Rohde & Schwarz Products: Radio Communication Tester R&S® CMU200

[1]CDMA2000® 1xEV-DO

Packet Data Testing with R&S® CMU200

Application Note

The Rohde & Schwarz R&S® CMU200 can be configured to perform packet data testing in a Mobile IP or Simple IP environment.

This application note is intended as a guide to configuring the necessary Mobile IP or Simple IP network elements and R&S® CMU200 instrument for CDMA2000 1xEV-DO.

ROHDE&SCHWARZ

Subject to change – T. Opferman, 2.2007 – 1CM64_01

Contents

1 Introduction

The R&S® CMU200 packet data testing application provides a turnkey solution for the user to test end-to-end data applications using the CDMA2000 1xEV-DO Default Packet Application. The R&S® CMU200 receives the data via an Ethernet interface, transforms the data into PPP packets and sends the packets to the mobile unit over the Radio Link Protocol. The R&S® CMU200 supports both Mobile IP and Simple IP data connections.

All necessary functionality needed to perform end-to-end data testing is provided by the R&S® CMU200; no external equipment is required other than the server running the data application. The R&S® CMU200 performs the PPP link establishment, PPP Authentication (for Simple IP connections) and Mobile IP registration / authentication.

The R&S® CMU200 unit also includes a FTP server and the PING application. These internal applications can be used to test end-to-end data transfers without connecting to an external data server.

2 Definitions

Gateway: A computer that interconnects two networks and passes packets from one to the other. A Gateway is often referred to as a router.

Home Agent: A router with an interface on the mobile node's home network which

- The mobile keeps informed of its current location as the mobile moves from network to network
- Intercepts packets destined to the mobile node's home address and tunnels them to the mobile node's current location

Foreign Agent: A router on the mobile node's foreign network which

- Assists the mobile in informing the home agent of its location
- De-tunnels packets for the mobile node which have been tunneled by the home agent
- Serves as a default router for packets generated by the mobile node

Mobile Node Home IP Address: A fixed IP address assigned to a mobile node itself. The IP address assigned to the mobile is from the mobile's Home Network. The address makes the mobile logically appear as if the mobile is attached to its Home Network. All outgoing IP packets from the mobile use the Mobile Node Home Address as the Source IP address, regardless where (which network) the mobile is located. And all incoming IP packets to the mobile have a Destination Address equal to the Mobile Node Home Address.

Mobile Home Agent IP Address: Each MIP (Mobile IP) mobile is associated with a Home Agent within the mobile's "home network". The IP Address of the mobile's Home Agent is programmed in the mobile and is used for registration and IP tunneling purposes.

Co-located Care of Address: An address temporarily assigned to a mobile node itself. In this case, the mobile node is the exit-point of the tunnel and decapsulates packets encapsulated for delivery by its home agent. A Co-located Care-of Address may be used by exactly one mobile node at any point in time.

Foreign Agent Care of Address: An address of a foreign agent that has at least one interface on a mobile node's visited, foreign link. In this case, the foreign agent decapsulates packets which been tunneled by the home agent and delivers them to the mobile node over the visited link.

IP Tunneling: Procedure that bypasses the standard Internet routing of a packet by encapsulating the packet within a new IP header containing an alternate destination IP

address. The Home Agent "tunnels" all packets destined to the mobile by appending a new IP header with a destination address equal to the care of address used by the mobile.

3 Mobile IP Overview

Mobile IP is a standard protocol that makes mobility transparent to applications and higher-level protocols. The protocol allows mobile nodes to travel outside their home area network without having to update their home IP address. In other words, a mobile node can connect to a foreign network and still be able to send/receive IP packets based on the home network IP address allocated to the phone. This is accomplished by allowing a mobile node to be associated with two IP addresses: a static "mobile home" IP address and a dynamic topologically correct care-of address.

There are two new network elements introduced in a Mobile IP environment – Home Agent and Foreign Agent. The Home Agent is responsible for receiving and delivering traffic destined to the mobile node's home IP address even when the mobile node is not physically attached to the home network. When the mobile node is attached to a foreign network, the Home Agent tunnels the traffic to the Foreign Agent using the mobile node's care-of address. The mobile node registers it's care of address with the Home Agent after the mobile establishes a PPP connection. The care-of address represents the actual location of the mobile node and is used by the Home Agent to route packets to the mobile node.

Figure 1 illustrates an example of a Mobile IP test environment where the R&S® CMU200 interfaces with a live Foreign Agent and Home Agent. In this sample IP test environment, the Foreign Agent and Home Agent implementations are provided by a free-ware solution from the Helsinki University of Technology called Dynamics. The Dynamics Mobile IP system (http://dynamics.sourceforge.net/) is a Mobile IP software solution for the Linux operating system.

The functionality of the R&S® CMU200 in this configuration is to behave like a gateway between the mobile node and the Foreign Agent. All Mobile IP messaging originating from the mobile is "IP forwarded" to the Foreign Agent and vice versa. The Foreign Agent and Mobile Node Home IP Addresses are known to the R&S® CMU200 in order to route messages between the Foreign Agent and Mobile.

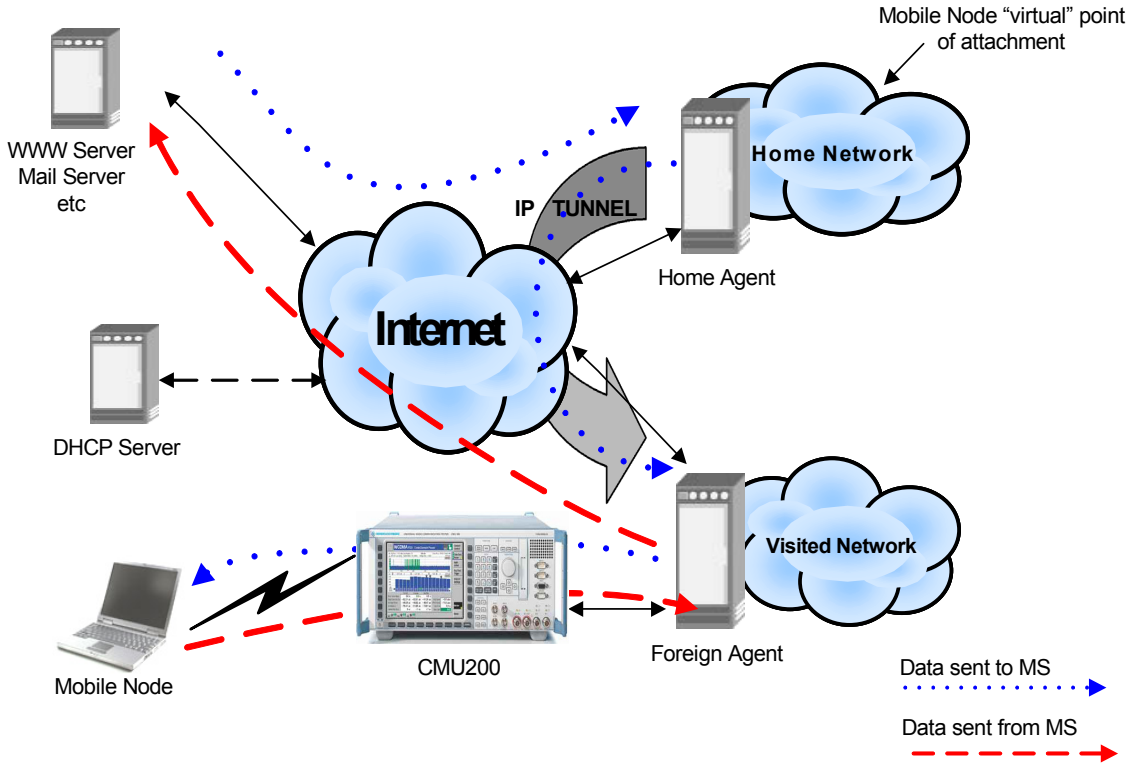


Figure 1. R&S® CMU200 Mobile IP test environment (Gateway mode)

The R&S® CMU200 can also be configured to support a subset of the Mobile IP functionality in the absence of the Foreign Agent and Home Agent. In this "stand-alone" mode, the R&S® CMU200 broadcasts a pre-configured Agent Advertisement messages to the mobile (Foreign Agents and Home Agents advertise their presence on the network by periodically broadcasting special Mobile IP messages called Agent Advertisements), performs MD5 authentication with the mobile and responds to the Mobile IP Registration Request message.

See Figure 2.

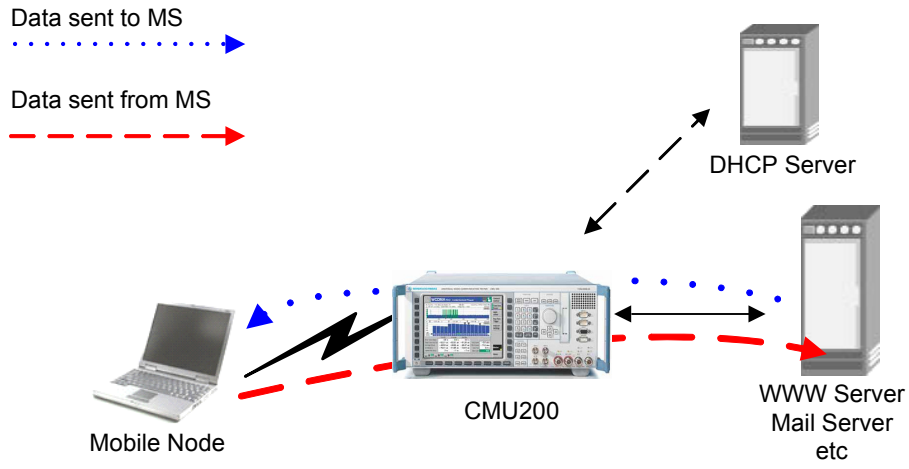


Figure 2. R&S® CMU200 Mobile IP test environment (Stand Alone mode)

4 CDMA2000 1xEV-DO Default Packet Application Overview

The Default Packet Application (DPA) is part of the 1xEV-DO Application Layer and is used for transporting user data between the Access Terminal and the Access Network. This application is made up of three separate protocols. The Radio Link Protocol provides retransmission and duplicate detection for an octet data stream, the Location Update Protocol defines the procedures which support mobility management and the Flow Control Protocol defines the flow control procedures to enable and disable packet flow. A PPP connection is established between the CMU200 (AN) and the AT andd is used to transmit IP datagrams over serial point to point links. See Figure 3 below.

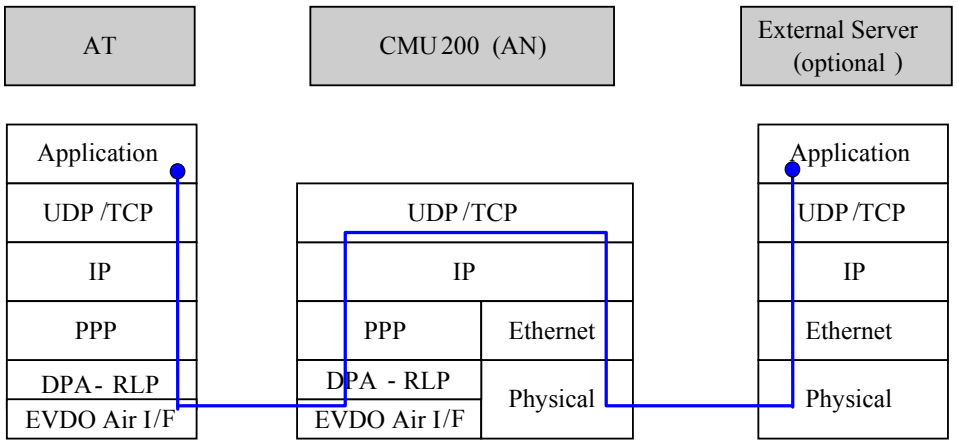


Figure 3. Packet Data Protocol Stack for the 1xEV-DO Default Packet Application

The Default Packet Application is supported in both the 1xEV-DO Release 0 and Release A TIA-856 standards. The difference between Release 0 and Release A, with respect to the Default Packet Application, is the maximum data rate supported. The higher data rates in Release A are achieved by supporting the Physical Layer Subtype 2 and the Reverse Link MAC Subtype 3 protocols. See the CDMA2000 1xEV-DO standard, TIA-856 [1] for more details on these protocols.

	Release 0	Release A
Rerverse Link	153.6 kbps	1.8 Mbps
Forward Link	2.4 Mbps	3.1 Mbps

5 Hardware and Software Requirements for the Dynamics Home Agent and Foreign Agent

This section details the hardware and software requirements for both the Home Agent and the Foreign Agent PCs. The current Dynamics software does not allow for the Home Agent and Foreign Agent to be running on the same PC.

PC Hardware Requirements	
CPU	Pentium 133MHz or better
RAM	64 MBytes or more
Monitor	VGA color monitor
1-2 Network Interface Cards	Successfully tested using the D-Link 10/100 Mbps Fast Ethernet PCI Adapter. Number of NICs needed depends on configuration (see below).

PC Software Requirements	
Linux OS	Mandrake 9.1 http://www.mandrakesoft.com/
Window Manager	KDE 3.1
Dynamics Mobile IP Software	dynamics-0.8.1 See http://dynamics.sourceforge.net/ for more details and latest version.

Additional Hardware Requirements	
4 port Ethernet Hub	Number of Ethernet Hubs (0 or 2) depends on configuration (see below). Successfully tested using NetGear 4 Port Ethernet Hub.

The Dynamics Home Agent and Foreign Agent configuration outlined above are not related in any way to the R&S® CMU200 Mobile IP implementation. This section simply provides an example implementation of a Foreign Agent and Home Agent that could be used when the R&S® CMU200 is configured to communicate with a live Foreign Agent and Home Agent (i.e. "gateway mode"). Please refer to the Dynamics and Mandrake web sites for details on specific licenese agreements.

The remaining sections describe how to set up the R&S® CMU200 and Mobile IP network elements for various configurations. The different configurations are as follows:

- R&S® CMU200 configured in a Mobile IP Gateway mode (see Figure 1) *without* DHCP enabled.
- R&S® CMU200 configured in a Mobile IP Stand Alone mode (see Figure 2) *without* DHCP enabled.

- R&S® CMU200configured in a Mobile IP Gateway mode (see Figure 1) *with* DHCP enabled.
- R&S® CMU200configured in a Mobile IP Stand Alone mode (see Figure 2) *with* DHCP enabled.

NOTE: the Dynamics Home Agent and Foreign Agent functionality could be used only if the R&S® CMU200 is configured in a Mobile IP Gateway Mode.

6 R&S® CMU200 Gateway Mobile IP Environment without DHCP

In this configuration, the R&S® CMU200 is setup to behave as a gateway between a live Foreign Agent and a CDMA2000 1xEV-DO MIP mobile phone. A sample test environment *without* DHCP is described in Figure 4.

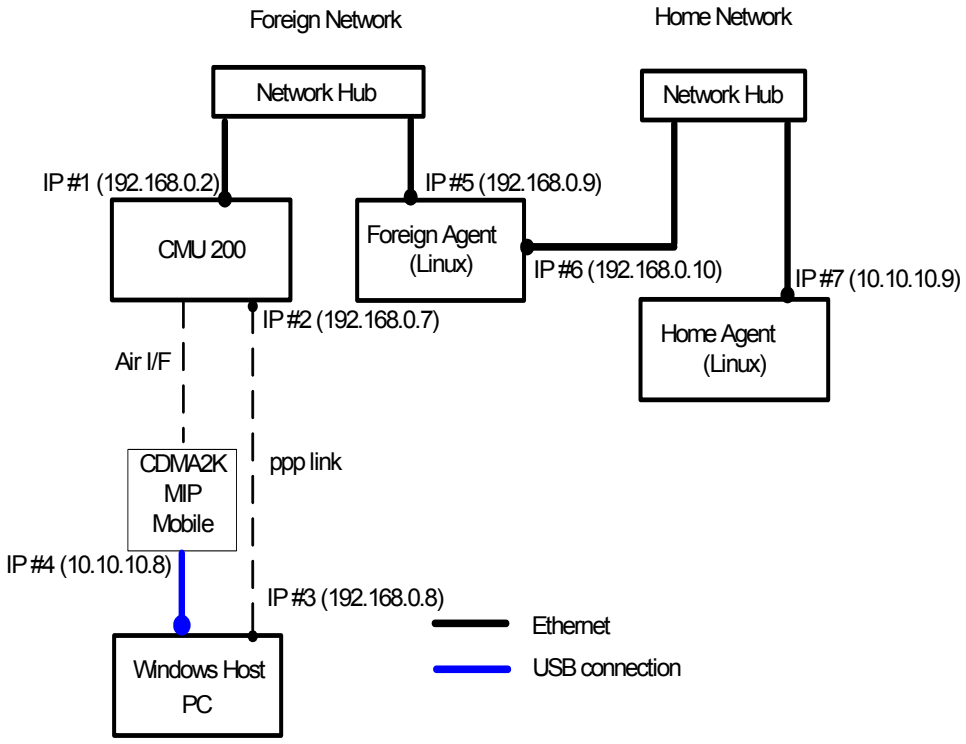


Figure 4. R&S® CMU200 (Gateway) Mobile IP test environment without DHCP

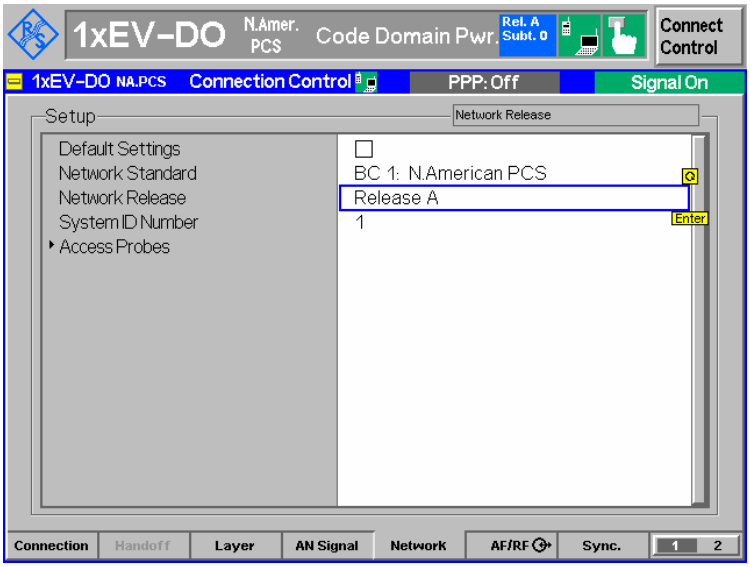
R&S® CMU200 Mobile IP Gateway Configuration without DHCP

STEP 1 – Configure the CDMA2000 1xEV-DO Network Release to be tested

- The R&S® CMU200 can be configured to operate in either CDMA2000 1xEV-DO Release A or Release 0. Release A is backwards compatible with Release 0. The main difference in terms of packet data between Release 0 and Release A is the rate at which the data is transmitted and received. See Section 4 above for more information.

