

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

¹CDMA2000®

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.



Subject to change – T. Opferman, 8.2005 – 1CM 51_3E v2.1

Contents

1	Introduction.....	3
2	Definitions.....	3
3	Mobile IP Overview	5
4	Hardware and Software Requirements for the Dynamics Home Agent and Foreign Agent	8
5	R&S® CMU200 Gateway Mobile IP Environment without DHCP	10
	R&S® CMU200 Mobile IP Gateway Configuration without DHCP... ..	11
	Dynamics Foreign Agent Configuration	15
	Dynamics Home Agent Configuration	20
	MIP Mobile Phone / Windows Host PC Configuration.....	25
	Making a Mobile IP Data Call and transferring data.....	26
6	R&S® CMU200 -Standalone Mobile IP Environment without DHCP ...	30
	R&S® CMU200 Mobile IP Stand Alone Configuration without DHCP	31
	MIP Mobile Phone / Windows Host PC Configuration.....	36
	Optional Windows PC Configuration	37
	Making a Mobile IP Data Call and transferring data.....	38
7	R&S® CMU200 -Gateway Mobile IP Environment with DHCP	40
	R&S® CMU200 Mobile IP Gateway Configuration with DHCP	41
	Dynamics Foreign Agent Configuration	44
	Dynamics Home Agent Configuration	47
	MIP Mobile Phone / Windows Host PC Configuration.....	49
	Making a Mobile IP Call and transferring data	49
8	R&S® CMU200 -Stand Alone Mobile IP Configuration with DHCP	50
	R&S® CMU200 Mobile IP Stand Alone Configuration with DHCP.. ..	50
	MIP Mobile Phone / Windows Host PC Configuration.....	51
	Optional Windows PC Configuration	51
	Making a Mobile IP Call and transferring data	51
9	Packet Data Mobility Management.....	52
	Triggering a Packet Zone Update in the <i>same</i> PDSN/FA	54
	Triggering a Packet Zone Update in a <i>different</i> PDSN/FA	55
	Testing the Packet Zone Connection Control feature	57
10	Network Controlled PPP Establishment and Release	59
	Testing BS Inactivity Control (PPP Connected to PPP Dormant) ..	59
	Testing BS Inactivity Control (PPP Dormant to PPP Connected) ..	60
	Testing MS Packet Dormant Timer Control	61
11	R&S® CMU200 Mobile IP Design Limitations	63
12	Dynamics Mobile IP Design Limitations	63
13	Simple IP.....	64
	R&S® CMU200 Simple IP Configuration without DHCP.....	64
14	References	66
15	R&S® CMU200 Ordering Information	66

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 service option 33. 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 its 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.

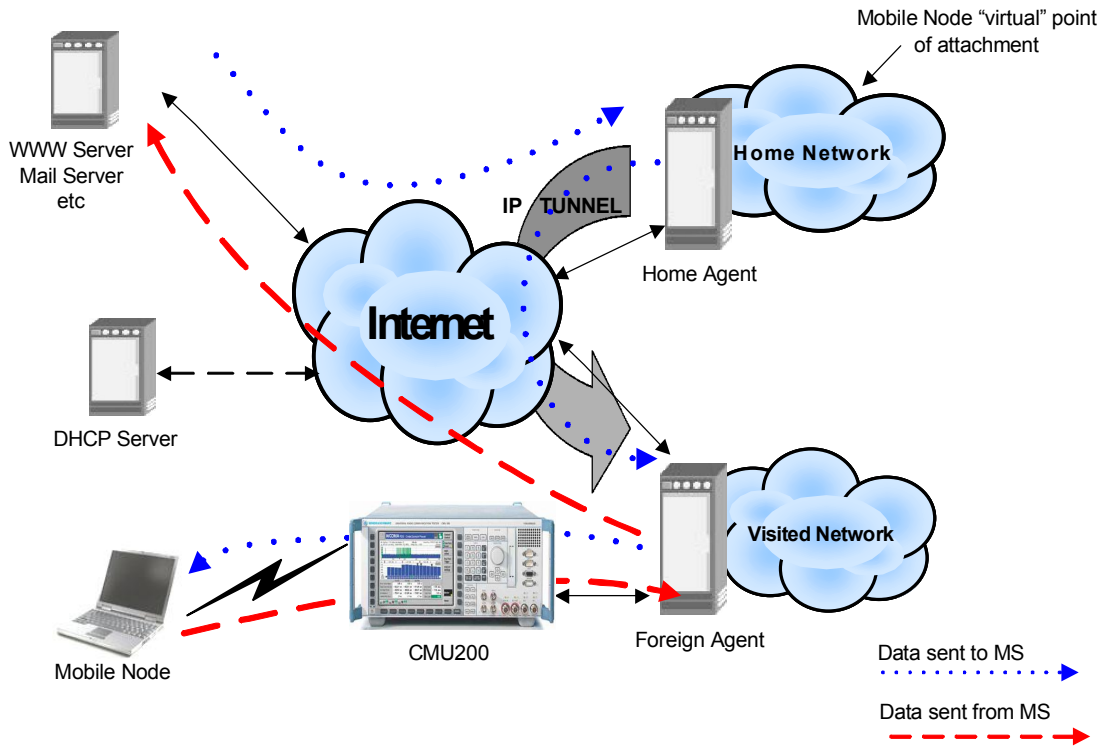


Figure 1. R&S® CMU200 Mobile IP test environment (Gateway mode)

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.

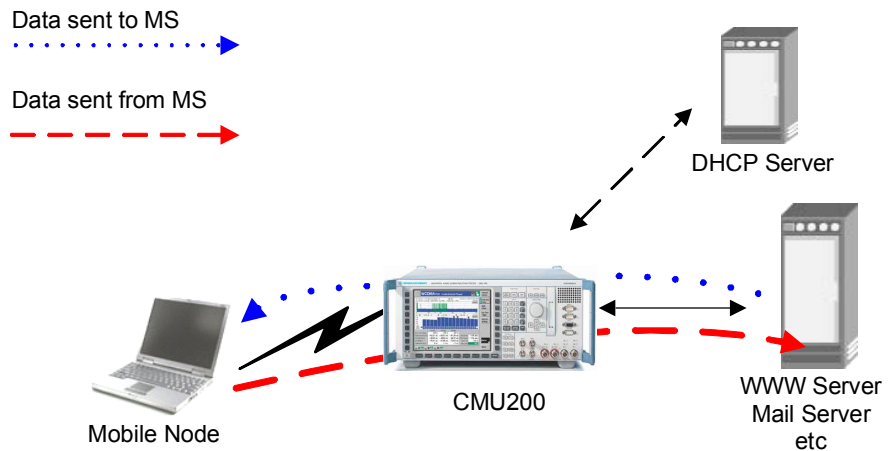


Figure 2. R&S® CMU200 Mobile IP test environment (Stand Alone mode)

4 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[®] CMU200 configured in a Mobile IP Gateway mode (see Figure 1) *with* DHCP enabled.
- R&S[®] CMU200 configured 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.

5 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 MIP Mobile phone. A sample test environment *without* DHCP is described in Figure 3.

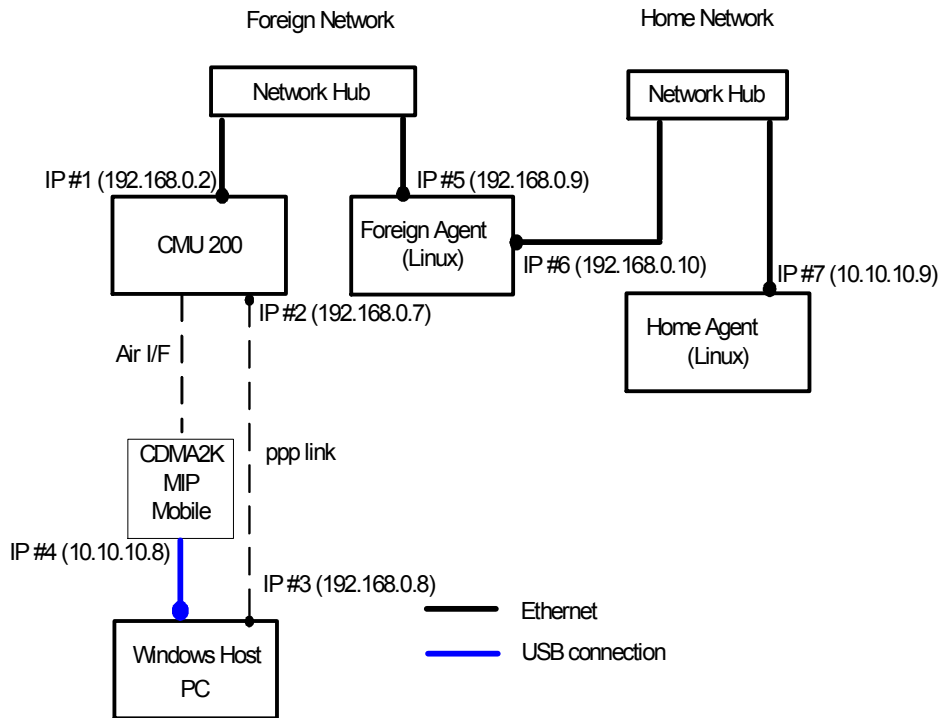


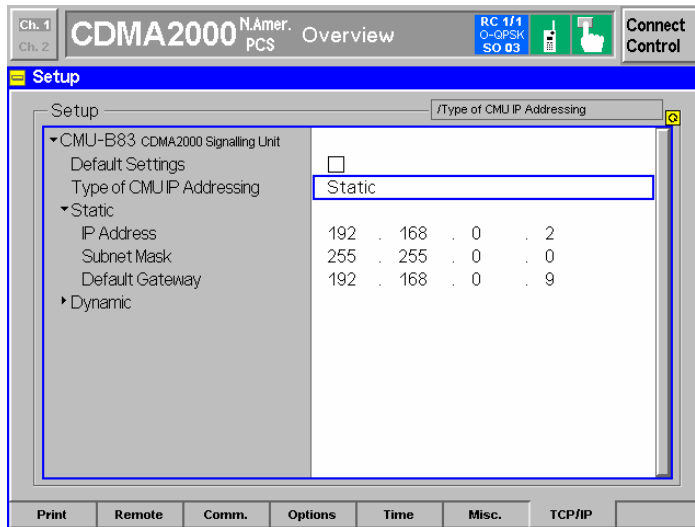
Figure 3. R&S[®] CMU200 (Gateway) Mobile IP test environment without DHCP

R&S[®] CMU200 Mobile IP Gateway Configuration without DHCP

STEP 1 - Configure the R&S[®] CMU200 to use static IP Addressing

- Ø 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:

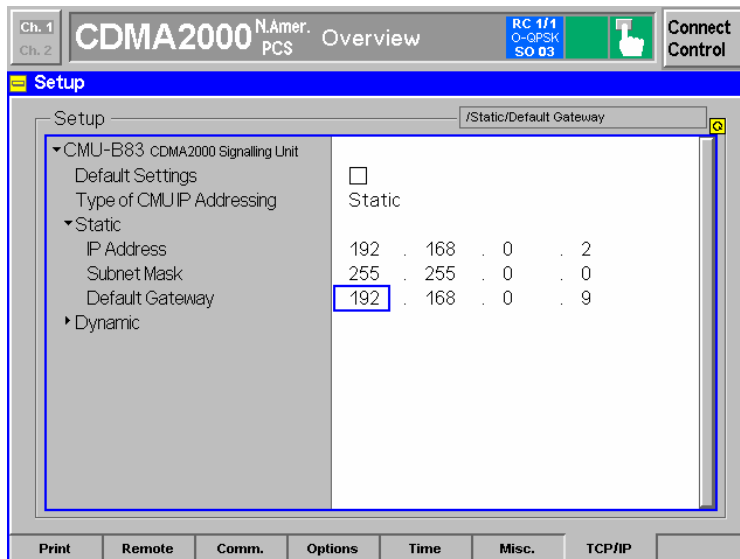
SETUP → TCP/IP



STEP 2 - Configure the R&S[®] CMU200 with static IP Addresses

The R&S[®] CMU200 can be configured with Static IP Addressing by setting the R&S[®] CMU200 IP Address, R&S[®] CMU200 Subnet Mask and R&S[®] CMU200 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** for the R&S[®] CMU200 and Mobile. These IP addresses must be configured to be within the R&S[®] CMU200's subnet.

