1]
Alias=/scripts
Path=c:\GD03_INET\scripts
DirectoryListing=0
Writable=0
Script=1
```

Figure 18 Webserver Lite configuration (.ini file)

Open the file WebServerLite.ini, as in Figure 18, and change the port number from 80 to 8080 (this is the port on which the webserver listens for requests).

Mobile Phone

There are several settings in the mobile phone which are only used by that phone's MMS client, and some of these will be set to factory defaults (usually relating to a network operator). For connection to the n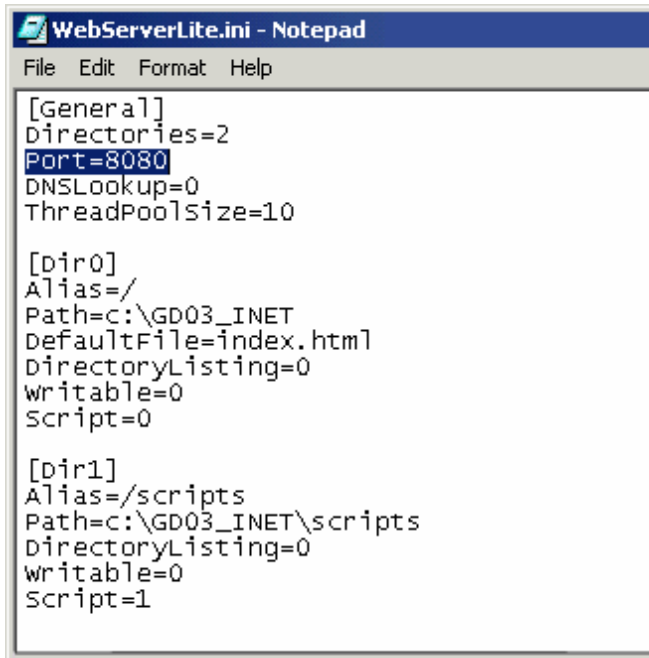etwork simulation, some of these values are ignored, and could even be left blank. However, many phones will not even try to connect without these settings, so they still must be set. There is no agreement between manufacturers on naming and location, so it is advisable to follow the relevant phone's user guide for finding and setting them, as well as following the guidelines given below.

Setting MMSC Parameters

The one setting which *must* be located and reset is the address for the Multimedia Message Service Center (MMSC). Typically, this will be preset to the MMSC of a network operator but we must tell the phone that MMS messages are to be routed through the MMSC in the network simulation. If it's location is not clear from the phone user guide, then start your search by looking for menu paths such as:

Settings>Messages>MMS>Service Center Address

Settings>Message Settings>Multimedia Messages >Homepage

Messages>Settings>MMS>Edit Active Settings >Homepage (or Service Center Address)

At the end of the correct path to the MMSC we are looking for a web page name (or IP address), probably with a Port number appended to it. This must be changed to the address for the MMSC in the ATE and the correct port, i.e. ***http://192.168.168.169:8090*** (or whatever IP address you have set for the Server PC, plus the MMS port number).

In addition, the following are recommended settings but, as above, it is not possible to predict the exact parameter name and menu location, as these vary from one manufacturer to another (even between different models from the same manufacturer):

Access Point: Ignored by ATE MMSC. Use a meaningful string for this context (e.g. R&S CMU200).

Retrieval Mode: Choose "Immediate".

Creation Mode: Choose "restricted" or "basic" (allows only core contetnt, with size restrictions).

Image/Message Size (restriction): Choose "None".

Expiry/Validity: Ignored by the ATE MMSC, but choose the value for maximum validity.

Requesting Reports (Delivery and Read): Switch off this option.

Deny Reports: Controls whether Read reports are sent. Enable report sending.

Anonymous Messages: Allow.

Adverts: Allow.

(These settings are fully described in the Software Manual for R&S CRTU-AA01, 1166.0958.02)

Over the Air Provisioning (OATP)

If your mobile phone supports OATP, then you have an easier way to set up the MMS parameters (using SMS), without having to search the phone menus. Open the ATE Control Panel and click the OTAP tab. This opens the OTAP pane for entering the MMS parameters, as can be seen in Figure 19, but you first have to set the message format (most mobile phones are OMA, but there is also SEN).
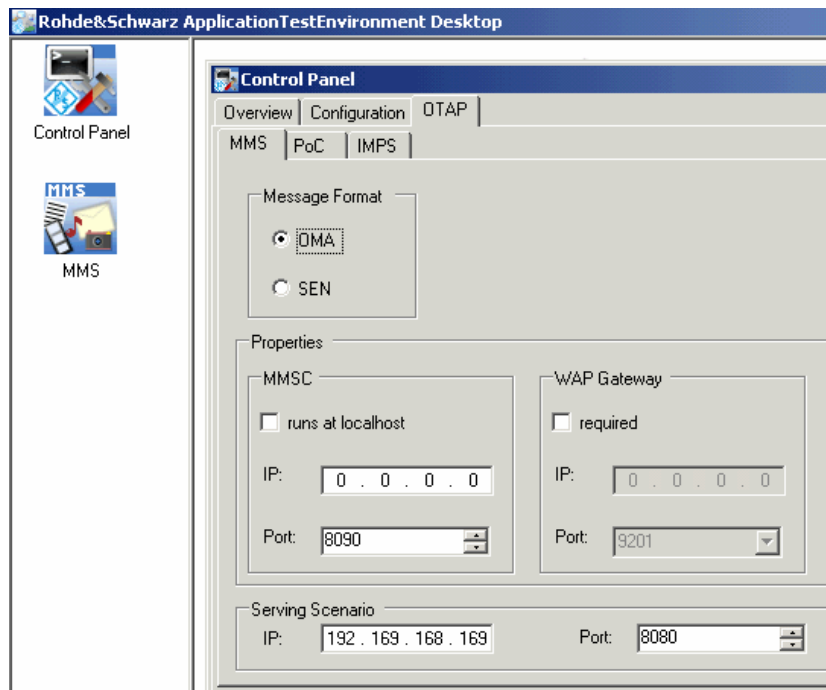
Once you have a link established to the mobile phone, do the following:

Enter the parameter values.

Click *Send* to send the SMS to the phone.

Normally, on receipt of the SMS, you have to confirm receipt, and may also need to *activate* the new parameters before they take effect.

Figure 19 Parameter entry for OATP

Email

This section describes how to configure the **Mercury** mail server, which is a Freeware download from the Pegasus mail site www.pmail.com (version 3.32 was used in the preparation of this document).

Installing the Mercury Mail server

The Mercury mail server supports the POP3 and SMTP protocols, among others, and has the ability to send, receive, store, and forward electronic mail from large numbers of clients.

Note: R&S disclaims any responsibility or liability for the above mentioned information. R&S makes no representation or warranty whatsoever as regards the existence, functionality or contents of the links or any relevant application.