The **Network Release** parameter can be found at:

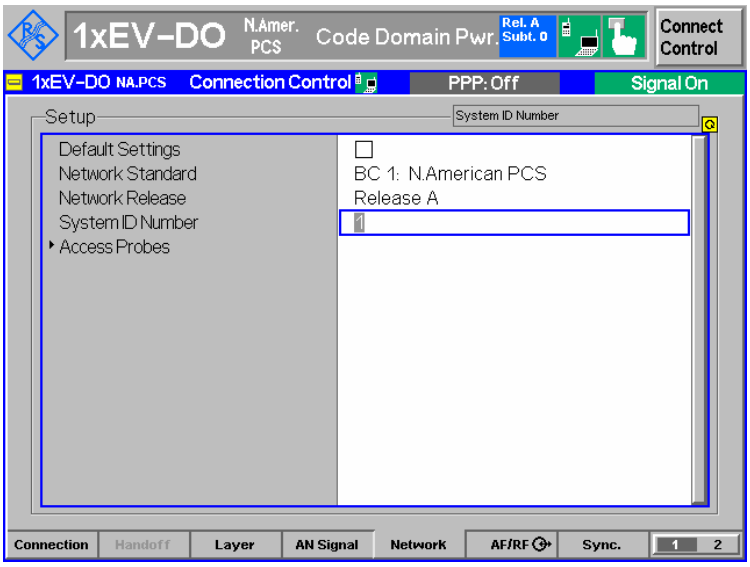
Connect Control: Network →Network Release



STEP 2 – Configure the CDMA2000 1xEV-DO System Idenfication (SID), Band Class and RF Channel

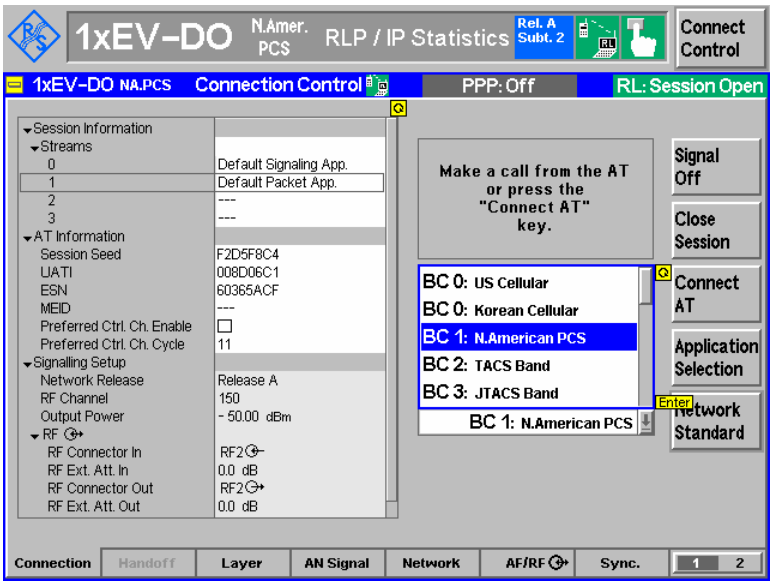
- The R&S® CMU200 can be configured to use a specific SID. The **System ID Number** parameter can be found at:

Connect Control: Network →System ID Number



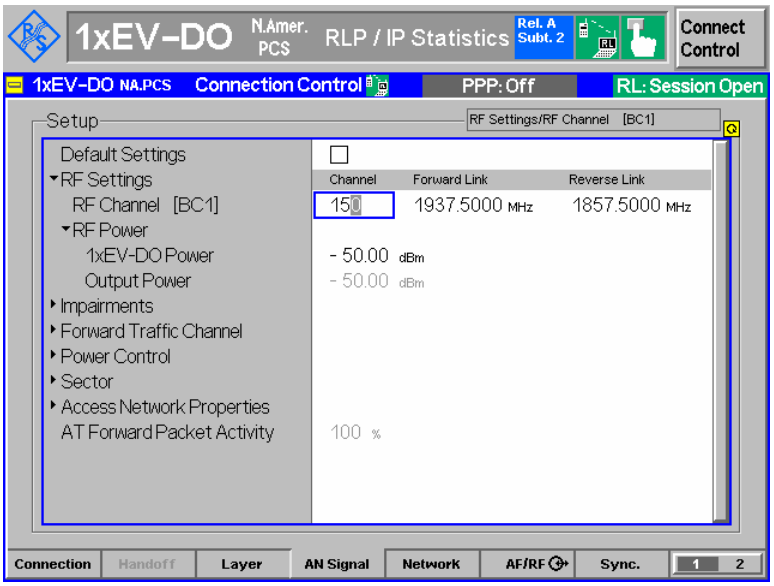
➢ The R&S® CMU200 can be configured to use a specific Band Class. The **Network Standard** parameter can be found at :

Connect Control: Connection→Network Standard



➢ The R&S® CMU200 can be configured to use a specific RF Channel. The **RF Channel** parameter can be found at :

Connect Control: ANSignal →RF Settings



STEP 3 – Configure the CDMA2000 1xEV-DO Sector ID informnation

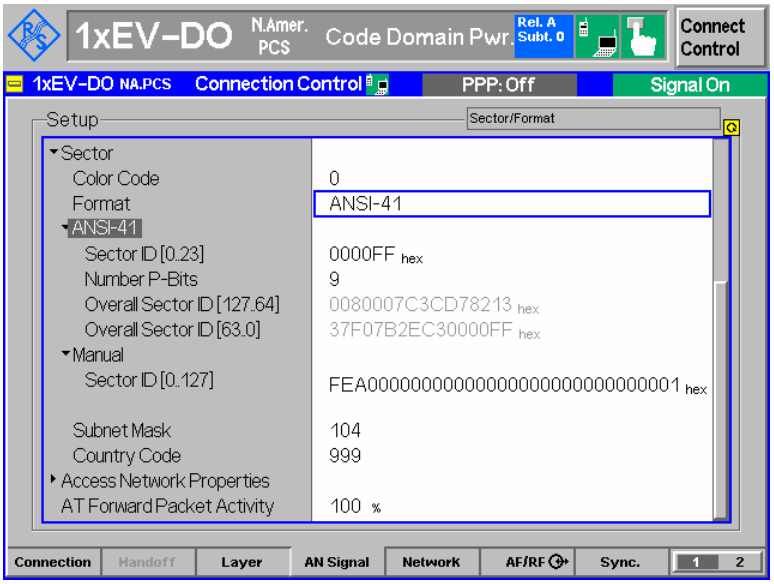
- The R&S® CMU200 can be configured to use either an ANSI-41 formatted sector ID or a user formatted sector ID (Manual format). In the ANSI-41 format mode, the CMU200 uses the **#P bits**, **SectorID24**, **SID** and a random number to generate a **Sector ID**. The format of the ANSI-41 Sector ID is as follows :

127				24 23	0
P-Bits (1-64 bits)	Format (2 bits)	SID (15 bits)	Random Number (87 - #P-Bits bits)	SectorID 24 (24 bits)	
0000. ..... .01	0 0	NNNN... NNNN	XXXX.... XXXX	XXXX ... XXXX	

In Manual Mode, the user can configure all 128 bits of the sector ID.

The **Sector ID** parameter can be found at:

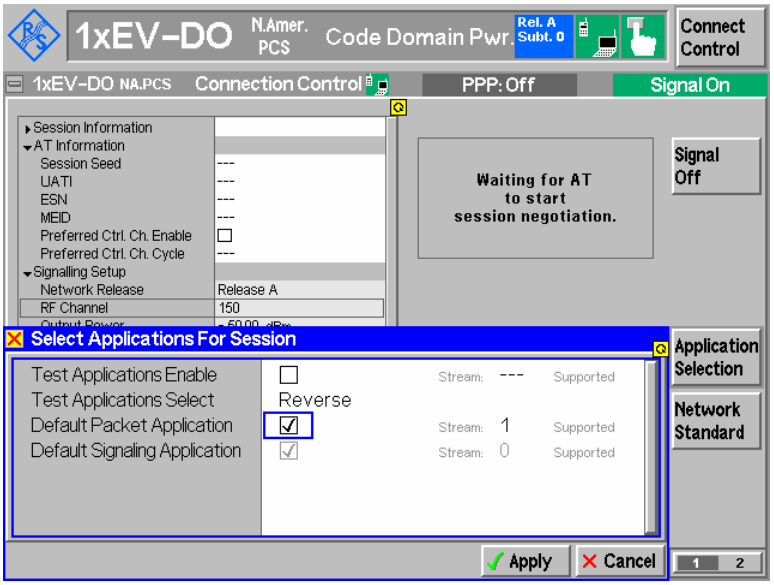
Connect Control: ANSignal →Sector



STEP 4 – Configure the CDMA2000 1xEV-DO Application to the Default Packet Application

- The Default Packet Application is used for packet data testing in CDMA2000 1xEV-DO. The **Application Binding** can be found at :

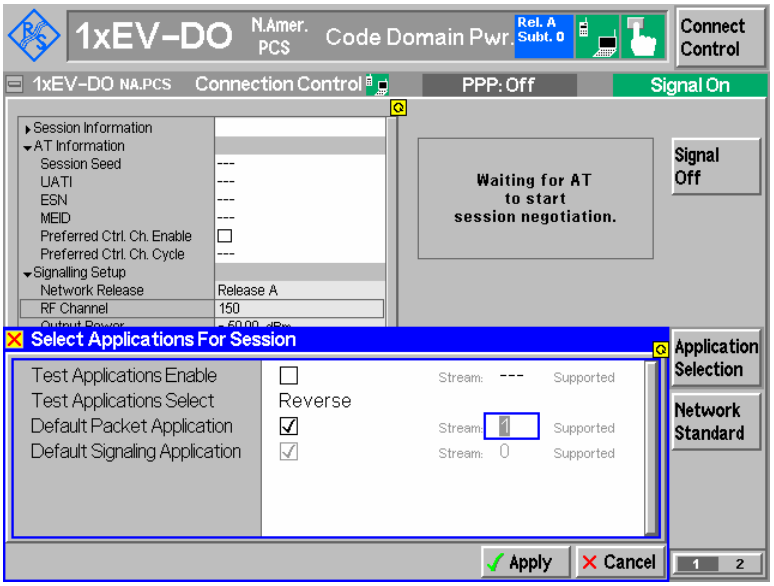
Connect Control: Connection →ApplicationSelection



STEP 5 – Configure the Default Packet Application Stream ID

- The Default Packet Application can be configured to run on **Stream ID** 1, 2 or 3. The Stream ID mapping can be found at:

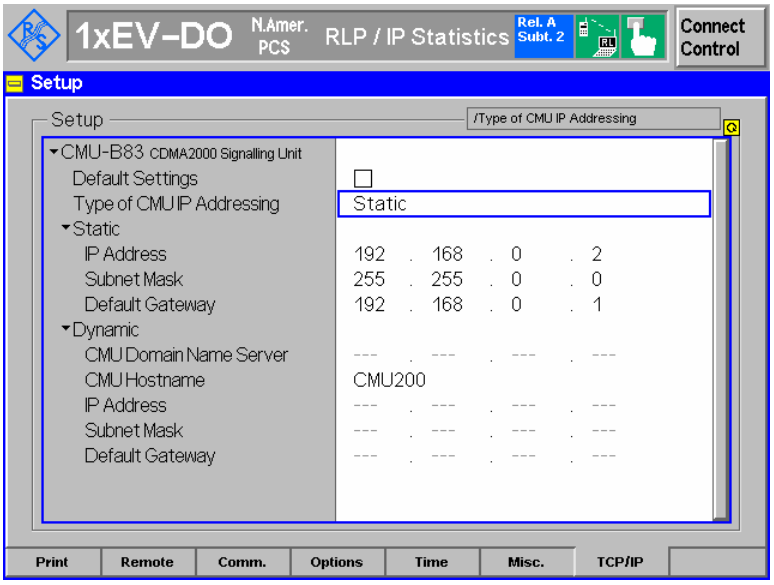
Connect Control: Connection →Application Selection



STEP 6 – Configure the R&S® CMU200 to use static IP Addressing

- The R&S® CMU200 can be configured to use Static IP Addressing by setting the **"Type of R&S® CMU200 IP Addressing"** to Static. The IP Addressing parameter can be found at:

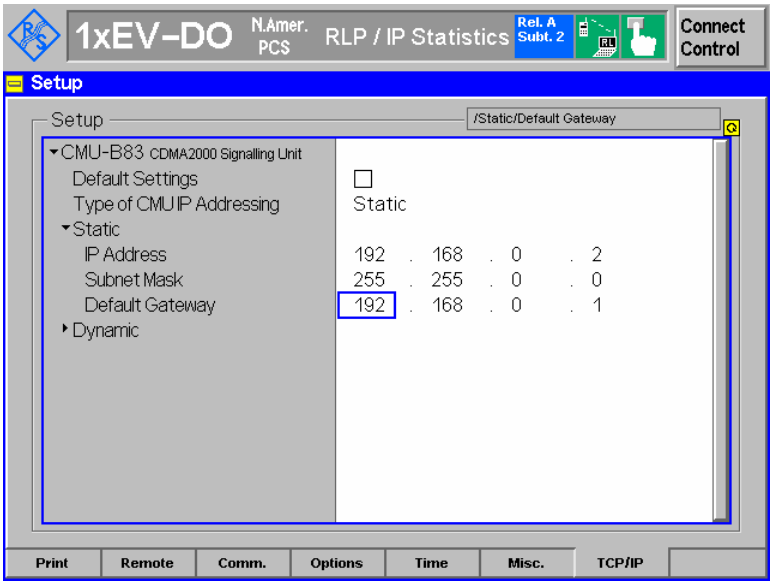
SETUP → TCP/IP



STEP 7 – Configure the R&S® CMU200's CMU-B83 with static IP Addresses

- The CMU-B83 can be configured with Static IP Addressing by setting the IP Address, Subnet Mask and Default Gateway. These parameters can be found at:

SETUP → TCP/IP



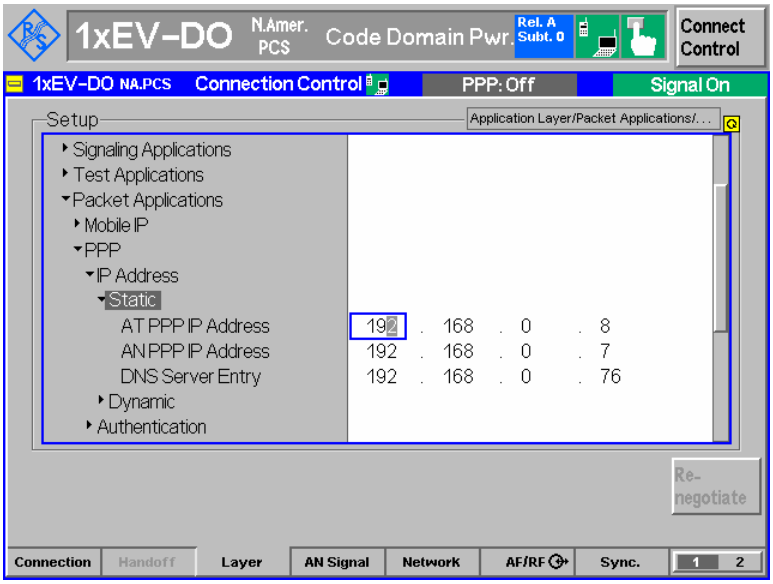
The R&S® CMU200 needs to be configured with the static **PPP IP addresses** and **DNS Address** for both the R&S® CMU200 and Mobile. These IP addresses must be configured to be within the R&S® CMU200's subnet.

In a mobile IP environment, the AT PPP IP address is *not* the IP address assigned to the mobile. A MIP capable mobile may use this AT PPP IP address as the co-located care of address in the case where a Foreign Agent care of address is not supplied in the Agent Advertisement message.

The AT PPP IP address will **not** be assigned to the mobile since the R&S® CMU200 does not support a co-located care of address, however, the AT PPP IP address should still be configured to be within the R&S® CMU200's subnet. The AN PPP IP Address is used internally for IP packet routing purposes and shall also be configured to be within the R&S® CMU200's subnet. The AN PPP and AT PPP IP Addresses assigned must be **different** than the CMU and Gateway IP Addresses (under SETUP -> TCP/IP).

