Clearwire Corporation
4400 Lake Washington Blvd.NE
Kirkland, WA 98033
425.216.7600 (phone)
425.216.7900 (fax)
www.clearwire.com

Huawei BTS Field Commissioning and Acceptance Test Plan (ATP) Guide

DRAFT

Document Number:
Version: 2.2
Thursday, January 26, 2012

CONFIDENTIAL & PROPRIETARY
Limited Distribution to Authorized Persons Only
Copyright © 2004 Clearwire Corporation.

All Rights Reserved.

1 References

Huawei BTS Network Commissioning Guide

2 Revisions

Date	Revision	Description	Author
June 1, 2009	1.0	Initial release.	**Jeff Fry**
September 2, 2009	1.4	Added Multi-carrier Section	**Jeff Fry**
September 8, 2009	1.5	Added section for interference checks after diplexer cut.	**Jeff Fry**
September 8, 2009	1.6	Added section for checking rolled fiber.	**Jeff Fry**
September 9, 2009	1.7	Highlighted and emphasized that manual configuration of the OMCH should be done only if requested by commissioning.	**Jeff Fry**
September 10, 2009	1.8	Added section for installation checks during diplexer cut.	**Jeff Fry**
September 17, 2009	1.9	Updated diplexer installation check for SPC202.	**Jeff Fry**
October 7, 2009	2.0	Updated clkmode to MANUAL for diplexer installation check.	**Jeff Fry**
October 16, 2009	2.1	Changed VSWR guidelines in Section 12.7.	**Jeff Fry**
April 15, 2009	**2.2**	**Added HapSat sections.**	**Jeff Fry**

3 Overview

The purpose of the commissioning and ATP process is to install a new site and bring it into commercial service. It is a multi-step process that involves checking hardware, programming software, and validating the site with field tests. It ultimately verifies field performance as a customer would experience.

Depending upon when microwave or backhaul is available to the site, the commissioning and validation steps are executed in a different order. Referring to Figure 1, if backhaul is available to the site, then Scenario 1 is followed. This also assumes that the commissioning team has provisioned the BTS into the EMS and ASN-GW. This quickly brings the site to commercial service.

If backhaul is not available, then Scenario 2 is followed. Scenario 2 programs the BTS with a non-commercial configuration in order to verify basic RF configuration such as sector orientation, frequency, and transmit power. When backhaul is available then the commercial RF parameters are configured and the site is fully verifyd including performing network entry and handovers.

In order to determine which sections in this document to follow please refer to Figure 1.

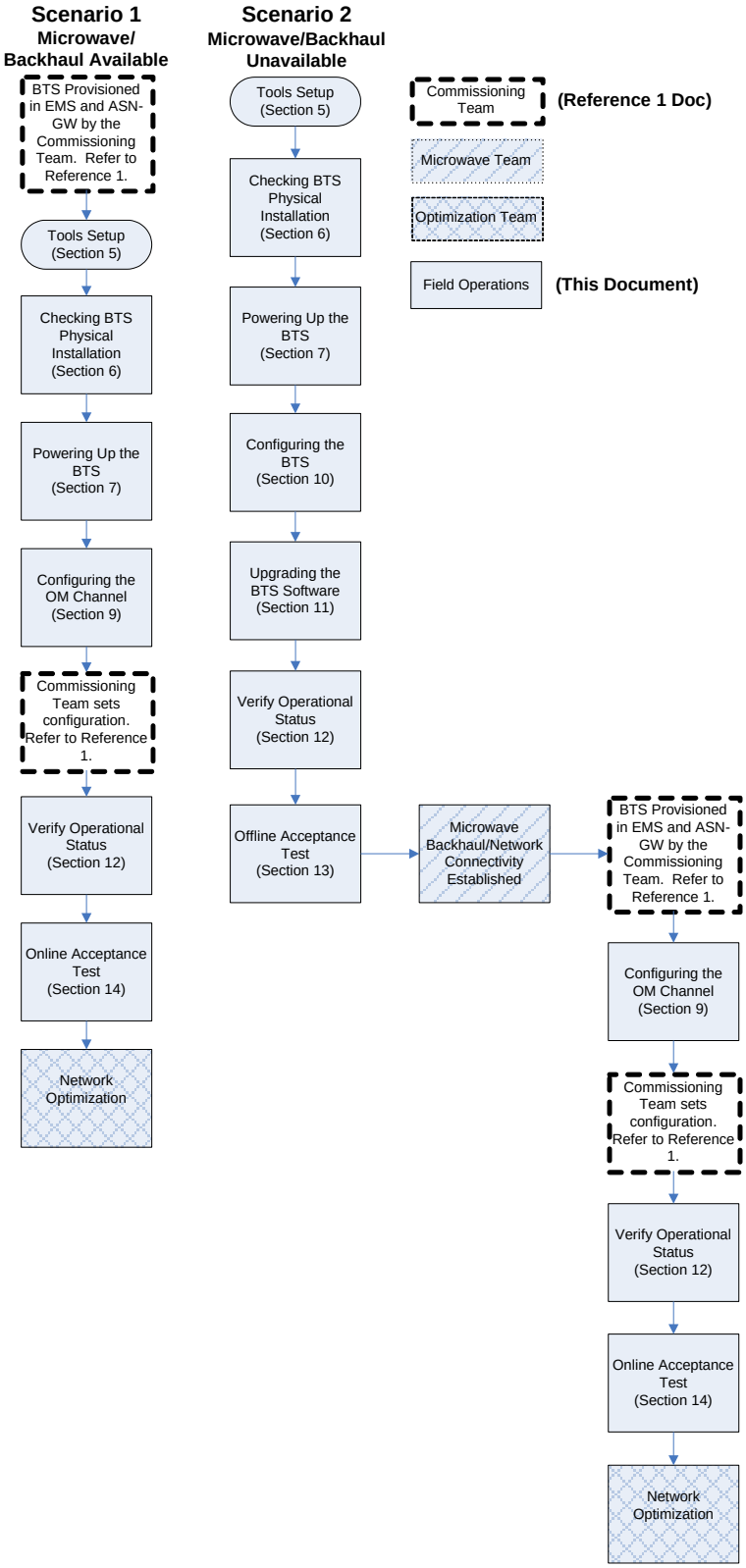


Figure 1: Commissioning Scenarios

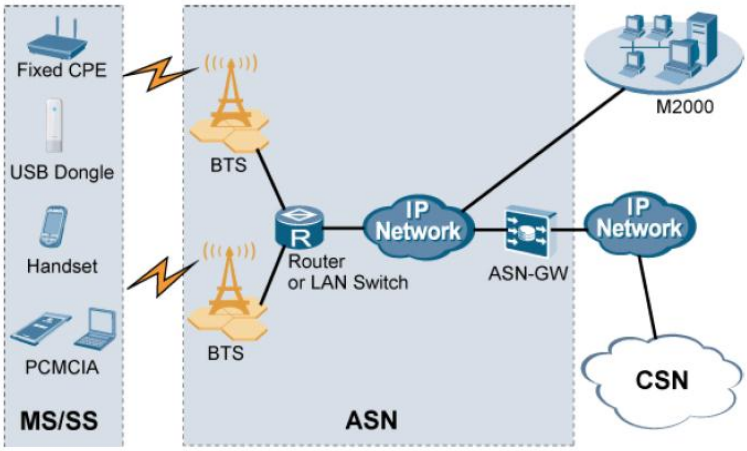


Figure 2: Network Architecture

4 Tools Setup

The following are the list of hardware, software, and data required.

Equipment	Quantity	Description
Laptop	1	IBM Thinkpad (T41, T42, T60, X60, R60) Dell (D400, D410, D600)
OS System	1	Windows XP Professional SP2
Device	1	Motorola Tornado
Connection Manager	1	SmithMicro "Clear" CM 1.01.0019 or newer
GPS	1	GlobalSat Waterproof Serial GPS Receiver BR-355
Power Supply	1	350-400 Watts
Cat-5 Patch Cable	1	Used for LMT and file transfer to DBS3900.
WiTT	1	Field test tool. Clearwire Sharepoint: Wimax-Operations -> Software -> WiTT
Java 1.5+	1	Software for running WiTT. http://java.sun.com/javase/downloads/index.jsp
Google Earth	1	Free map software. http://earth.google.com/download-earth.html
RF-EMSS Site Data	1	From ClearVision.

TABLE 1: List of Hardware, Software, and Data

4.1 SmithMicro "Clear" Connection Manager Configuration

In order to collect drive data on a specific sector, the connection manager must be initially configured for Clearwire's private NAP ID. This will prevent customers form accidently connecting to the site.

The NAP ID (network access provider identification) is an identifier that is part of the BSID (base identification) that is broadcast in the downlink by each DAP. As part of network entry, a device reads this NAP ID in order to determine whether to complete network entry on the site. NAP IDs can be public (for commercial use) or private (for testing). During commissioning, we will use a private NAP ID in order to prevent customers from connecting to the un-commissioned DAP. After EMS bootstrap, the connection manager is then reconfigured for the commercial NAP ID.

The following explains how to configure the connection manager for the private NAP ID.

1. In the Connection Manager, access the *Profiles* menu.

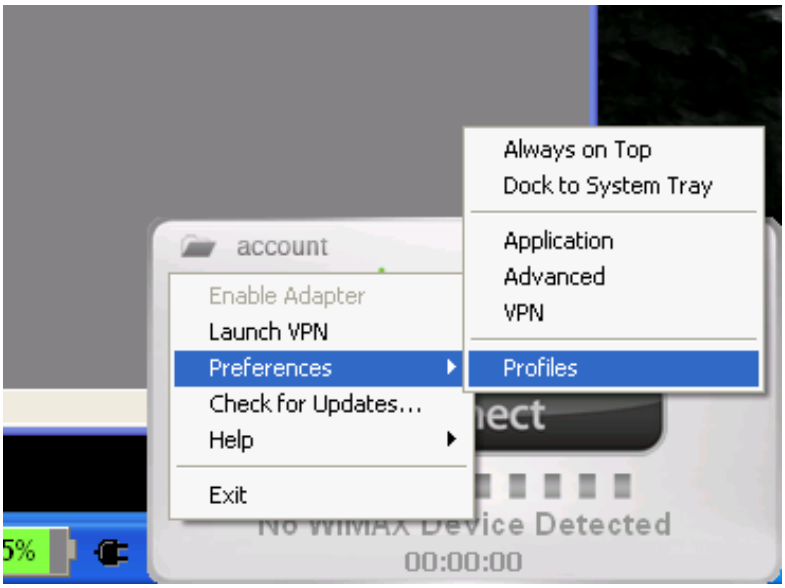


Figure 1: Profiles Menu

2. Hold the Control + Shift keys and Click the *Add* button.

3. Select the *Wimax* profile type.

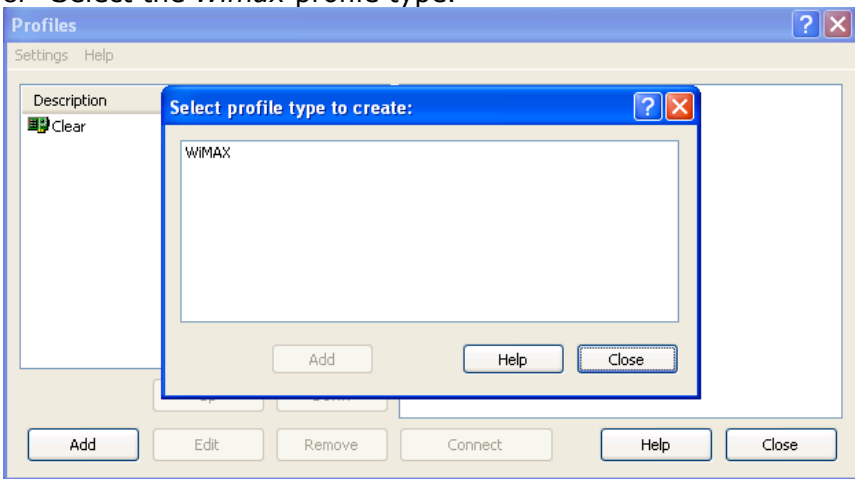


Figure 2: Wimax Profile Type

4. For the profile options, check *Override Identity*, *Select TLS Certificate*, and *Filter By Network Access Provider ID*.