The mail server is installed from the self-extracting executable in which it is distributed, as follows:

1. Double-click the downloaded *Setup.exe*.
2. Click *New Installation*.
3. Click *No NetWare Support*.
4. Accept the default directory path (C:\Mercury) and click *OK*.
5. Click *No Pegasus Mail integration*.
6. Accept the default directory path (C:\Mercury\mail) for mailbox directory and Click *OK*.
7. Select *MercuryS – SMTP Server Module* and "*Mercury – POP3 Server Module*, Click *OK*.
8. Click *Install no SMTP client*
9. Enter the dummy domain name *crtu.net* and username *Admin*, Click *OK*.
10. Click *Normal* for the relay control.
11. Enter *C:\MERCURY\QUEUE* for mail queue location, Click *OK*.
12. Click *Install Mercury/32* for installation.
13. Start the Mercury Server and select *Manage local users...* from the Configuration menu.
14. Create a user with Username *DtsUser* and Password *dtspass*.
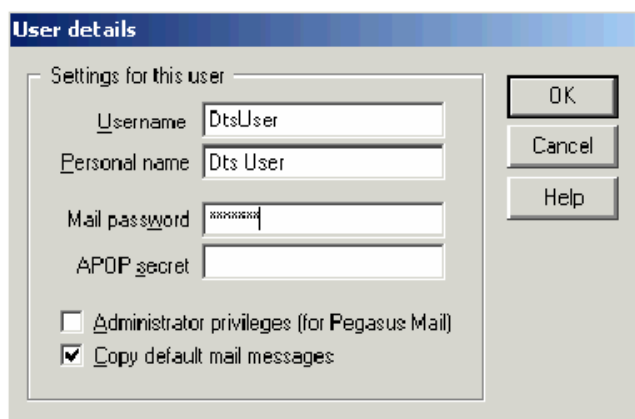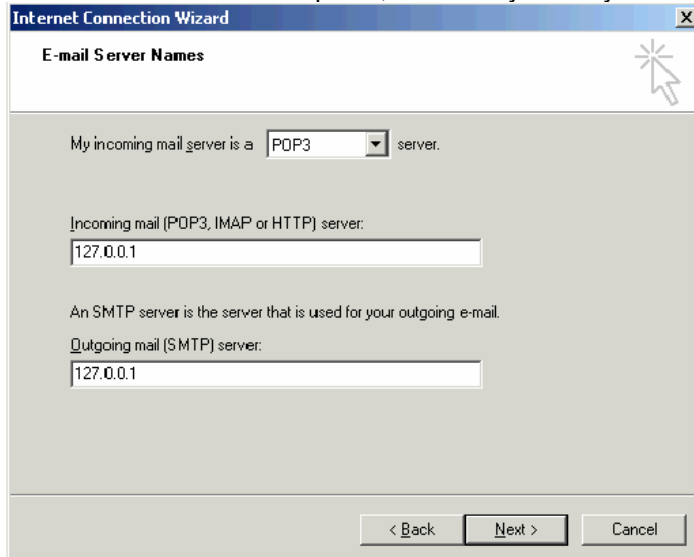15. Create a second user with Username *Testuser* and Password *testpass*.

Figure 20 Adding Users

Configuration of Outlook Express

With Mercury mail server installed, we now need a mail client to send and receive mail. This example uses Microsoft Outlook Express, which may already be installed on the Server PC.

1. Launch Outlook Express.
2. Select **Accounts** from the Tools menu.
3. Click **Add** and select **Mail**.
4. Enter **DtsUser** in Display Name, click **Next**.
5. Enter **DtsUser@crtu.net** in Email address, click **Next**.
6. Enter the E-mail server addresses as in Figure 21 and click **Next**.

On the next screen, enter account name **DtsUser** and password **dtspass**.

Click **Next**.

Figure 21 Setting up the server addresses

Note: The mail account can be tested by clicking on **Send/Receive** in Outlook Express, with the Mercury mail server running. Outlook Express should successfully connect to the server.

Configuring the Mobile Phone

Some settings must be made in the mobile in order to access the E-mail server. These will vary according to the type of mobile and the access method used (Circuit Switched or GPRS).

It will be assumed here that the profile for connecting the mobile using DATS is already established as described earlier. This could, for example, be used to access WAP servers using the connection, though E-mail can be transferred over either a Circuit Switched or GPRS session.

The following settings are those required for correct configuration of the E-mail service on the mobile:

Setting Name	Value
Mailbox Name	DATS
Access Point	An access point set up correctly for DATS (i.e. that used for WAP testing with the DATS)
My mail address	testuser@crtu.net
Outgoing Mail Server	192.168.1.19
User Name	Testuser
Password	testpass
Incoming Mail Server	192.168.1.19
Mailbox Type	POP3
Security	Off

4 Launch Services

Web Server Lite

To start Web Server Lite on the Server PC:

Double-click the Desktop shortcut, or navigate to c:\http_server and double-click ***webserverlite.exe.***

(To stop Webserver Lite, close the windows.)
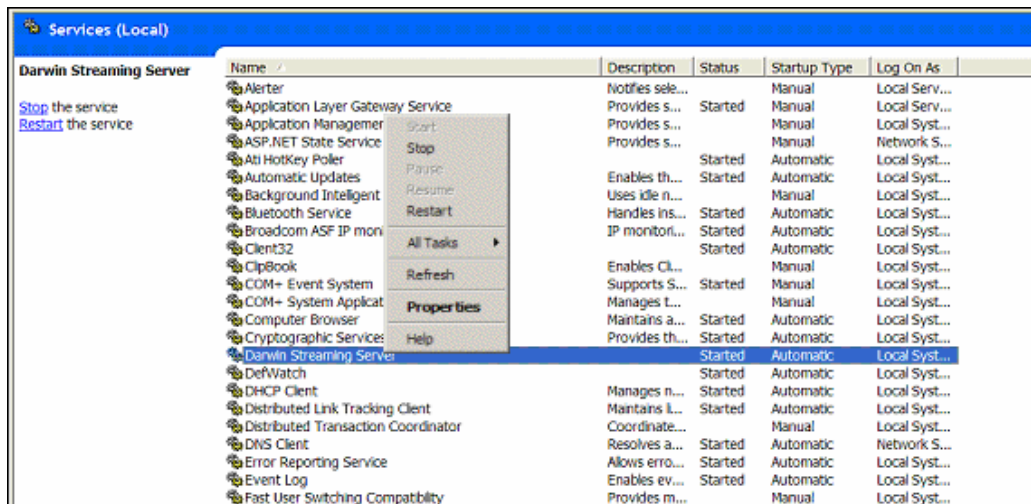
Darwin Streaming Server (DSS)

Figure 22 Starting the Darwin Streaming Server

1. Open the Windows Control Panel and double-click ***Administrative Tools***.

2. Double-click ***Services*** to display the list of available services.

3. Right-click ***Darwin Streaming Server*** to see the command list, as in Figure 22.

4. Click ***Restart*** (or ***Start*** if the service is installed with manual start).

MMS

(1) Double-click the Desktop shortcut, or navigate to c:\GD03_INET and double-click ***webserverlite.exe.***

(2) Start ATE Desktop and select ***MMS***.

(3) Click ***Start Server*** to start the MMS server running.

  The button changes to Stop Server (as in Figure 16).

Note: *the server must be started before any MMS transactions can be performed.*

FTP Server

Either open c:\Ftp_Server and double-click *Ftpserve.exe*, or,

Double-click the *FTP_Server* shortcut on the Server PC Desktop.