The PPP IP Addresses and DNS Server IP Address can be found at:

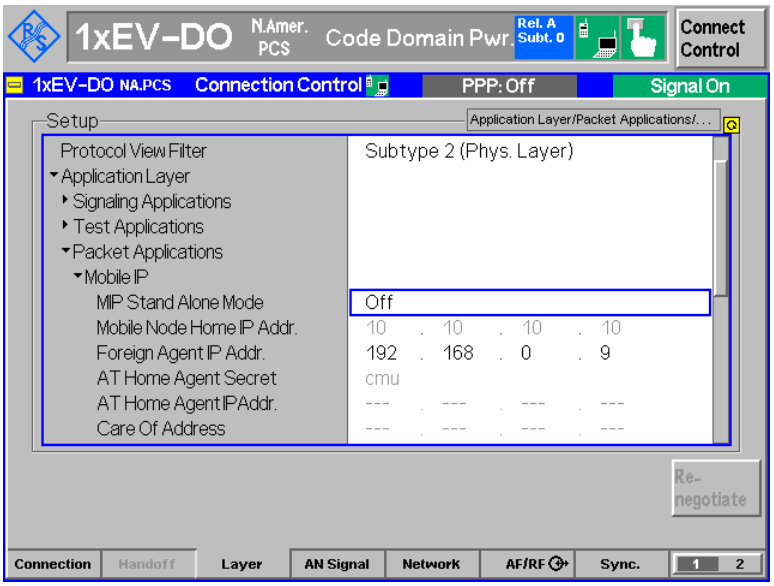
Connect Control: Layer→ApplicationLayer → Packet Applications → PPP→ IP Addresses



STEP 8 – Configure the R&S® CMU200 to act as a Mobile IP Gateway

- The R&S® CMU200 can be configured to work in the Mobile IP Gateway mode by setting the **"Stand Alone"** flag to OFF. The Stand Alone parameter can be found at:

Connect Control: Layer→ApplicationLayer → Packet Applications → Mobile IP



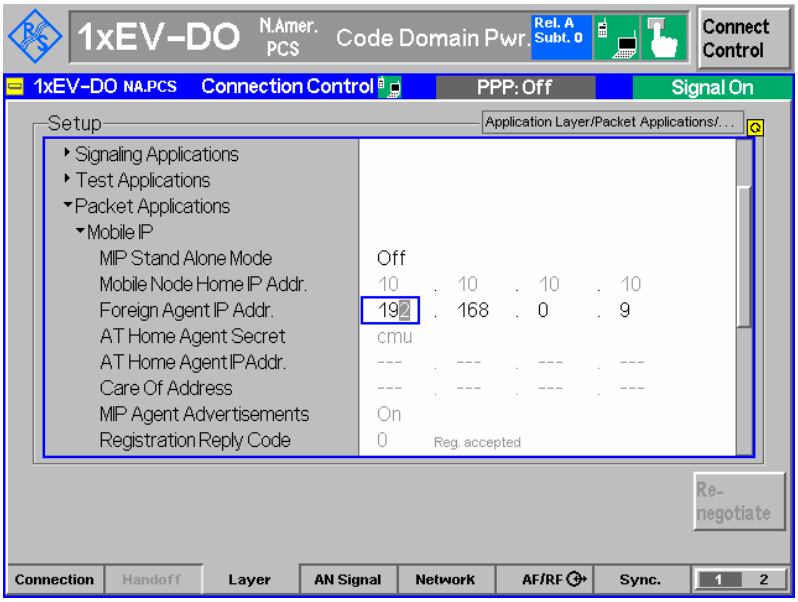
STEP 9 – Configure the R&S® CMU200 with the Foreign Agent IP Address

- The **Foreign Agent IP Address** can be found at:

Connect Control: Layer→ApplicationLayer → Packet Applications → Mobile IP

NOTE: The Foreign Agent IP Address is adjustable only if the R&S® CMU200 is configured in a non-Stand Alone mode (Stand Alone = OFF).

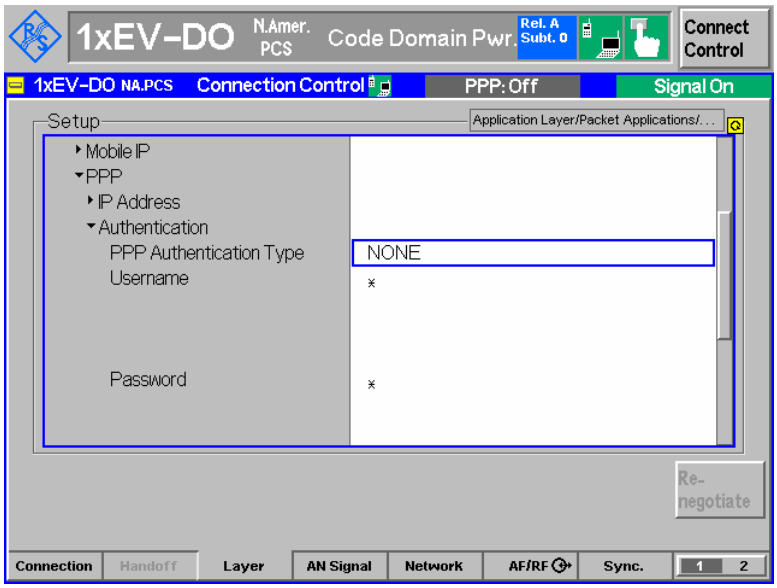
The Foreign Agent IP Address can act as the Default Gateway for the R&S® CMU200 (see step 7 above).



STEP 10 – Configure PPP Authentication

- PPP Authentication must be **disabled** for mobile IP calls. Setting the **"PPP Authentication"** parameter to NONE disables the Authentication. The **"PPP Authentication"** parameter can be found at:

Connect Control: Layer→ApplicationLayer → Packet Applications → PPP→ Authentication

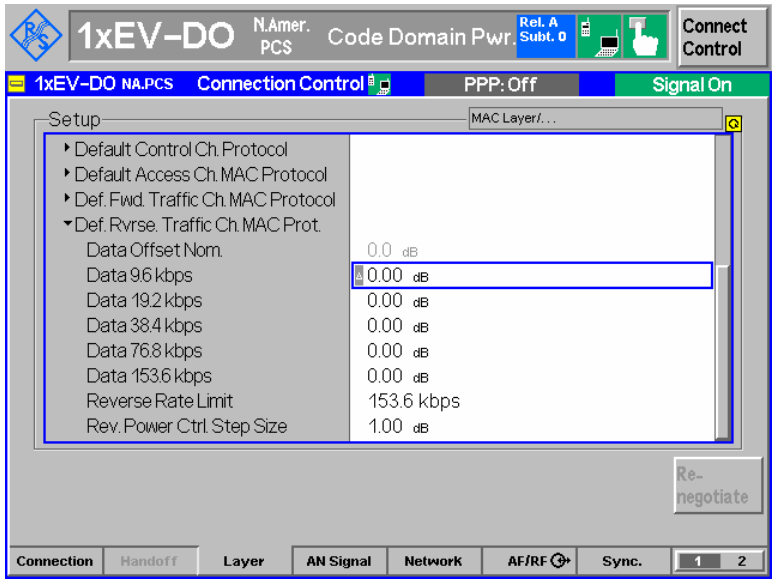


STEP 11 – Configure the CDMA2000 1xEV-DO protocol stack data related parameters

The R&S® CMU200 provides the user with configuring various CDMA2000 1xEV-DO protocol level parameters. The relevant parameters for data testing are highlighted below. See the CDMA2000 1xEV-DO standard, TIA-856 [1] for more details.

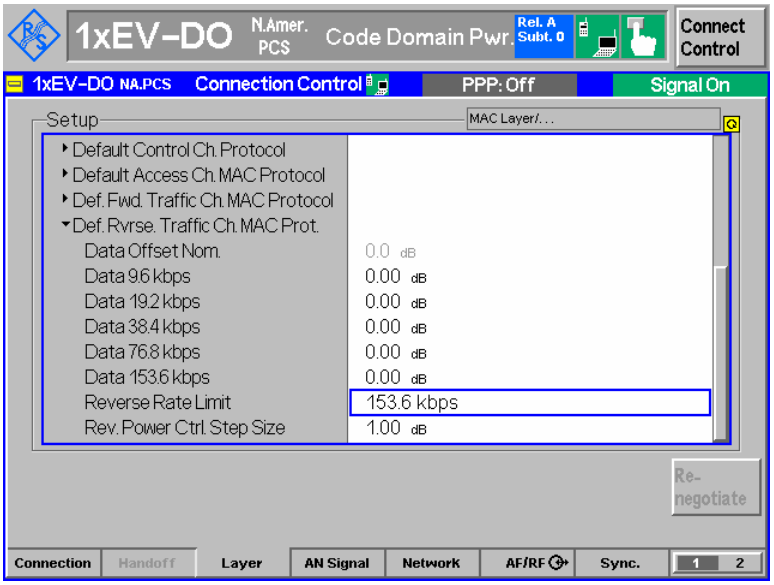
- The R&S® CMU200 provides the user with the ability to configure the ratio of reverse link data channel power (at 9.6kbps, 19.2kbps, 38.4kbps, 76.8kbps and 153.6kbps) to the nomial reverse link data channel power (at 9.6kbps, 19.2kbps, 38.4kbps, 76.8kbps and 153.6kbps) . These settings are for 1xEV-DO Release 0 only. The nominal offset of the reverse link data channel power to pilot channel power is set to 0 dB and is not configurable. The **Data Offset** parameters can be found at :

Connect Control: Layer→MAC Layer→Def Rvrse Traffic Ch MAC Prot



- The R&S® CMU200 provides the user with the ability to configure the highest data rate that the access terminal is allowed to use on the reverse traffic channel. This setting is for 1xEV-DO Release 0 only. The **Reverse Rate Limit** parameter can be found at :

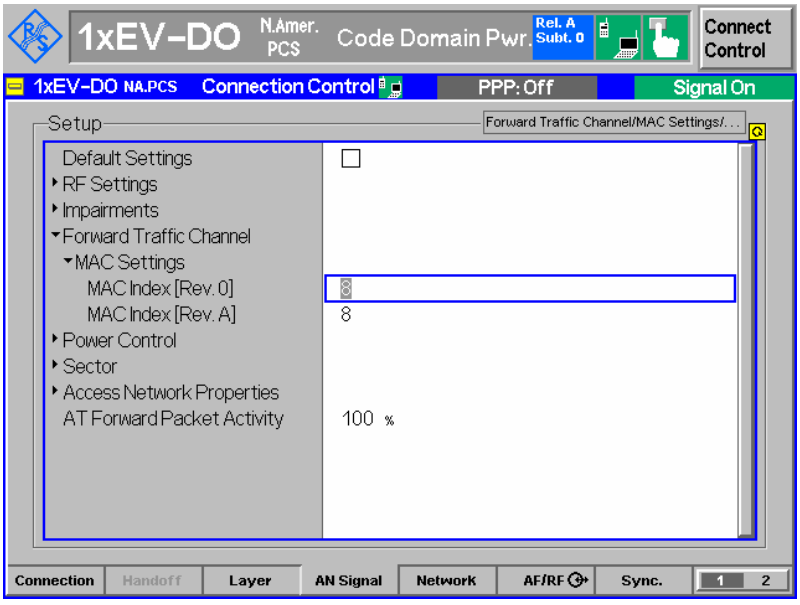
Connect Control: Layer→MAC Layer→Def Rvrse Traffic Ch MAC Prot



STEP 12 – Configure the MAC Index used on the Forward Link Traffic Channel

- The R&S® CMU200 provides the user with the ability to configure the **MAC Index** used for addressing packets on the Forward Link Traffic Channel. There is a separate MAC Index defined for Release 0 and Release A.

Connect Control: ANSignal →Forward Traffic Channel→MAC Settings



Dynamics Foreign and Home Agent Configuration

See Appendix A.

MIP Mobile Phone / Windows Host PC Configuration

STEP 1 – Configure MIP Mobile phone when the R&S® CMU200 is configured as a Mobile IP Gateway

- Access Mobile IP configuration

  Using a phone configured for Mobile IP, access the configuration information. A MSL may be necessary to access this information. The MSL refers to a 6 digit algorithmic code that is specific to a particular phone ESN. The MSL is owned by the carrier and is not always available without an agreement.

- Set *MN-HA Secret*

  The MN-HA secret should correspond to the value entered in the Home Agent Configuration "shared secret" field under the **SECURITY** parameter when the R&S® CMU200 is configured in a Mobile IP Gateway Configuration. This is the secret used at the Home Agent and Mobile during the MD5 Authentication Algorithm. See Appendix A.

- Set *MN-HA SPI*

  The MN-HA SPI should correspond to the value entered in the Home Agent Configuration "SPI" field under the **SECURITY** parameter. This value is used as a look up index in the Home Agent's database to retrieve the mobile's shared secret information. See Appendix A.

- Set *Reverse Tunneling*

  Disable Reverse Tunneling. This value should correspond to the value entered in the Home Agent and Foreign Agent **EnableReverseTunneling** configuration parameter. See Appendix A.

- Set *Primary Home Agent IP Address*

  The Primary Home Agent IP Address should correspond to the IP Address defined at the Home Agent (IP #7). See Figure 4. Since authentication between the Home Agent and Foreign Agent has been disabled, there are not any configuration parameters that need set at the Foreign and Home Agents. See Appendix A.

- Set *Mobile Home Address*

  The Mobile Home Address should correspond to one of the allowable values defined in the **AUTHORIZEDNETWORK** parameter defined in the Foreign Agent's configuration and also in the **AUTHORIZEDLIST** parameter defined in the Home Agent's configuration. This is the IP address allocated to the mobile and should be part of the Home Agent's subnet. See Appendix A.

STEP 2 – Configure Windows Host PC connected to the Mobile

- Install necessary drivers for the mobile phone modem (USB or Serial connection)
- Add new modem
- Add new network connection

- User may optionally configure the DNS address for this network connection

➢ Connect mobile phone to PC via USB or Serial connection

➢ Query mobile's modem to ensure it's properly configured

➢ Install optional tools (freeware) used for generating traffic

- Iperf – UDP/TCP traffic generator
- FTP server

The Iperf traffic generator and FTP server are not related in any way to the R&S® CMU200 Mobile IP implementation. They are examples of tools that could be used to generate IP traffic. Please refer to their web sites for details on any license agreements.

Making a Mobile IP CDMA2000 1xEV-DO Data Call and transferring data

STEP 1 – Establish a Mobile IP CDMA200 1xEV-DO Default Packet Application call

The AT must first open a session with the CMU200 (this is similar to Registering in CDMA2000 1xRTT). In order for the AT to open a session on the CMU200, the following CMU200 parameters need to be configured properly based on the AT's preferred roaming list. Refer to steps 2 and 3 above.

- Band Class
- RF Channel
- Sector ID

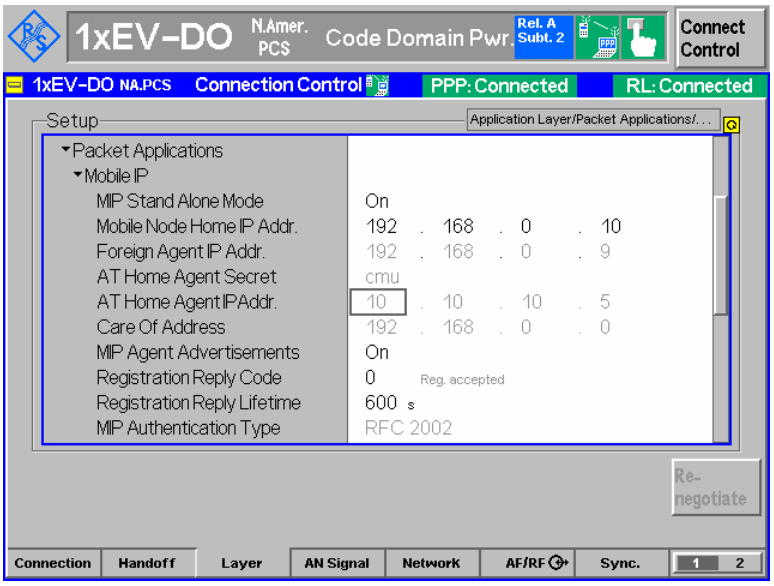
Once a session is opened, the Dial-Up connection can be used to establish a data call with "**#777**" as the dialed number.

STEP 2 – Verify Mobile IP Information

The Mobile Node Home IP Address, Mobile Node Home Agent IP Address and Care Of Address used by the phone are captured and displayed by the CMU200.

➢ The Mobile IP Information can be found at

Connect Control: Layer→ApplicationLayer → Packet Applications → Mobile IP



Once the call is active, data can be transferred using various mechanisms described below (3a – 3d):

STEP 3a – Use the FTP server within the R&S® CMU200 to transfer data

Anonymous FTP access is allowed on the R&S® CMU200 using the username 'ftp', with password 'ftp'. The R&S® CMU200 contains three binary test files of varying sizes. These files can be deleted to make room to upload new files to the R&S® CMU200. The AN PPP IP Address can be used to access the FTP server (found at *Connect Control: Layer→ApplicationLayer → Packet Applications → PPP→ IP Address).*

- On the Windows Host PC:

```
ftp << AN PPP IP Addr >>
```

STEP 3b – Attempt to PING the mobile from the Home Agent

- On the Home Agent Linux box :

```
ping << Mobile Home IP Addr >>
```

The Mobile Home IP Address is the IP Address programmed in the mobile. The Mobile Home IP address can also be obtained from STEP 2 above.