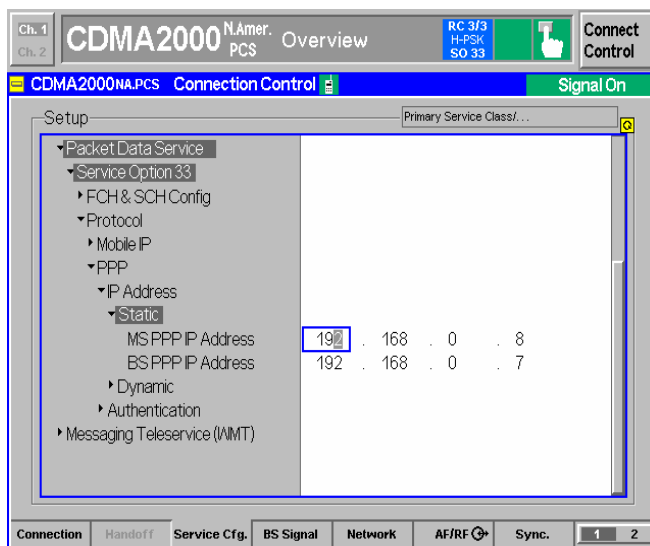
In a mobile IP environment, the MS PPP IP address is *not* the IP address assigned to the mobile. A MIP capable mobile may use this MS PPP IP address as the co-located care of address in the case where a Foreign Agent care of address is not supplied in the Agent Advertisement message.

The MS PPP IP address will **not** be utilized by the mobile since the R&S[®] CMU200 does not support a co-located care of address, however, the MS IP address should still be configured properly. The BS 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 BS PPP and MS 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:

Service Config → Packet Data Service → Service Option 33 → Protocols → PPP → IP Address

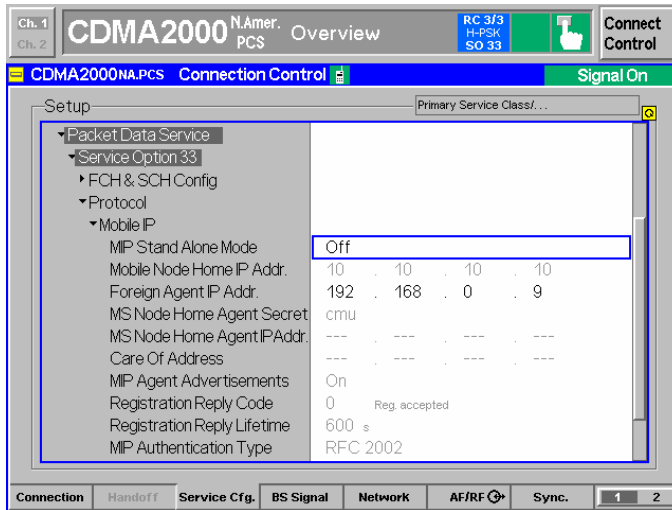


STEP 3 - Configure the R&S[®] CMU200 to act as a Mobile IP Gateway

Ø 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:

Service Config → Packet Data Service → Service Option 33 → Protocols → Mobile IP



STEP 4 - Configure the R&S[®] CMU200 with the Foreign Agent IP Address

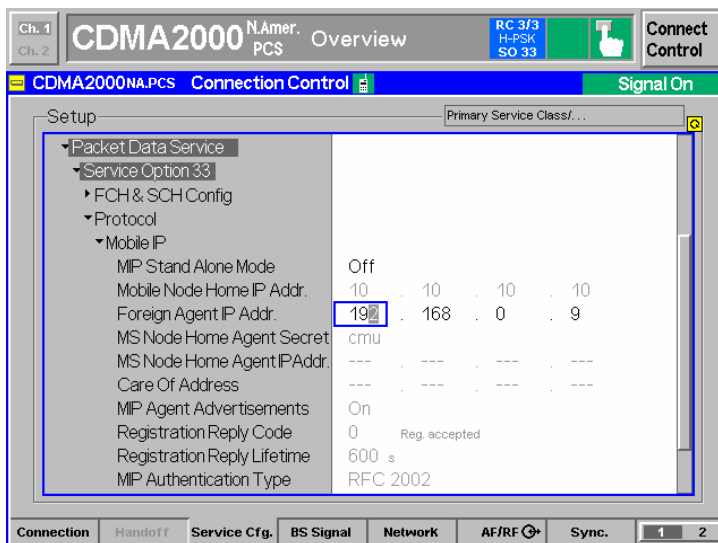
Ø The Foreign Agent IP Address can be found at:

Connect Control:

Service Config → Packet Data Service → Service Option 33 → Protocols → 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 2 above).

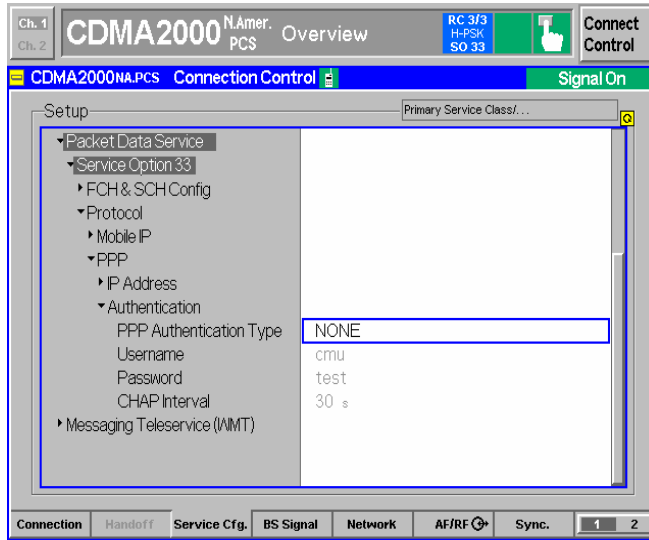


STEP 5 – Configure PPP Authentication

Ø 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:

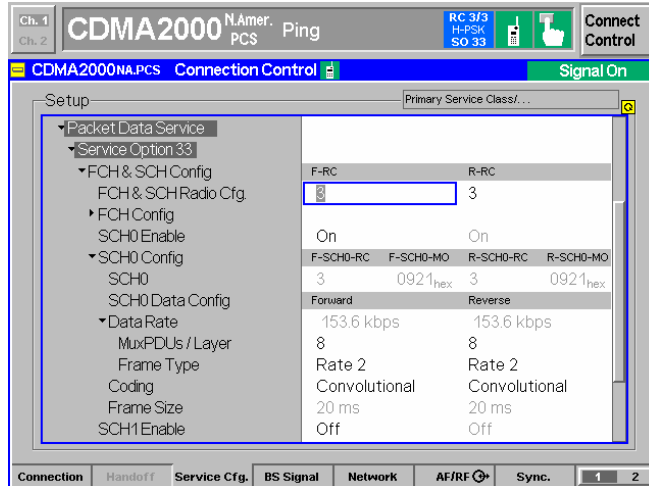
Connect Control:

Service Config → Packet Data Service → Service Option 33 → Protocols → PPP → Authentication



STEP 6 – Configure the Traffic Channels assigned to the SO33 data call

∅ The configuration for the SO33 traffic channels is very similar to the SO32 traffic channels with the exception of the configuration of data generation.



Dynamics Foreign Agent Configuration

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

- Ø 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/>).
- Ø Login as 'root'
- Ø Create a directory for the software (e.g. /usr/src/MobileIP) and move the tar file into the new directory.
- Ø 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/
```

- Ø '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.

- Ø 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.

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

```
>> make check
```
- Ø 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.)

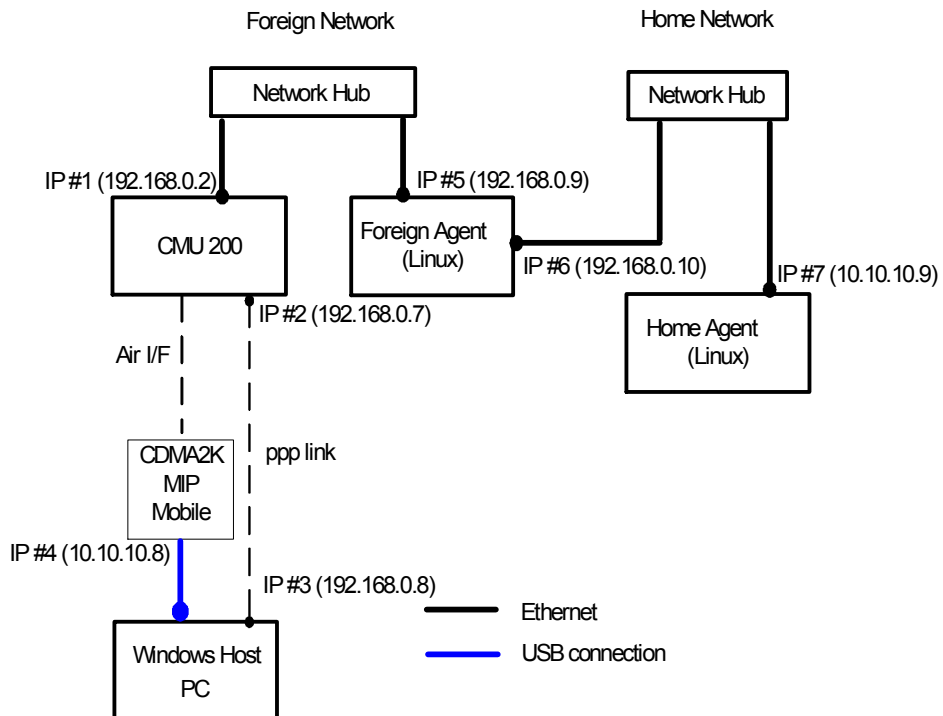


Figure 4. R&S[®] CMU200 (Gateway) Mobile IP test environment without DHCP

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

- Ø Login as 'root'
- Ø Execute netconf from the start menu:
Start→ Configuration→ Networking→ netconf
- Ø 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 5; 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
```

```
Session Edit View Bookmarks Settings Help
[root@foreignAgent root]# route
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.0.0      *              255.255.255.0  U        0      0      0 eth0
10.10.10.0       *              255.255.255.0  U        0      0      0 eth1
127.0.0.0        *              255.0.0.0      U        0      0      0 lo
default          192.168.0.10  0.0.0.0        UG       0      0      0 eth0
[root@foreignAgent root]#
```

STEP 4 – Foreign Agent Configuration – dynfad.conf

Ø Change into the Foreign Agent directory

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

Ø 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)

Ø Login as 'root'

Ø 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

Ø Login as 'root'

Ø Load the IP tunneling module (execute once)

```
>> insmod ipip
```

Ø 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
```

Ø 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

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

- Ø '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.

- Ø 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.

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

```
>> make check
```

- Ø 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.)

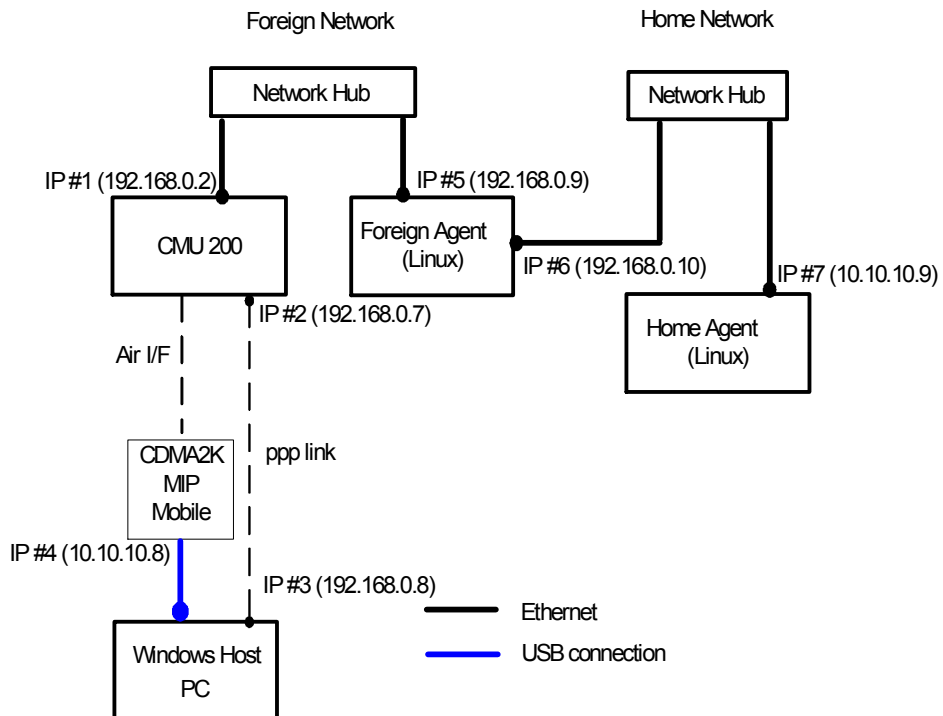


Figure 5. R&S[®] CMU200 (Gateway) Mobile IP test environment without DHCP

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

- Ø Login as 'root'
- Ø Execute netconf from the start menu:
Start → Configuration → Networking → netconf
- Ø 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
- Ø Select "Routing and Gateways"
 - Configure Default Gateway – leave empty; enable routing selected
 - Configure Routed Daemon
 - § Uncheck both boxes
 - "Dismiss" to accept changes

Ø Select “Quit”

Ø 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)

Ø Login as ‘root’

Ø 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
```