The startup screen is displayed, as in Figure 23

Figure 23 FTP Startup
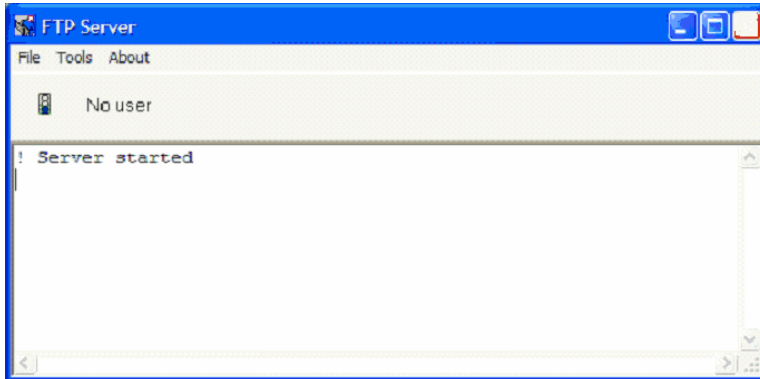
Email

When starting the mail server, DATS should already be running.

Click *Start|(All) Programs|Mercury for win32| Mercury for win32.*

Note that the **Kannel WAP gateway** and **Web Server Lite** need not be started when testing E-mail.

The appropriate signalling mode (Circuit Switched or GPRS) should be selected in the DATS signalling configuration menu before selecting *Run Test*.

5 Link Setup

(E)GPRS

Press *Connection* tab

Press *Network Support* tab

Use knob to select *GSM+EGPRS* and press knob to validate your selection.
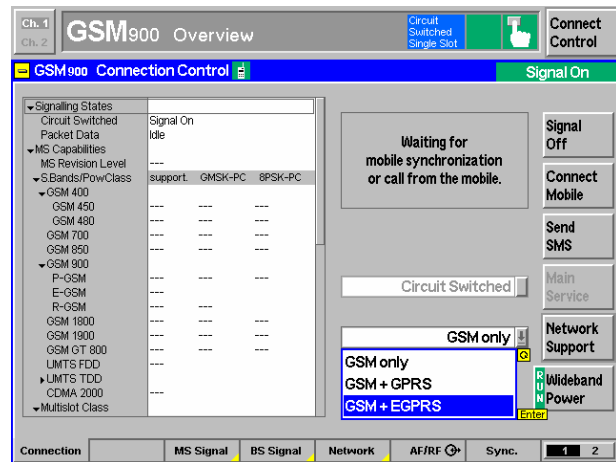

Figure 24 Configure network support
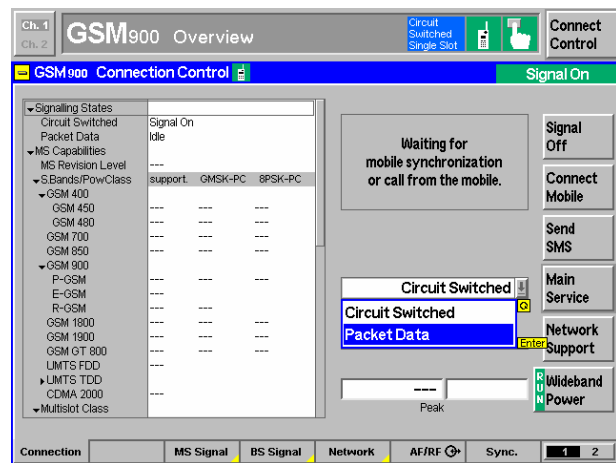
Press *Main Service* tab

Select *Packet Data*

Figure 25 Select packet data

Press *Service Selection* tab

Scroll down in the list box and select *Application Test*.

A yellow box displays the message

Initializing Application Test **Please Wait Approx. 30 Sec.**

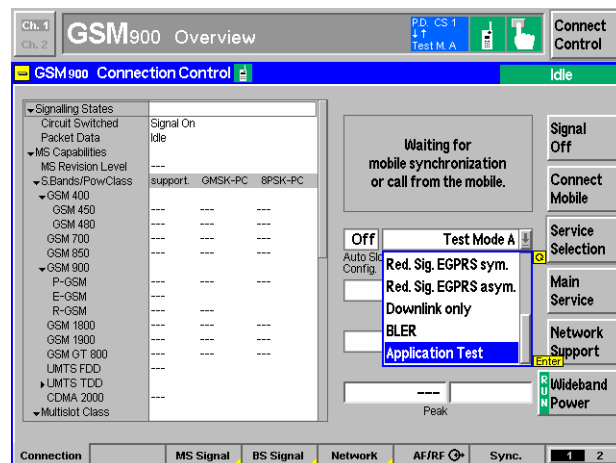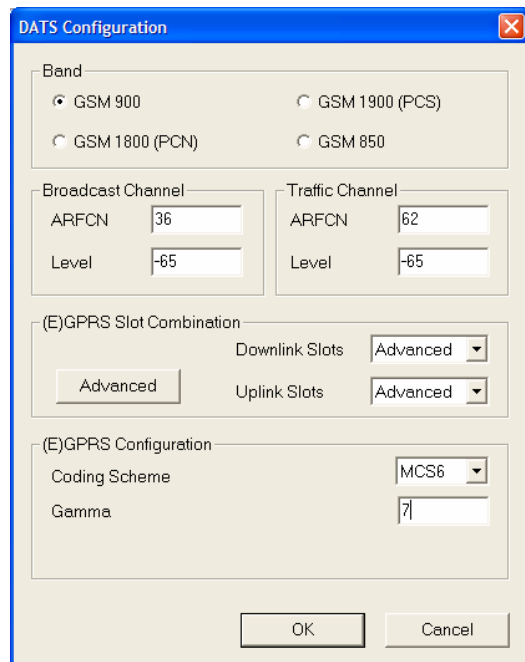The R&S CMU is now ready.

Figure 26 Initialise Application Test

Before starting a packet data session, you must launch and configure the **R&S CRTU-GD03** (DATS) software. On the Server PC desktop, double-click the **CRTU-GD03** icon, click **Test – Configuration – Signaling,** to open the DATS Configuration pane:

Select band (the same band that was previously selected on the R&S CMU**.**

Set the Broadcast Channel:

ARFCN **36**

Level **-65**

Set the Traffic Channel:

ARFCN **62**

Level **-65**

Click **Advanced**.