STEP 3c – Attempt to PING the MIP mobile from R&S® CMU200

- The PING measurement can be found at

Connect Control:

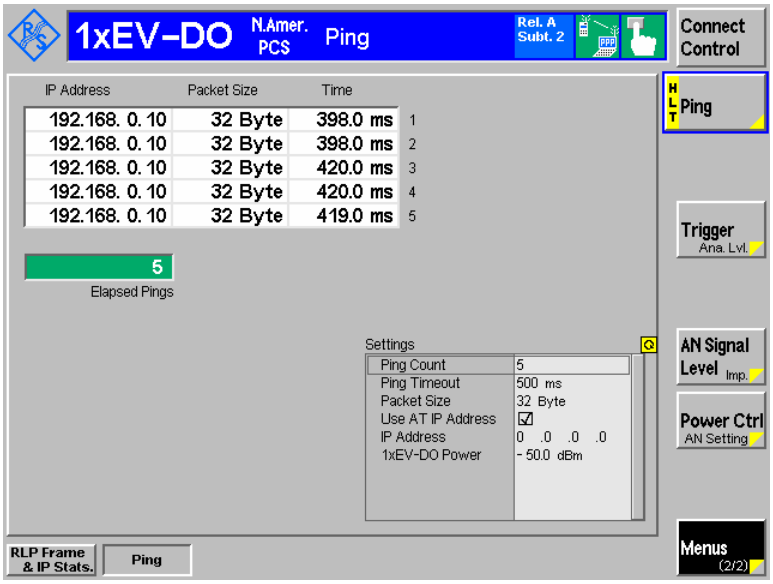
Menu (1/2)→ Ping

- Select the "Use AT IP Address" tab and check the box.

  This configures the PING measurement to use the IP Address allocated to the Mobile.

- Set the Ping Count, Timeout and Packet Size

➢ Run the PING measurement



STEP 3d – Transfer data to the mobile (forward link direction) using Iperf freeware packet generator tool

➢ On the Windows Host PC connected to the mobile, execute the following iperf command from the DOS command line :

```
> iperf -s -u -i 2
```

This command configures iperf to accept incoming UDP traffic on the default port 5001and displays packet statistics every 2 seconds.

➢ On the Home Agent Linux box (assuming iperf has been installed), execute the following iperf command from the command line :

```
> iperf -c << Mobile Home IP Addr >> -u -t 5000 -b 1000k
```

This configures the Home Agent to setup a connection with the Windows Host PC connected to the mobile and transfer UDP traffic for 5000 seconds at a bandwidth of 1 Mbps to the Mobile's IP Address.

NOTE: the execution of these 2 commands could be reversed (along with changing the Mobile Home IP Address to the Home Agent's IP Address) to test transferring data in the uplink direction.

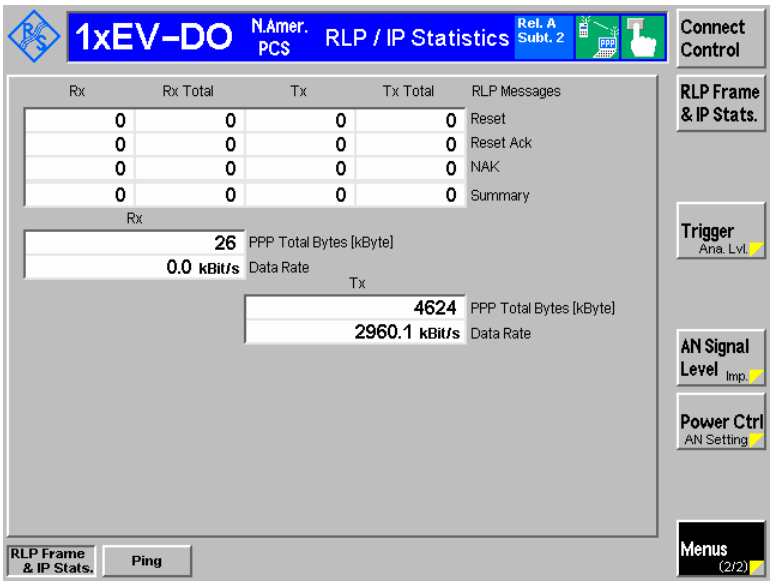
STEP 4 – Monitor packet data flow statistics on the R&S® CMU200

The R&S® CMU200 monitors the RLP messaging (Reset, Reset Ack, NAK), PPP data count and data transfer rate for the data call.

➢ The RLP/IP statistics measurement can be found at:

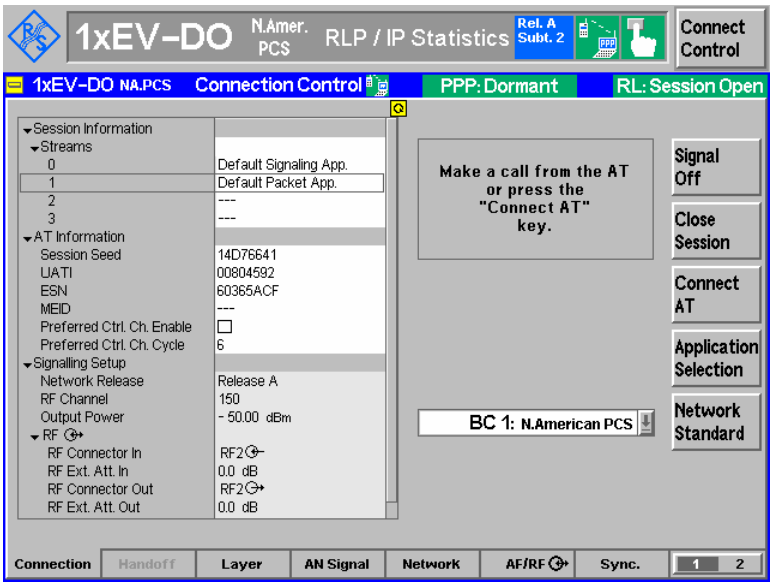
Connect Control:

Menu (1/2)→ RLP/IP Stats



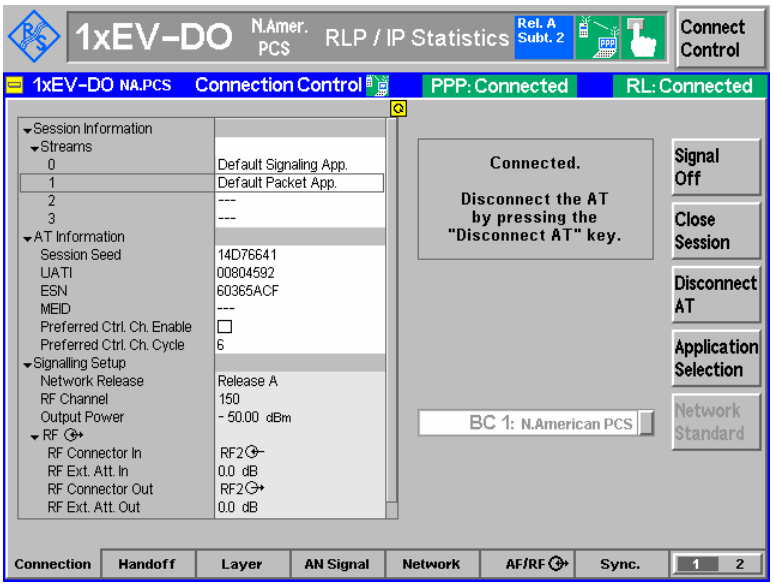
STEP 5 – Take the mobile into a PPP Dormat State

The R&S® CMU200 can put the mobile into a PPP Dormant (assuming no data is being transfered) state by simply selecting Disconnect AT button from the MMI. The state will transition from “PPP Connected” to “PPP Dormant”.



STEP 6 – Bring mobile back to PPP Connected

The R&S® CMU200 can manually bring the mobile back into a PPP Connected state by simply selecting Connect AT button from the MMI. The state will transition from “PPP Dormant” to “PPP Connected”.


1xEV-DO
N.Amer. PCS
RLP / IP Statistics
Rel. A Subt. 2
Connect Control
1xEV-DO NA.PCS
Connection Control
PPP: Connected
RL: Connected
Session Information
Streams
0 Default Signaling App.
1 Default Packet App.
2 ---
3 ---
AT Information
Session Seed 14D76641
UATI 00804592
ESN 60365ACF
MEID ---
Preferred Ctrl. Ch. Enable
Preferred Ctrl. Ch. Cycle 6
Signalling Setup
Network Release Release A
RF Channel 150
Output Power - 50.00 dBm
RF
RF Connector In RF2
RF Ext. Att. In 0.0 dB
RF Connector Out RF2
RF Ext. Att. Out 0.0 dB
Connected.
Disconnect the AT by pressing the "Disconnect AT" key.
BC 1: N.American PCS
Signal Off
Close Session
Disconnect AT
Application Selection
Network Standard
Connection
Handoff
Layer
AN Signal
Network
AF/RF
Sync.
1
2

7 R&S® CMU200 -Standalone Mobile IP Environment without DHCP

In this configuration, the R&S® CMU200 is setup to simulate the Foreign Agent and Home Agent functionality. A sample test environment *without* DHCP is described in Figure 5.

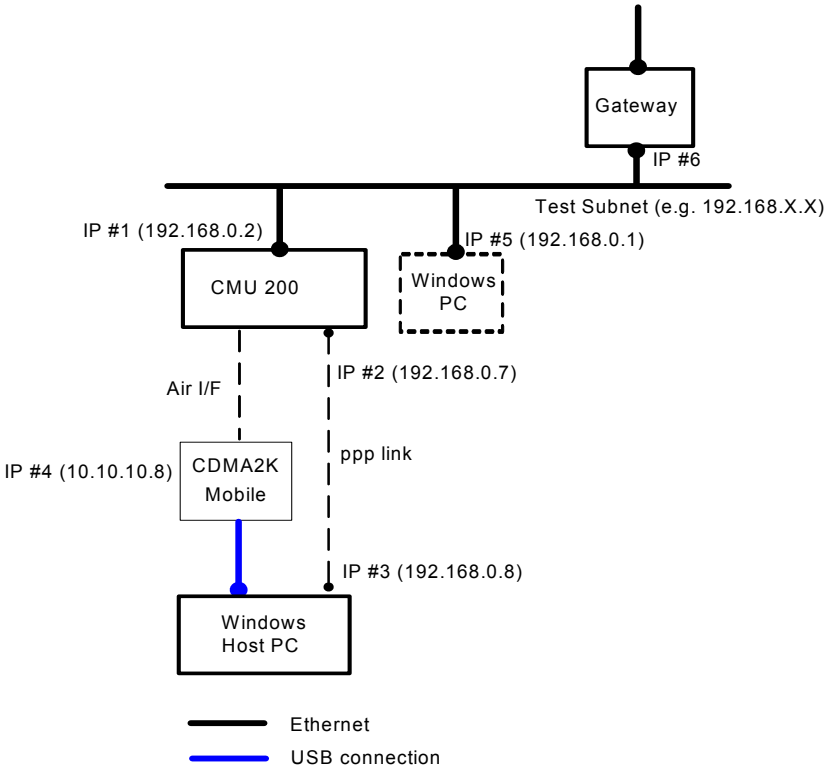


Figure 5. R&S® CMU200 (Stand Alone) Mobile IP test environment

R&S® CMU200 Mobile IP Stand Alone Configuration without DHCP

STEP 1 – Configure the CDMA2000 1xEV-DO Network Release to be tested

STEP 2 – Configure the CDMA2000 1xEV-DO System Idenfication (SID)

STEP 3 – Configure the CDMA2000 1xEV-DO Sector ID informnation

STEP 4 – Configure the CDMA2000 1xEV-DO Application to the Default Packet Application

STEP 5 – Configure the Default Packet Application Stream ID

See chapter 6; section "R&S® CMU200 Mobile IP Gateway Configuration without DHCP"; steps 1-5.

STEP 6 – Configure the R&S® CMU200 use static IP Addressing

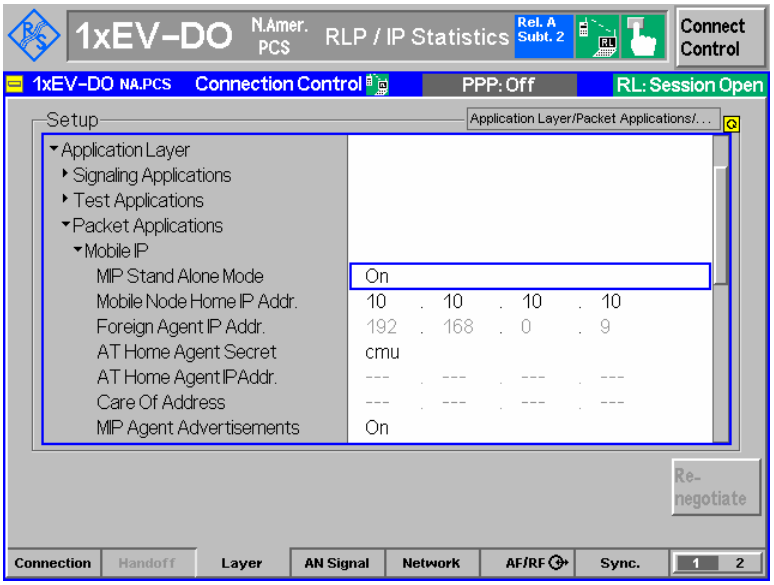
See chapter 6; section "R&S® CMU200 Mobile IP Gateway Configuration without DHCP"; steps 6 and 7.

The R&S® CMU200 Default Gateway should be configured to use the IP Address of the Gateway, IP Address #6 (see Figure 5).

STEP 7 – Configure the R&S® CMU200 in Mobile IP Stand Alone mode

- The R&S® CMU200 can be configured to work in the Stand Alone mode by setting the **"Stand Alone"** flag to ON. The Stand Alone parameter can be found at:

Connect Control: Layer→ApplicationLayer → Packet Applications → Mobile IP

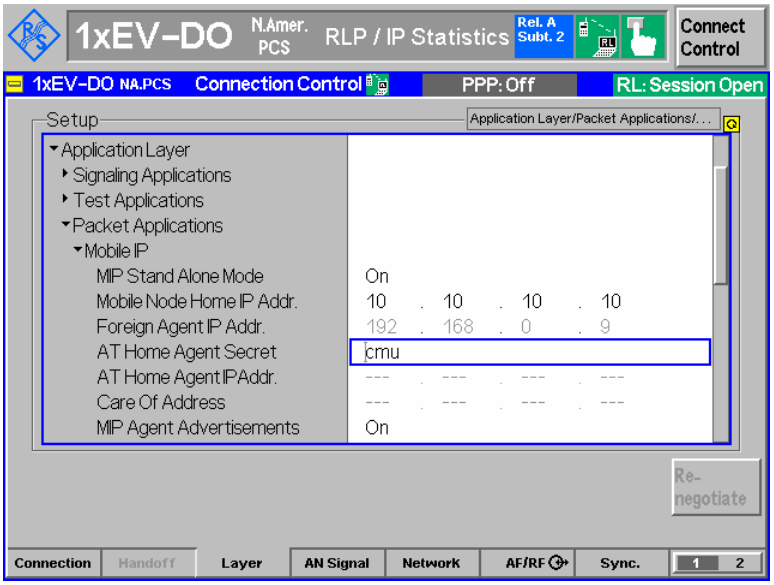


STEP 8 – Configure the Mobile IP Home Agent Secret

This secret is used by the R&S® CMU200 to do Mobile IP MD5 Authentication. This value should match the MN-HA secret programmed in the mobile phone (see chapter 7; section "MIP Mobile Phone / Windows Host PC Configuration"; step 1 below)

- The Mobile IP secret can be configured using the "**AT Home Agent Secret**" parameter found at:

Connect Control: Layer→ApplicationLayer → Packet Applications → Mobile IP



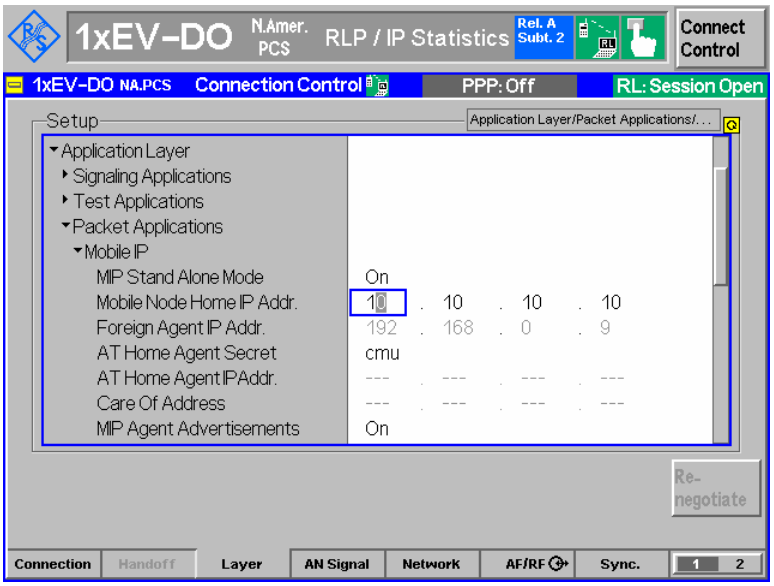
STEP 9 – Configure the Mobile Node Home IP Address (optional)

The R&S® CMU200 (in a MIP Stand Alone mode) allocates the **AT Home IP Addr** to the mobile in the Registration Reply message in the case where the Home IP Address is not programmed in the mobile (IP Address set to "0.0.0.0").

If there is a Home IP Address programmed in the mobile, the **Mobile Node Home IP Addr** is not used by the R&S® CMU200. The R&S® CMU200 allocates the IP Addressed programmed in the phone to the mobile in the Registration Reply message.