Ø 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

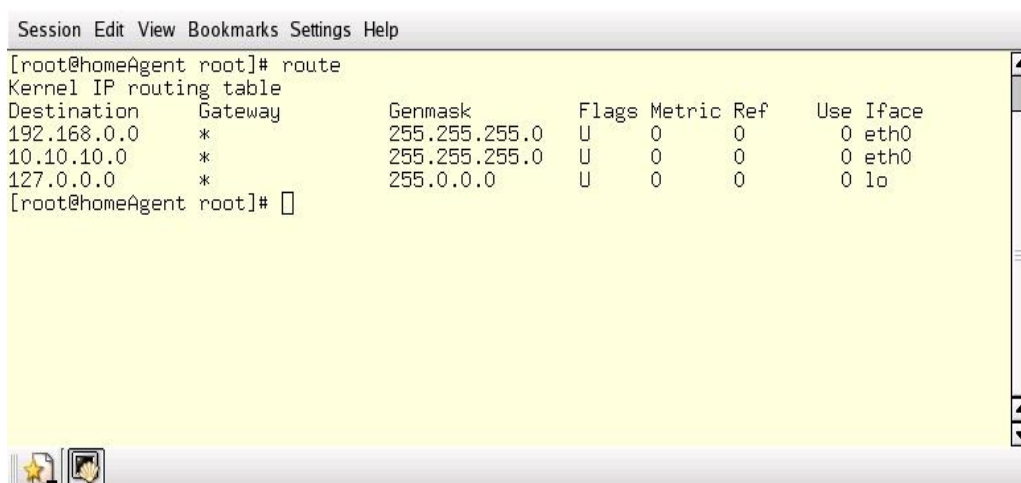
Example ‘route’ commands using 192.168.0.X as the Foreign Agent network and 10.10.10.X as the Home Agent Network:

```
>> 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
```



```
Session Edit View Bookmarks Settings Help
[root@homeAgent root]# route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
192.168.0.0 * 255.255.255.0 U 0 0 0 eth0
10.10.10.0 * 255.255.255.0 U 0 0 0 eth0
127.0.0.0 * 255.0.0.0 U 0 0 0 lo
[root@homeAgent root]#
```

STEP 4 – Home Agent Configuration – dynhad.conf

Ø Change into the Home Agent directory

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

Ø 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 identifier 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.

Ø Login as 'root'

Ø 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

Ø Login as 'root'

Ø Load the IP tunneling module (execute once)

```
>> insmod ipip
```

Ø 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
```

Ø 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.

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

Ø 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.

Ø 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.

Ø 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.

Ø Set *Reverse Tunneling*

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

Ø 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 3. 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.

Ø 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.

STEP 2 – Configure Windows Host PC connected to the Mobile

Ø Install necessary drivers for the mobile phone modem (USB or Serial connection)

Ø Add new modem

Ø Add new network connection

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

Ø Connect mobile phone to PC via USB or Serial connection

Ø Query mobile’s modem to ensure it’s properly configured

Ø 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 the web sites for details on any license agreements.

Making a Mobile IP Data Call and transferring data

STEP 1 – Establish a Mobile IP data call

Using the Dial-Up connection, establish a data call using “#777” as the dialed number.

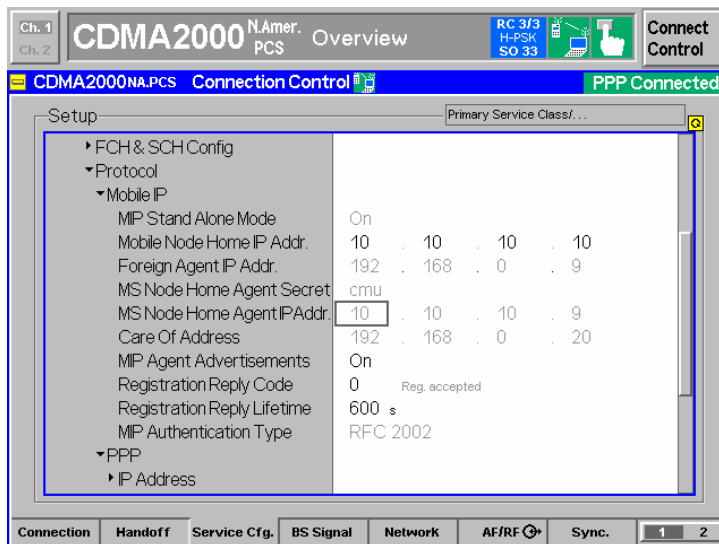
STEP 2 – Verify Mobile IP Information received at the CMU.

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 CMU.

∅ The Mobile IP Information can be found at

Connect Control:

Service Config → Packet Data Service → Service Option 33 → Protocols → MIP



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 (2k, 20k, and 200k in size). These files can be deleted to make room to upload new files to the R&S® CMU200. The BS PPP IP Address can be used to access the FTP server (found at *Service Config → Packet Data Service → Service Option 33 → Protocols → PPP → IP Address*).

- Ø On the Windows Host PC:

```
ftp << BS PPP IP Addr >>
```

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

- Ø 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

- Ø The PING measurement can be found at

Connect Control:

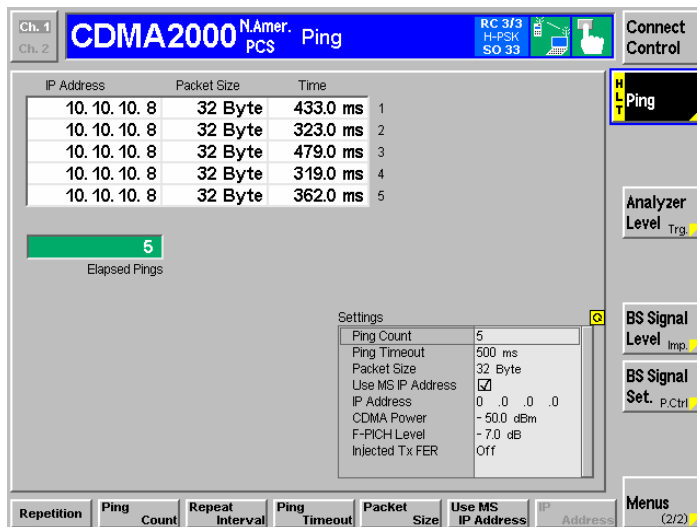
Menu (1/2)→ Ping

- Ø Select the “Use MS IP Address” tab and check the box.

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

- Ø Set the Ping Count, Timeout and Packet Size

- Ø Run the PING measurement



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

- Ø 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 5001 and displays packet statistics every 2 seconds.

- Ø 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 10k
```

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 10 kbps 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 frames, PPP data count and data transfer rate for the SO33 data call.

- Ø The RLP/IP statistics measurement can be found at:

Connect Control:

Menu (1/2) → RLP/IP Stats

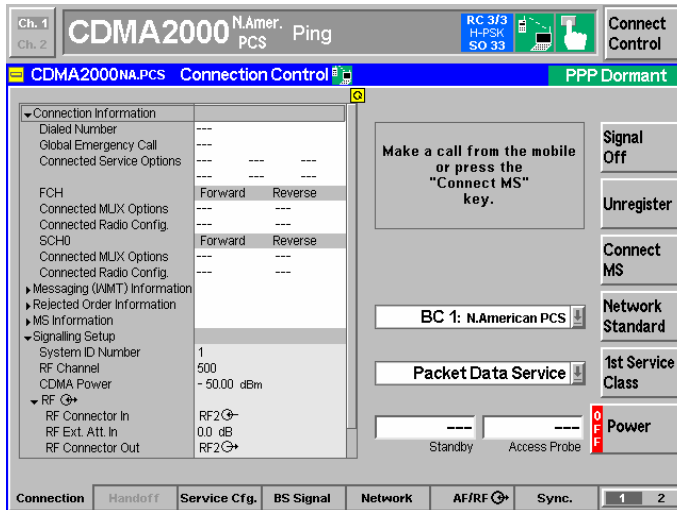
Rx	Rx Total	Tx	Tx Total	RLP Frame Type
0	1	0	1	Data (Unsegmented)
0	1	0	1	Data (Segmented)
3	787	6	3618	Fill
44	13095	0	0	Idle
2	435	0	18	NAK
0	8	0	0	SYNC
0	8	0	0	ACK
0	0	0	8	SYNCAK
0	38	44	11053	B_Data
0	126	296	72827	C_Data
0	32	8	2179	D_Data
0	0	0	0	Reassembly
0	31	96	42690	Blank
0	0	0	0	Invalid
49	14562	450	132395	Summary

Summary Statistics:

- PPP Total Bytes Rx: 6742, Data Rate: 0.0 kbit/s
- PPP Total Bytes Tx: 3315738, Data Rate: 105.1 kbit/s

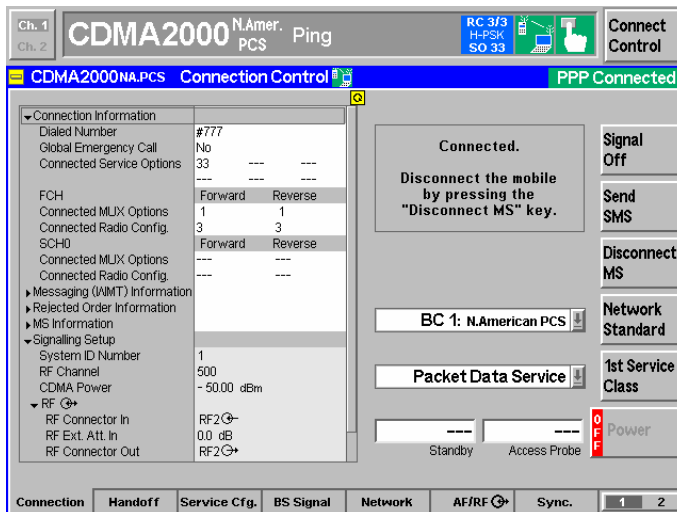
STEP 5 – Take the mobile into a PPP Dormant State

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



6 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 4.