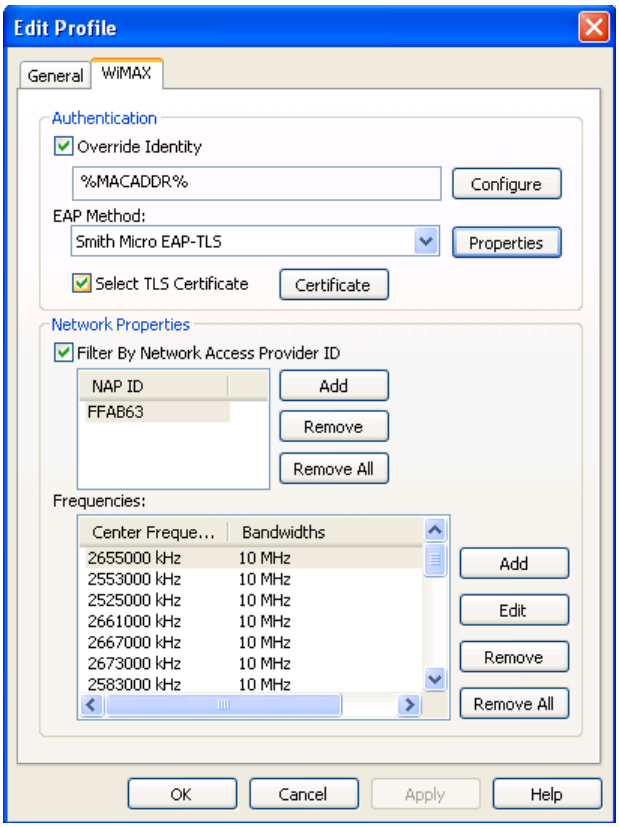


Figure 3: New Profile

5. Click the *Certificate* button and then check *Attempt to Load Embedded Device Certificate first*. Click *OK*.

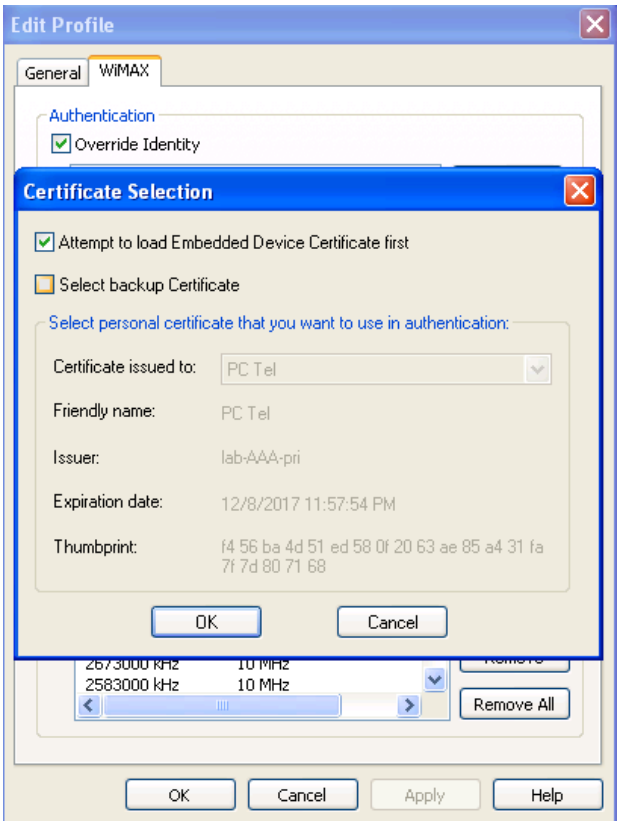


Figure 4: Choose Certificate Method

6. Click the *Add* button under *Filter by Network Access Provider ID* area. Specify the NAP ID for your market. Click *OK.*

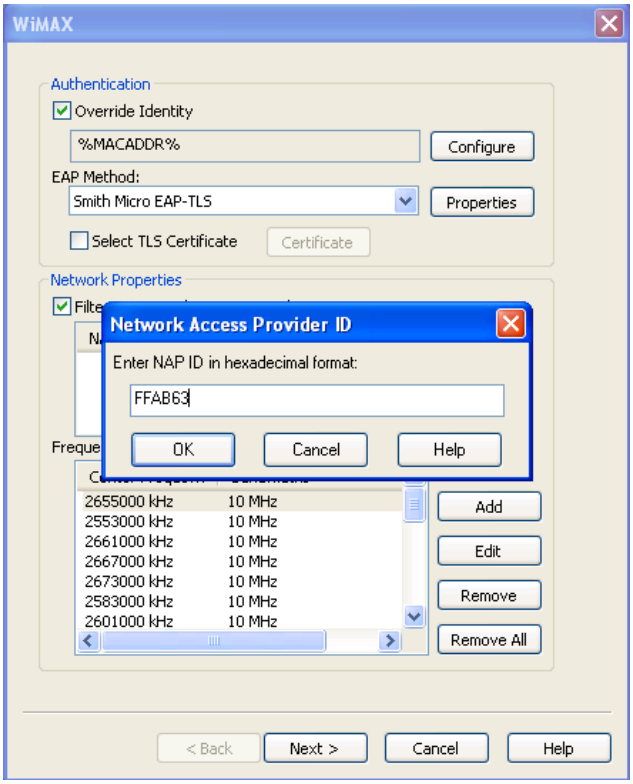


Figure 5: Setting the NAP ID

7. If necessary, add or remove frequencies by clicking *Add* or *Remove* under the *Frequencies* area. Click *OK*.

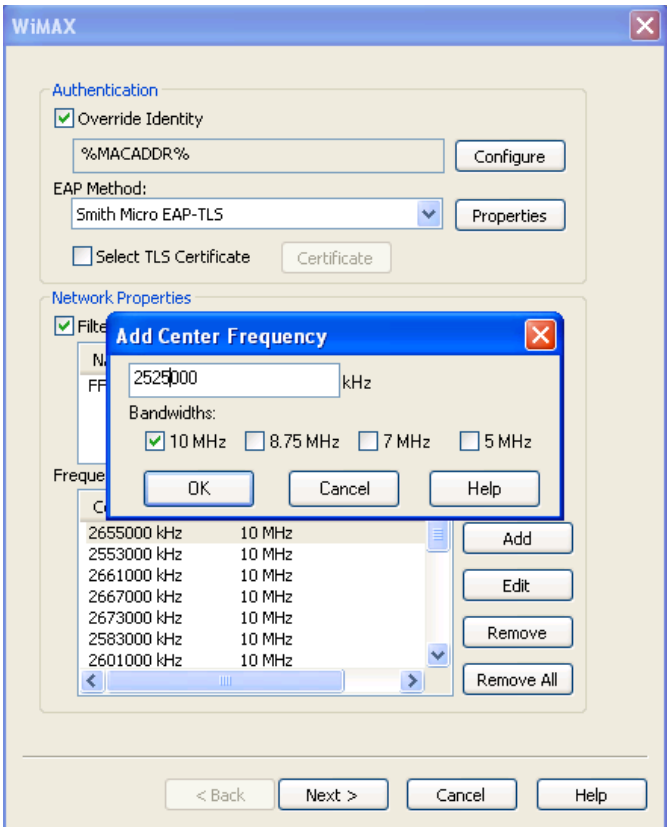


Figure 6: Adding Frequencies

8. Click *Next* >.
9. Specify **Private** for the *Profile name*.
10. For *Connection options*, select *Automatic*. Click *Finish*.

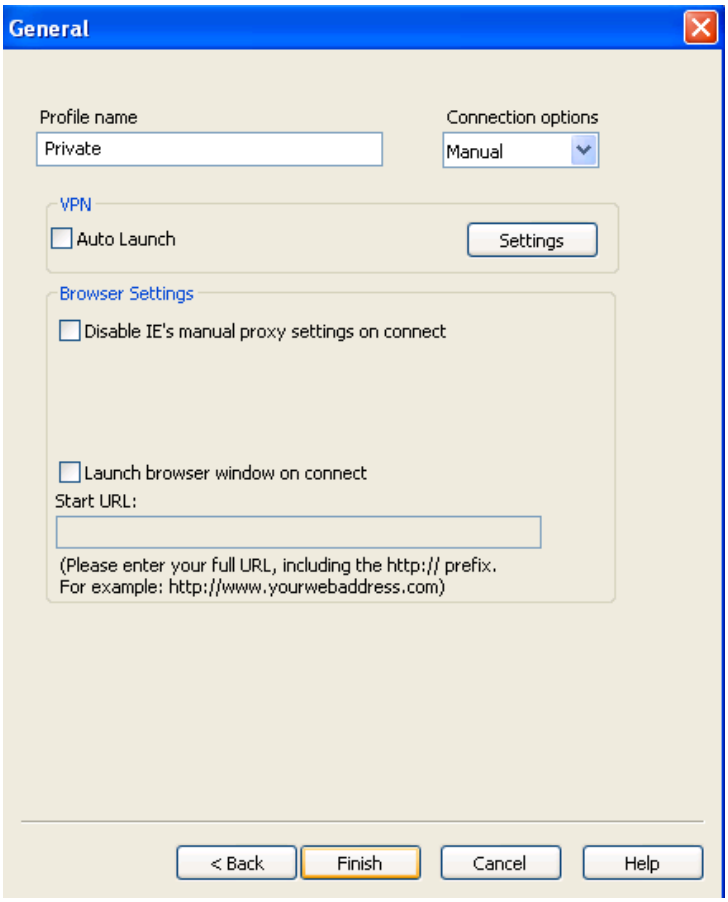


Figure 7: Profile Name

11. Select the *Private* profile and click the *Up* button to move it to the top of the list. After EMS bootstrap, you will need to revert back to the commercial NAP ID. To do this, move the *Clear* profile to the top.

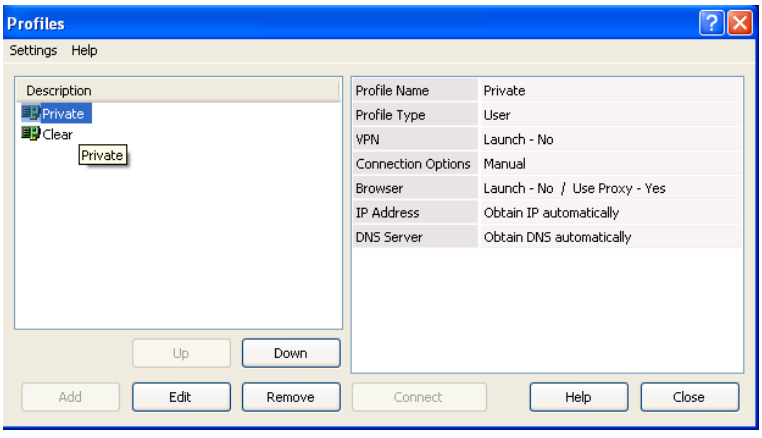


Figure 8: Private Preferred Profile

12. The connection manager is now configured. Click *Close*.

4.2 FreeFTPd

FreeFTPd is a free FTP/FTPS/SFTP server that enables user to access remote files over TCP/IP network.

FreeFTPd Installation

1. Download and install freeFTPd from http://www.freeftpd.com/?ctt=download.
2. Use the default setting for the installation
3. Start freeFTPd.
4. Click the Users menu option to open the users window.
5. Click the Add button.
    a. Login should be "apftp"
    b. Authorization should be set to "Password stored as SHA1 hash"
    c. Password should be set to "apftp"
    d. Confirmation password should be setup to "apftp"
    e. All other settings should be correct.