- The Mobile Node Home IP Address can be configured using the "**Mobile Node Home IP Addr**" parameter found at:

Connect Control: Layer→ApplicationLayer → Packet Applications → Mobile IP

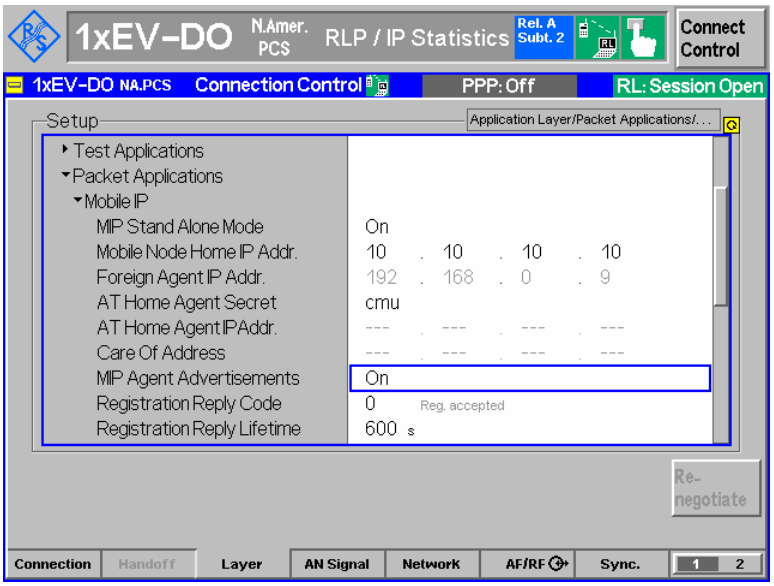


STEP 10 – Configure the ability to send Agent Advertisements

The **MIP Agent Advertisements** parameter is used by the R&S® CMU200 (in a MIP Stand Alone mode) to determine if Agent Advertisements are sent to the mobile or not. Setting the value to ON enables the R&S® CMU200 to broadcast a Mobile IP Agent Advertisement when solicited. A setting of OFF disables the broadcasting.

The enabling/disabling of Agent Advertisements can be configured using the "**MIP Agent Advertisements**" parameter found at:

Connect Control: Layer→ApplicationLayer → Packet Applications → Mobile IP

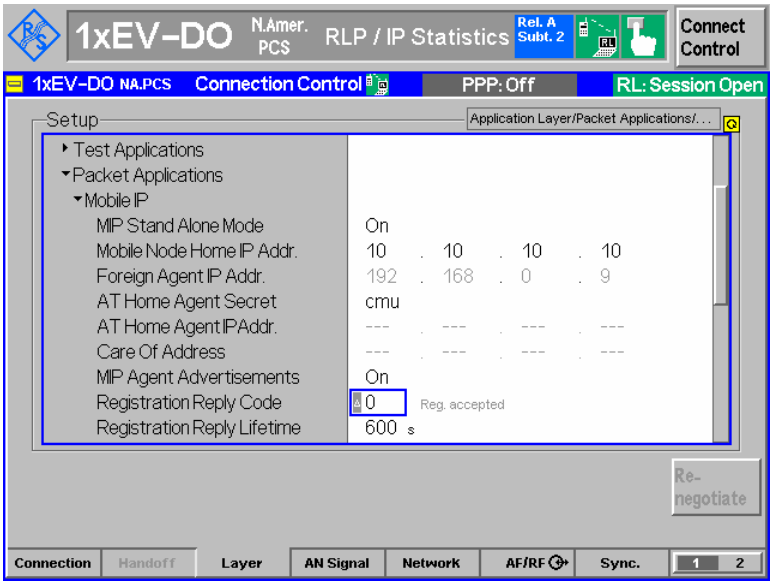


STEP 11 – Configure the Registration Reply code to use

The **RegistrationReply Code** parameter is used by the R&S® CMU200 when building the Registration Reply to the mobile. This value is used in the Cause Code field of the Registration Reply message sent to the mobile and can be used to test the different failure conditions at the network.

The Registration Reply code can be configured using the "**RegistrationReply Code**" parameter found at:

Connect Control: Layer→ApplicationLayer → Packet Applications → Mobile IP

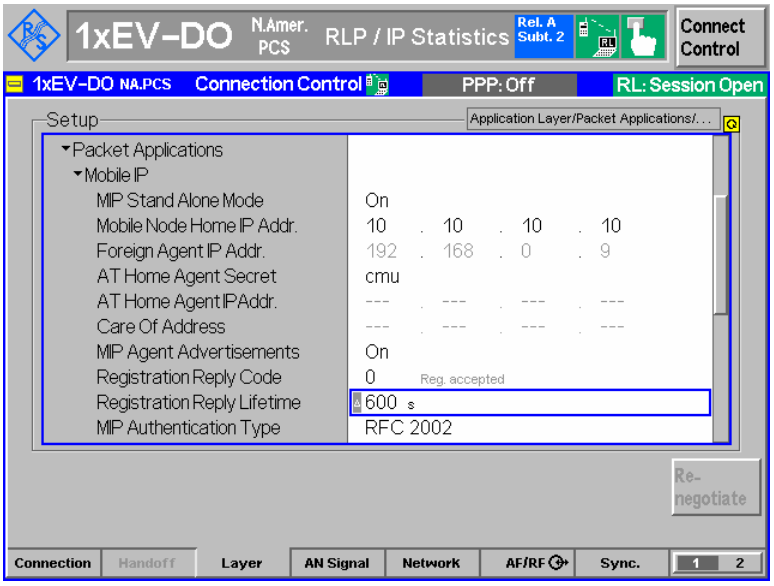


STEP 12 – Configure the Registration Reply Lifetime to use

The **RegistrationReply Lifetime** parameter is used by the R&S® CMU200 when building the Registration Reply and Agent Advertisement messages to the mobile. This value defines the number of seconds remaining before the registration is considered expired. A value of 0 indicates a request for deregistration and a value of 65535 indicates infinity.

The Registration Reply Lifetime can be configured using the "**RegistrationReply Lifetime**" parameter found at:

Connect Control: Layer→ApplicationLayer → Packet Applications → Mobile IP

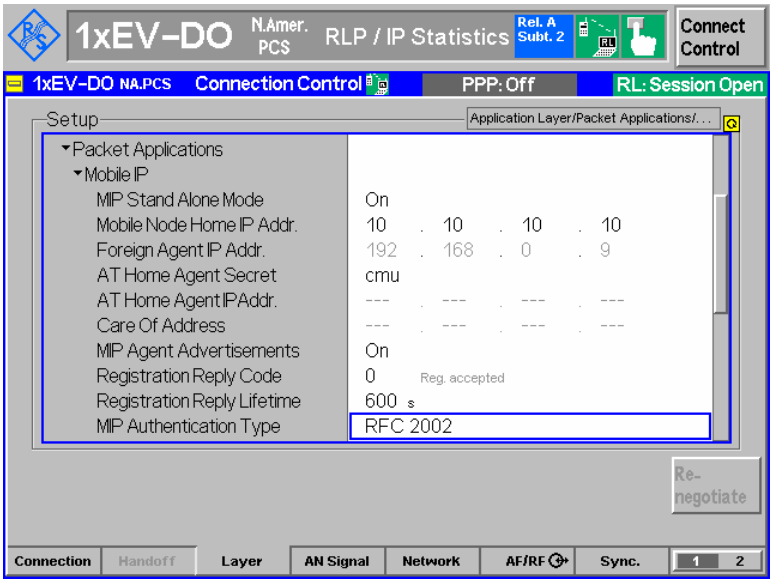


STEP 13 – Configure the Mobile IP **Authentication Type** to use

The **MIP Authentication** parameter is used by the R&S® CMU200 when encrypting/decrypting the Mobile IP messages. This value defines the authentication style used. A value of RFC 2002 (RFC 2002bis) indicates that the authentication procedure defined in RFC2000 (RFC 2002bis) is used.

The Mobile IP Authentication Type can be configured using the "**MIP Authentication**" parameter found at:

Connect Control: Layer→ApplicationLayer → Packet Applications → Mobile IP



STEP 14 – Configure **PPP Authentication**

See chapter 6; section "R&S® CMU200 Mobile IP Gateway Configuration without DHCP"; step 10 above.

STEP 15 – Configure the CDMA2000 1xEV-DO protocol stack data related parameters

See chapter 6; section "R&S® CMU200 Mobile IP Gateway Configuration without DHCP"; step 11 above.

STEP 16 – Configure the MAC Index used on the Forward Link Traffic Channel

See chapter 6; section "R&S® CMU200 Mobile IP Gateway Configuration without DHCP"; step 12 above.

MIP Mobile Phone / Windows Host PC Configuration

STEP 1 – Configure MIP Mobile phone when the R&S® CMU200 is in a Mobile IP Stand Alone mode.

Please refer to chapter 5; section "MIP Mobile Phone / Windows Host PC Configuration"; step 1 for the Mobile configuration except for the following parameters:

- Set *MN-HA Secret*

  The MN-HA secret should correspond to the value entered in the "**AT Home Agent Secret"** parameter in section "R&S® CMU200 Mobile IP Stand Alone Configuration without DHCP"; step 8 above. This is the secret used at the R&S® CMU200 and Mobile during the MD5 Authentication procedure.

- *MN-HA SPI*

  May use the default MN-HA SPI setting. This value is not used at the R&S® CMU200 when configured in a Mobile IP Stand Alone Mode.

- *Primary Home Agent IP Address*

  May use the default Primary Home Agent IP Address. This value is not used at the R&S® CMU200 when configured in a Mobile IP Stand Alone Mode.

- *Mobile Home IP Address*

  May use the default Mobile Home IP Address. This value is the IP Address allocated to the mobile and displayed at the R&S® CMU200 (see chapter 6; section "Making a Mobile IP Data Call and transferring data"; step 2).

STEP 2 – Configure Windows Host PC connected to the Mobile

See chapter 6; section "MIP Mobile Phone / Windows Host PC Configuration"; step 2.

Optional Windows PC Configuration

This PC could be configured to send/receive data to/from the Mobile.

STEP 1 - Configure the Windows PC Ethernet adapter with a static IP Address (IP #5) within the test subnet (see Figure 5)

Under Control Pannel→ "Network and Dial-Up Connections", select the Properties of the network connection interfacing with the CMU.

Select the Properties of the Internet Protocol (TCP/IP) component

Choose "Use the following IP addresses" and fill in the static IP Addresses

STEP 2 – Set up the routing tables

All data being sent to the mobile from the Windows PC needs to go through the R&S® CMU200. A route entry must be configured on the Windows PC to ensure data destined to the mobile is routed via the R&S® CMU200.

Execute the following commands:

```
>> route delete <<Mobile IP Subnet>>
>> route add <<Mobile IP Subnet>> mask 255.255.255.0 <<CMU IP (IP#1)>>
```

Example –

Assume the following R&S® CMU200 IP Address settings:

R&S® CMU200 IP Address: 192.168.0.2

Gateway IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

And mobile phone IP setting:

Mobile Home IP Address: 10.10.10.8

```
>> route delete 10.10.10.0 (assuming route exists already)
>> route add 10.10.10.0 mask 255.255.255.0 192.168.0.2
```

Making a Mobile IP CDMA2000 1xEV-DO Data Call and transferring data

STEP 1 – Establish a Mobile IP CDMA200 1xEV-DO Default Packet Application call

STEP 2 – Verify Mobile IP Information received at the CMU.

STEP 3a – Use the FTP Server within the R&S® CMU200 to transfer data

See chapter 6; section "Making a Mobile IP CDMA2000 1xEV-DO Data Call and transferring data"; steps 1-3a.

STEP 3b – Attempt to PING the mobile from the optional Windows PC

- On the Windows PC :

```
ping << Mobile Home IP Addr >>
```

The Mobile Home IP Address is the IP Address programmed in the mobile. The Mobile Home IP address can also be obtained from step 2 above.

STEP 3c – Attempt to PING the MIP mobile from R&S® CMU200

See chapter 6; section "Making a Mobile IP CDMA2000 1xEV-DO Data Call and transferring data"; step 3c.

STEP 3c – Transfer data to the mobile (forward link direction) using Iperf freeware packet generator tool

- On the Windows Host PC connected to the mobile, execute the following iperf command from the DOS command line :

```
> iperf –s –u –i 2
```

This command configures iperf to accept incoming UDP traffic on the default port 5001and displays packet statistics every 2 seconds.

- On the optional Windows PC (assuming iperf has been installed), execute the following iperf command from the command line :

```
> iperf –c << Mobile Home IP Addr >> –u –t 5000 –b 1000k
```

This configures the Windows PC to setup a connection with the Windows Host PC connected to the mobile and transfer UDP traffic for 5000 seconds at a bandwidth of 1 Mbps to the Mobile's IP Address.

NOTE: the execution of these 2 commands could be reversed (along with changing the Mobile Home IP Address to the Home Agent's IP Address) to test transferring data in the uplink direction.

STEP 4 – Monitor packet data flow statistics on the R&S® CMU200

See chapter 6; section "Making a Mobile IP CDMA2000 1xEV-DO Data Call and transferring data"; step 4.

8 R&S® CMU200 -Gateway Mobile IP Environment with DHCP

In this configuration, the R&S® CMU200 is setup to behave as a gateway between the Foreign Agent and MIP Mobile phone. A sample test environment *with* DHCP is described in Figure 6.

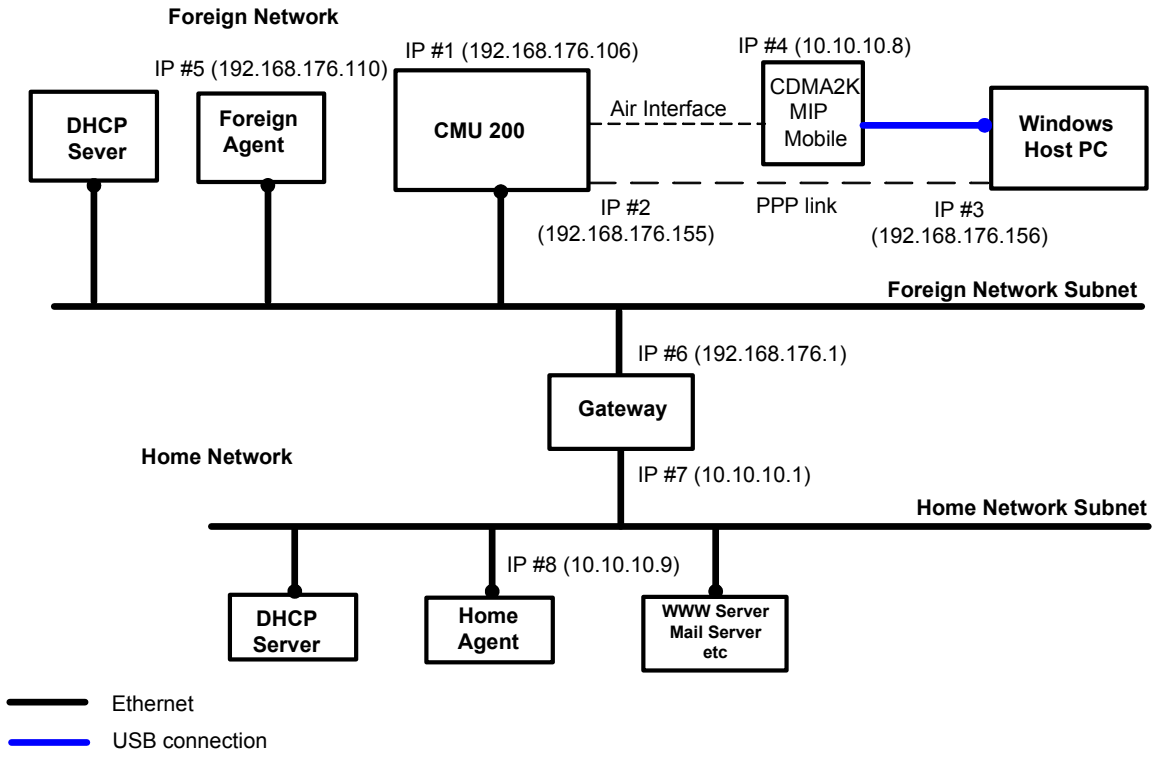


Figure 6. R&S® CMU200 (Gateway) Mobile IP test environment with DHCP

R&S® CMU200 Mobile IP Gateway Configuration with DHCP

STEP 1 – Configure the CDMA2000 1xEV-DO Network Release to be tested

STEP 2 – Configure the CDMA2000 1xEV-DO System Idenfication (SID)

STEP 3 – Configure the CDMA2000 1xEV-DO Sector ID informnation

STEP 4 – Configure the CDMA2000 1xEV-DO Application to the Default Packet Application

STEP 5 – Configure the Default Packet Application Stream ID

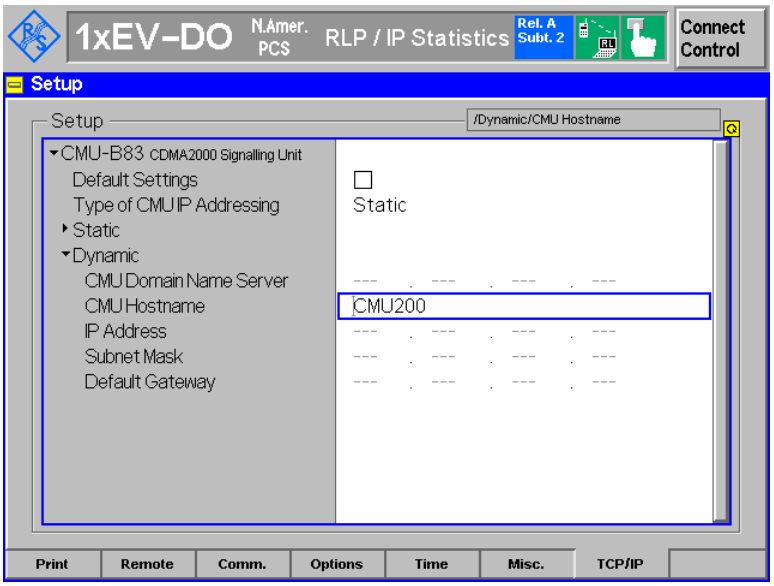
See chapter 6; section "R&S® CMU200 Mobile IP Gateway Configuration without DHCP"; steps 1-5.