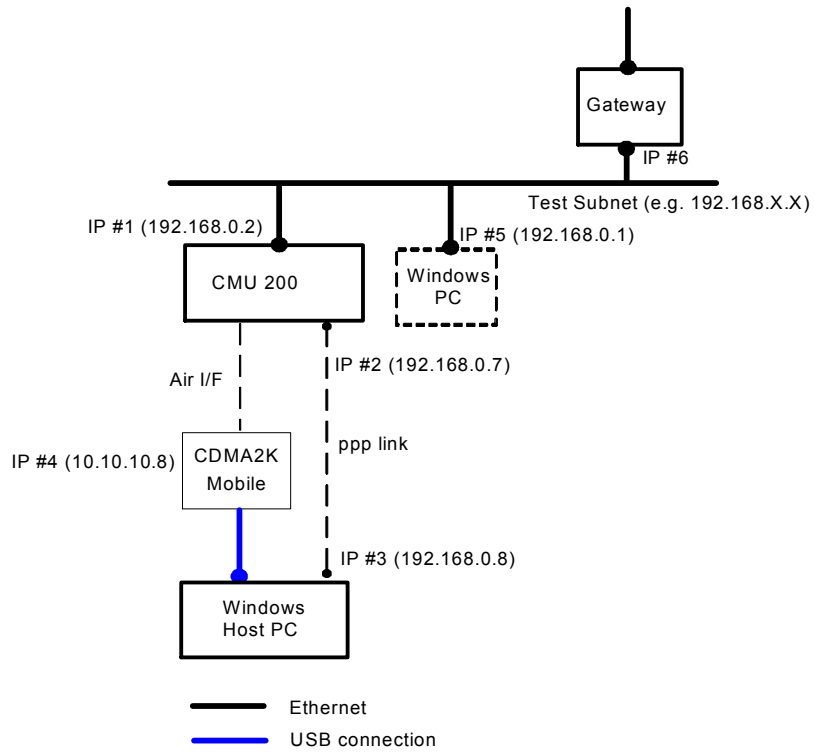


Figure 6. R&S[®] CMU200 (Stand Alone) Mobile IP test environment

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

STEP 1 - Configure the R&S[®] CMU200 use static IP Addressing (see chapter 5; section “R&S[®] CMU200 Mobile IP Gateway Configuration without DHCP”; steps 1 and 2)

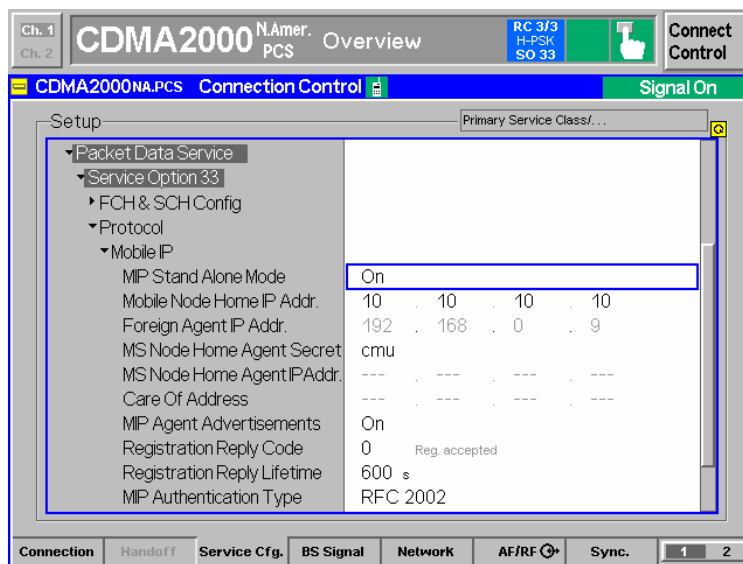
The R&S[®] CMU200 Default Gateway should be configured to use the IP Address of the Gateway, IP Address #6 (see Figure 4).

STEP 2 - 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:

Service Config → Packet Data Service → Service Option 33 → Protocols → Mobile IP



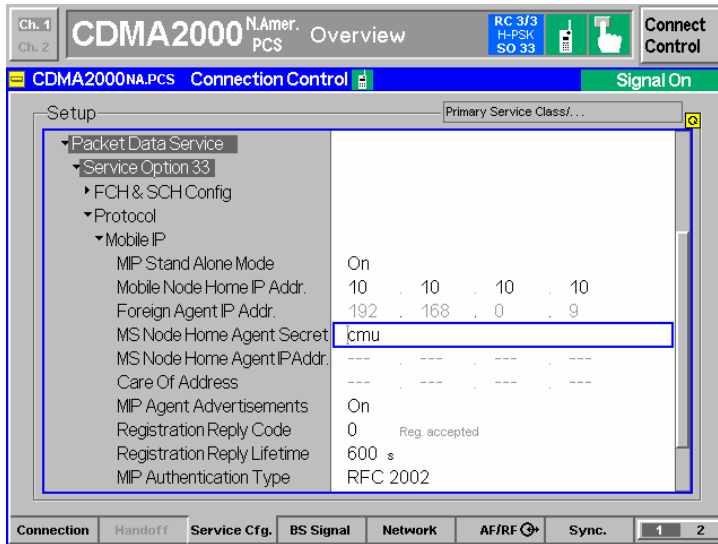
STEP 3 - Configure the Mobile IP Home Agent Secret

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 6; section “MIP Mobile Phone / Windows Host PC Configuration”; step 1 below)

∅ The Mobile IP secret can be configured using the “**MS Node Home Agent Secret**” parameter found at:

Connect Control:

Service Config → Packet Data Service → Service Option 33 → Protocols → Mobile IP



STEP 4 - Configure the Mobile Node Home IP Address (optional)

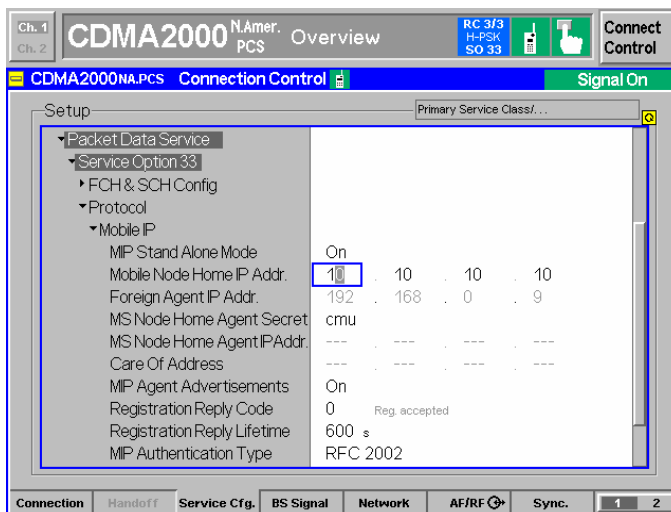
The R&S® CMU200 (in a MIP Stand Alone mode) allocates the **Mobile Node Home IP Addr** to the mobile in the Registration Reply message in the case where the Home IP Address is not programmed in the mobile (IP Address set to “0.0.0.0”).

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.

Ø The Mobile Node Home IP Address can be configured using the “**Mobile Node Home IP Addr**” parameter found at:

Connect Control:

Service Config → Packet Data Service → Service Option 33 → Protocols → Mobile IP

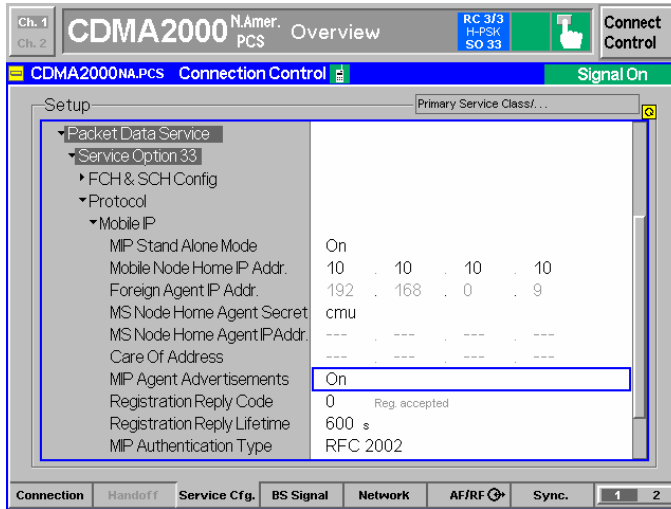


STEP 5 - Configure the ability to send Agent Advertisements

The **MIP Agent Advertisements** parameter is used by the R&S® CMU200 (in a MIP Stand Alone mode) to determine if Agent Advertisements can be 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:

Service Config → Packet Data Service → Service Option 33 → Protocols → Mobile IP

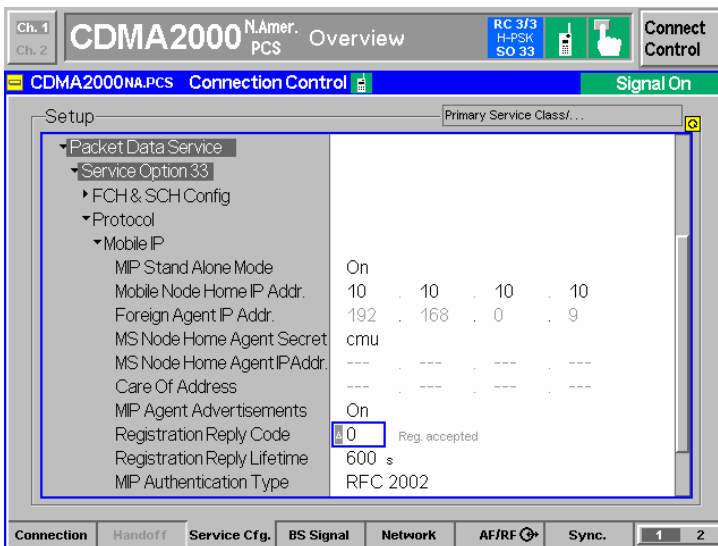


STEP 6 - Configure the Registration Reply code to use

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:

Service Config → Packet Data Service → Service Option 33 → Protocols → Mobile IP

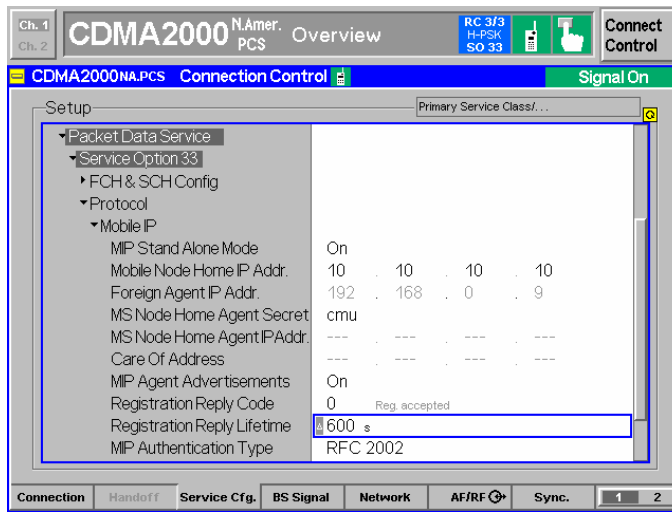


STEP 7 - Configure the Registration Reply Lifetime to use

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:

Service Config → Packet Data Service → Service Option 33 → Protocols → Mobile IP

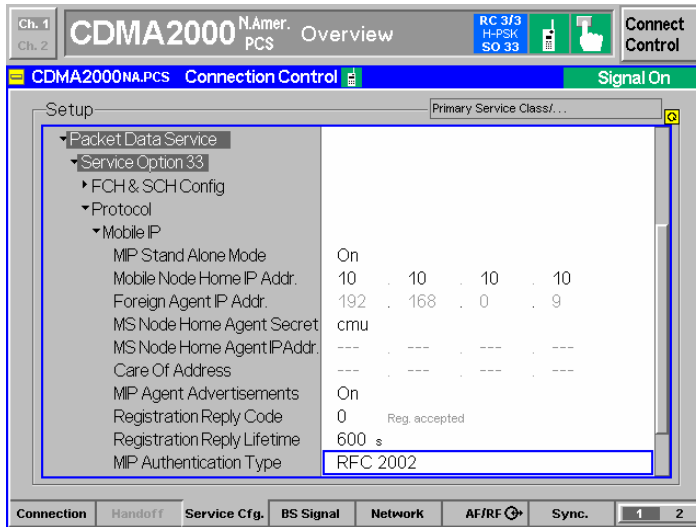


STEP 8 - Configure the Mobile IP Authentication Type to use

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:

Service Config → Packet Data Service → Service Option 33 → Protocols → Mobile IP



STEP 9 – Configure PPP Authentication (see chapter 5; section “R&S[®] CMU200 Mobile IP Gateway Configuration without DHCP”; step 5 above)

STEP 10 – Configure the Traffic Channels assigned to the SO33 data call (see chapter 5; section “R&S[®] CMU200 Mobile IP Gateway Configuration without DHCP”; step 6 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:

Ø *Set MN-HA Secret*

The MN-HA secret should correspond to the value entered in the “**MS Node Home Agent Secret**” parameter in section “R&S[®] CMU200 Mobile IP Stand Alone Configuration without DHCP”; step 3 above. This is the secret used at the R&S[®] CMU200 and Mobile during the MD5 Authentication procedure.

Ø *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.

Ø *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.