4.3 WiTT

The Wimax Tester Tool (WiTT) was created to help test Beceem-based Wimax devices such as USB, ExpressCard and PCMCIA on the Windows platform. It is a tool that will typically be used for drive tests. It provides GPS integration and mapping that allows the collection of metrics along a drive route.

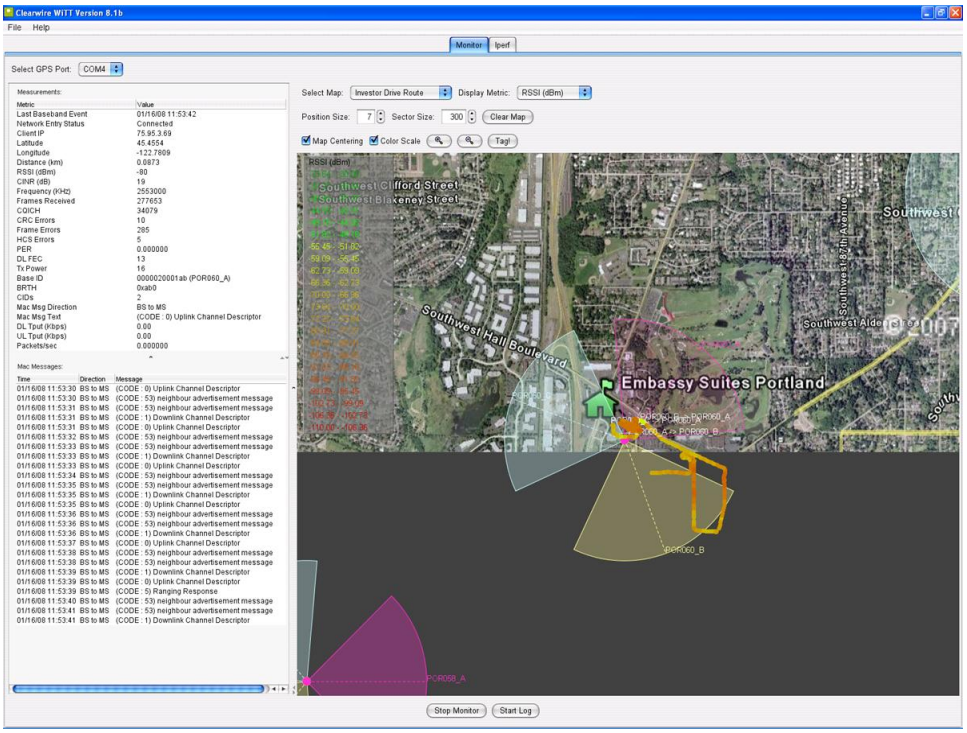


Figure 9: WiTT User Interface

The following lists the high-level features that WiTT provides:

- Real-time display of GPS, baseband, MAC messages, and OS throughput statistics.
- Logging of GPS, baseband, MAC messages, and OS throughput statistics to a CSV file for processing.
- Real-time map tracking while displaying the current position colored per current RSSI, CINR, DL-Tput, and UL-Tput (and more) color scale.
- Ability to load additional map images and select maps on the fly.
- Map zooming and centering per your current location.
- Ability to save the current map image.
- Visual display of handovers and custom text tagging at current position.
- Audible indication if network entry, network drop and handovers.

- Full-screen mode of real-time map for presentations.
- Iperf integration

Statistics

The following lists the statistics that are displayed and logged by WiTT:

Last Baseband Event
Network Entry Status
Client IP
Latitude
Longitude
Distance (km)
RSSI (dBm)
CINR (dB)
Frequency (KHz)
Frames Received
CQICH
CRC Errors
Frame Errors
HCS Errors
PER
DL FEC
Tx Power
Base ID
BRTH
CIDs
Mac Msg Direction
Mac Msg Text
DL Tput (Kbps)
UL Tput (Kbps)
Packets/sec
Packets Outbound Discarded
Packets Received Errors
Current Bandwidth
Packets Received/sec
Packets Received Non-Unicast/sec
Output Queue Length
Packets Received Discarded
Packets Sent Unicast/sec
Packets Outbound Errors
Packets Received Unknown
Packets Received Unicast/sec
Packets Sent/sec
Packets Sent Non-Unicast/sec

Installation

If a previous version of WiTT is installed, uninstall it completely by running the WiTT uninstaller from Start->Programs->Clearwire->WiTT->Uninstall WiTT.

1. WiTT is a Java-based tool that requires Java 1.5.0 or higher. Java can be downloaded from the Sun web site: http://java.sun.com/javase/downloads/

2. Go to

   https://share.clearwire.com/WIMAX%20%20Operations/Forms/AllItems.aspx?RootFolder=%2fWIMAX%20%20Operations%2fSoftware%2fWiTT

   and download the WiTT package.

3. Launch witt—vX.X-install.jar by double-clicking the file.

4. Follow the steps of the installer to install WiTT. Accept the default selections.

5. Launch WiTT from Start->Programs->Clearwire->WiTT.

Monitoring

The following describes how to start using WiTT to monitor statistics.

6. Ensure your GPS is connected and your Beceem-based Wimax device is connected.

7. If drive testing, ensure your other network connections such as Wifi and OpenVPN are disabled.

8. Launch WiTT.

9. Select the appropriate map.

10. Select the 'Start Monitor' button at the bottom.

That's it! You should now see your current location on the map and statistics being displayed to the left. At any time, you can select 'Stop Monitor' to stop the monitoring.

Logging

WiTT logs all the displayed statistics to a CSV file. This CSV file is created in the installation directory of Witt (C:\Program Files\WiTT).

The following steps describe how to start logging.

11. Ensure your GPS is connected and your Beceem-based Wimax device is connected.

12. Launch WiTT.

13. Select the appropriate map.

14. Select the 'Start Monitor' button at the bottom. The 'Start Log' button will now be enabled.

15. Select the 'Start Log' button. This creates a CSV file with a named based on the selected map and the time. For example, the following is a file name created when logging the 'PDX Warehouse' map.

'PDX Warehouse02008_January_16-12_11_56_stats.csv'

That's it! You are now logging statistics to a CSV in the installation directory. At any time, you can select 'Stop Log' to stop the logging.

Adding New Maps for WiTT

RF engineering will be supplying the MAP to use for WiTT

Prior to performing the acceptance test on the site, you may need to upload a new map to WiTT in order to view your desired coverage area. WiTT supports the adding of new maps. The following describes how to upload a new map using Google Earth. Google Earth can be download for free from: http://earth.google.com/download-earth.html

1. Launch Google Earth and navigate to your site and desired coverage area.

2. When you are satisfied with the view, switch to full screen mode under View->Full Screen (or F11).

Figure 10: Google Earth Full Screen View

3. When uploading a new map image to WiTT, the northwest and southeast latitude and longitude coordinates of the corners are required for image calibration. These coordinates must be in decimal format. Google Earth must be configured to do this under Tools->Options->3D View-> Show Lat/Long->Decimal Degrees. Once this is set, your cursor latitude and longitude coordinates will appear in the lower left of the Google Earth view. For your desired view, record the northwest and southeast corner coordinates. It's very important that this be as accurate as possible.

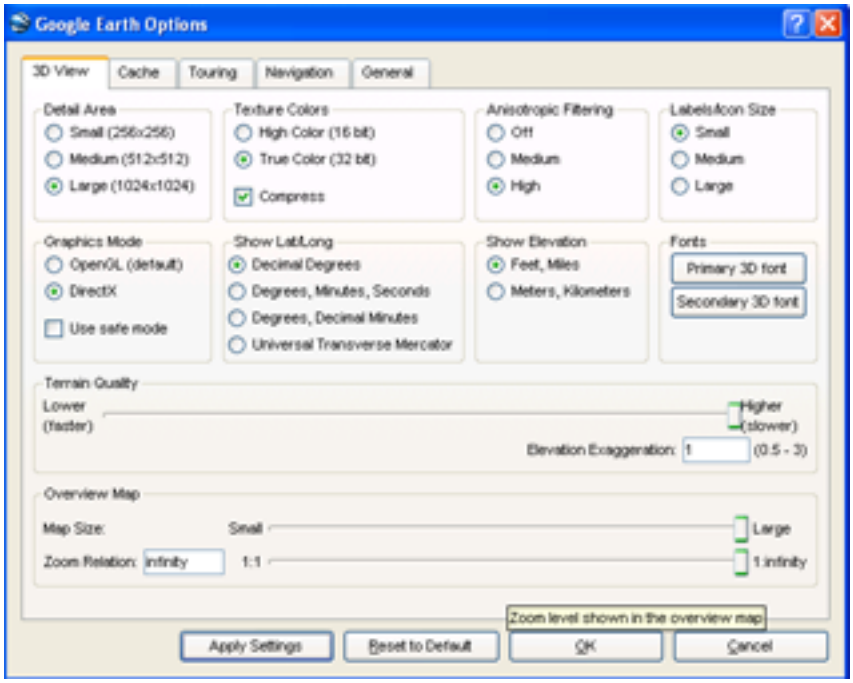


Figure 11: Google Earth Latitude and Longitude Settings

4. Now save your Google Earth view as an image using File->Save Image. Remember your image file location.

5. In WiTT, select Maps->Manage Maps to launch the Map Management Dialog.

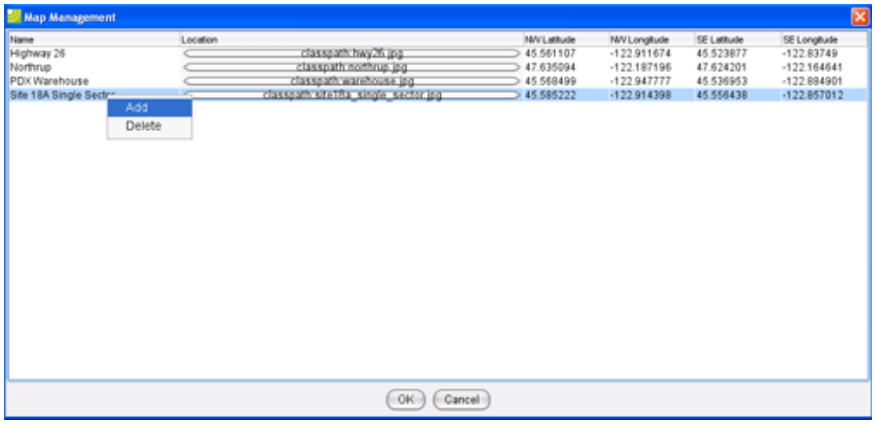


Figure 12: Map Management Dialog

6. Right-click and select 'Add' from the popup menu.

7. For the new row, specify your map name, navigate to your image location, and specify the northwest and southeast coordinates.

8. Select 'OK' in the dialog and your map image will be available immediately in the WiTT map selection pull down.

Adding New Bases to WiTT

WiTT allows you to add new bases to be displayed in the map view. This will probably need to be done when commissioning new sites. WiTT allows you to specify the name, location, azimuth, beamwidth and color of the base to be displayed.