Set **Multislot Class** to an appropriate value (depends on the phone's multi-shot capability)

Set **Coding Scheme** to **MCS6.**

Set **Gamma** to **7.**

Click .**OK**

Figure 27 DATS configuration

To start the (E)GPRS session, click the Green light icon in the Menu Bar. Ensure that the message "BTS Ready" is displayed:
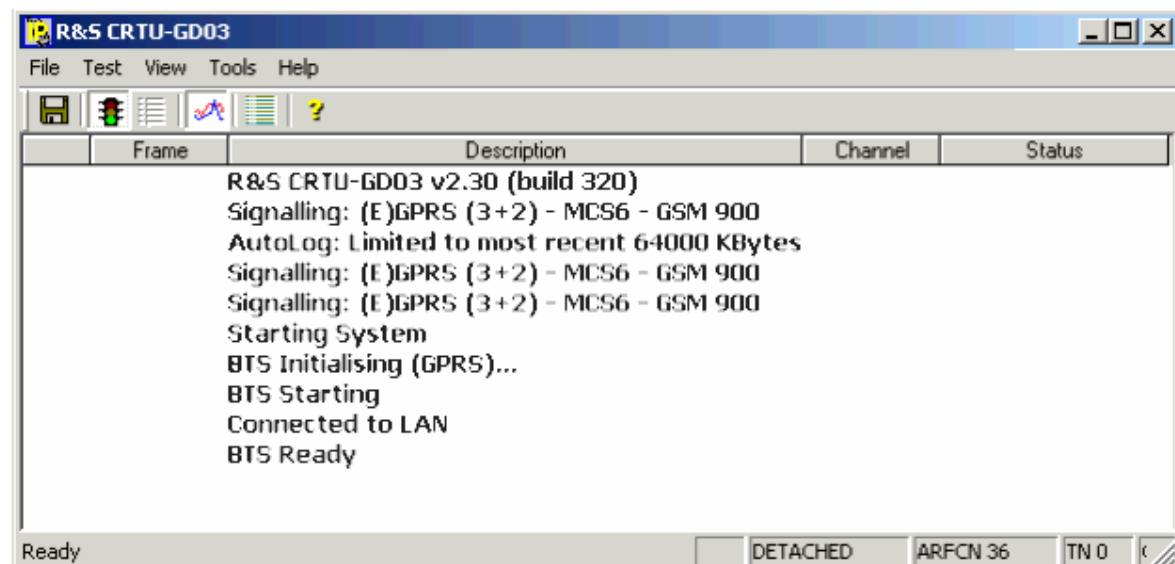
Figure 28 Starting the (E)GPRS session

Finally, switch on the mobile phone and wait for "Attach completed".

WCDMA

Figure 29 Set the data rate
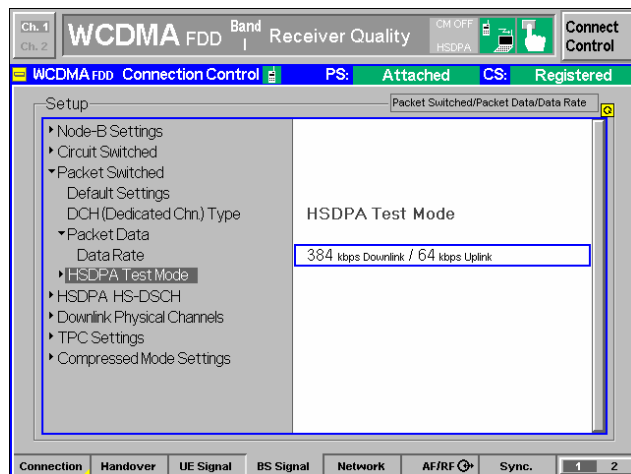
Set the Data Rate:

Press *BS Signal* tab

Expand **Packet Switched** item

Expand **Packet Data**

Set *Data Rate* to:
384 kbps Downlink / 64 kbps Uplink or to
64 Kbps Downlink / 64 kbps Uplink

Figure 30 Set packet data service

Set Packet Data Service:

Press **Network** tab.

Set **Packet Switch Domain** to **On**.

Expand *Requested UE Data* and turn OFF *security* or *authentification* if necessary.

Finally, switch on the mobile phone.

CDMA2000

Figure 31 Launch CDMA2000
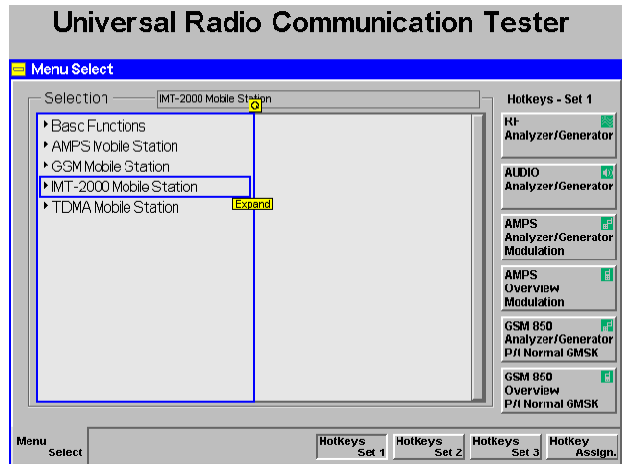
Launch CDMA2000:

Press **Menu select** key to invoke the Main R&S CMU Menu.

Use the down arrow or knob to select the **IMT2000 Mobile Station** function group.

Figure 32 Select frequency band
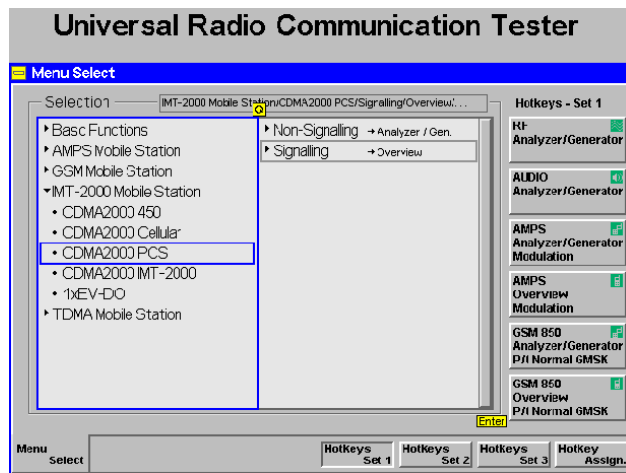
Use the down arrow or knob key to select the desired frequency band, on this occasion **CDMA2000 PCS**.

Use right, up/down arrows and/or knob to select **Signaling –> overview** mode.

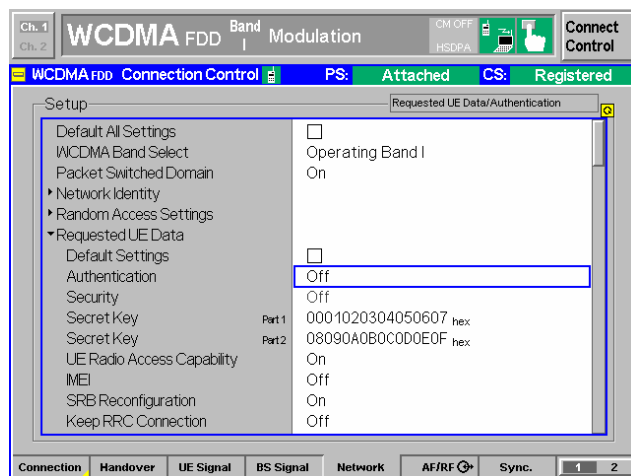
Figure 33 Select packet data service
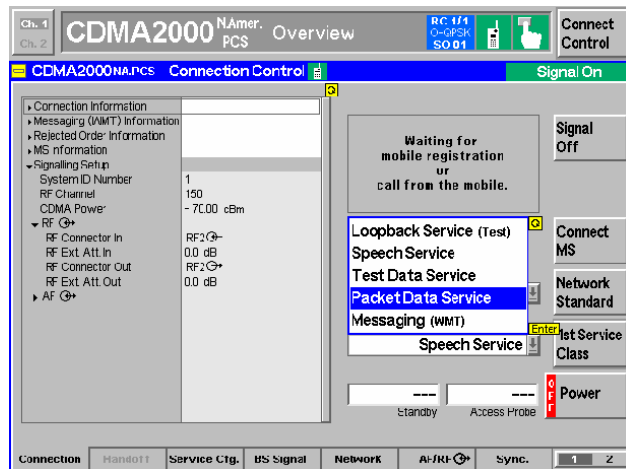
Press the Knob to start the CDMA2000 PCS mode and invoke the Connection Control Menu.