Ø *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 5; section “Making a Mobile IP Data Call and transferring data”; step 2).

STEP 2 – Configure Windows Host PC connected to the Mobile

See chapter 5; 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 4)

Under Control Panel → “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 Data Call and transferring data

STEP 1 – Establish a Mobile IP data call

Using the Dial-Up connection created in section “MIP Mobile Phone / Windows Host PC Configuration” above, establish a data call using “#777” as the dialed number.

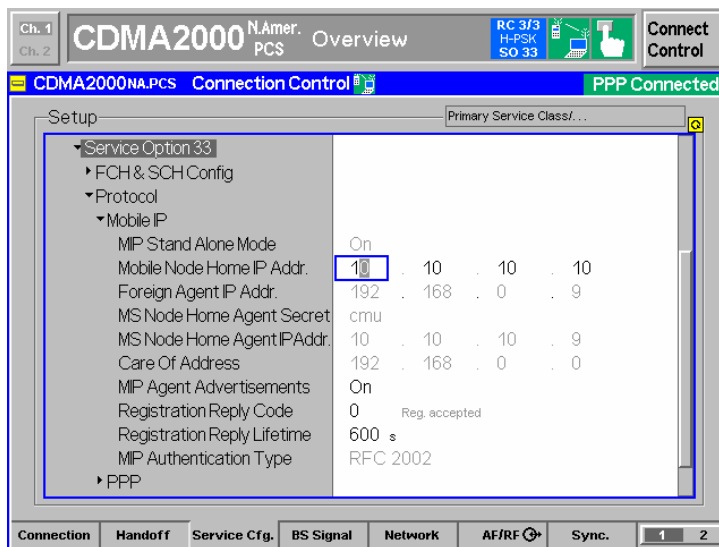
STEP 2 – Verify Mobile IP Information received at the CMU.

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 CMU.

Ø The Mobile IP Information can be found at

Connect Control:

Service Config → Packet Data Service → Service Option 33 → Protocols → MIP



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

See chapter 5; section “Making a Mobile IP Data Call and transferring data”; step 3a.

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

Ø 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 5; section “Making a Mobile IP Data Call and transferring data”;step 3c.

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

- Ø 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.

- Ø 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 10k
```

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 10 kbps 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 5; section “Making a Mobile IP Data Call and transferring data”;step 4.

7 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 5.

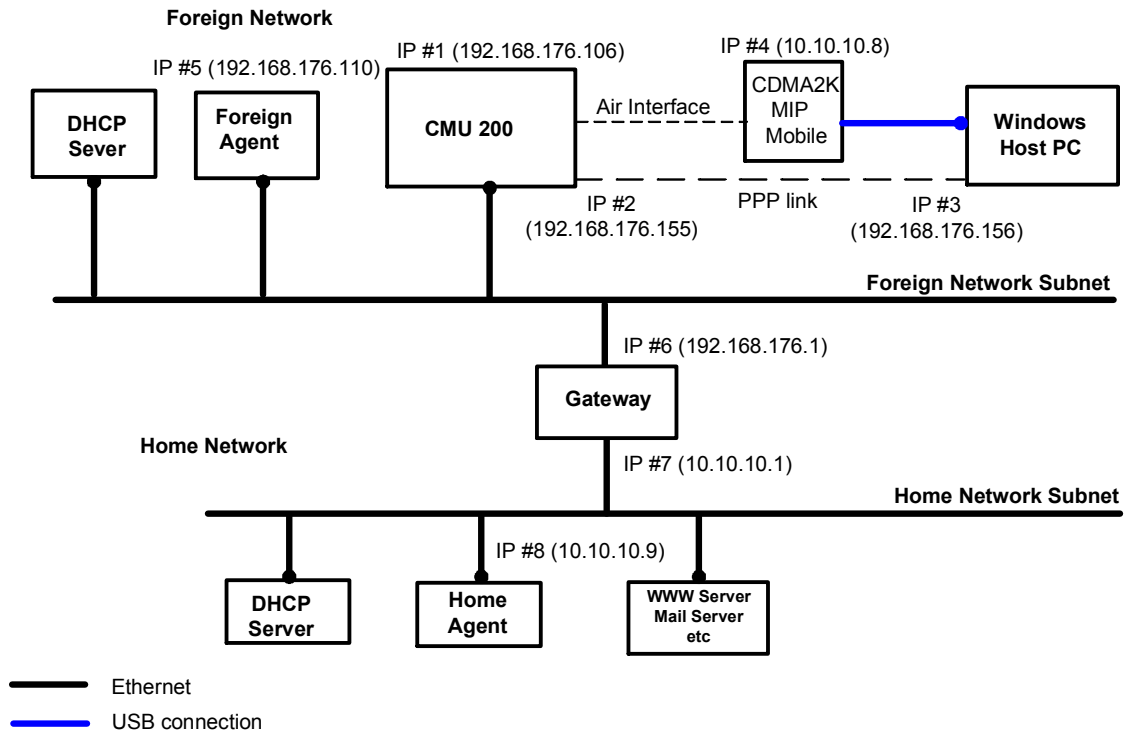


Figure 7. R&S[®] CMU200 (Gateway) Mobile IP test environment with DHCP

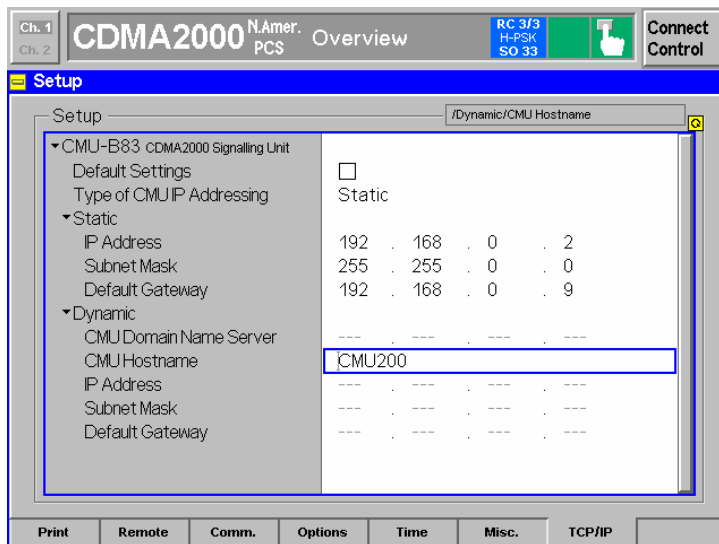
R&S[®] CMU200 Mobile IP Gateway Configuration with DHCP

STEP 1 - 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*



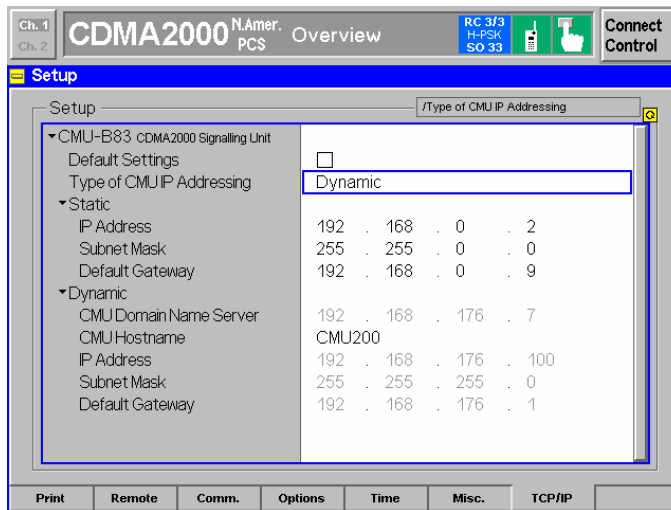
STEP 2 - Configure the R&S[®] CMU200 to use DHCP in order to acquire the IP Addresses.

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, MS PPP IP Address and the BS 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.



Ø 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 BS PPP IP Address and the MS PPP IP Address.

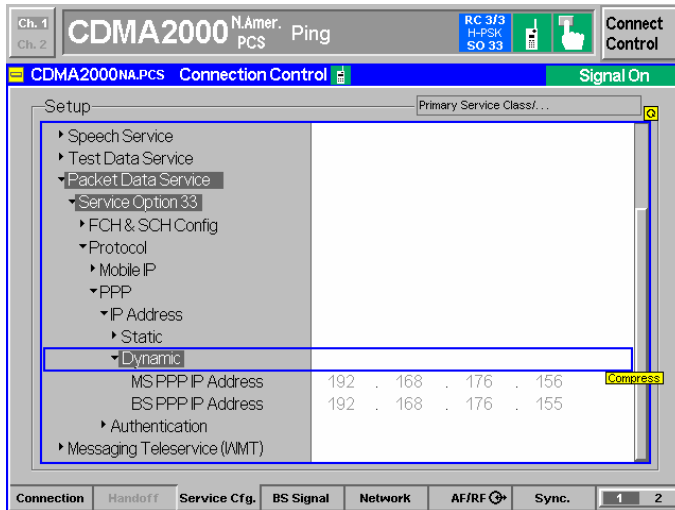
In a mobile IP environment, the MS PPP IP address is *not* the IP address assigned to the mobile. A MIP capable mobile may use this MS PPP IP address as the co-located care of address in the case where a Foreign Agent care of address is not supplied in the Agent Advertisement message.

The MS 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 MS PPP IP address should still be configured properly. The BS 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 BS PPP and MS PPP IP Addresses assigned must be **different** than the CMU and Gateway IP Addresses (under Misc -> TCP/IP).

Connect Control:

Service Config → Packet Data Service → Service Option 33 → Protocols →

PPP → IP Address



STEP 3 - Configure the R&S[®] CMU200 to act as a Mobile IP Gateway (see chapter 5; section “CMU200 Mobile IP Gateway Configuration without DHCP”; Step 3)

STEP 4 - Configure the R&S[®] CMU200 with the Foreign Agent IP Address (see chapter 5; section “CMU200 Mobile IP Gateway Configuration without DHCP”; Step 4)

STEP 5 – Configure PPP Authentication (see chapter 5; section “R&S[®] CMU200 Mobile IP Gateway Configuration without DHCP”; Step 5)

STEP 6 – Configure the Traffic Channels assigned to the SO33 data call (see chapter 5; section “R&S[®] CMU200 Mobile IP Gateway Configuration without DHCP”; step 6)

Dynamics Foreign Agent Configuration

This configuration is slightly different from the Dynamics Foreign Agent Configuration in Chapter 5. It requires configuring the network interface cards in a dynamic (DHCP) configuration. Only these differences will be documented - references to Chapter 5 will be used whenever possible.

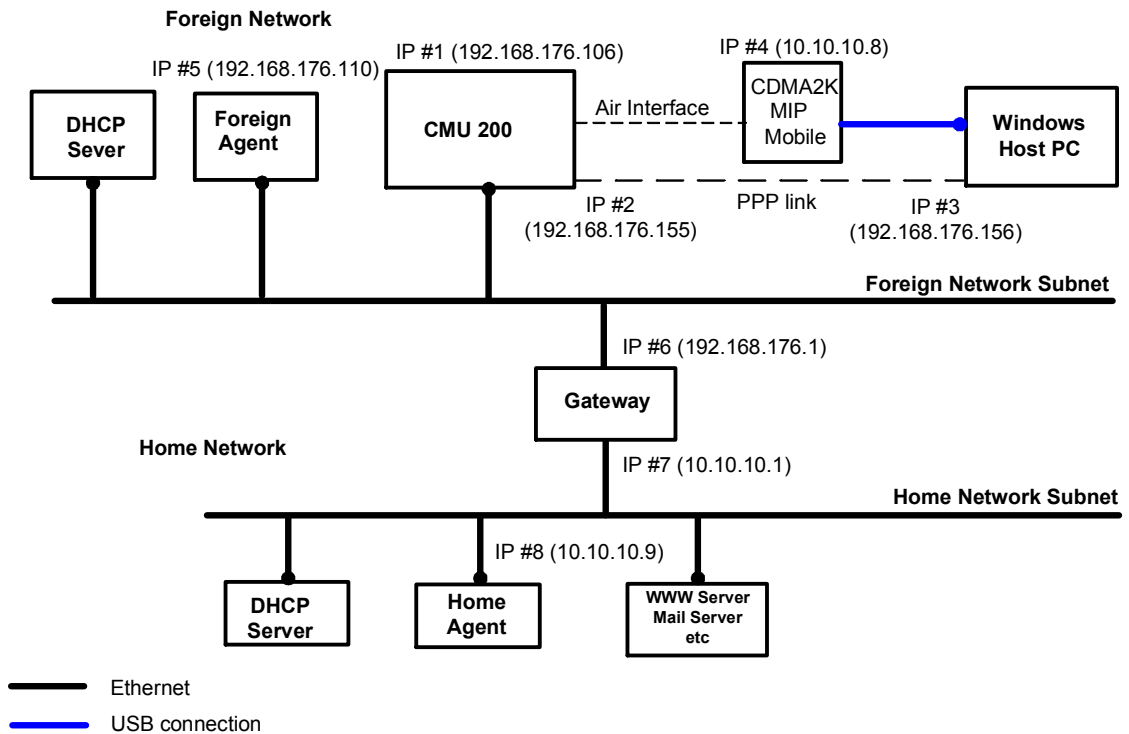


Figure 8. R&S[®] CMU200 (Gateway) Mobile IP test environment with DHCP

STEP 1 – Compile Dynamics Mobile IP Foreign Agent v0.8.1 Software on Mandrake 9.1 See chapter 5; section “Dynamics Foreign Agent Configuration”; step 1 above.

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

See chapter 5; section “Dynamics Foreign Agent Configuration”; step 2 above. Replace only the following sections:

- Ø 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)
 - “Accept” Changes

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

- Ø Select “Routing and Gateways”
 - Configure Default Gateway as IP#6; enable routing selected
 - Configure Routed Daemon
 - § Uncheck both boxes
 - “Dismiss” to accept changes

STEP 3 – Linux Networking Configuration (Network Routing Tables)

See chapter 5; section “Dynamics Foreign Agent Configuration”; step 3 above. Replace only the following sections:

- Ø 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 chapter 5; section “Dynamics Foreign Agent Configuration”; step 4 above. Replace only the following sections:

- Ø Edit the dynfad.conf file
 - 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
```
 - Configure **HighestFAIPAddress** parameter