Figure 13: Base Displayed in WiTT

1. In WiTT, select Maps->Manage Bases.

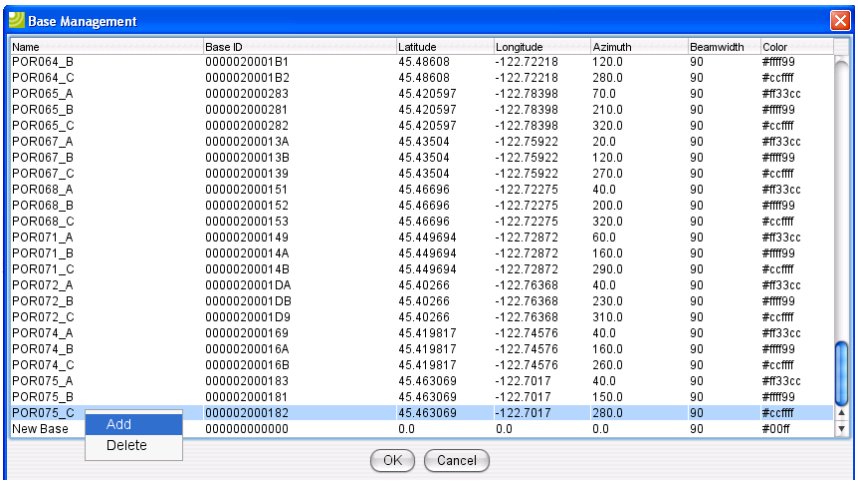


Figure 14: Base Management Dialog

2. Right-click and select ‘Add’ from the popup menu.

3. For the new row, specify your name, base ID, location coordinates, azimuth, beamwidth and color.

4. Select ‘OK’ in the dialog and your base will be available immediately in the WiTT map view.

5 BTS Overview

5.1 Overview

The section describes the hardware components and configuration of a Huawei Wimax DBS3900 BTS. Standard commissioning involves a single BBU (Baseband unit) chassis connected to 3 RRUs (Remote Radio Unit).

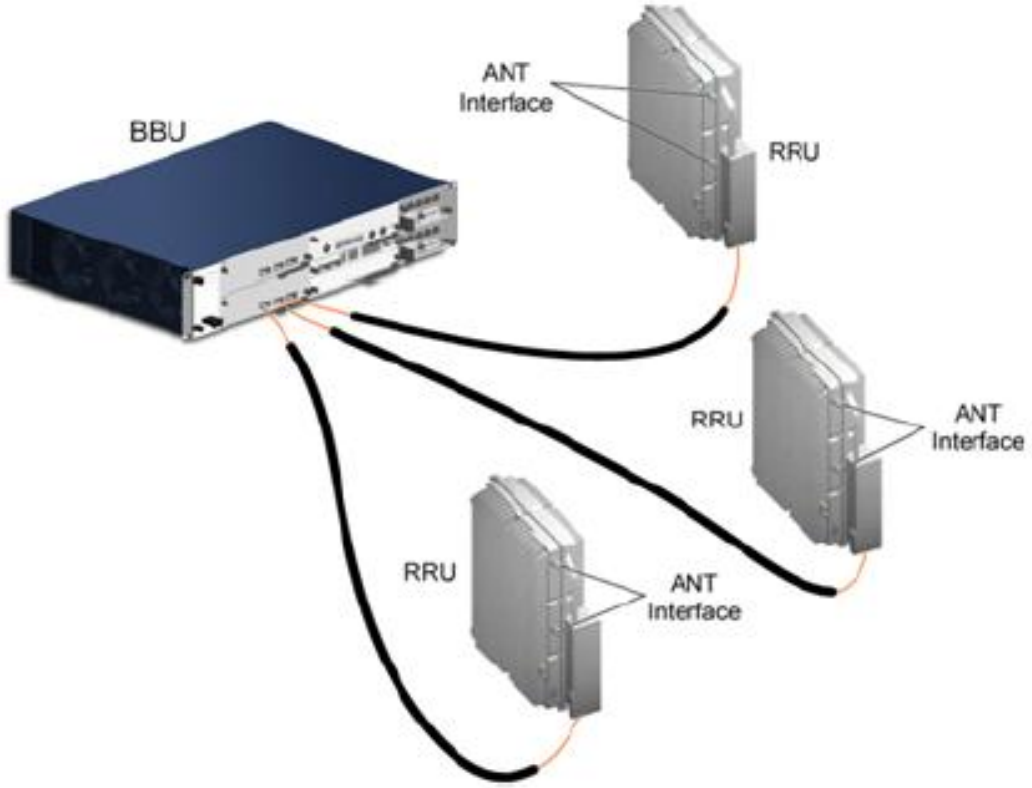


Figure 15: BBU with 3 RRUs

The BBU chassis has the following cards installed:

Card	Location	Description
BMPT	Slot 7	The BMPT is the main processing and transmission board.
BBI	Slot 3	The BBBI is the baseband processing and radio interface unit.
UPEU	UPEU1 Slot	The UPEU is the chassis power supply unit.
FAN	Fan Slot	The fan unit for the chassis.
BSBC	Backplane	The BSBC is the backplane of the chassis and provides power supply and service channels for each board.

FAN	SLOT0 BBBI	SLOT4 USCU	UPEU0
	SLOT1 BBBI	SLOT5 USCU	
	SLOT2 BBBI	SLOT6 reserved	UPEU1
	SLOT3 BBBI	SLOT7 BMPT	

Figure 16: BBU Chassis Slot Locations

The typical new site will have one BMPT, one BBI, and one UPEU. The FAN and BSBC modules are standard components.

5.2 BMPT

The BMPT is the main processing unit and includes three Ethernet ports for access to the BTS. These are labeled ETH, FE/GE0, and FE/GE1 on the card. ETH is the local maintenance port. FE/GE0 is the backhaul interface for OAM and signaling/traffic. The port is connected to the site switch. FE/GE1 is reserved for future use.

Figure 17: BMPT Card

Ports SFP0, SPF1, USB, and TST are not used.

RST is the reset switch for the board.

The GPS labeled connection is the GPS connection for the BTS and serves as the reference clock source.

The following table describes the LED indicators for the BMPT.

Port/LED Name	Color	State	Meaning
RUN	Green	On	There is power, but there is a fault.
		Off	No power.
		Blinking quickly	Board is loading.
		Blinking slowly	Normal operation.
ALM	Red	On	Critical alarm is active.
		Off	No alarm.
		Blinking	An alarm is active.
ACT	Green	On	BMPT is primary.
		Off	BMPT is standby.
ETH	Green (Link)	On	Connected.
		Off	Not connected.
	Orange (Act)	On	Data transmitting.
		Off	No data transmitting.
FE/GE0	Green (Link)	On	Connected.
		Off	Not connected.
	Orange (Act)	On	Data transmitting.
		Off	No data transmitting.

Figure 18: BMPT LED Indicators

5.3 BBI

The BBI card is the baseband and radio processing unit. The BBI is connected to the RRUs via optical ports located on the front panel.

Figure 19: BBI Card

The following table describes the LED indicators for the BBI.

Port/LED Name	Color	State	Meaning
RUN	Green	On	There is power, but there is a fault.
		Off	No power.
		Blinking quickly	Board is loading.
		Blinking slowly	Normal operation.
ALM	Red	On	Critical alarm is active.
		Off	No alarm.
		Blinking	An alarm is active.
ACT	Green	On	The board is operating normally.
		Off	The board is not operational.
LINK	Green	On	Link is normal.
		Off	Link is faulty.
ACT	Green	On	Data transmitting.
		Off	No data transmitting.

Figure 20: BBI LED Indicators

5.4 UPEU

The UPEU is the power supply unit for the chassis. It converts the -48 V DC input power to +12 V DC output power. A switch on the front panel can be used to power down the chassis.

Figure 21: UPEU Card

5.5 FAN

The FAN unit provides cooling for the chassis.

The following table describes the LED indicators for the FAN unit.

Port/LED Name	Color	State	Meaning
State	Green	Blinking quickly	The board is not registered with the chassis.
		Blinking slowly	Normal operation.
	Red	On	Critical alarm is active.
		Off	No power.

6 Checking BTS Physical Installation

6.1 Installing Hardware for Multi-Carrier

The default installation of a BBU supports 3 carriers with a single BBI card and 3 fiber cables connected. In some cases, additional carriers are required and this will be indicated in Clearvision by additional carrier IDs A2, B2, and C2. The field team must then add a second BBI card in slot 2 and connect the 2nd set of fiber from the RRU (s). This can be done before or after the commissioning process.

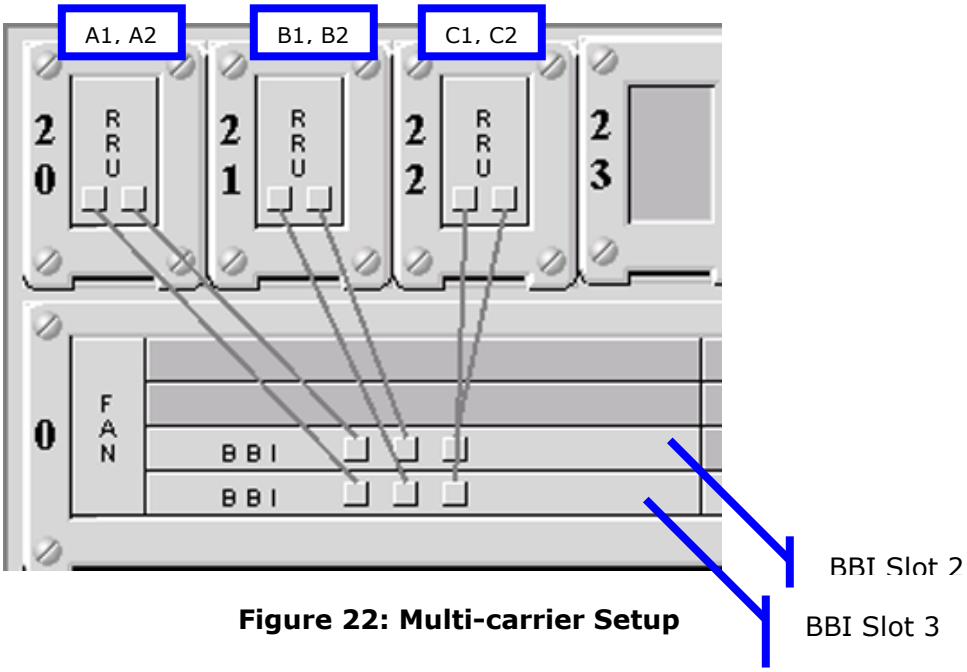


Figure 22: Multi-carrier Setup

6.2 Fiber Cabling Check

The new BTS may have a single BBI card that supports 3 sectors or carriers. This BBI card is located in slot 3 or the bottom left slot. RRU fiber cables for A1, B1, and C1 should be connected as shown:

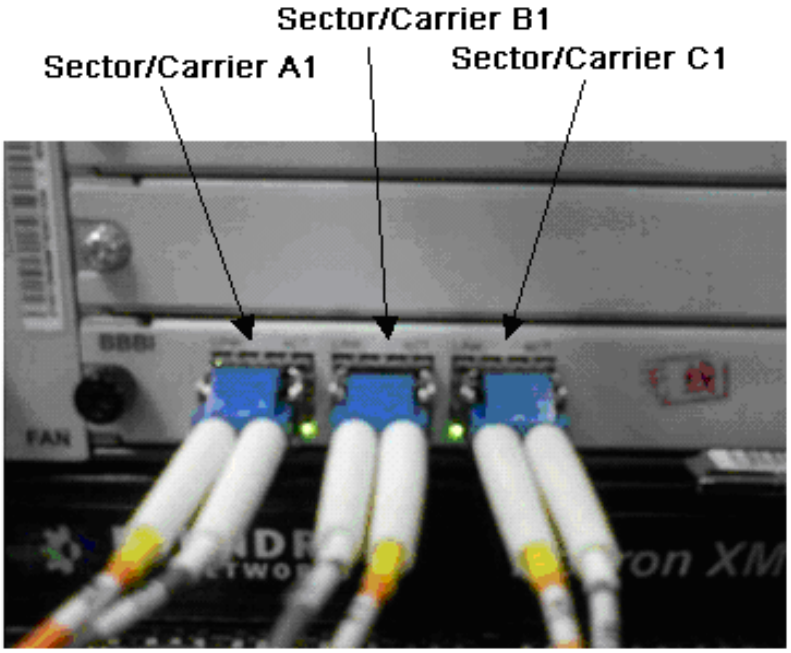


Figure 23: BBI Fiber Connections for 3 Sector/Carriers

If the BTS is configured for 4 or more carriers (A2,, B2, and C2), then a second BBI is added to slot 2. The second set of fibers corresponding to the 2nd port on the RRU are used for these additional carriers. These fibers are connected to the second BBI in the same left-to-right (A2, B2, C2) order.