Select Packet Data service:

Press *Connection* tab.

Press *1st Service Class* tab.

Use the knob to navigate and select *Packet Data Service*. (This option will only pop up if the R&S CMU-K87 or K0 option is available).
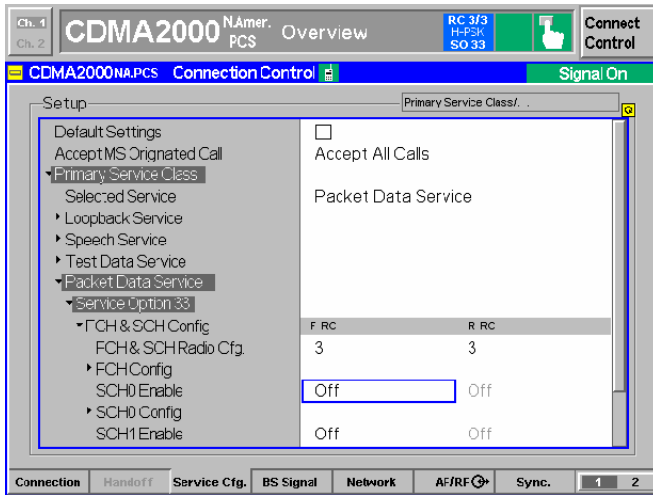
Figure 34 Set up service to packet data service SO

Set up Service to Packet Data Service SO:

Press *Service Cfg*. Tab.

Expand *Packet Data Service* item.

Expand *Service Option33* item.

Expand *FCH & SCH Config* item.

Turn ON *SCH0 Enable.*
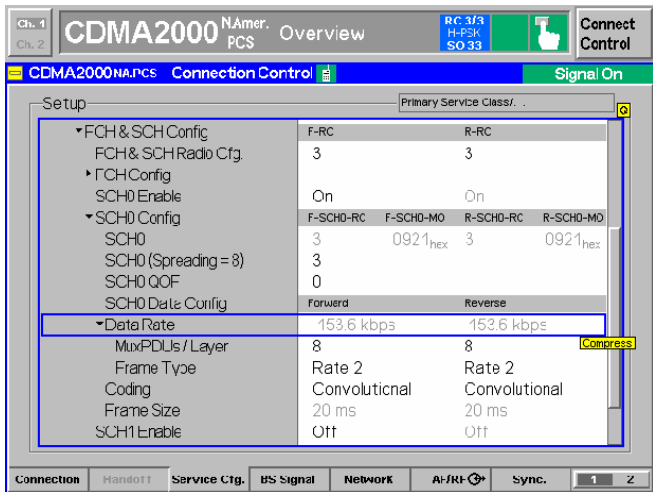
Figure 35 Set up supplementary channel

Set up Supplementary Channel:

Expand *SCH0 Config* item.

Scroll Down to *Data Rate* and expand.

Set *MuxPDUs/Layer* to **8** for *Forward* and *Reverse*.

Set *Frame Type* to *Rate 2* for *Forward* and *Reverse*.

Data Rate should display *153.6 Kbps*.
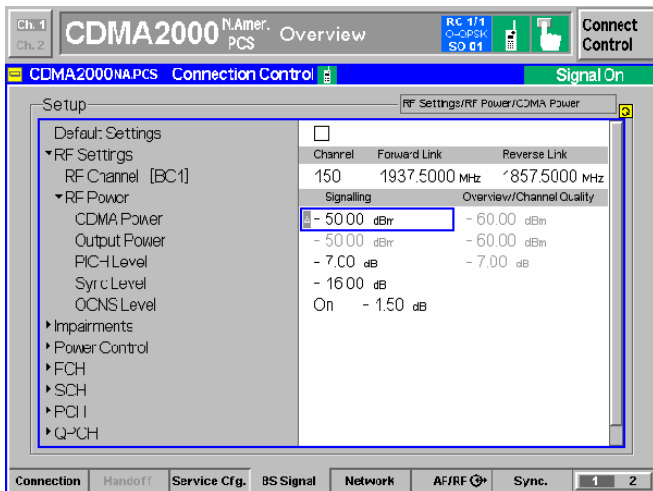
Figure 36 Set up BS signal screen

Set up BS Signal Screen:

Press *BS Signal* tab

Set *RF Channel* to **150**

Set *CDMA Power* to *-50* dBm
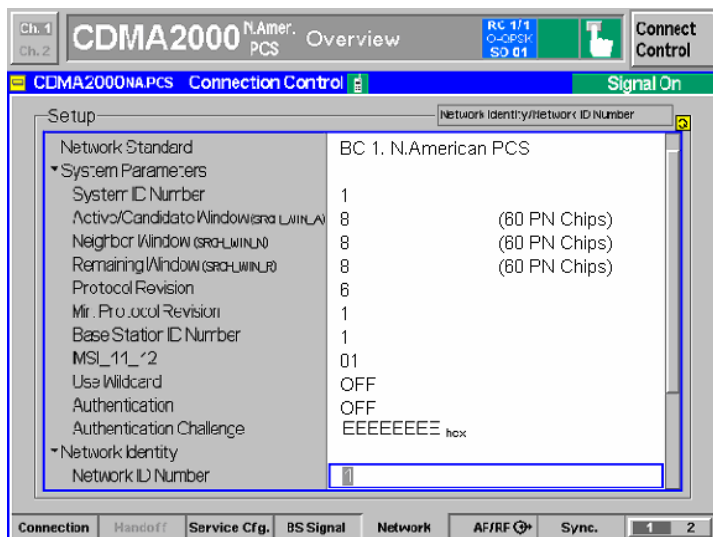
Figure 37 Set network screen

Set Network Screen:

Press *Network* tab.
Expand *System Parameters* item.
Set *System ID Number* to *1.*
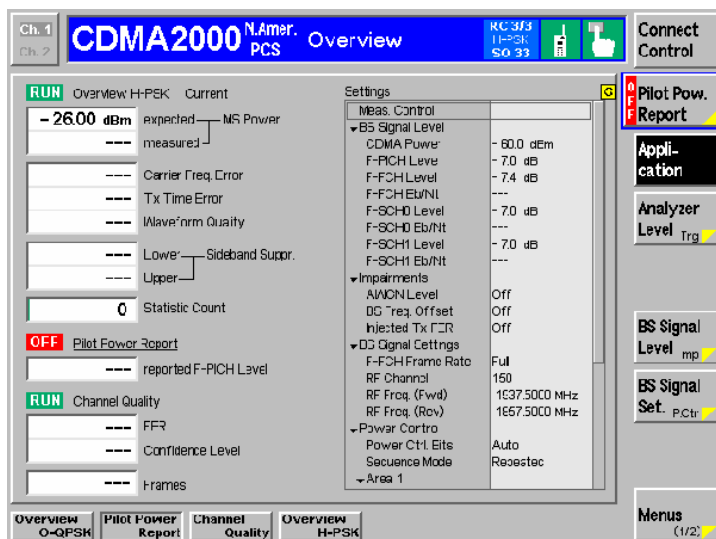
Figure 38 Disable the pilot report

Disable the Pilot Report:

Press **Connnect/Control** tab.
Press **Menus** tab.