Set this parameter equal to the IP Address specified in the INTERFACES element (IP #5)
 - 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 chapter 5; section “Dynamics Foreign Agent Configuration”; step 5 above.

STEP 6 – Start Foreign Agent daemon

See chapter 5; section “Dynamics Foreign Agent Configuration”; step 6 above.

Dynamics Home Agent Configuration

This configuration is slightly different from the Dynamics Home Agent Configuration in Chapter 5. It requires configuring the network interface cards in a dynamic (DHCP) configuration. Only these differences will be documented - references to Chapter 5 will be used whenever possible.

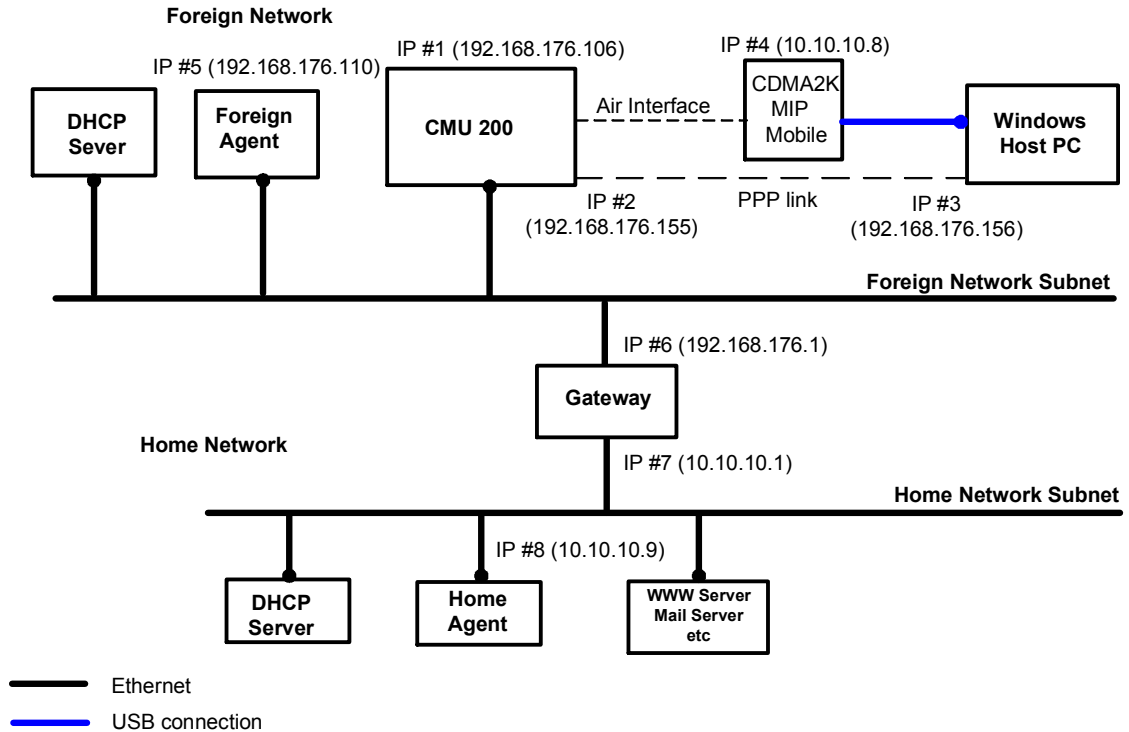


Figure 9. R&S® CMU200 (Gateway) Mobile IP test environment with DHCP

STEP 1 – Compile Dynamics Mobile IP Home Agent v0.8.1 Software on Mandrake 9.1 See chapter 5; section “Dynamics Home Agent Configuration”; step 1 above.

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

See chapter 5; section “Dynamics Home Agent Configuration”; step 2 above. Replace only the following sections:

- Ø 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
- Ø 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 chapter 5; section “Dynamics Home Agent Configuration”; step 3 above. Replace only the following sections:

- Ø 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 chapter 5; section “Dynamics Home Agent Configuration”; step 4 above. Replace only the following sections:

- Ø 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 chapter 5; section “Dynamics Home Agent Configuration”; step 5

STEP 6 – Start Home Agent daemon

See chapter 5; section “Dynamics Home Agent Configuration”; step 6.

MIP Mobile Phone / Windows Host PC Configuration

(See chapter 5; section “MIP Mobile Phone / Windows Host PC Configuration “)

Making a Mobile IP Call and transferring data

(See chapter 5; section “Making a Mobile IP Call and transferring data”)

8 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 6.

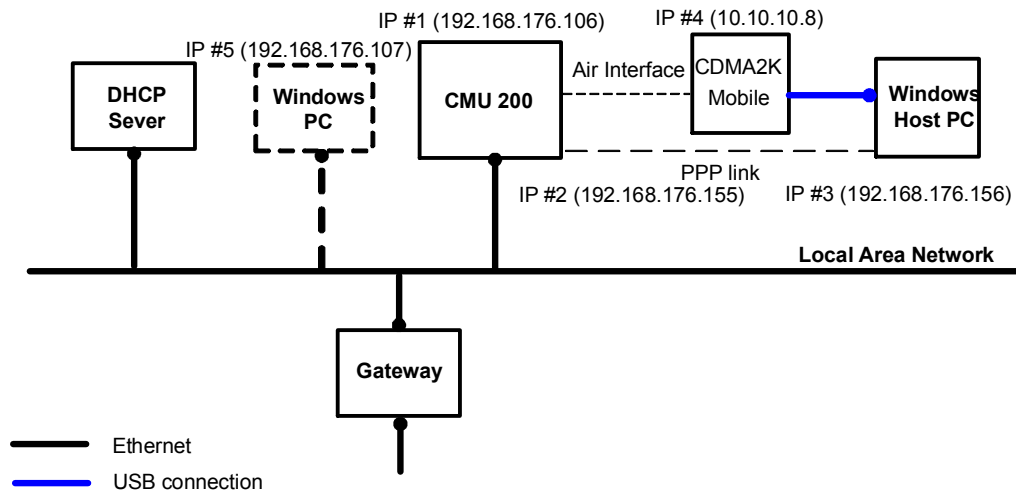


Figure 10. R&S[®] CMU200 (Stand Alone) Mobile IP test environment with DHCP

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

STEP 1 - Configure the R&S[®] CMU200 with a hostname (see chapter 7; section “R&S[®] CMU200 Mobile IP Gateway Configuration with DHCP”; step 1).

STEP 2 - Configure the R&S[®] CMU200 to use DHCP in order to acquire the IP Addresses (see chapter 7; section “R&S[®] CMU200 Mobile IP Gateway Configuration with DHCP”; step 2).

STEP 3 - Configure the R&S[®] CMU200 in Mobile IP Stand Alone mode (see chapter 6; section “R&S[®] CMU200 Mobile IP Stand Alone Configuration without DHCP”; step 2)

STEP 4 - Configure the Mobile IP Home Agent Secret (see chapter 6; section “R&S[®] CMU200 Mobile IP Stand Alone Configuration without DHCP”; step 3)

STEP 5 – Configure PPP Authentication (see chapter 5; section “R&S[®] CMU200 Mobile IP Gateway Configuration without DHCP”; step 5)

STEP 6 – Configure the Traffic Channels assigned to the SO33 data call (see chapter 5; section “R&S[®] CMU200 Mobile IP Gateway Configuration without DHCP”; step 6)

MIP Mobile Phone / Windows Host PC Configuration

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

9 Packet Data Mobility Management

In a CDMA2000 packet data environment, packet zones are defined for each coverage area controlled by a Packet Control Function. Each Packet Data Service Node (PDSN)/Foreign Agent pair services one or more Packet Control Functions. If the mobile moves into a new packet zone serviced by a different PDSN/Foreign Agent, the network establishes a new PPP connection. In this scenario, a Mobile IP capable phone is also required to re-register with the Home Agent after changing packet zones. The Mobile IP re-registration is needed to establish a new IP tunnel and to update the Care of Address.

The R&S[®] CMU200 includes functionality to test Packet Data Mobility Management in a PPP Dormant state. The user has the ability to modify the packet zone id broadcast in the *Enhanced System Parameters* Message state. To simulate a change in PDSN/Foreign Agents, a new parameter, **targetPDSN**, has been added. This new parameter has two different modes - **targetPDSN** “changed” and **targetPDSN** “unchanged”.

The **targetPDSN** “changed” mode simulates a PDSN/Foreign Agent change (see Figure 11 – transition from Zone B to Zone C). In this mode, the R&S[®] CMU200 allocates a traffic channel and then establishes a new PPP connection. Mobile IP capable phones will then perform a Mobile IP registration with the Home Agent. To verify that a re-registration occurs, a new Care Of Address is allocated to the mobile.

The **targetPDSN** “unchanged” mode simulates the mobile moving between zones controlled by the same PDSN/Foreign Agent (see Figure 11 – transition from Zone A to Zone B). In this mode, the R&S[®] CMU200 simply acknowledges the packet zone change and does not re-establish the PPP connection with the mobile.

IS-707A, section 2.2.5 defines a new procedure at the mobile called Packet Zone Reconnection Control. This procedure causes a mobile to initiate connection of the packet data service option whenever it moves into a new packet data zone not currently stored in its internally stored list of visited packet data zones. This functionality can be controlled and tested by sending a *Service Option Control Message* to the mobile. The R&S[®] CMU200 provides the capability to configure and send the *Service Option Control Message*.