6.3 Ethernet Cabling Check

The BTS has one backhaul Ethernet connection on the BMPT FE/GE0 for OAM and signaling/traffic. Ensure this is connected to Port 12 on the site switch.

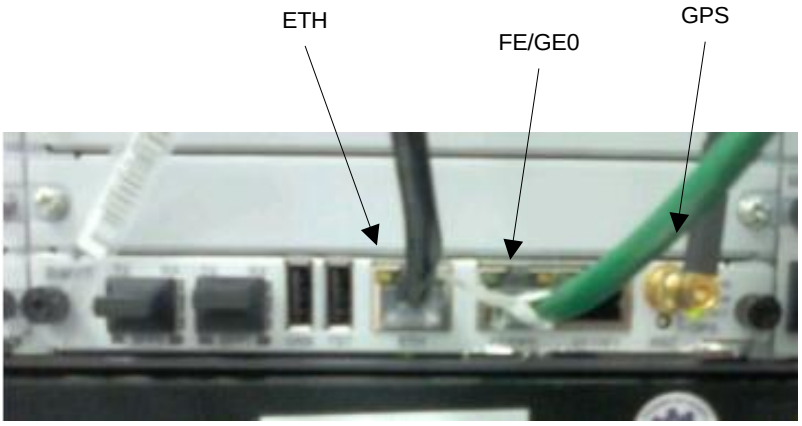


Figure 24: BMPT Ethernet Connections

6.4 GPS Cabling Check

Ensure that the GPS is connected to the RF GPS connector on the BMPT card. Refer to figure 23.

6.5 Power Cabling Check

The BTS contains one power supply unit. Check that the power cabling is connected.

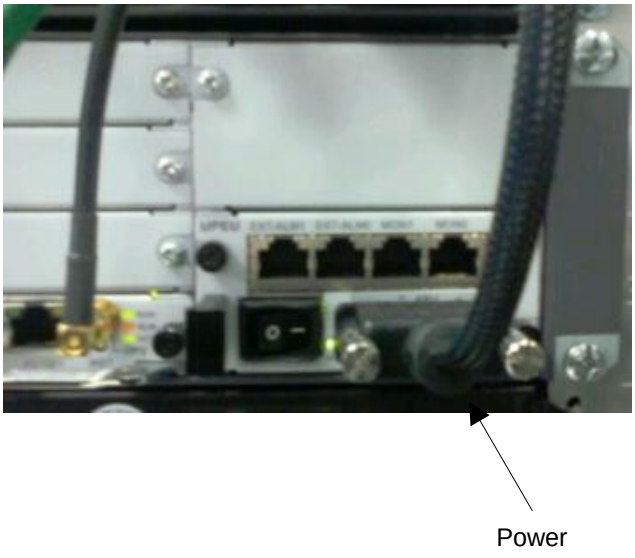


Figure 25: BMPT Power Connection

Check the power connections on the PB1. Refer to Figure X. (Need picture of this. PB1?)

7 Powering Up the BTS

The BTS power procedure is simple and only requires applying power to the RRUs and BBU chassis. Apply power at the PB1. Power on the RRUs and then the BBU chassis.

8 Accessing the BTS LMT

The BTS provides a web-based local maintenance terminal (LMT) for configuring and troubleshooting. The LMT will be used to commission the site and check status. Follow the steps below to access the LMT.

1. Connect an Ethernet from your laptop to the BTS Ethernet port labeled ETH.

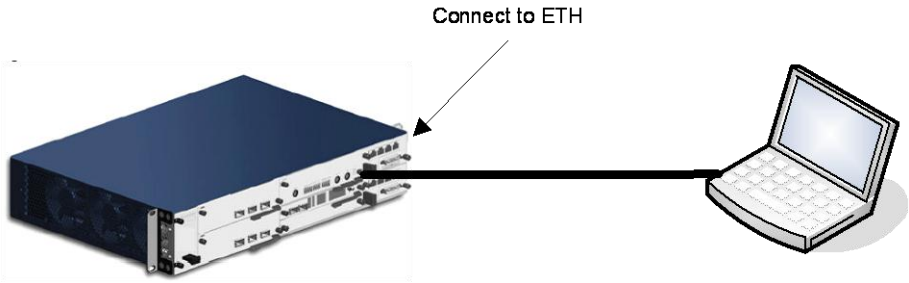


Figure 26: Laptop Connected to BTS

2. Configure your laptop network interface for 192.168.0.101/255.255.255.0 with no default gateway.

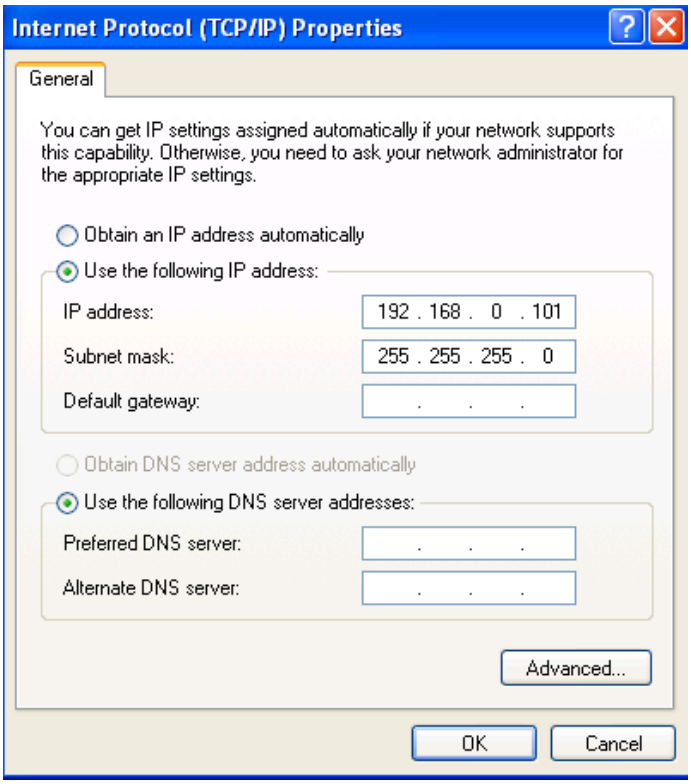


Figure 27: Network Interface Properties for LMT Access

3. Launch your browser and go http://192.168.0.100.
4. Log in using *admin/admin123.*

Figure 28: LMT Login Screen

5. You'll presented with the main LMT screen for the BTS.

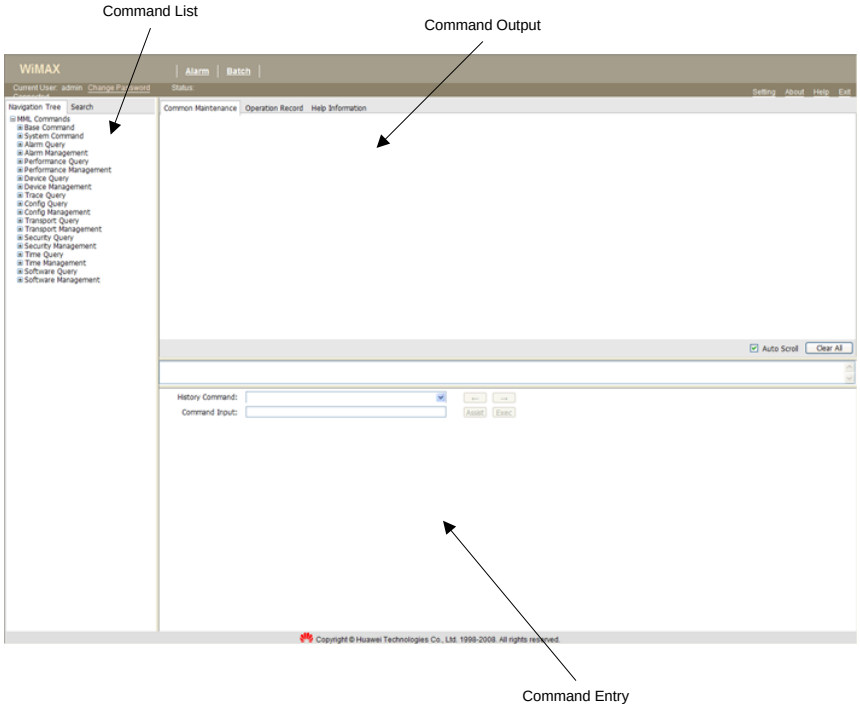


Figure 29: BTS LMT

The BTS LMT window is divided into 3 areas: Command List, Command Entry, and Command Output. For the procedures in this document, commands will be selected from the Command List, command parameters and execution will occur in the Command Entry, and output will be observed in the Command Output. The commands are referred to as MML commands (Man-to-Machine Language).

9 Querying and Configuring the BTS with HapSat

HapSat is a tool that was created to assist in performing site acceptance against the Huawei DBS3900. HapSat provides the ability to execute commands without the tedious and error-prone manual entry of MML commands. Additionally, command sets provide the ability to execute multiple commands quickly. All the MML commands listed in this document are available in HapSat and can be executed with a one-button click. Although HapSat provides an easy-to-use tool for performing tasks, a field tech should still be familiar with executing MML commands using the BTS LMT.

For additional HapSat documentation, please refer to the User Guide that is included in the HapSat installation.

9.1 Installation

If a previous version of HapSat is installed, uninstall it completely by running the HapSat uninstaller from Start->Programs->Clearwire->HapSat->Uninstall HapSat.

1. HapSat is a Java-based tool that requires Java 1.5.0 or higher. Java can be downloaded from the Sun web site: http://java.sun.com/javase/downloads/

2. Go to

   https://share.clearwire.com/WIMAX%20%20Operations/Forms/AllItems.aspx?RootFolder=%2fWIMAX%20%20Operations%2fSoftware%2fHapSat

   Portal: Technology Strategy & Standards Portal > WiMAX - Operations > Software > HapSat

   and download the HapSat package.

3. Launch hapsat—vX.X-install.jar by double-clicking the file.

4. Follow the steps of the installer to install HapSat. Accept the default selections.

5. Launch HapSat from Start->Programs->Clearwire->HapSat.

9.2 Executing HapSat Commands

By default, HapSat includes some typical MML commands that are used for site acceptance. Additional commands can be added by editing the hapsat_config.xml file in the HapSat installation directory. See the Appendix for an example HapSat configuration file with example commands. Also see the Appendix for notes and descriptions of some of the included commands. On launch, HapSat loads this file automatically to import commands.

The following steps describe how to execute commands with HapSat.