Press **Overview** tab.
Press **Application** tab.
Press **Pilot Power** Report tab and Turn Off the measurement.
Press **Connect Control** tab.
Press *Connection* tab.
Expand *MS Information* in the connection Control box.

The R&S CMU is now ready for a packet data call. Switch on the mobile phone.

6 Run the Application Tests

Web serving

First, we download an html page:

In the phone browser, enter the address of the HTML page to be downloaded:

http://192.168.168.169/index.html

The requested page is displayed on the mobile phone.

Now download a graphic file:

In the phone browser, enter the following address:

http://192.168.168.169/picture.gif
The picture is downloaded to the phone and displayed.

Video Streaming

In the phone's browser, enter the following to initiate the video stream:

rtsp://198.168.168.169/RS1-50kbps.3gp

The clip is streamed to the phone and displayed.

MMS

To test the MMS system you can send an MMS from the phone, using the network simulation's IP address as the "phone number" ---- the message will be returned to the phone.

To use any IP address as a phone number, the octets must be expressed in full. So, for example, 192.168.0.2 expands to 192.168.000.002:

Create an MMS message on the phone, perhaps a picture with some text.

For the destination number enter *192168168169* and send the MMS. The phone will announce that the message has been sent, and shortly after (following a "Push" from the network) it will announce that you have a new message: this is, of course, the returning message that you recently sent.

File Transfer (FTP)

Setup dialup networking (WCDMA/EGPRS)
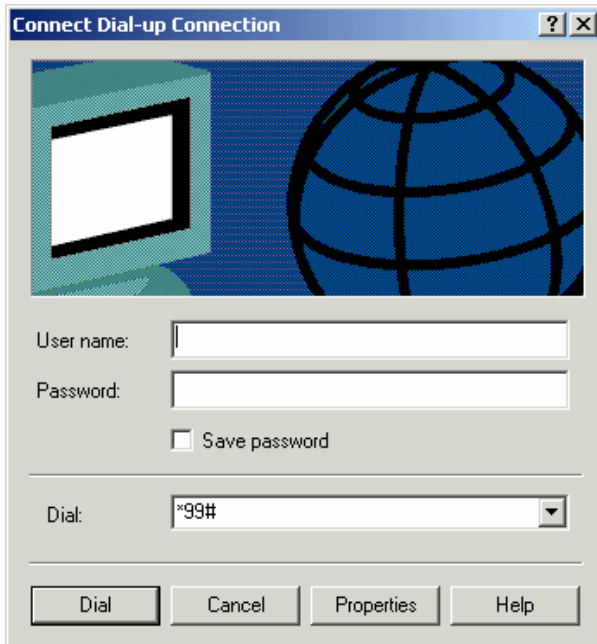
Open the dial-up Networking for your WCDMA/EGPRS phone.

Ensure the number is set to *99#.

Click **Dial**.

Disconnection

To disconnect the packet data call, click the toolbar icon for the connection and when the dialogue pane is displayed, click **Disconnect**.

Figure 39 Dial-up networking

Setup dialup networking (CDMA2000)

Open the Dial-up Networking for the CDMA2000 phone you are using.

Click **Dial**.

Disconnection

To disconnect the packet data call, click the packet connection icon on the toolbar.

Click **Disconnect**.

Figure 40 Dial-up networking

Start modem card

From HyperTerminal on the Client PC, you send AT commands to start the modem:

Start the Modem:

1. Type twice *ATZ <enter>*. Modem is set in Echo mode.
2. Type *AT+CGMM*. Modem type should display as **ATI1.**
3. Type *AT+CFUN?* Test if radio is ON (**+CFUN: 1**) or OFF.(**+CFUN: 0**).
4. If Radio is OFF type the command *AT+CFUN=1 <enter>* and wait until **+CFUN: 1** is displayed.

Attach the Modem:

1. Type *AT+CGATT? <enter>*. The modem will answer **+CGATT: 0** if not attached or **+CGATT: 1** if attached.
2. Type *AT+CGATT=1* to attach the modem, if necessary.

Setup a PDP context:

Type *AT+CGDCONT =1,"IP","","192.168.000.020",0,0*

This is the IP address of the phone given by the PPP adapter during the packet data session.

Setup a packet call:

1. Type the command *AT+CGACT =1,1* to active a PDP context.
2. Type the command *AT+CGACT =0,1* to release the PDP context.

Start FTP session

The FTP server should already be running on the Server PC. If not, double-click the FTP shortcut. Alternatively, navigate to c:\FTP_Server and double-click the program icon ftpserve.exe.

To connect to FTP from the Client PC, open a Command Prompt window (or you can use another suitable tool, such as Total Commander) and type *ftp 192.168.168.169.*

A username and password are not required for the ftp client.

Type *hash* (toggles on and off the printing of a # sign for each data block downloaded).

Type *dir* for a listing of available files.

To download a file, use *get <filename>*, for example: *get map.gif*.

To upload a file, use *put <filename>*, for example: *put cmu_hspda.pdf*.

When you are finished with FTP, type *quit*.

Email

Start the email facility in the mobile phone.

Create an email and send it to dtsuser@crtu.net.

Start Outlook Express on the Server PC.

Click *Send/Receive* to download the email from the mail server.

Reply to the email, or else create a new message and send it to testuser@crtu.net.

Appendix A - Introduction to IP Addressing and Ports

Keywords: IP Address   CIDR   IPv4   IPv6   NAT   PAT   VLSM   DNS

An IP (Internet Protocol) address uniquely identifies every "Host" (or "Node") connection on an IP Network. Perhaps the best example is the Internet itself, a vast network of computers worldwide, where every directly connected node has such a unique address. Today, most people are familiar with Domain Names for websites (www.Rohde-Schwarz.com, for example) but these are simply a user-friendly disguise for an IP Address. Typically, the web browser that is in use (e.g. Internet Explorer, Mozilla Firefox) obtains a translation of the Domain Name into the relevant IP address, transparently to the user (usually by accessing a "DNS Server"). The resulting IP address identifies the access point on the Internet for the particular site.

An IP address is actually a 32-bit binary number, but is most often represented by four groups of numbers, in "dotted decimal" format (e.g. 206.215.49.9). Each "octet" is the decimal value (0 to 255) of an 8-bit binary number, as can be seen here:

Table 5.1   IP Address Format

Binary	11001110	11010111	00110001	00001001
Decimal	206	215	49	9

In the early days of the Internet, it was thought that 2^{32} unique addresses (32-bit binary number = 4,294,967,296) would be plenty enough for every node to be directly connected, each with its own unique IP address. This was quickly disproved (for some time, the Internet has been roughly doubling in size every year), and refinements were required. The first of these was Classless Inter-Domain Routing (CIDR), which makes much better use of the available address range (the original classification makes a lot of the addresses effectively unavailable), but it is not an adequate solution in the longer term. The real solution would seem to be IPv6, which is currently in the process of introduction. With IP addresses extended from 32 to 128 bits it is inconceivable that IPv6 will not be a durable solution.