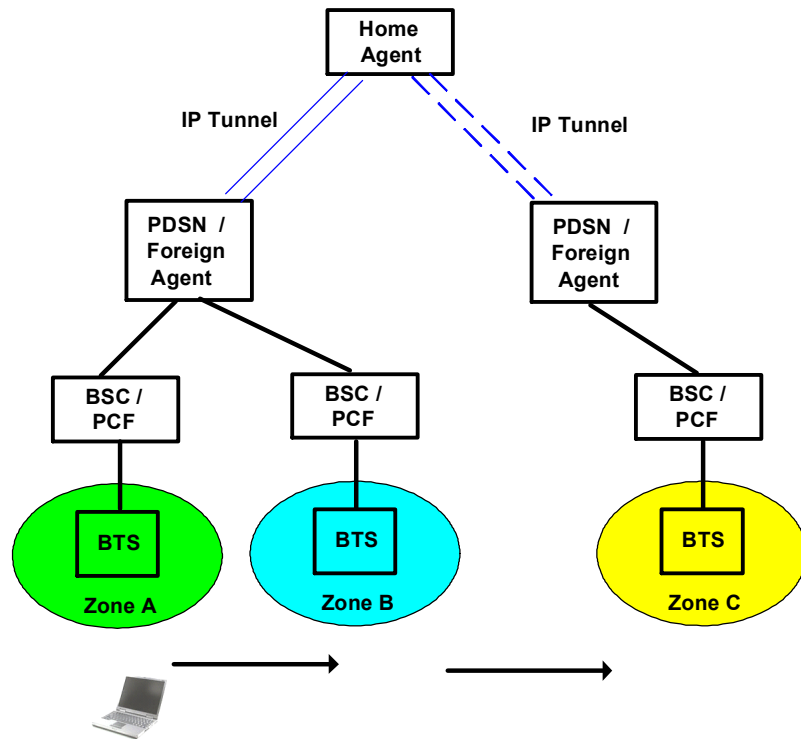


Figure 11. Packet Data Mobility Management

Triggering a Packet Zone Update in the same PDSN/FA

STEP 1 – Configure the system in a Stand Alone Mode (see Section 6)

STEP 2 – Trigger a SO33 data call and put the mobile into a PPP Dormant state

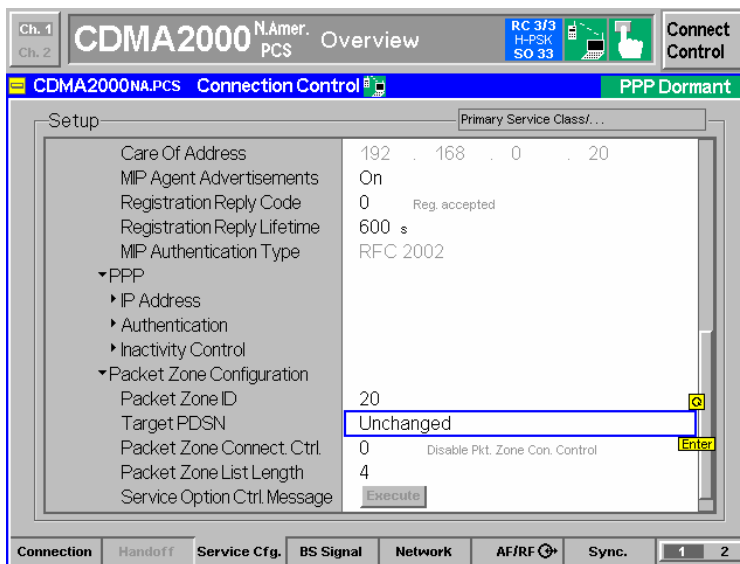
The R&S[®] CMU200 can put the mobile into a PPP Dormant (assuming no data is being transferred) state by simply selecting Disconnect MS button from the MMI. The state will transition from “PPP Connected” to “PPP Dormant”.

STEP 3 – Set the “targetPDSN” to unchanged

Ø The **targetPDSN** parameter can be found at:

Connect Control:

Service Config → Packet Data Service → Service Option 33 → Protocols → Mobile IP → Packet Zone Configuration



STEP 4 – Change the packet zone id

Ø The **PacketZoneID** parameter can be found at:

Connect Control:

Service Config → Packet Data Service → Service Option 33 → Protocols → Mobile IP → Packet Zone Configuration

When the packet zone id is changed, the *Extended System Parameters Message* is updated with the new packet zone id. The mobile reads the new overhead messages and sends up an *Origination Message* with the Data Ready to Send (DRS) bit equal to 0 (assuming the mobile does not have data to send). A *BS Ack* is sent in response to the *Origination Message*; no traffic channel is set up; no PPP connection established; the Care of Address remains unchanged.

Triggering a Packet Zone Update in a *different* PDSN/FA

STEP 1 – Configure the system in a Stand Alone Mode (see Chapter 6)

STEP 2 – Trigger a SO33 data call and put the mobile into a PPP Dormant state

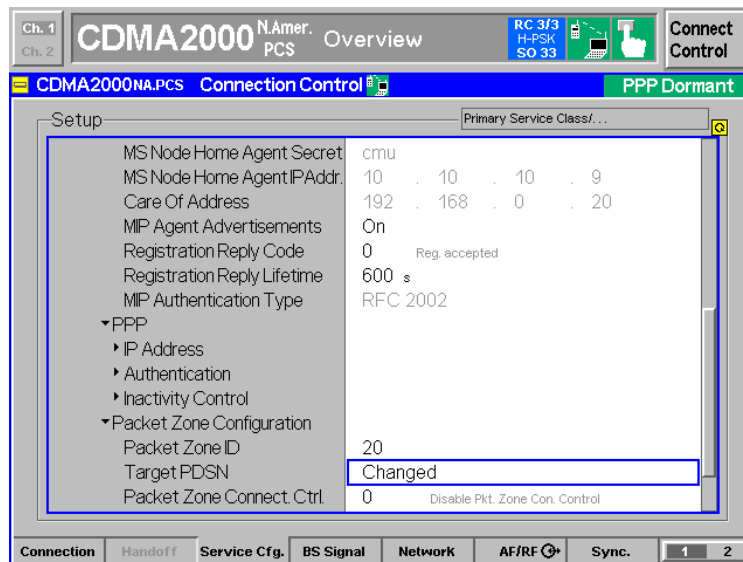
The R&S[®] CMU200 can put the mobile into a PPP Dormant (assuming no data is being transferred) state by simply selecting Disconnect MS button from the MMI. The state will transition from “PPP Connected” to “PPP Dormant”.

STEP 3 – Set the “targetPDSN” to changed

∅ The **targetPDSN** parameter can be found at:

Connect Control:

Service Config → Packet Data Service → Service Option 33 → Protocols → Mobile IP → Packet Zone Configuration



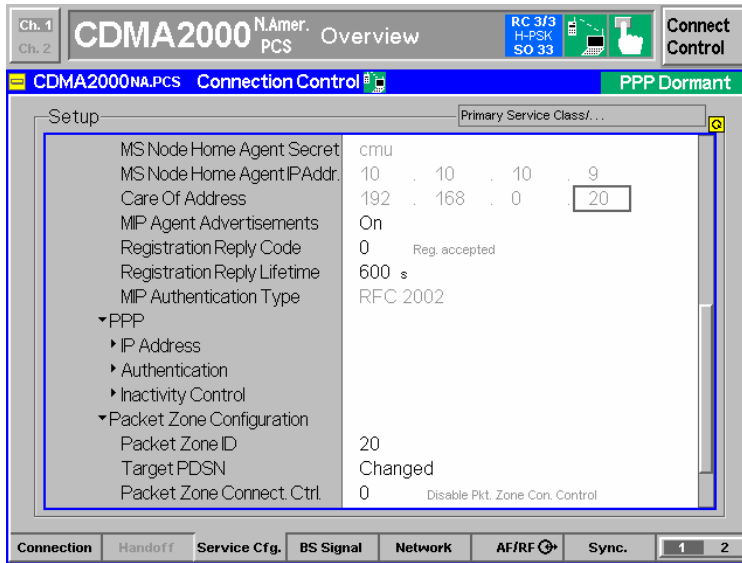
STEP 4 – Change the packet zone id

∅ The **PacketZoneID** parameter can be found at:

Connect Control:

Service Config → Packet Data Service → Service Option 33 → Protocols → Mobile IP → Packet Zone Configuration

When the packet zone id is changed, the *Extended System Parameters Message* is updated with the new packet zone id. The mobile reads the new overhead messages and sends up an *Origination Message* with the Data Ready to Send (DRS) bit equal to 0 (assuming the mobile does not have data to send). A traffic channel is set up so that the signaling for a new PPP connection and Mobile IP registration (for Mobile IP capable mobiles) can take place. In this scenario, the Care Of Address is updated to reflect a new Foreign Agent is being utilized (for Mobile IP capable mobiles)



Testing the Packet Zone Connection Control feature

Refer to TIA/IS-707-A for more details on Packet Zone Connection Control.

STEP 1 – Configure the system in a Stand Alone Mode (see Chapter 6)

STEP 2 – Trigger a SO33 data call (mobile must be in a PPP Connected state)

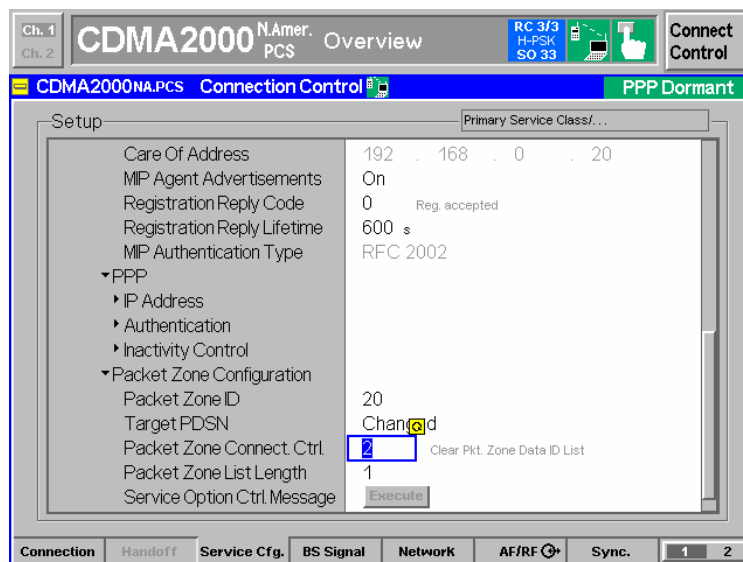
STEP 3 – Configure the Packet Zone Connection Control

Ø The **PacketZoneConnectCtl** parameter can be found at:

Connect Control:

Service Config → Packet Data Service → Service Option 33 → Protocols → Mobile IP →

Packet Zone Configuration



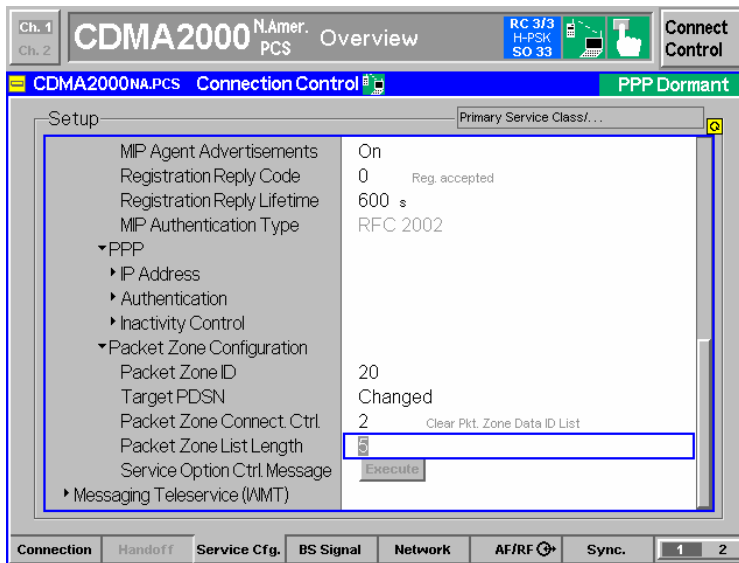
STEP 4 – Configure the Packet Zone List Length (optional)

Ø The **PacketZoneListLength** parameter can be found at:

Connect Control:

Service Config → Packet Data Service → Service Option 33 → Protocols → Mobile IP →

Packet Zone Configuration

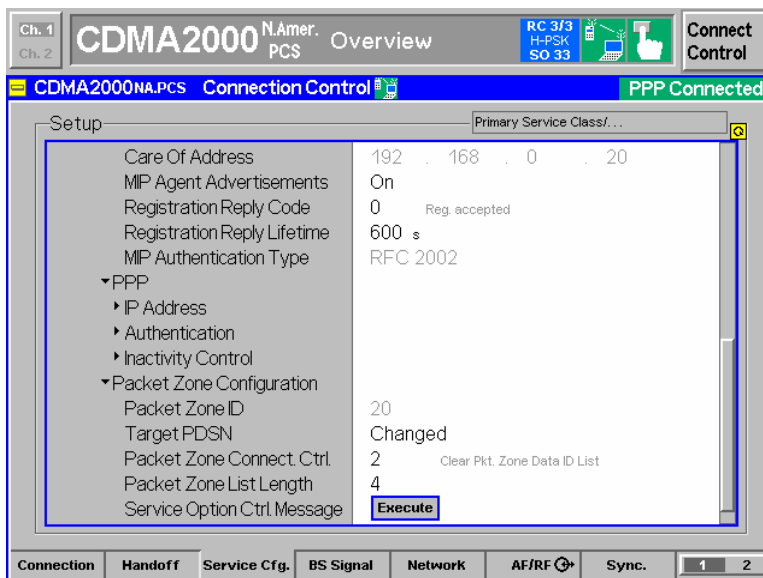


STEP 5 – Send the *Service Option Control Message* to the mobile

Ø The **Execute** button triggers the sending of the *Service Option Control Message* and can be found at:

Connect Control:

Service Config → Packet Data Service → Service Option 33 → Protocols → Mobile IP → Packet Zone Configuration



10 Network Controlled PPP Establishment and Release

In a CDMA2000 packet data environment, the network has the ability to automatically transition the MS from PPP Dormant to PPP Connected if there is data to transmit to the MS. The network also has the ability to transition the MS 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 **Network 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 MS directed data has been received for a period of **Network PPP Inactivity Timer** seconds. The R&S[®] CMU200 will transition the MS from PPP Dormant to PPP Connected once MS directed data is received. The automatic transitioning from PPP Dormant to PPP Connected is disabled if the **Network PPP Inactivity Timer** is set to "OFF".