1. Launch HapSat.

2. Enter the IP address and login username and password.

3. Select 'Connect' and wait for the connection to be established.

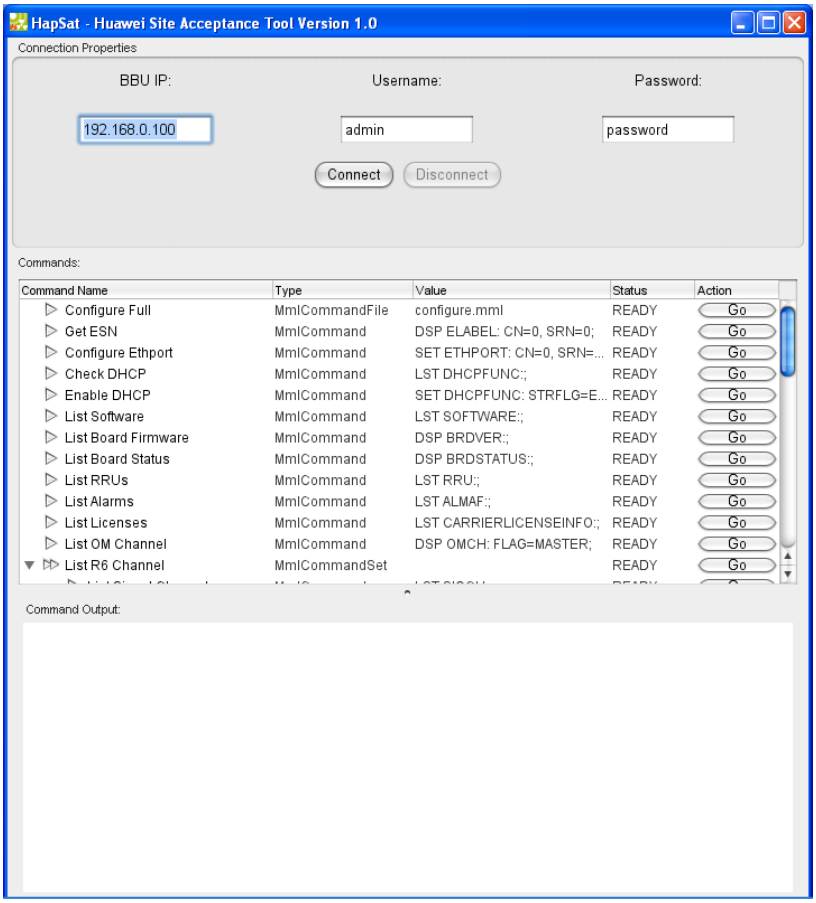


Figure 30: HapSat GUI

4. When ready, select the 'Go' button for the command you would like to execute. The 'Status' column provides feedback on the execution of the command.

5. When complete, the 'Status' column will provide completion status. If the command produces output, select the row of the command and view the output in the 'Command Output' text area.

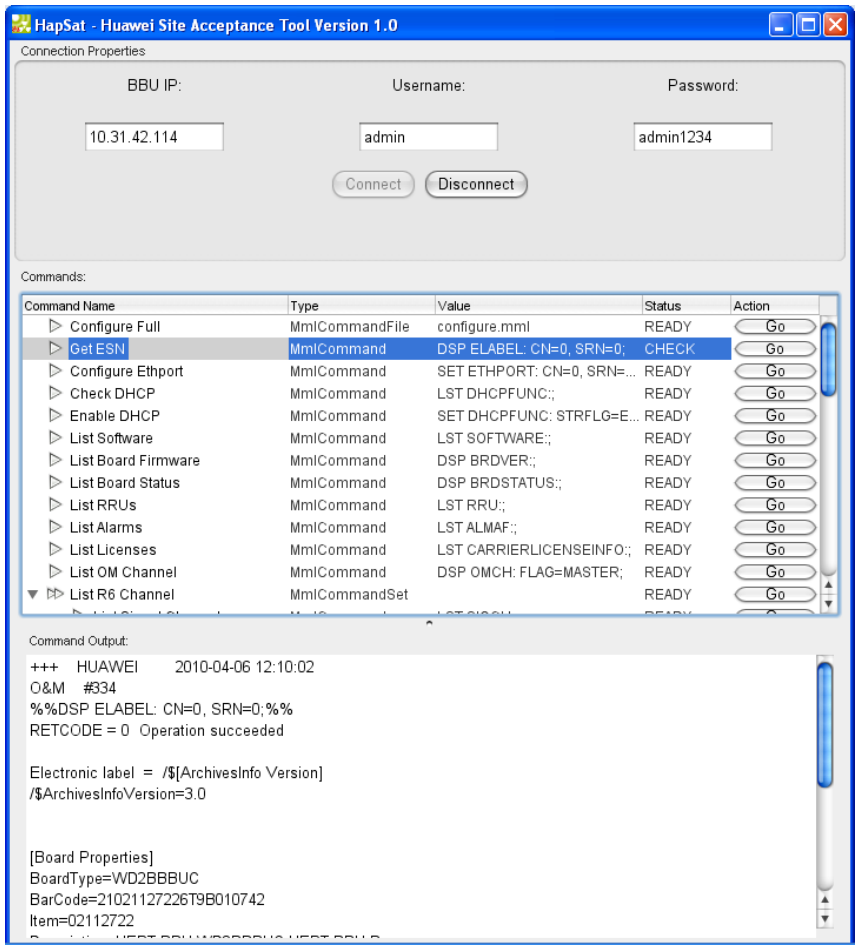


Figure 31: Executing a Command and Viewing Output

6. When complete, select 'Disconnect' to disconnect from the BBU.

7. If needed, debug output is created in messages.log located in the HapSat installation directory. This can be used to troubleshoot errors or failures.

9.3 BBU Configuration with HapSat

HapSat includes a special command "Configure Default Offline Configuration" that will configure the BBU for offline configuration mode. This uses a default MML configuration script file located in the HapSat installation directory:

C:\Program Files\HapSat\configure.mml

This is the same set of commands that are used to configure a BBU in the Huawei field commissioning guide. Executing this command will execute all the MML commands in this file to modify hardware

and software configuration. If necessary, you can modify this file to change frequencies or other parameters.

10 Configuring the OM Channel

10.1 Configuration via DHCP

The OM channel is the operations and maintenance connection that allows the commissioning team to configure and upgrade the BTS. The field commissioning team must set up this channel by enabling the Ethernet backhaul interface. Once enabled the interface receives a management IP address via DHCP. This allows the commissioning team to manage the BTS from the Huawei EMS. The following steps enable the Ethernet interface.

1. Log into the BTS LMT as described section 8.

2. Execute the following command to retrieve the ESN number.

```
/*Get ESN*/

DSP ELABEL: CN=0, SRN=0;
```

3. Provide this ESN number to the commissioning team before going to the next step.

```
+++    HUAWEI          2009-05-21 05:31:50
O&M    #1975
%%DSP ELABEL: CN=0, SRN=0;%%
RETCODE = 0  Operation succeeded

Electronic label  =  /$[ArchivesInfo Version]
/$ArchivesInfoVersion=3.0


[Board Properties]
BoardType=WD2BBBUC
BarCode=21021127226T92027028   ←ESN
Item=02112722
Description=HERT BBU,WD2BBBUC,HERT BBU Box
Manufactured=2009-02-22
VendorName=Huawei
IssueNumber=00
CLEICode=
BOM=

(Number of results = 1)


---    END
```

4. Execute the following command to configure the Ethernet interface.

```
/*Set Ethernet Port*/

SET ETHPORT: CN=0, SRN=0, SN=7, SSN=0, PT=ETH, PN=0, PA=ELEC,
MTU=1500, SPEED=100M, DUPLEX=FULL, FERAT=10, FERDT=8;
```

5. Notify the commissioning team that the Ethernet interface is now configured. The commissioning team will enable the backhaul port on the site switch. This will initiate the DHCP process for configuring the OM channel and the assigned management IP.

6. Verify the BTS DHCP function is operating with the following command.

```
/*List DHCP Func*/

LST DHCPFUNC:;
```

7. This should show as *enabled*.

```
%%LST DHCPFUNC:;%%
RETCODE = 0  Operation succeeded

LST DHCPFUNC Result
------------------
              Enable Flag  =  Enable
Start Time Threshold[min]  =  3
(Number of results = 1)


---    END
```

8. If it is disabled, use the SET DHCPFUNC to enable it. This command can be used to reset the BTS DHCP agent by disabling and the enabling.

```
/*SET DHCP Func*/

SET DHCPFUNC: STRFLG=ENABLE;
```

10.2 Manual Configuration (Only if Requested by Commissioning)

In the event that DHCP fails, the commissioning team may ask you to assign the OM channel IP manually. **Only perform these steps if requested by the commissioning team.** Use the following commands. The RED highlight indicates information that must be provided by commissioning.

```
/*Add Next Hop VLAN Mapping for OM Channel*/

ADD ARPVLAN: NEXTHOPIP="10.60.20.1", VLANMODE=SINGLEVLAN,
VLANID=12;

/*Add Interface IP Address*/

ADD ITFIP: CN=0, SRN=0, SN=7, SSN=0, PT=ETH, PN=0,
IP="10.60.20.32", MASK="255.255.252.0";

/*Add OM Channel*/

ADD OMCH: FLAG=MASTER, LOCALIP="10.60.20.32",
LOCALMASK="255.255.252.0", PEERIP="10.85.25.18",
PEERMASK="255.255.255.224", BRT=NO, CN=0, SRN=0, SN=7, SSN=0;

/*Add IP Route*/

ADD IPRT: CN=0, SRN=0, SN=7, SSN=0, DSTIP="0.0.0.0",
DSTMASK="0.0.0.0", RT=NEXTHOP, NEXTHOPIP="10.60.20.1", PREF=60;
```

11 Upgrading the BTS Software (If Needed)

11.1 Check BTS Software Version

The BTS software must be checked in order to determine whether a software upgrade is needed. Execute the following steps:

1. In the command entry, type:

```
LST SOFTWARE
```

2. The out put should look like the following. From this, you can determine whether a local software upgrade is needed. If so, proceed to section 9.3.

```
%%LST SOFTWARE:;%%
RETCODE = 0  Operation succeeded

Result of software query
------------------------
Storage Area  Software Version       Software Status

Standby Area  V300R002C01B032SPC004  Available
Main Area     V300R002C02B025        Available

(Number of results = 2)
```

11.2 Local Software Upgrade (If Needed)

Board Software Upgrade

Follow the next steps to perform a local software upgrade for the application software for the BMPT, BBI, and RRU.

1. If not running, start your local FTP server (on your laptop). Note the username and password for your FTP server.

2. Place the BTS application software package in the root directory of your FTP server.

3. Log into the BTS LMT.

4. In the command input area enter:

```
DLD SOFTWARE
```

5. Specify your FTP server, username, and password.
6. For the software type, specify "SOFTWARE".
7. Execute the command. Progress of the download should appear in the output window:

```
%%DLD SOFTWARE: IP="192.168.0.101", USR="apftp", PWD="*****";%%
RETCODE = 0  Progress report, Operation succeeded

Report Type  =  DOWNLOAD SOFTWARE
     Status  =  Progressing
   Progress  =  08%
 Session ID  =  65539
```

The following is reported when the software download is complete:

```
%%DLD SOFTWARE: IP="192.168.0.101", USR="apftp", PWD="*****";%%
RETCODE = 0  Progress report, Operation succeeded

Report Type  =  DOWNLOAD SOFTWARE
     Status  =  Success
 Session ID  =  65536

---    END
```

8. When the software download is complete, enter:

```
LST SOFTWARE
```

The new software appears in the STANDBY area:

```
%%LST SOFTWARE:;%%
RETCODE = 0  Operation succeeded

Result of software query
------------------------
Storage Area  Software Version  Software Status

Standby Area  V300R002C02B026   Available
Main Area     V300R002C02B025   Available
(Number of results = 2)


---    END
```

Bootrom Software Upgrade

Follow the next steps to perform a local software upgrade for the bootrom software for the BMPT, BBI, and RRU.