Although largely phased out in favour of CIDR, the class-based system is a good introduction to IP addressing and is still common in documentation. There are five classes of address defined, with the leading bits of the first octet identifying in which class the address belongs. IP addresses in Classes A, B, and C notionally split into a Network section, and a Host or Node section:

Table 5.2   IP Address Classification

Class of Address	First bit(s)	1st Octet Value	Network Section	Node Section
A	0	1 to 126	First octet	Last three octets
B	10	128 to 191	First two octets	Last two octets
C	110	192 to 223	First three octets	Fourth octet
D	1110	224 to 239	n/a	n/a
E	1111	240 to 255	n/a	n/a

Class A: 126 very large networks, each with a possible 16,777,214 nodes.

Class B: A possible 16,384 "medium-sized" networks, each able to support 65,534 nodes.

Class C: Up to 2,097,152 networks, each with a maximum of 254 nodes.

(Classes D and E are reserved, reducing the range of publicly available IP addresses)

IP Subnet Addressing

There are various reasons for subnetting a network. For example, you may wish to incorporate different types of physical network in an IP network, or achieve more control over network traffic (the latter is especially important in Ethernet networks, where heavy traffic can result in degraded network performance due to multiple collisions).

"Gateways", or "Routers", are used to split the network into smaller sections: i.e. into subnets.

Subnet Masks

A subnet mask allows separate identification of the network and host (node) components of an IP address. A bitwise **AND** applied to the IP address and subnet mask reveals the network address as a result. This is easily seen with the Class-based "self-encoded" or "natural" masks, which are 255.0.0.0 for Class A addresses, 255.255.0.0 for Class B, and 255.255.255.0 for Class C, as illustrated here (for Class B):

10011110	11010101	00010001	00001010	158.213.17.10	IP Address
11111111	11111111	00000000	00000000	255.255.000.000	Subnet Mask

------------------------- bitwise **AND** -------------------------

10011110	11010101	00000000	00000000	158.213.000.000	Network Address

The network can be subnetted further by adding more bits to the self-encoded submask for a particular class. This time, the bitwise **AND** delivers the subnet address, as in this example:

10011110	11010101	00010001	00001010	158.213.17.10	IP Address
11111111	11111111	*1111*0000	00000000	255.255.*24*0.000	Subnet Mask

------------------------- bitwise **AND** -------------------------

10011110	11010101	000*1*0000	00000000	158.213.16.000	Subnet Address

In this case, using a four-bit extension to the subnet mask, there are 16 possible subnets (actually only 14 in non-CIDR addressing, since all 0s and all 1s are not allowed). Each subnet has available over 4000 host addresses (using the 12 rightmost bits of the IP address).

Variable Length Subnet Mask (VLSM)

Whilst the concepts described above largely still apply in CIDR, there is a major difference: the fixed size default subnet mask for each class leads to a potentially large number of unused (and unusable) IP addresses, and this is fixed in CIDR by the Variable Length Subnet Mask (VLSM). This scheme is much more efficient in its allocation of IP addresses, and allows that allocation to be more clearly hierarchical (greatly reducing the amount and complexity of routing information held online worldwide). CIDR uses the VLSM to allocate IP addresses to subnets according to the actual need, rather than by the fixed allocation built in to the Class-based system. In particular, the Network/Host division can be at any of the address bits, and this can be seen in the way network details are now expressed: still with the four octets, but with the addition of a "prefix length" number which identifies how many of the leftmost bits are shared by a given IP address "group" (or alternatively, defines the length of the all 1s section in the subnet mask, and by implication the number of 0s that follow).

IANA issues very large, "short-prefix" CIDR blocks to Regional Internet Registries (RIR): for example, the block 62.0.0.0/8, with over 16 million addresses, was issued to RIPE, the European RIR.

Now consider the IP address 208.130.29.33, which at one time was in use by the www.freesoft.org web server (a single IP address, i.e. a host, where the prefix length is assumed, but strictly speaking it could be expressed as 208.130.29.33/32). Block 208.128.0.0/11 (over 2 million host addresses) was issued to MCI by the North American RIR. MCI then leased an Internet connection to ARS, assigning the 208.130.28.0/22 block (over 1000 addresses), and from this allocation ARS used a /24 block for its publicly accessible servers. One of these 32 possible host addresses was 208.130.29.33.

Network Address Translation and TCP Ports

Detailed knowledge of Network and Port Address Translation is not required for understanding the network simulation by the R&S CMU/ATE combination, but the following overview provides an introduction.

All IP addresses for "public" use have to be unique (in that context). This is guaranteed by the IANA (Internet Assigned Numbers Authority), which is ultimately responsible for IP address allocation. Such unique IP addresses are said to be "registered". Typically, a private network will be a LAN (Local Area Network) with mostly internal traffic between computers on that LAN. In the absence of external traffic, the IP addresses need only be unique internally, and could all be "unregistered" (in practice, there will almost always be devices on the LAN which *do* use registered IP addresses).

Network Address Translation

Using Network Address Translation (NAT), a small group of registered IP addresses (in fact, even just one) can represent on the Internet a whole group of computers inside a private network.

The key to understanding NAT is that each IP packet has a header that initially contains:

Source Address (SA)   the actual IP address of the sending computer

Destination Address (DA)   the (perceived) IP address of the receiving computer

When a LAN member with an Inside Local address (only visible to other LAN members) tries to access a computer on the public network (Outside Global address), its first packet is intercepted by the router, which makes an entry in an Address Translation Table and modifies the packet header accordingly: the original SA (Inside Local address) is mapped to a new SA that is a registered, IANA-assigned "Inside Global" address. The modified packet is forwarded to the destination, which responds to the Inside Global address (not the Inside Local address of the *real* sender). The router now does a reverse lookup in the Address Translation Table and then forwards the response to the computer at the original Inside Local address. The router continues using the table entry for address translation (in both directions) until communication between the two computers ceases. This is shown in Figure 5-1.
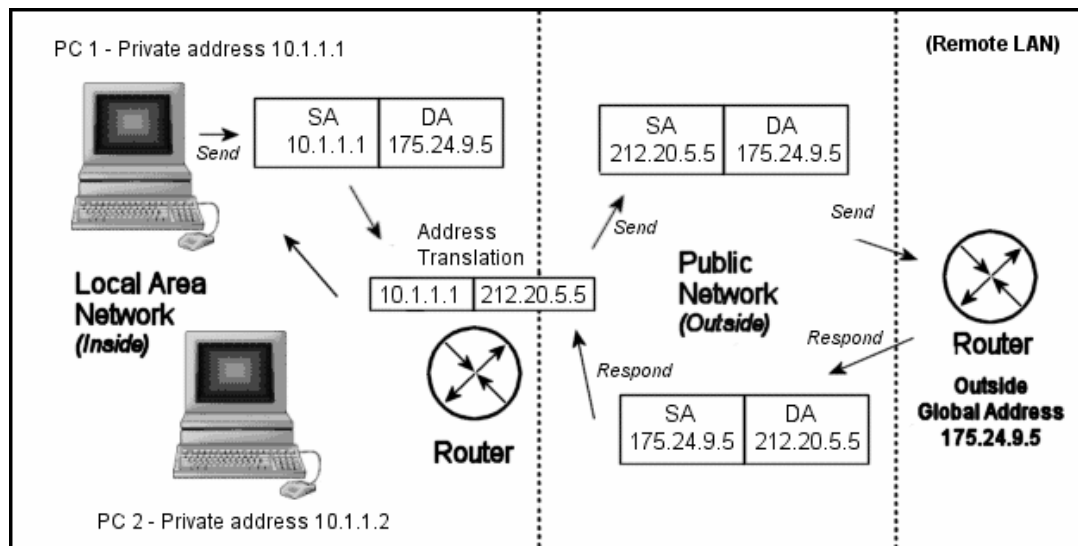
Figure 5-1   Network Address Translation

If Inside Local address 10.1.1.1 *always* translates to Inside Global 212.20.5.5 this is termed **Static NAT** (or sometimes **Inbound Mapping**) and is useful when an "inside" computer needs a lot of access to the public network, especially if it must be accessible *from* the public network.