According to IS707; section 2.2.4, the MS maintains a timer to control how long it delays before originating a packet data service option from the PPP Dormant state. The network can configure this timer on the MS by sending a *Service Option Control Message* to the MS with the timer value. The user can configure this timer on the R&S[®] CMU200 via the **MS Dormant Timer** and **MS Dormant Timer Control** parameters.

Testing BS Inactivity Control (PPP Connected to PPP Dormant)

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

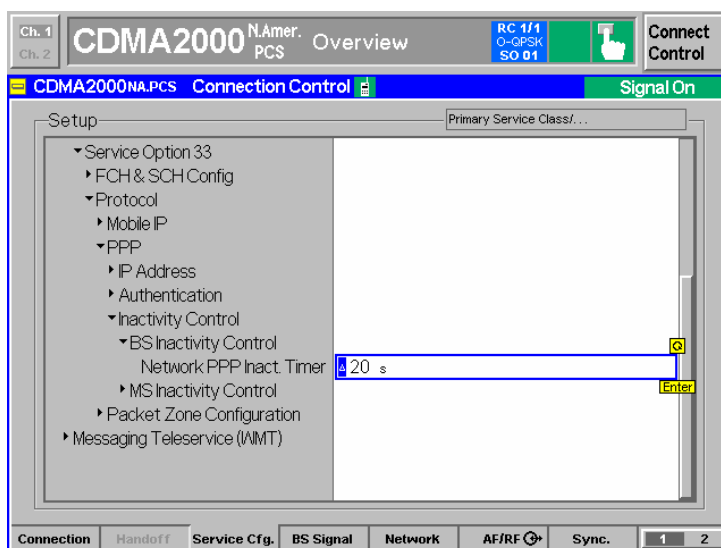
This parameter controls when and if the R&S[®] CMU200 will transition the MS from PPP Connected to PPP Dormant.

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

Ø The **Network PPP Inact Timer** parameter can be found at:

Connect Control:

Service Config → *Packet Data Service* → *Service Option 33* → *Protocols* → *PPP* → *Inactivity Control* → *BS Inactivity Control*



STEP 2 – Trigger a SO33 data call (mobile must be in a PPP Connected state) and do not transmit any data to the MS.

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

Testing BS Inactivity Control (PPP Dormant to PPP Connected)

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

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

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

∅ The **Network PPP Inact Timer** parameter can be found at:

Connect Control:

Service Config → Packet Data Service → Service Option 33 → Protocols → PPP → Inactivity Control → BS Inactivity Control

STEP 2 – Establish a SO33 data call and wait for the call to become PPP Dormant.

STEP 3 – Transmit data to the MS

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

Testing MS Packet Dormant Timer Control

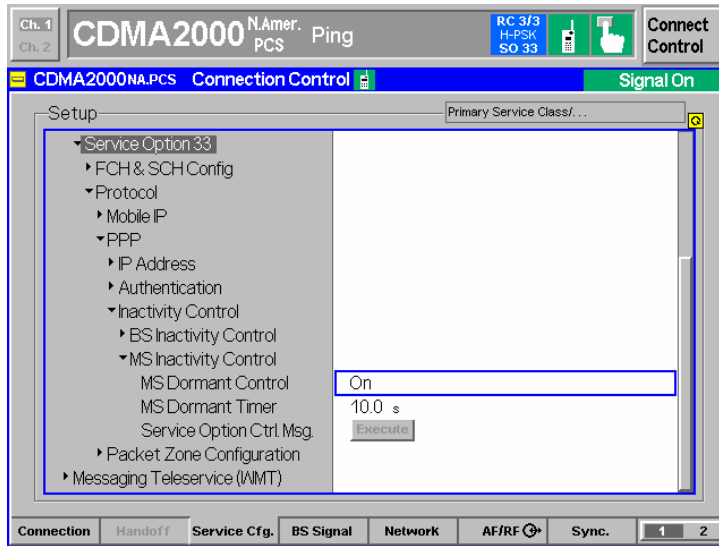
STEP 1 – Configure the MS Dormant Control and Dormant Timer parameters.

See IS 707; section 2.2.4 for more details on these parameters.

Ø The **MS Dormant Cntrl** and **MS Dormant Timer** parameters can be found at:

Connect Control:

Service Config → Packet Data Service → Service Option 33 → Protocols → PPP → Inactivity Control → MS Inactivity Control



STEP 2 – Establish a SO33 data call

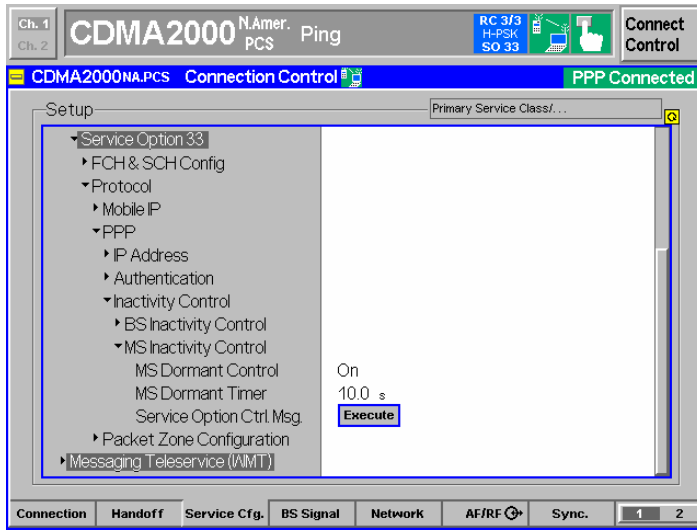
STEP 3 – While the call is PPP Connected, send the *Service Option Control Message* to the mobile.

The MS will then use this timer value (according to IS707) when attempting to re-establish the PPP Connection.

Ø Selecting the Execute button triggers the sending of the SOCM.

Connect Control:

Service Config → Packet Data Service → Service Option 33 → Protocols → PPP → Inactivity Control → MS Inactivity Control



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 De-Registration (mobile moving from FA back to HA)
- R&S[®] CMU200 does not fully support a Mobile Node Home IP Address equal to “0.0.0.0”
R&S[®] CMU200 Gateway Mode – the software has not been tested on the R&S[®] CMU200 since the Dynamics Mobile IP software does not support a Mobile Node Home IP Address equal to “0.0.0.0”
R&S[®] CMU200 Stand Alone Mode - This **is supported** in standalone mode and the IP Address assigned to the MIP mobile is defined by the **MSNodeHomeIPAddress** parameter.

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 SO33 data calls that do not support the Mobile IP functionality. The differences between Mobile IP and Simple IP calls are as follows:

- Mobile IP Registration/Authentication 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 **MS 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 5) or dynamic IP Addressing (see Chapter 7)

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

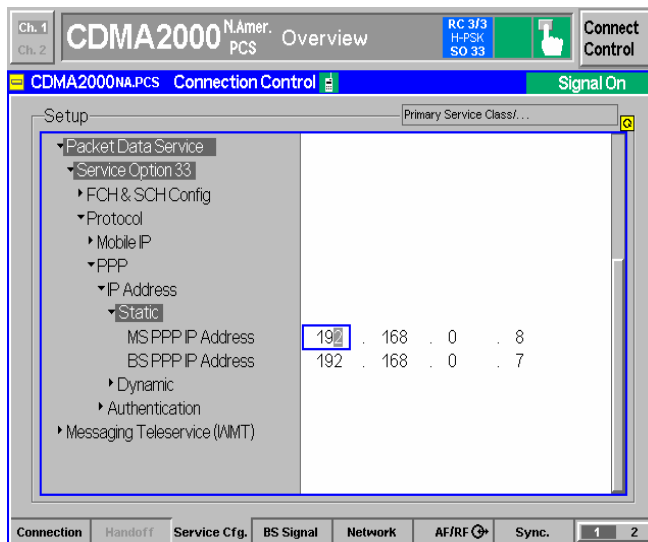
The BS PPP and MS PPP IP Addresses assigned must be **different** than the CMU and Gateway IP Addresses (under Misc -> TCP/IP).

The PPP IP Addresses can be found at:

Connect Control:

Service Config → Packet Data Service → Service Option 33 → Protocols →

PPP → IP Address



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. If the selected

authentication protocol is CHAP, the CHAP interval is also configurable. The CHAP interval defines how often the mobile is re-authenticated with the system.

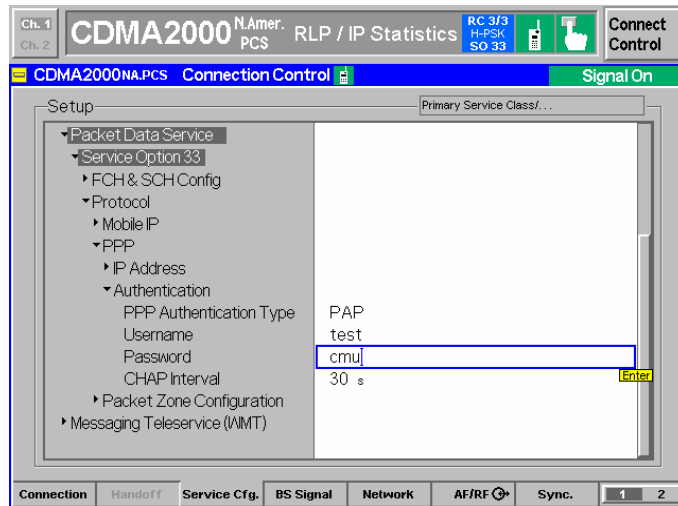
See RFC 1334 for more details.

The PPP Authentication parameters can be found at:

Connect Control:

Service Config → Packet Data Service → Service Option 33 → Protocols →

PPP → Authentication



14 References

Mobile IP, The Internet Unplugged, James D. Solomon

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

TIA/IS-707-A-3, Data Service Option, Addendum 3

RFC 1334 – PPP Authentication Protocols

15 R&S[®] CMU200 Ordering Information

R&S [®] CMU200	Universal Radio Communications Tester	1100.0008.02
R&S [®] CMU-B83	CDMA2000 Signaling Unit	1150.0301.02
R&S [®] CMU-U65	3G Measurement DSP	1100.7402.04
R&S [®] CMU-B87	Interface for CDMA2000 Data Test (Includes Message Monitor Software)	1150.2433.00
R&S [®] CMU-K83	CDMA2000 (450 MHz band)	1150.3500.02
R&S [®] CMU-K84	CDMA2000 (cellular band)	1150.3600.02
R&S [®] CMU-K85	CDMA2000 (PCS band)	1150.3700.02
R&S [®] CMU-K86	CDMA2000 (IMT-2000 band)	1150.3800.02
R&S [®] CMU-K87	CDMA2000 Data Testing	1150.4007.02

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>

This application note and the supplied programs may only be used subject to the conditions of use set forth in the download area of the Rohde & Schwarz website.