STEP 6 - Configure the R&S® CMU200 with a hostname.

The hostname (rather than an IP Address) can then be used to communicate with the R&S® CMU200. The R&S® CMU200 hostname is registered with the DNS server during the IP Address acquisition phase.

The R&S® CMU200 can be configured with a hostname by setting the **"CMU200 Hostname"** parameter under:

SETUP → TCP/IP



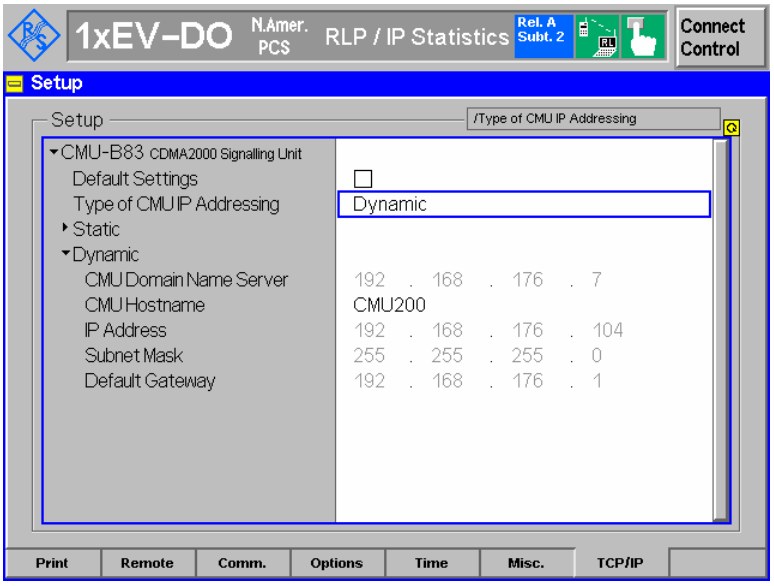
STEP 7 - Configure the R&S® CMU200 to use DHCP in order to acquire the IP Addresses.

The R&S® CMU200 is configured to interface with the DHCP server for acquiring all IP Addresses (R&S® CMU200 IP Address, R&S® CMU200 Gateway IP Address, R&S® CMU200 Subnet mask, AT PPP IP Address and the AN PPP IP Address).

The R&S® CMU200 can be configured to use Dynamic IP Addressing by setting the **"Type of CMU IP Addressing"** to Dynamic. The IP Addressing parameter can be found under:

SETUP → TCP/IP

Once the IP Addressing Mode is set to Dynamic, the R&S® CMU200 initiates communication with the DHCP server to acquire the IP Addresses. If the allocation was successful, the R&S® CMU200 IP Addresses are displayed.



➢ Verify that the DHCP server also allocated the dynamic **PPP IP Addresses**

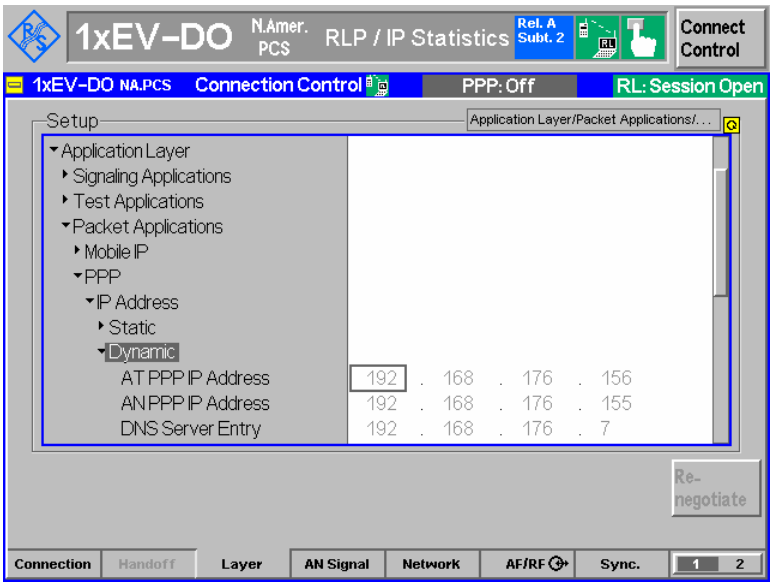
NOTE: The DHCP server must be configured to support the "Mobile IP Home Agent" option (the code for this option is 68). This TAG is used to return two IP Addresses that are used by the R&S® CMU200 for the AN PPP IP Address and the AT PPP IP Address.

In a mobile IP environment, the AT PPP IP address is *not* the IP address assigned to the mobile. A MIP capable mobile may use this AT PPP IP address as the co-located care of address in the case where a Foreign Agent care of address is not supplied in the Agent Advertisement message.

The AT PPP IP address is **not** utilized by the mobile since the R&S® CMU200 does not support a co-located care of address, however, the AT PPP IP address should still be configured properly. The AN PPP IP Address is used internally for IP packet routing purposes and should also be configured to be within the R&S® CMU200's subnet. The AN PPP and AT PPP IP Addresses assigned must be **different** than the CMU and Gateway IP Addresses (under Misc -> TCP/IP).

Connect Control:

Connect Control: Layer→ApplicationLayer → Packet Applications → PPP→ IP Addresses→Dynamic



STEP 8 - Configure the R&S® CMU200 to act as a Mobile IP Gateway

STEP 9 - Configure the R&S® CMU200 with the Foreign Agent IP Address

STEP 10 – Configure PPP Authentication

STEP 11 – Configure the CDMA2000 1xEV-DO protocol stack data related parameters

See chapter 6; section “R&S® CMU200 Mobile IP Gateway Configuration without DHCP”; step 11 above.

STEP 12 – Configure the MAC Index used on the Forward Link Traffic Channel

See chapter 6; section “R&S® CMU200 Mobile IP Gateway Configuration without DHCP”; step 12 above.

Dynamics Foreign and Home Agent Configuration

See Appendix B.

MIP Mobile Phone / Windows Host PC Configuration

See chapter 6; section “MIP Mobile Phone / Windows Host PC Configuration “.

Making a Mobile IP Call and transferring data

See chapter 6; section “Making a Mobile IP Call and transferring data”.

9 R&S® CMU200 -Stand Alone Mobile IP Configuration with DHCP

In this configuration, the R&S® CMU200 is setup to simulate the Foreign Agent and Home Agent functionality. A sample test environment *with* DHCP is described in Figure 7.

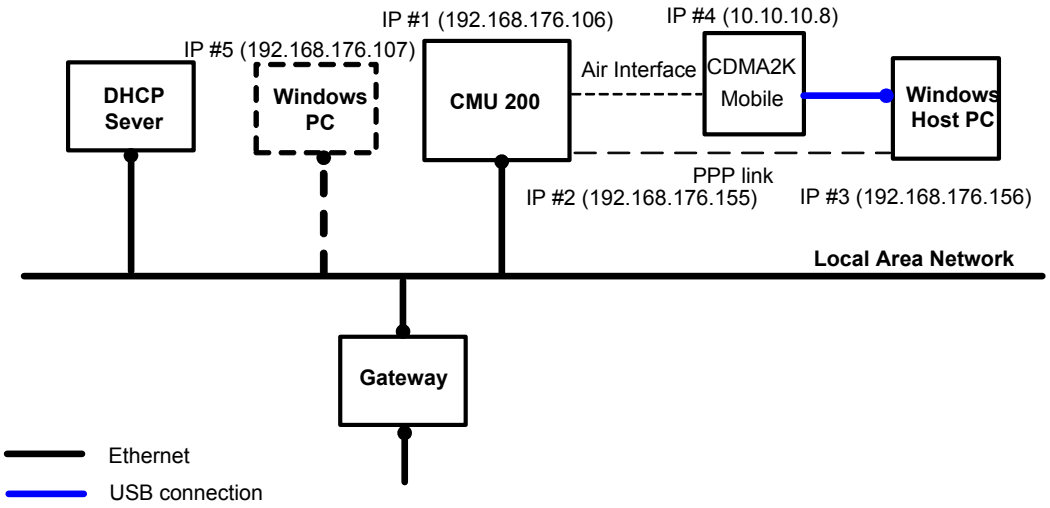


Figure 7. R&S® CMU200 (Stand Alone) Mobile IP test environment with DHCP

R&S® CMU200 Mobile IP Stand Alone Configuration with DHCP

STEP 1 – Configure the CDMA2000 1xEV-DO Network Release to be tested

STEP 2 – Configure the CDMA2000 1xEV-DO System Idenfication (SID)

STEP 3 – Configure the CDMA2000 1xEV-DO Sector ID informnation

STEP 4 – Configure the CDMA2000 1xEV-DO Application to the Default Packet Application

STEP 5 – Configure the Default Packet Application Stream ID

See chapter 6; section "R&S® CMU200 Mobile IP Gateway Configuration without DHCP"; steps 1-5.

STEP 6 - Configure the R&S® CMU200 with a hostname

STEP 7 - Configure the R&S® CMU200 to use DHCP in order to acquire the IP Addresses

See chapter 8; section "R&S® CMU200 Mobile IP Gateway Configuration with DHCP"; steps 6-7

STEP 8 - Configure the R&S® CMU200 in Mobile IP Stand Alone mode

See chapter 7; section "R&S® CMU200 Mobile IP Stand Alone Configuration without DHCP"; step 7.

STEP 9 - Configure the Mobile IP Home Agent Secret

See chapter 7; section "R&S® CMU200 Mobile IP Stand Alone Configuration without DHCP"; step 8.

STEP 10 – Configure PPP Authentication

STEP 11 – Configure the CDMA2000 1xEV-DO protocol stack data related parameters

See chapter 6; section "R&S® CMU200 Mobile IP Gateway Configuration without DHCP"; step 11 above.

STEP 12 – Configure the MAC Index used on the Forward Link Traffic Channel

See chapter 6; section "R&S® CMU200 Mobile IP Gateway Configuration without DHCP"; step 12 above.

MIP Mobile Phone / Windows Host PC Configuration

See chapter 7; section "MIP Mobile Phone / Windows Host PC Configuration.

Optional Windows PC Configuration

This PC could be configured to send/receive data to/from the Mobile.

STEP 1 - Configure the Windows PC Ethernet adapter with a dynamic IP Address

STEP 2 – Set up the routing tables

All data being sent to the mobile from the Windows PC needs to go through the R&S® CMU200. A route entry must be configured on the Windows PC to ensure data destined to the mobile is routed via the R&S® CMU200.

Execute the following commands:

```
>> route delete <<Mobile IP Subnet>>
>> route add <<Mobile IP Subnet>> mask 255.255.255.0 <<CMU IP (IP#1)>>
```

Example –

Assume the following R&S® CMU200 IP Address settings:

R&S® CMU200 IP Address: 192.168.176.106

Gateway IP Address: 192.168.176.1

Subnet Mask: 255.255.255.0

And mobile phone IP setting:

Mobile Home IP Address: 10.10.10.8

```
>> route delete 10.10.10.0 (assuming route exists already)
>> route add 10.10.10.0 mask 255.255.255.0 192.168.176.106
```

Making a Mobile IP Call and transferring data

See chapter 7; section “Making a Mobile IP Call and transferring data”.

10 Network Controlled PPP Establishment and Release

In a CDMA2000 1XEV-DO packet data environment, the network has the ability to automatically transition the AT from PPP Dormant to PPP Connected if there is data to transmit to the AT. The network also has the ability to transition the AT from PPP Connected to PPP Dormant if data is not being transmitted to the mobile after a specified period of time. This functionality is controlled by a parameter called **AN PPP Inactivity Timer**. If the timer is non-zero, the R&S® CMU200 will transition the call from PPP Connected to PPP Dormant if no AT directed data has been received for a period of **AN PPP Inactivity Timer** seconds. The R&S® CMU200 will transition the AT from PPP Dormant to PPP Connected once AT directed data is received. The automatic transitioning from PPP Dormant to PPP Connected is disabled if the **AN PPP Inactivity Timer** is set to "OFF".

Testing AN Inactivity Control (PPP Connected to PPP Dormant)

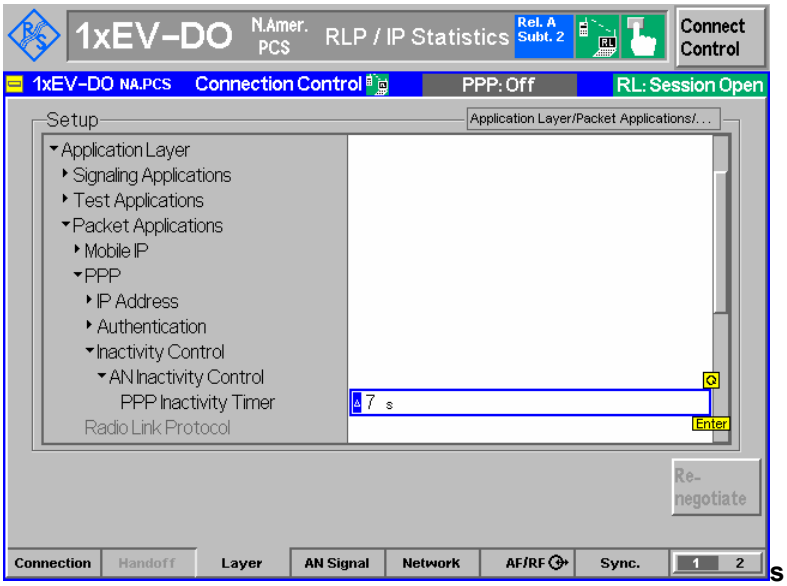
STEP 1 – Configure the AN PPP Inactivity Timer to a non-zero value

This parameter controls when and if the R&S® CMU200 will transition the AT from PPP Connected to PPP Dormant.

NOTE: if the timer is set to OFF, this functionality is disabled.

- The **AN PPP Inactivity Timer** parameter can be found at:

Connect Control: Layer → Application Layer → Packet Applicaiton→ PPP → Inactivity Control → AN Inactivity Control



STEP 2 – Initiate a Default Packet Application call and do not transmit any data to the AT.

The call will transition to PPP Dormant after **AN PPP Inact Timer** seconds.

Testing AN Inactivity Control (PPP Dormant to PPP Connected)

STEP 1 – Configure the AN PPP Inactivity Timer to a *non-zero* value

This parameter controls if the R&S® CMU200 will transition the AT from PPP Dormant to PPP Connected.

NOTE: if the timer is set to OFF, this functionality is disabled.

- The **AN PPP Inact Timer** parameter can be found at:

Connect Control: Layer → Application Layer → Packet Applicaiton→ PPP → Inactivity Control →AN Inactivity Control

STEP 2 – Establish a Default Packet Application call and wait for the call to transition to PPP Dormant.

STEP 3 – Transmit data to the AT

A call will be established and the AT will transition to PPP Connected and receive the data.

11 R&S® CMU200 Mobile IP Design Limitations

- R&S® CMU200 does not support IPv6
- R&S® CMU200 does not support a co-located care-of IP Address
- R&S® CMU200 does not allow the mobile to move between Foreign Agents – only one Foreign Agent can be connected to the R&S® CMU200.
- R&S® CMU200 does not support Mobile IP De-Registration (mobile moving from FA back to HA)

12 Dynamics Mobile IP Design Limitations

- Mobile Node Home IP Address equal to “0.0.0.0“ not supported
- Both Home Agent and Foreign Agent running on same Linux machine not supported

13 Simple IP

Simple IP calls are Default Packet Application calls that do not support the Mobile IP functionality. The differences between Mobile IP and Simple IP calls are as follows:

- Mobile IP Registration/Authenticaiton is **not** performed with Simple IP calls
- PPP Authentication is allowed (CHAP or PAP) for Simple IP calls
- The IP Address allocated to a Simple IP call is assigned during PPP link establishment (IPCP protocol). The value assigned to the mobile is determined by the **AT PPP IP Address** parameter.

R&S® CMU200 Simple IP Configuration without DHCP

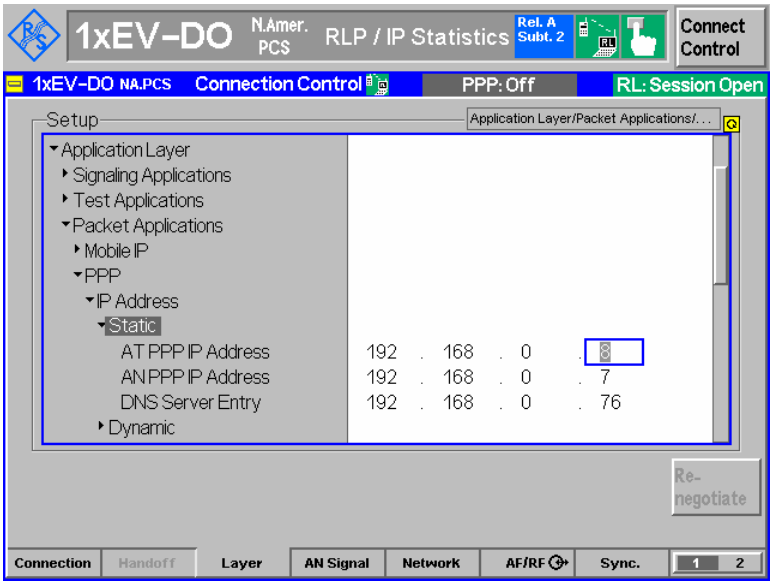
STEP 1 - Configure the R&S® CMU200 to use static IP Addressing (see Chapter 6) or dynamic IP Addressing (see Chapter 8)

STEP 2 - Configure the IP Addresses to be used for the Simple IP mobile (static IP Addressing)

The AN PPP and AT PPP IP Addresses assigned must be **different** than the CMU and Gateway IP Addresses (under Misc -> TCP/IP).