When the network has a block of registered IP addresses (as is common), then **Dynamic NAT** can be configured. Now, an Inside Local address is mapped to the first available registered IP address from the pool. When the mapping is no longer in use, its translation table entry is removed and the Inside Global address is released back to the pool. This allows a potentially large group of computers inside the LAN to share one or a few Inside Global (registered) addresses, over time.

Port Address Translation

Port Address Translation (PAT), often referred to as "NAT overloading", allows multiple private addresses to be mapped simultaneously to just one or a few external addresses.

With reference to Figure 5-1, the Inside Local addresses for *both* computers shown in the LAN can each be mapped simultaneously to 212.20.5.5, but this requires the addition of internally unique "port number" information, to distinguish between the two mappings.

The assigned source port must be above 1023, since ports below 1024 are reserved for standard services. For example, port 80 is reserved for HTTP protocol, so the destination port for access to a web site page will, by default, be port 80.

So now the address translation table (as well as the IP packet header) carries source and destination port numbers in addition to IP address mapping, but the source port alone is sufficient for the router to identify an individual table entry. Consider the scenario shown in Figure 5-2, whose starting point is the IP arrangement used earlier (see Figure 5-1):

> PC 1 is running two applications, one of which accesses a web page at 175.24.9.5, the other talking to an application at the remote address 175.20.5.7.

> PC 2 is also running two applications, one accessing the same web page as PC1 (175.24.9.5), the other talking to an application at the remote address 213.18.1.2.
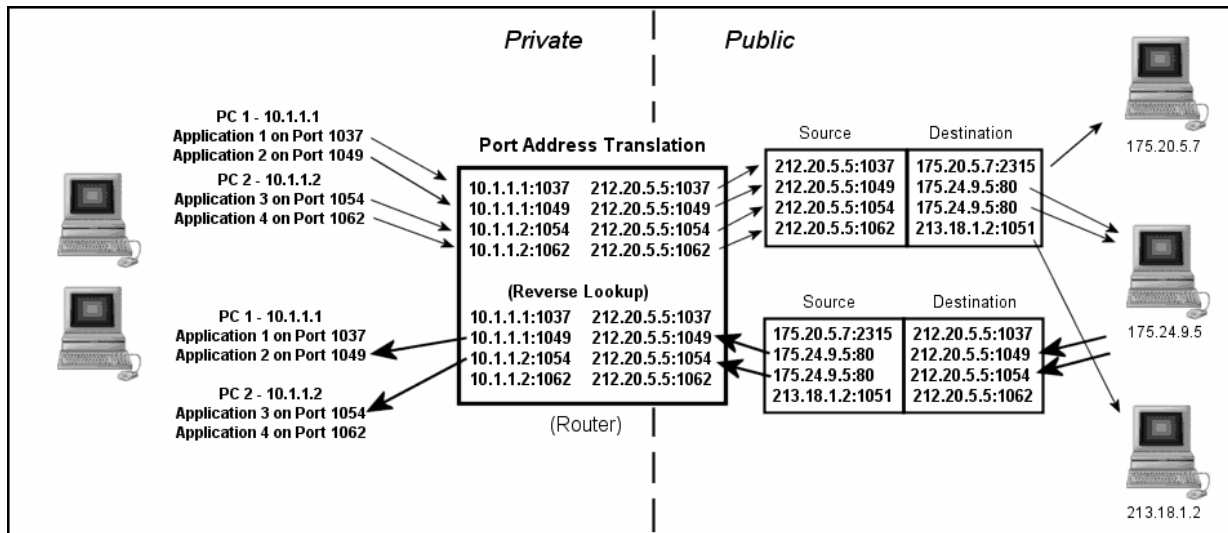
Figure 5-2   Port Address Translation

Even when a large number of applications run on many computers in the private network, they can all be mapped to a single registered IP address, though PAT still essentially works in the same way if there are several registered IP addresses in the pool.

Note especially that when two (or more) applications access the same remote address, the unique source port numbers enable correct routing of any response back to the relevant application. Even if the two web page accesses in Figure 5-2 were from different sessions on the same computer, this still holds true. In that case, all source and destination information would be identical ---- except for the source port numbers (which ensure correct reverse lookups for responses).

Appendix B – Frequently Used Abbreviations

The following list of abbreviations is offered as an aid to reading this guide and other documents to which it makes reference.

ATE	Application Test Environment
AE	Application Enabler
CDMA	Code Division Multiple Access
CDMA2000	CDMA version of the IMT-2000 standard
CIDR	Classless Inter-Domain Routing
DNS	Domain Name System (as in DNS Server)
DUT	Device Under Test
EDGE	Enhanced Data Rates for GSM Evolution
EGPRS	Enhanced General Packet Radio Service (also known as EDGE)
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
HTTP	Hyper Text Transfer Protocol
IP	Internet Protocol
LAN	Local Area Network
MM	Multimedia Message
MMS	Multimedia Messaging Service
MMS-C	MMS Center
MO	Mobile Originated
MT	Mobile Terminated
NAT	Network Address Translation
OPSW	Operational Software
PAT	Port Address Translation
RAN	Radio Access Network
TCP	Transmission Control Protocol
UE	User Equipment
WAN	Wide Area Network
WAP	Wireless Application Protocol
WCDMA	Wideband Code Division Multiple Access
WSP	Wireless Session Protocol

Appendix C - Mandatory R&S CMU200 HW/SW Configuration

R&S CMU-K92: (E)GPRS Application Testing

R&S CMU-B21 v14   Universal Signalling Unit

R&S CMU-B54 v14   Signalling Module

R&S CMU-B56 v14   3GPP Signalling Unit
(including Ethernet USU connector)

R&S CMU-B95/-B96   Additional RF Generator

R&S CMU-U65 v04   Measurement DSP Module

R&S CMU-K20…24   Required GSM Frequency Bands

R&S CMU-K42/K43   GPRS/EGPRS

R&S CMU-K96: WCDMA Application Testing

R&S CMU-B21 v14   Universal Signalling Unit

R&S CMU-B68 v02   Layer 1 Board

R&S CMU- B56 v14   3GPP Signalling Unit
(including Ethernet USU connector)

R&S CMU-U65 v04   Measurement DSP Module

R&S CMU-K65   WCDMA Analyser

R&S CMU-K66   WCDMA Generator

R&S CMU-K61/62/63/67/68/69   WCDMA Bands
   (at least one)

R&S CMU-K87: CDMA Application Testing
R&S CMU-B87: Interface CDMA Datatest

R&S CMU-B83   CDMA2000 Signalling Unit

R&S CMU-U65   Measurement DSP Module

R&S CMU-K83…..86   CDMA2000 Bands

   (at least one)

Index