1. If not running, start your local FTP server (on your laptop). Note the username and password for your FTP server.
2. Place the BTS application software package in the root directory of your FTP server.
3. Log into the BTS LMT.
4. In the command input area enter:

```
DLD SOFTWARE
```

5. Specify your FTP server, username, and password.
6. For the software type, specify "BOOTROM".
7. Execute the command. Progress of the download should appear in the output window:

```
%%DLD SOFTWARE: IP="192.168.0.101", USR="apftp", PWD="*****";%%
RETCODE = 0  Progress report, Operation succeeded

Report Type  =  DOWNLOAD SOFTWARE
     Status  =  Progressing
   Progress  =  08%
 Session ID  =  65539
```

The following is reported when the software download is complete:

```
%%DLD SOFTWARE: IP="192.168.0.101", USR="apftp", PWD="*****";%%
RETCODE = 0  Progress report, Operation succeeded

Report Type  =  DOWNLOAD SOFTWARE
     Status  =  Success
 Session ID  =  65536

---    END
```

8. Next, execute the following command to load the software the running area. For the software type, specify "BOOTROM". Specify the new software label for the version.

```
LOD SOFTWARE
```

Progress of the loading should appear in the output window:

```
%%LOD SOFTWARE: SV="V300R002C02B026";%%
RETCODE = 0  Progress report, Operation succeeded

Report Type  =  LOAD SOFTWARE
     Status  =  Progressing
   Progress  =  78%
 Session ID  =  65537

---   END
```

The following is reported when the loading is complete:

```
%%LOD SOFTWARE: SV="V300R002C02B026";%%
RETCODE = 0  Progress report, Operation succeeded

   Report Type  =  LOAD SOFTWARE
        Status  =  Success
    Session ID  =  65537
  Total Boards  =  5
Succeed Boards  =  5
 Failed Boards  =  0

---   END
```

Activate Software

The following steps will activate the software and load it into RAM.

1. To activate the software, enter the following and specify the new software version:

```
ACT SOFTWARE
```

2. Progress of the activation should appear in the output area:

```
%%ACT SOFTWARE: OT=NE, SV="V300R002C02B026";%%
RETCODE = 0  Progress report, Operation succeeded

Report Type  =  ACTIVATE SOFTWARE
     Status  =  Progressing
   Progress  =  06%
 Session ID  =  65539
```

3. The board LEDs can be used to monitor the activation status. Refer to section 5 for LED status descriptions.

During activation, BMPT will reboot. Outage time is approximately 5 minutes. The following is reported when the activation is complete:

```
%%ACT SOFTWARE: OT=NE, SV="V300R002C02B026";%%
RETCODE = 0  Progress report, Operation succeeded

   Report Type  =  ACTIVATE SOFTWARE
        Status  =  Success
    Session ID  =  65540
  Total Boards  =  5
Succeed Boards  =  5
 Failed Boards  =  0

---    END
```

4. When activation is complete, check the software version. The new software version should be listed in the main area.

```
LST SOFTWARE
```

5. Next, check the bootrom version.

```
DSP BRDVER
```

6. The correct bootrom version should be displayed.

```
%%DSP BRDVER: CN=0;%%
RETCODE = 0  Operation succeeded

Result of current board software query
--------------------------------------
Subrack No.  Slot No.  Type    Software Version  Hardware Version     BOOTROM Version  Operation Result

22           0         RRU     11.011.10.013     MRRU.HWEI.bB3610200  11.011.10.013    Operation
succeeded
21           0         RRU     11.011.10.013     MRRU.HWEI.bB3610200  11.011.10.013    Operation
succeeded
20           0         RRU     11.011.10.013     MRRU.HWEI.bB3610200  11.011.10.013    Operation
succeeded
0            43        CMU     NULL              0                    NULL             Ru Not Online
0            33        PSU     NULL              0                    NULL             Operation
succeeded
0            44        BAT     NULL              0                    NULL             Operation
succeeded
0            32        PMU     NULL              0                    NULL             Ru Not Online
0            19        BBUPWR  NULL              0                    NULL             Operation
succeeded
0            16        BBUFAN  NULL              0                    NULL             Operation
succeeded
0            3         BBI     V300R002C02B026   WIMAX.BBBI.0.1       2.3.1.1          Operation
succeeded
0            7         MPT     V300R002C02B025   WIMAX.MPT.0.0        03.001.01.004    Operation
succeeded
(Number of results = 11)


---    END
```

12 Verifying Operational Status

After the upgrade is complete, the BTS status must be verified before performing drive tests. The next sections will verify the operational status of the BTS.

12.1 Verify Alarm Status

1. Log into the BTS LMT.
2. In the command input area enter:

```
LST ALMAF
```

3. The active alarms should be displayed in the output area. The only acceptable alarm is *Alarm of No User of Carriers*. This is a minor alarm that indicates no users are on the sector/carrier. There should be no other alarms.

12.2 Verify Fiber Status

The following steps will verify the fiber (and optical transceivers) for each of the sectors.

1. Log into the BTS LMT.
2. In the command input area execute the following commands:

```
GET OPTICALPORTINFO: RACKNO=0, SUBRACKNO=20, BOARDNO=0;
```

```
GET OPTICALPORTINFO: RACKNO=0, SUBRACKNO=21, BOARDNO=0;
```

```
GET OPTICALPORTINFO: RACKNO=0, SUBRACKNO=22, BOARDNO=0;
```

3. Each of these commands checks the fiber to the RRU. Each should return a valid response that includes the optical characteristics:

```
%%GET OPTICALPORTINFO: RACKNO=0, SUBRACKNO=22, BOARDNO=0;%%
RETCODE = 0  Operation succeeded

RRU optical port information
----------------------------
OPTICALPORTINDEX  INPOSITIONSTATUS  OPTICALMODULETYPE  VENDORNAME        OPTICALMODE  WAVELENGTH(nm)
RATING(100Mbps)  LINKLENGTH9M1KU(9μm)  LINKLENGTH9M100U(9μm)  LINKLENGTH50M(50μm)
LINKLENGTH625M(62.5μm)  TEMPERATURE(dedegrees Celsius)  VOLTAGE(mV)  CURRENT(mA)  OUTPUTPOWER(uW)
INPUTPOWER(uW)

0                 INPOSITION        ESFP              FINISAR CORP.     MULTIMODE    850             42
0                      0                      15                    7                      36
3393         5           377             373
1                 NOT INPOSITION    SFP               NULL              SINGLEMODE   0               0
0                      0                      0                     0                      0
0            0           0               0
```

```
(Number of results = 2)

---  END
```

4. An invalid response will be show in red:

```
%%GET OPTICALPORTINFO: RACKNO=0, SUBRACKNO=20, BOARDNO=0;%%
RETCODE = 1611202576  board unconfig or uninstall


---  END
```

12.3 Verify GPS Status

Follow the next steps to verify sector GPS status.

1. Log into the BTS LMT.

2. In the command input area enter:

```
DSP CLKSTAT
```

3. This will list the GPS state. Normal operation should appear as Normal and Locked:

```
%%DSP CLKSTAT:;%%
RETCODE = 0  Operation succeeded

System Clock State
------------------
       Current clock source  =  GPS
Current clock source status  =  Normal
            Clock work mode  =  Auto
                 PLL status  =  Locked
                  Center DA  =  31325
                 Current DA  =  31304
                 Initial DA  =  31325
(Number of results = 1)
```

12.4 Verify Clock Source

Follow the next steps to verify the BTS clock source.

1. Log into the BTS LMT.

2. In the command input area enter:

```
LST TIMESRC
```

3. GPS should be listed as the time source. A valid response should appear as:

```
%%LST TIMESRC:;%%
RETCODE = 0  Operation succeeded

Time Source Information
-----------------------
TIMESOURCE  =  GPS
(Number of results = 1)


---    END
```

12.5 Verify Carrier Status

Follow the next steps to verify sector RF transmission status.

1. Log into the BTS LMT.
2. In the command input area enter:

```
DSP CARRIERSTATUS
```

3. This will list the operational state of each of the sectors. Normal operation should appear as:

```
%%DSP CARRIERSTATUS:;%%
RETCODE = 0  Operation succeeded
CARRIER STATUS INFO
-------------------
SECTORID  CARRIERID  BLOCKFLAG  RESOUCESTATE  OPERTIONSTATUS
0         0          UnBlocked  Available     Available
1         0          UnBlocked  Available     Available
2         0          UnBlocked  Available     Available

(Number of results = 3)
---    END
```

12.6 Verify R6 ASN-GW Connectivity

Follow the next steps to verify R6 ASN-GW connectivity status. This is very important for network entry.

1. Log into the BTS LMT.
2. In the command input area enter:

```
LST SIGCH
```

3. This will list the R6 IP information and should appear as seen below with *Local Signaling IP* set to the R6 IP of the

site. The *Peer Signaling IP* should be set to the ASN-GW IP.

```
LST SIGCH:;
WA-SEA610
+++    HUAWEI        2009-07-29 10:40:54
O&M    #15174
%%/*38927*/LST SIGCH:;%%
RETCODE = 0  Operation succeeded

LST SIGCH Result
----------------
Local Signaling IP  =  10.60.24.42 <- check site specific R6 IP
 Peer Signaling IP  =  10.85.25.96 <- check for ASN-GW IP
       Cabinet No.  =  0
       Subrack No.  =  0
          Slot No.  =  7
(Number of results = 1)


---    END
```

4. Check that the ASN-GW identification has been entered with the following command:

```
LST MIXCFG
```

5. This will list the R6 IP information and identifier as seen below. Specifically, check the ASN-GW IP and the ID.

```
LST MIXCFG:;
WA-SEA610
+++    HUAWEI        2009-07-29 12:05:36
O&M    #15312
%%/*60150*/LST MIXCFG:;%%
RETCODE = 0  Operation succeeded

                     MaxLatency  =  0
                MsRelR1MsgType  =  BWA_MS_RELMSG_RNG-ABORT
                          GWIp  =  10.85.25.96 <- Check ASN-GW IP
                          GWId  =  0000-0000-0064  <- Check ID
                   TEKLifetime  =  700
         Sleep send type switch  =  BWA_SLP_SEND_SWITCH_OFF
      Dynamic server flow switch  =  BWA_Dynsf_SWITCH_OFF
  MS MAC for dynamic server flow  =  A9CC-CDDD-E123
           No user check period  =  28800
User access fail times Threshold  =  80
     User Reduce number Threshol  =  40
(Number of results = 1)


---    END
```

6. Check that the LGCPORT has been set correctly:

```
LST LGCPORT:;
```

```
LST LGCPORT Result
------------------
                              Cabinet No.  =  0
                              Subrack No.  =  0
                                 Slot No.  =  7
                           Logical Port No.  =  0
                              Subslot No.  =  0
                                Port Type  =  Ethernet
                                 Port No.  =  0
                        TX Bandwidth[kbps]  =  100000
                        RX Bandwidth[kbps]  =  100000
            TX Committed Burst Size[kbit]  =  100000
            TX Excessive Burst Size[kbit]  =  100000
                TX Traffic Shaping Switch  =  Off
   Realtime Traffic Measure Period[100ms]  =  5
TX Realtime Traffic Filter Coefficient[%]  =  25
RX Realtime Traffic Filter Coefficient[%]  =  25
                   Traffic Control Switch  =  On
            OM FTP Traffic Control Switch  =  Off
                          PQ Queue Number  =  5
            Congestion Time Threshold[ms]  =  100
      Congestion Clear Time Threshold[ms]  =  50
(Number of results = 1)


---    END
```

7. Check that the IPPATH has been set correctly:

```
LST IPPATH:;


LST IP Path Result
------------------
        IP Path ID  =  0
       Cabinet No.  =  0
       Subrack No.  =  0
          Slot No.  =  7
  Logical Port No.  =  0
      IP Path Type  =  QoS
              DSCP  =  63
          Local IP  =  10.60.24.42 <- Check site specific R6 IP
           Peer IP  =  10.85.25.96 <- Check ASN-GW IP
IP Path Check Flag  =  Disable

(Number of results = 1)
```

8. Verify connectivity to the ASN-GW by pinging it. Specify the R6 IP address for the source address and the ASN-GW address as the destination address:

```
PING: CN=0, SRN=0, SN=7, SRCIP="10.60.24.69", DSTIP="10.85.25.96",
CONTPING=DISABLE;

PING 10.85.25.96: 32  data bytes
   Reply from 10.85.25.96: bytes=32 Sequence=1 ttl=63 time=1 ms
   Reply from 10.85.25.96: bytes=32 Sequence=2 ttl=63 time=1 ms
   Reply from 10.85.25.96: bytes=32 Sequence=3 ttl=63 time=1 ms
```

```
   Reply from 10.85.25.96: bytes=32 Sequence=4 ttl=63 time=1 ms
   --- 10.85.25.96 ping statistics ---
   4 packet(s) transmitted
   4 packet(s) received
   Percent 0.00 packet lost <- Successful ping to the ASN-GW
   round-trip min/avg/max = 1/1/1 ms

   13 reports in total
---    END
```

12.7 Verify Handover Configuration

Follow the next steps to verify handover configuration.