The PPP IP Addresses can be found at:

Connect Control: Layer → Application Layer → Packet Applicaiton→ PPP → IPAddresses



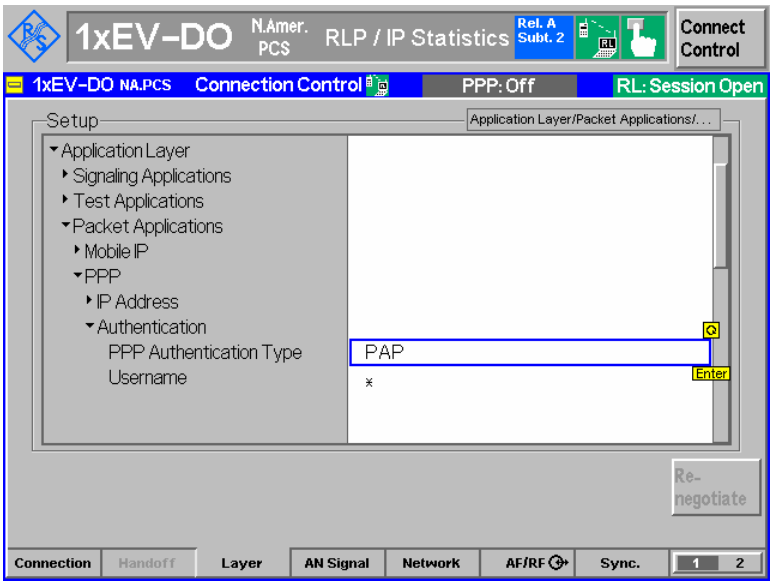
STEP 3 - Configure PPP Authentication

For Simple IP calls, both the PAP and CHAP authentication protocols are supported. The username and password are configurable for both authentication protocols.

See RFC 1334 for more details.

The PPP Authentication parameters can be found at:

Connect Control: Layer → Application Layer → Packet Applicaiton→ PPP → Authentication



14 Rerferences

[1] TIA- 856-A-1 – CDMA2000 High Rate Packet Data – Air Interface Specification – Addendum 1

[2] Mobile IP, The Internet Unplugged, James D. Solomon

[3] http://dynamics.sourceforge.net/ - The Dynamics Mobile IP system, originally developed at Helsinki University of Technology (HUT)

RFC 1334 – PPP Authentication Protocols

15 R&S® CMU200 Ordering Information

R&S® CMU200	Universal Radio Communications Tester
R&S® CMU-B83 Var 12	CDMA2000 signalling unit (supports CMU-B88)
R&S® CMU-B83 Var 22	New CDMA2000 signalling unit (ready for CMU-B89)
R&S® CMU-U83 Var 22	CDMA2000 signalling unit, upgrade from CMU-B83 Var 12
R&S® CMU-B85 Var 22	Speech Coder for 8K BASIC, 8K EVRC, 13K (for CMU-B83 Var 22)
R&S® CMU-U85 Var 22	Speech Coder for 8K BASIC, 8K EVRC, 13K (for CMU-B83 Var 22) upgrade from CMU-B85 Var 12
R&S® CMU-K839	1xEV-DO, 450MHz (Band Class 5, 11)
R&S® CMU-K849	1xEV-DO, Cellular band (Band Class 0, 2, 3, 7, 9, 10, 12)
R&S® CMU-K859	1xEV-DO, PCS band (Band Class 1, 4, 8, 14, 15)
R&S® CMU-K869	1xEV-DO, IMT band (Band Class 6, 13)
R&S® CMU-PK800	SW Package for 1xEV-DO
R&S® CMU-U65	3G Measurement DSP module
R&S® CMU-B88	1xEV-DO Transmitter Board (for CMU-B83 Var 12)
R&S® CMU-B89	1xEV-DO Signaling Module (for CMU-B83 Var 22)
R&S® CMU-B87	Interface for CDMA2000 / 1xEV-DO Data Testing
R&S® CMU-K88	1xEV-DO Access Terminal Test (NSig only)
R&S® CMU-K87	CDMA2000 / 1xEV-DO Data Testing

Appendix A – Dynamics Software Configuration without DHCP

Dynamics Foreign Agent Configuration

STEP 1 – Compile Dynamics Mobile IP Foreign Agent v0.8.1 Software on Mandrake 9.1

- Obtain the Dynamics Mobile IP software tar file (dynamics-0.8.1.tar) containing all of the source code and documentation (http://dynamics.sourceforge.net/).
- Login as 'root'
- Create a directory for the software (e.g. /usr/src/MobileIP) and move the tar file into the new directory.
- Extract the files from the tar file from the new directory using the following command

  ```
  >> tar –xvf dynamics-0.8.1.tar
  ```

  This will expand the tar file and create the following directory:

  ```
  /usr/src/MobileIP/dynamics-0.8.1/
  ```

- 'cd' to the directory containing the package's source code (`/usr/src/MobileIP/dynamics-0.8.1/`) and execute the 'configure' command :

  ```
  >> ./configure
  ```

  Ensure that there are no errors when executing the 'configure' command.

- Compile the software by executing the following command from the directory containing the package's source code (`/usr/src/MobileIP/dynamics-0.8.1/`):

  ```
  >> make
  ```

  Ensure that there are no errors when executing the 'make' command. It may be necessary to install additional GNU C libraries (Start→ Configuration→ Packaging→ Install Software) to get a clean compile.

- Optionally, type 'make check' to run any self-tests that come with the package:

  ```
  >> make check
  ```

- Install the programs, data files and documentation:

  ```
  >> make install
  ```

(Additional information about compilation, installation and execution is located in the /usr/src/MobileIP/dynamics-0.8.1/INSTALL and README documents.)

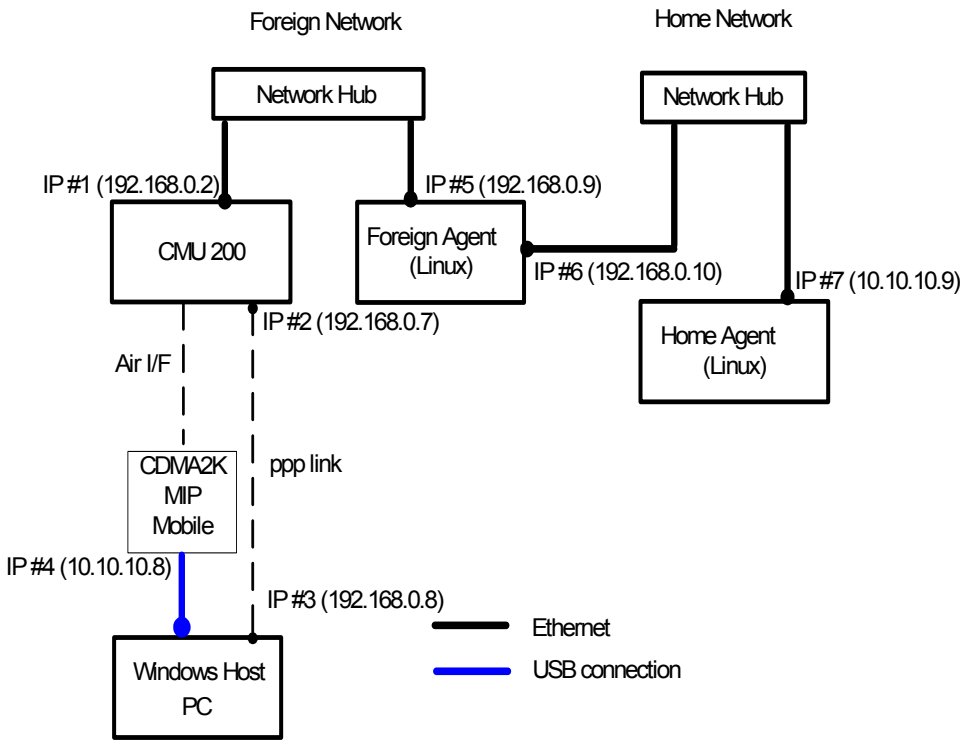


Figure 8. R&S® CMU200 (Gateway) Mobile IP test environment without DHCP

STEP 2 – Linux Networking Configuration (Ethernet Adapters and Gateway)

- Login as 'root'
- Execute netconf from the start menu:

  Start→ Configuration→ Networking→ netconf
- Select "Host name and IP network devices"
  - Configure Adapter 1 – this is the Ethernet interface connected to the R&S® CMU200
    - Enabled
    - Manual
    - Configure the IP Address (IP#5). This IP Address should match the Gateway IP Address configured in the R&S® CMU200. See chapter 6; section "R&S® CMU200 Mobile IP Gateway Configuration without DHCP"; step 1.
    - Configure the Netmask (e.g. 255.255.255.0)
    - Select net device (eth0)
  - Configure Adapter 2 – this is the Ethernet interface connected to the Home Agent
    - Enabled
    - Manual
    - Configure the IP Address (IP#6).

- Configure the Netmask (e.g. 255.255.255.0)
- Select net device (eth1)

- "Accept" Changes

NOTE: IP#5 and IP#6 must be on the same subnet as the R&S® CMU200. E.g. If the R&S® CMU200 has an IP Address of 192.168.0.2 and netmask 255.255.255.0, the Foreign Agent IP Addresses must reside in the 192.168.0.X subnet.

- Select "Routing and Gateways"

- Configure Default Gateway as IP#6; enable routing selected
- Configure Routed Daemon
  - Uncheck both boxes
- "Dismiss" to accept changes

- Select "Quit"
- Select "Do It"

(After Step 2, you will need to reboot Linux machine for these routing changes to take effect)

STEP 3 – Linux Networking Configuration (Network Routing Tables)

- Login as 'root'

Example 'route' commands using 192.168.0.X as the Foreign Agent network and 10.10.10.X as the Home Agent Network.

Delete all routes with a destination of 192.168.0.X

Example 'route del' command to remove an existing route:

```
>> route del –net 192.168.0.0 netmask 255.255.255.0 dev eth1
```

- Add following routes:

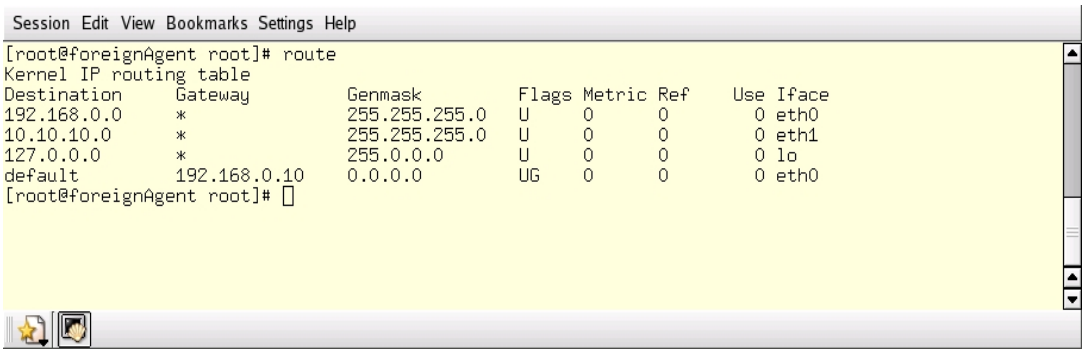
1. All packets destined to Foreign Agent network go out **eth0** device
2. All packets destined to Home Agent network go out **eth1** device

```
>> route add –net 192.168.0.0 netmask 255.255.255.0 dev eth0

>> route add –net 10.10.10.0 netmask 255.255.255.0 dev eth1
```

Display the route table for this example (default Gateway of 192.168.0.10)

```
>> route
```



STEP 4 – Foreign Agent Configuration – dynfad.conf

- Change into the Foreign Agent directory

  `>> cd /usr/src/MobileIp/dynamics-0.8.1/src/fa`

- Edit the dynfad.conf file
  - Configure **INTERFACES** parameter

    Set the eth0 and eth1 IP addresses equal to the IP Address of the Adapter interfacing with the Home Agent (IP#6)

Example INTERFACES configuration based on an IP#6 of 192.168.0.10.

```
INTERFACES_BEGIN
eth0          3       1        10        192.168.0.10
eth1          2       -1       20        192.168.0.10
INTERFACES_END
```

  - Configure **HighestFAIPAddress** parameter

    Set this parameter equal to the IP Address specified in the INTERFACES element (IP #6)

  - Configure **UpperFAIPAddress** parameter

    Set this parameter equal to the IP Address specified in the INTERFACES element (IP #6)

  - Configure **RegistrationTTLCheck** parameter

    Set this parameter equal to 0

  - Configure **EnableReverseTunneling** parameter

    Set this parameter equal to FALSE

    (The rest of the configuration elements could be left as the default values)

STEP 5 – Configuration of Ethereal (optional)

- Login as 'root'
- Execute Ethereal

  `>> ethereal &`

This tool will allow the user to decode all IP packets sent to/from the Foreign Agent.

STEP 6 – Start Foreign Agent daemon

- Login as 'root'
- Load the IP tunneling module (execute once)

```
>> insmod ipip
```

- Enable IP forwarding and turn off reverse filtering (execute once)

```
>> echo 1 > /proc/sys/net/ipv4/ip_forward
>> echo 0 > /proc/sys/net/ipv4/conf/all/rp_filter
```

- Change into the Foreign Agent directory and start the Foreign Agent daemon with debugging enabled:

```
>> cd /usr/src/MobileIp/dynamics-0.8.1/src/fa
>> ./dynfad --fg --debug --config ./dynfad.conf
```

(Additional information about compilation, installation and execution is located in the /usr/src/MobileIP/dynamics-0.8.1/INSTALL and README documents.)

At this point, you should see Agent Advertisements being broadcasted from the Foreign Agent to the R&S® CMU200. This can be verified by monitoring the network traffic using a network analyzer, e.g. Ethereal.

Dynamics Home Agent Configuration

STEP 1 – Compile Dynamics Mobile IP Home Agent v0.8.1 Software on Mandrake 9.1

- Obtain the Dynamics Mobile IP software tar file (dynamics-0.8.1.tar) containing all of the source code and documentation.
- Login as 'root'
- Create a directory for the software (e.g. /usr/src/MobileIP) and move the tar file into the new directory.
- Extract the files from the tar file from the new directory using the following command

```
>> tar –xvf dynamics-0.8.1.tar
```

  This will expand the tar file and create the following directory:

```
/usr/src/MobileIP/dynamics-0.8.1/
```

- 'cd' to the directory containing the package's source code (`/usr/src/MobileIP/dynamics-0.8.1/`) and execute the 'configure' command :

```
>> ./configure
```

  Ensure that there are no errors when executing the 'configure' command.

- Compile the software by executing the following command from the directory containing the package's source code (`/usr/src/MobileIP/dynamics-0.8.1/`):

```
>> make
```

Ensure that there are no errors when executing the 'make' command. It may be necessary to install additional GNU C libraries (Start→ Configuration→ Packaging→ Install Software) to get a clean compile.

- Optionally, type 'make check' to run any self-tests that come with the package:

  ```
  >> make check
  ```

- Install the programs, data files and documentation:

  >> make install

(Additional information about compilation, installation and execution is located in the /usr/src/MobileIP/dynamics-0.8.1/INSTALL and README documents.)

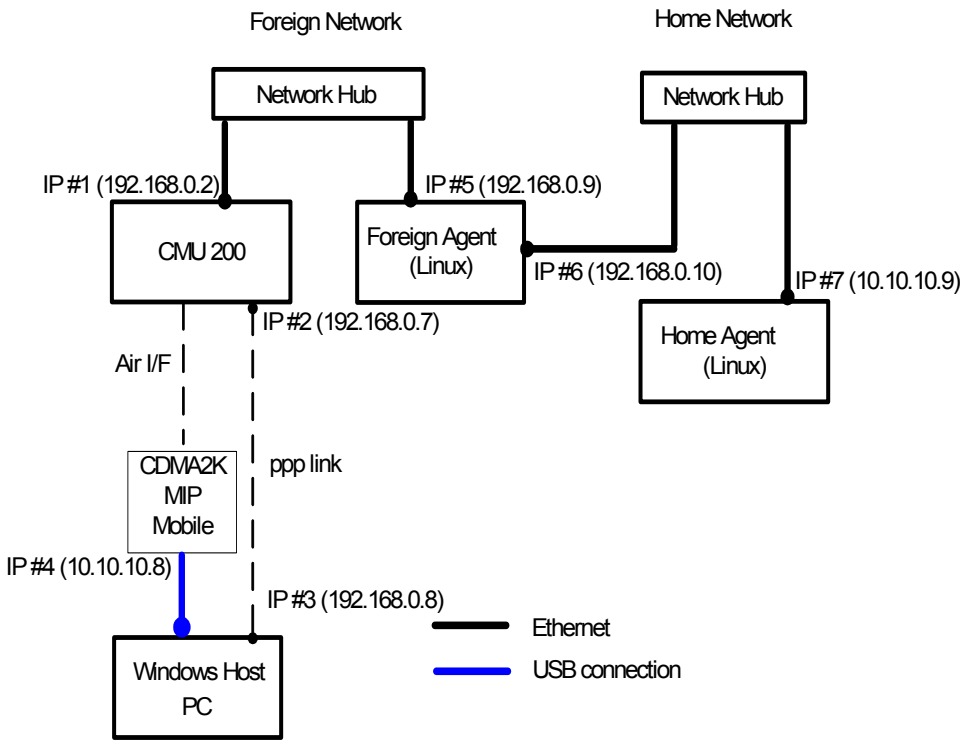


Figure 9. R&S® CMU200 (Gateway) Mobile IP test environment without DHCP

STEP 2 – Linux Networking Configuration (Ethernet Adapter and Gateway)

- Login as 'root'
- Execute netconf from the start menu:

  Start→ Configuration→ Networking→ netconf
- Select "Host name and IP network devices"
  - Configure Adapter 1 – this is the Ethernet interface connected to the Foreign Agent
    - Enabled
    - Manual
    - Configure the IP Address (IP#7).
    - Configure the Netmask (e.g. 255.255.255.0)
    - Select net device (eth0)
  - Accept Changes

- Select "Routing and Gateways"
  - Configure Default Gateway – leave empty; enable routing selected
  - Configure Routed Daemon
    - Uncheck both boxes
  - "Dismiss" to accept changes

- Select “Quit”
- Select “Do It”

  (After Step 2, you may need to reboot Linux machine for these routing changes to take effect)

STEP 3 – Linux Networking Configuration (Network Routing Tables)

- Login as ‘root’
- Delete any unnecessary routes

  Example ‘route del’ command to remove an existing route :

```
>> route del –net 192.168.0.0 netmask 255.255.255.0 dev eth1
```

- Add following routes (if not already configured)

  1. All packets destined to Foreign Agent network go out **eth0** device
  2. All packets destined to Home Agent network go out **eth0** device

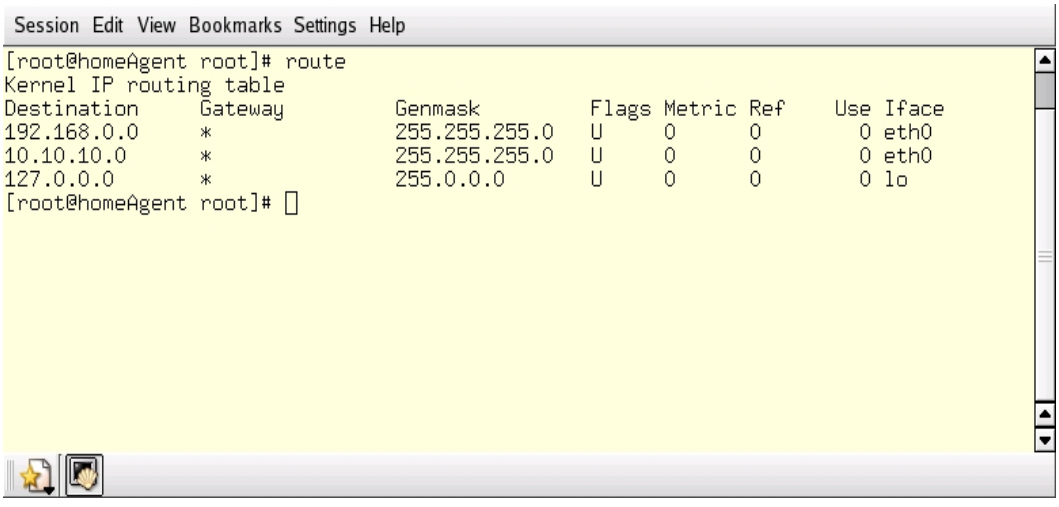
  Example ‘route’ commands using 192.168.0.X as the Foreign Agent network and 10.10.10.X as the Home Agent Network:

```
>> route add –net 192.168.0.0 netmask 255.255.255.0 dev eth0

>> route add –net 10.10.10.0 netmask 255.255.255.0 dev eth0
```

  Display the route table for this example

```
>> route
```



STEP 4 – Home Agent Configuration – dynhad.conf

- Change into the Home Agent directory

  ```
  >> cd /usr/src/MobileIp/dynamics-0.8.1/src/ha
  ```

- Edit the dynhad.conf file

  - Configure **INTERFACES** parameter

    Set the eth0 IP address equal to the IP Address of the Adapter (IP#7). If the IP address field is left blank, the primary address of the interface is used.

    ```
    INTERFACES_BEGIN
    eth0          1   1         10
    INTERFACES_END
    ```

  - Configure **EnableReverseTunneling** parameter

    Set this parameter equal to FALSE

  - Configure **AUTHORIZEDLIST** parameter

    Set the SPI (Security Parameter Index) and IP Address equal to what is programmed in the mobile phone. SPI is the key identificator for the rest of the security parameters on the same line. This value is used as a look up index in the Home Agent's database to retrieve the mobile's shared secret information.

    # on the same line

    Example AUTHORIZEDLIST configuration based on a SPI of 1234 and mobile Node Home IP Address of 10.10.10.8.

    ```
    AUTHORIZEDLIST_BEGIN
    # SPI            IP
    1234         10.10.10.8
    AUTHORIZEDLIST_END
    ```

  - Configure **SECURITY** parameter

    Set the SPI (Security Parameter Index), Authentication Algorithm and secret code equal to what is programmed in the mobile phone.

    Below is an example of a SECURITY configuration based on a SPI of 1234, MD5 Authentication Algorithm and a secret code of "cmu".

    ```
    SECURITY_BEGIN

    #       auth.    replay  timestamp       max           shared
    # SPI   alg.     meth.   tolerance       lifetime      secret

    1234     1          0           600          120           "cmu"

    SECURITY_END
    ```

  (The rest of the configuration elements could be left as the default values)

STEP 5 – Configuration of Network Analyzer tool (optional)

Ethereal is a network protocol analyzer, or "packet sniffer", that lets you capture and interactively browse the contents of network frames.

- Login as 'root'
- Execute Ethereal

  ```
  >> ethereal &
  ```

  This tool will allow the user to decode all IP packets sent to/from the Home Agent.

STEP 6 – Start Home Agent daemon

- Login as 'root'
- Load the IP tunneling module (execute once)

  ```
  >> insmod ipip
  ```

- Enable IP forwarding and turn off reverse filtering (execute once)

  ```
  >> echo 1 > /proc/sys/net/ipv4/ip_forward
  >> echo 0 > /proc/sys/net/ipv4/conf/all/rp_filter
  ```

- Change into the Home Agent directory and start the Home Agent daemon with debugging enabled:

  ```
  >> cd /usr/src/MobileIp/dynamics-0.8.1/src/ha
  >> ./dynhad --fg --debug --config ./dynhad.conf
  ```

(Additional information about compilation, installation and execution is located in the /usr/src/MobileIP/dynamics-0.8.1/INSTALL and README documents.)

At this point, you should see Agent Advertisements being broadcasted from the Home Agent. This can be verified by monitoring the network traffic using a network analyzer, e.g. Ethereal.

Appendix B – Dynamics Software Configuration with DHCP

Dynamics Foreign Agent Configuration

This configuration is slightly different from the Dynamics Foreign Agent Configuration in Appendix A. It requires configuring the network interface cards in a dynamic (DHCP) configuration. Only these differences will be documented - references to Appendix A will be used whenever possible.

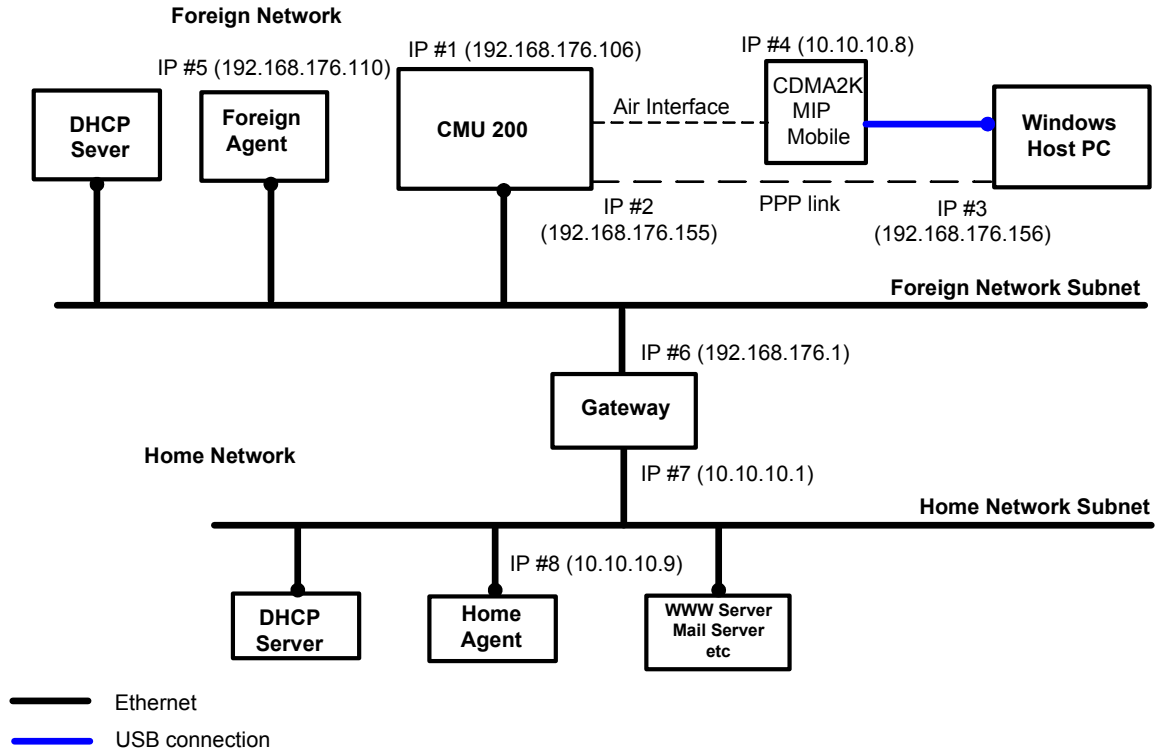


Figure 10. R&S® CMU200 (Gateway) Mobile IP test environment with DHCP

STEP 1 – Compile Dynamics Mobile IP Foreign Agent v0.8.1 Software on Mandrake 9.1
See Appendix A; section "Dynamics Foreign Agent Configuration"; step 1 above.

STEP 2 – Linux Networking Configuration (Ethernet Adapters and Gateway)

See Appendix A; section "Dynamics Foreign Agent Configuration"; step 2 above. Replace only the following sections:

- Select "Host name and IP network devices"
  - Configure Adapter 1 – this is the Ethernet interface connected to the Foreign Network Subnet

- Enabled
- Automatic
- Select net device (eth0)

o "Accept" Changes

NOTE: IP#5 and IP#6 will be on the same subnet as the R&S® CMU200.

➢ Select "Routing and Gateways"

o Configure Default Gateway as IP#6; enable routing selected

o Configure Routed Daemon

- Uncheck both boxes

o "Dismiss" to accept changes

STEP 3 – Linux Networking Configuration (Network Routing Tables)

See Appendix A; section "Dynamics Foreign Agent Configuration"; step 3 above. Replace only the following sections:

➢ Add following routes:

1. All packets destined to Foreign Agent network go out **eth0** device
2. All other packets go out **eth0** device via the Default Gateway

Example 'route' command using 192.168.176.X as the Foreign Agent network and 10.10.10.X as the Home Agent Network:

```
>> route add –net 192.168.176.0 netmask 255.255.255.0 dev eth0
```

STEP 4 – Foreign Agent Configuration – dynfad.conf

See Appendix A; section "Dynamics Foreign Agent Configuration"; step 4 above. Replace only the following sections:

➢ Edit the dynfad.conf file

o Configure **INTERFACES** parameter

Set the eth0 IP addresses equal to the IP Address assigned to the Adapter interfacing with the Home Agent (IP#5). By leaving the IP Address field blank, the primary address of the interface is used.

```
INTERFACES_BEGIN
eth0          3    1          10
INTERFACES_END
```

o Configure **HighestFAIPAddress** parameter

Set this parameter equal to the IP Address specified in the INTERFACES element (IP #5)

o Configure **UpperFAIPAddress** parameter

Set this parameter equal to the IP Address specified in the INTERFACES element (IP #5)

STEP 5 – Configuration of Ethereal (optional)

See Appendix A; section “Dynamics Foreign Agent Configuration”; step 5 above.

STEP 6 – Start Foreign Agent daemon

See Appendix A; section “Dynamics Foreign Agent Configuration”; step 6 above.

Dynamics Home Agent Configuration

This configuration is slightly different from the Dynamics Home Agent Configuration in Appendix A. It requires configuring the network interface cards in a dynamic (DHCP) configuration. Only these differences will be documented - references to Appendix A will be used whenever possible.

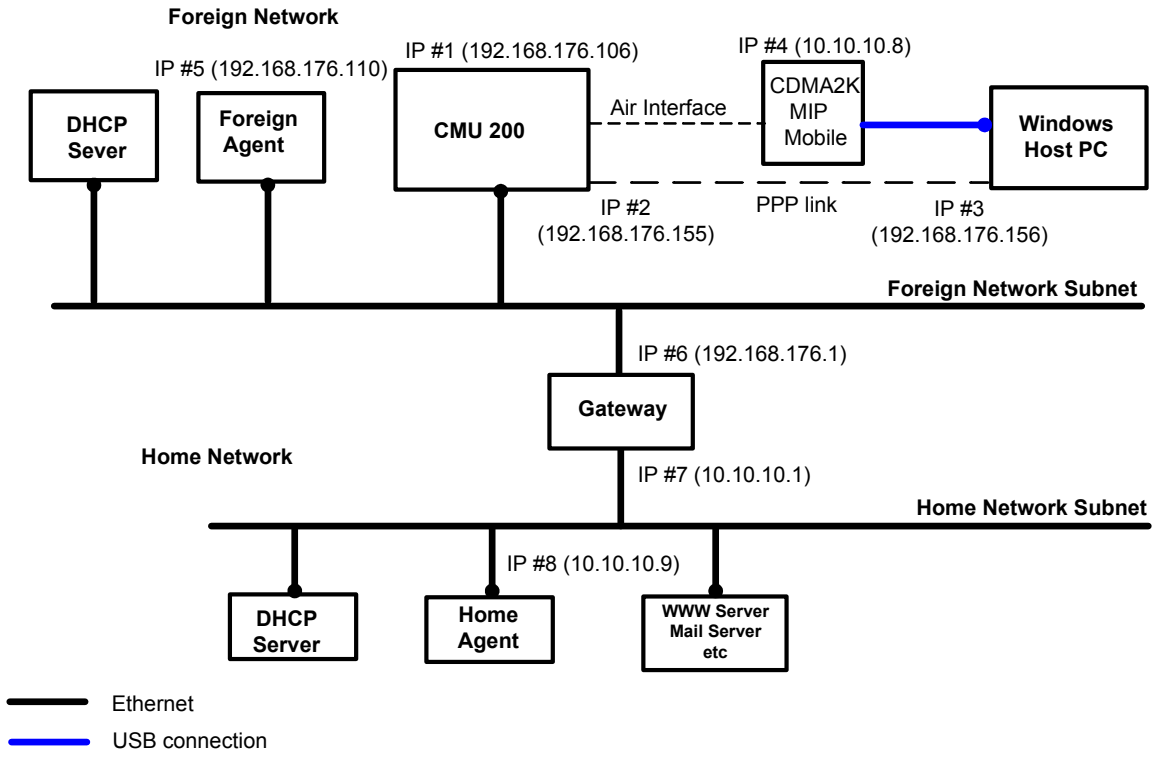


Figure 11. R&S® CMU200 (Gateway) Mobile IP test environment with DHCP

STEP 1 – Compile Dynamics Mobile IP Home Agent v0.8.1 Software on Mandrake 9.1

See Appendix A; section “Dynamics Home Agent Configuration “; step 1 above.

STEP 2 – Linux Networking Configuration (Ethernet Adapter and Gateway)

See Appendix A; section “Dynamics Home Agent Configuration”; step 2 above. Replace only the following sections:

- Select “Host name and IP network devices”
  - Configure Adapter 1 – this is the Ethernet interface connected to the Home Network Subnet
    - Enabled
    - Automatic
    - Select net device (eth0)
  - Accept Changes

- Select “Routing and Gateways”
  - Configure Default Gateway as IP#7; enable routing selected
  - Configure Routed Daemon
    - Uncheck both boxes
  - “Dismiss” to accept changes

STEP 3 – Linux Networking Configuration (Network Routing Tables)

See Appendix A; section “Dynamics Home Agent Configuration”; step 3 above. Replace only the following sections:

- Add following routes (if not already configured)

1. All packets destined to Home Agent network go out **eth0** device
2. All other packets go out **eth0** device via the Default Gateway

```
>> route add –net 10.10.10.0 netmask 255.255.255.0 dev eth0
```

STEP 4 – Home Agent Configuration – dynhad.conf

See Appendix A; section “Dynamics Home Agent Configuration”; step 4 above. Replace only the following sections:

- Edit the dynhad.conf file
  - Configure **INTERFACES** parameter

Set the eth0 IP address equal to the IP Address of the Adapter (IP#8). If the IP address field is left blank, the primary address of the interface is used.

```
INTERFACES_BEGIN
eth0          1   1         10
INTERFACES_END
```

STEP 5 – Configuration of Ethereal (optional)

See Appendix A; section “Dynamics Home Agent Configuration”; step 5

STEP 6 – Start Home Agent daemon

See Appendix A; section “Dynamics Home Agent Configuration”; step 6

[1] CDMA2000® is a registered trademark of the Telecommunications Industry Association (TIA -USA)

ROHDE & SCHWARZ GmbH & Co. KG · Mühldorfstraße 15 · D-81671 München · P.O.B 80 14 69 · D-81614 München ·
Telephone +49 89 4129 -0 · Fax +49 89 4129 - 13777 · Internet: http://www.rohde-schwarz.com