1. Log into the BTS LMT.

2. In the command input area enter:

```
LST NBR
```

3. This will list all the neighbors configured for each sector. At a minimum, intracell neighbors should be configured. The following example below shows a sure with intracell neighbors only.

```
LST NBR:;
RTB0003-HUA-BBU
+++    HUAWEI        2009-07-29 16:47:17
O&M    #1898
%%/*1040*/LST NBR:;%%
RETCODE = 0  Operation succeeded

CBSID           NBRBSID

0000-0800-0300  0000-0800-0310 <-Sector A Neighbor
0000-0800-0300  0000-0800-0320 <-Sector A Neighbor
0000-0800-0310  0000-0800-0300 <-Sector B Neighbor
0000-0800-0310  0000-0800-0320 <-Sector B Neighbor
0000-0800-0320  0000-0800-0300 <-Sector C Neighbor
0000-0800-0320  0000-0800-0310 <-Sector C Neighbor
(Number of results = 6)
```

4. In the command input area enter:

```
LST TRIGGER
```

5. This will list all the handover triggers for each sector. Two trigger types should be configured for each sector as seen below.

```
LST TRIGGER:;
RTB0002-HUA-BBU
+++    HUAWEI        2009-07-29 16:50:57
O&M    #15424
%%/*1128*/LST TRIGGER:;%%
RETCODE = 0  Operation succeeded

TRIGGER INFO
```

```
------------
SECTORID  CARRIERID  TRIGGERID  TRIGGERTYPE  TRIGGERFUNCTION  TRIGGERACTION  TRIGGERVALUE
TRIGGERAVERDURATION

0         0          0          0            3                2              6
10
0         0          1          0            6                3              30
20
1         0          0          0            3                2              6
10
1         0          1          0            6                3              30
20
2         0          0          0            3                2              6
10
2         0          1          0            6                3              30
20
(Number of results = 6)
```

12.8 Verify Licenses

Follow the next steps to verify handover configuration.

1. Log into the BTS LMT.
2. In the command input area enter:

```
LST CARRIERLICENSEINFO
```

3. This will list the license configuration for all sectors and carriers. Ensure that all values are ON.

```
CARRIER LICENSE INFO
--------------------
SECTORID  CARRIERID  BASIC  ETHCS  MOBILITY  TWOANTENNAMIMO  FOURANTENNAMIMO
AIRITFENCRYPT

0         0          ON     ON     ON        ON              ON                ON
1         0          ON     ON     ON        ON              ON                ON
2         0          ON     ON     ON        ON              ON                ON
(Number of results = 3)
```

13 Verifying Expedience and Wimax Installation During Diplexer Cut

After cutting over diplexers with Expedience and Wimax installed, it is necessary to perform various checks to validate the installation. In order to this, some configuration must be performed on the Huawei Wimax BTS. Then noisefloor and VSWR checks must be formed on both the Expedience and Huawei Wimax BTS. This section explains the steps to perform these tasks.

Note: Sections 12.1 and 12.2 can be completed prior to the antenna and diplexer installations. Sections 12.3 to 12.10 should be performed after the antenna and diplexer installations are completed.

13.1 Verify Expedience Noisefloor Pre Diplexer Cut

Prior to the diplexer cut, the Expedience noisefloor must be measured on all BTS sectors. These values will be used to determine whether Wimax has introduced interference after the cut. Use the following steps to take these noisefloor readings.

1. Telnet and log into the Expededience BTS.

2. Execute the following command to clear the interference counters.

```
interference -r
```

3. Wait approximately 2 minutes and execute the following command to get new interference readings.

```
SuperUser>interference

Time: Tue Sep  8 21:36:48 2009

Seconds since last clear: 1735 seconds

Instantaneous symbol counts:

  Bad symbol 1 counts per FFAGC (from 0 to 11):

    0,0,0,330233,139826,2538,42,0,13,2,0,0

  Bad symbol 2-6 counts per FFAGC (from 0 to 11):

    0,0,0,2021249,335451,10862,173,9,78,6,0,0

  Good symbol counts per FFAGC (from 0 to 11) for 'me':
```

```
    0,0,0,0,0,0,26120,131,9784,460,1,1

  Good symbol counts per FFAGC (from 0 to 11) for other bases:

    0,0,0,0,514,130416,236,56,51,0,0,0

  Total symbols received destined for other bases: 131291

Count of symbols received destined for other bases (per base):

  These counts are accumulated periodically in a background task.
```

4. Take the highlighted GREEN values and use the embedded Excel table to calculate the noisefloor.

Bin->	0	1	2	3	4	5	6	7	8	9	10	11	Sums	
Counts->	0	0	0	3111148	285216	168	33	5	1	1	0	0	3396572	Noise Floor
Bin*Counts->	0	0	0	9333444	1140864	840	198	35	8	9	0	0	10475398	3.08410892

13.2 Configure the Huawei BTS

The BTS is delivered from the factory with a default configuration that only includes one RRU. The following steps must be executed in order to configure the hardware for a 3-sector BTS.

1. Power up the BBU and RRUs.

2. Log into the BTS LMT as described section 8.

3. This procedure only works on BTS software version SPC202 and higher. Execute the following MML command in the command input area to verify the software.

```
LST SOFTWARE
```

4. The main area should show SPC202 or higher.

```
LST SOFTWARE:;
WA-SEA0005
+++    HUAWEI        2009-09-17 20:30:22
O&M    #101614
%%/*47549*/LST SOFTWARE:;%%
RETCODE = 0  Operation succeeded

Result of software query
------------------------
Storage Area  Software Version   Software Status

Main Area     V300R002C02SPC202  Available
Standby Area  V300R002C02SPC200  Available
```

```
(Number of results = 2)


---    END
```

5. If the BBU was just powered up, it will take approximately 15 mins for the RRUs to boot up. Use the following command to check the status of the RRUs.

```
LST SOFTWARE
```

6. If status is *StartingUp* then the RRUs are not ready. A *Normal* status indicates that the RRUs are ready and you may proceed with the following steps.

```
DSP BRDSTATUS:;
WA-SEA0005
+++    HUAWEI          2009-09-17 20:34:48
O&M    #101620
%%/*50883*/DSP BRDSTATUS:;%%
RETCODE = 0  Operation succeeded

Display board status
--------------------
RACKNO   SUBRACKTYPE   SUBRACKNO   BOARDNO   AVAILSTATUS   ADMINSTATUS

0        BBU           0           3         NORMAL        Unlocked
0        BBU           0           7         NORMAL        Unlocked
0        BBU           0           16        NORMAL        Unlocked
0        BBU           0           19        NORMAL        Unlocked
0        RRU           20          0         NORMAL        Unlocked
0        RRU           21          0         NORMAL        Unlocked
0        RRU           22          0         NORMAL        Unlocked
(Number of results = 7)
```

7. Access the Batch window by clicking the Batch link at the top of the window

8. Copy and paste the following commands into the command input area and execute. The RED highlight indicates market specific information that must be provided. The YELLOW highlighted lines may fail with an error. This can be ignored.

```
/* Block sector in order to add and remove factory configured RRU*/

MOD CARRIERBLOCKFLAG: SECTORID=0, CARRIERID=0, BLOCKFLAG=BLOCKED;

RMV CARRIERBASICINFO: SECTORID=0, CARRIERID=0;

RMV SECTOR: SECTORID=0;

RMV RRU: RACKNO=0, SUBRACKNO=23, BOARDNO=0;

RMV SUBRACK: RACKNO=0, TYPE=RRU, SUBRACKNO=23;
```

```
RMV BTSINFO: OPERATORID=46;

/* Add Bts Info*/

ADD BTSINFO: OPERATORID=7,SITEID=0;

/* Add subracks*/

ADD SUBRACK: RACKNO=0, SUBRACKPOS=1, SUBRACKNAME="RRU01",
IS_REMOTE=YES, TYPE=RRU, SUBRACKNO=20;

ADD SUBRACK: RACKNO=0, SUBRACKPOS=2, SUBRACKNAME="RRU02",
IS_REMOTE=YES, TYPE=RRU, SUBRACKNO=21;

ADD SUBRACK: RACKNO=0, SUBRACKPOS=3, SUBRACKNAME="RRU03",
IS_REMOTE=YES, TYPE=RRU, SUBRACKNO=22;

/* Add RRUs*/

ADD RRU: RACKNO=0, SUBRACKNO=22, BOARDNO=0, BBI_SUBRACKNO=0,
RRUTYPE=RRU3702, BBI_BOARDNO=3, BBI_CPRINO=2;
ADD RRU: RACKNO=0, SUBRACKNO=21, BOARDNO=0, BBI_SUBRACKNO=0,
RRUTYPE=RRU3702, BBI_BOARDNO=3, BBI_CPRINO=1;
ADD RRU: RACKNO=0, SUBRACKNO=20, BOARDNO=0, BBI_SUBRACKNO=0,
RRUTYPE=RRU3702, BBI_BOARDNO=3, BBI_CPRINO=0;

/* add sector(using AntA& AntB only!!)*/

ADD SECTOR: SECTORID=0, TXANTNUM=4, RXANTNUM=4;

ADD SECTOR: SECTORID=1, TXANTNUM=4, RXANTNUM=4;

ADD SECTOR: SECTORID=2, TXANTNUM=4, RXANTNUM=4;

/* Add Carrier Basic Information*/

ADD CARRIERBASICINFO: SECTORID=0, CARRIERID=0, RACKNO=0, SUBRACKNO=0,
BOARDNO=3, CPRIID=0, CENTRALFREQUENCY=2673500, BANDWIDTH=10M,
DLZONETYPE=PUSC_ALL, ULZONETYPE=PUSC_ALL, SUBFRAMERATIO=29_18,
DLSEGMENTNO=0, CDMAGROUPSTART=0, EIRP=370, CELLRADIUS=COMMON,
TIMEDURATION=86400000, RNGPOWERTHRELD=30, ANTBITMAP=4T4R,
PREAMBLEINDEX=0;


ADD CARRIERBASICINFO: SECTORID=1, CARRIERID=0, RACKNO=0, SUBRACKNO=0,
BOARDNO=3, CPRIID=1, CENTRALFREQUENCY=2630500, BANDWIDTH=10M,
DLZONETYPE=PUSC_ALL, ULZONETYPE=PUSC_ALL, SUBFRAMERATIO=29_18,
DLSEGMENTNO=1, CDMAGROUPSTART=16, EIRP=370, CELLRADIUS=COMMON,
TIMEDURATION=86400000, RNGPOWERTHRELD=30, ANTBITMAP=4T4R,
PREAMBLEINDEX=33;

ADD CARRIERBASICINFO: SECTORID=2, CARRIERID=0, RACKNO=0, SUBRACKNO=0,
BOARDNO=3, CPRIID=2, CENTRALFREQUENCY=2650500, BANDWIDTH=10M,
DLZONETYPE=PUSC_ALL, ULZONETYPE=PUSC_ALL, SUBFRAMERATIO=29_18,
DLSEGMENTNO=2, CDMAGROUPSTART=32, EIRP=370, CELLRADIUS=COMMON,
TIMEDURATION=86400000, RNGPOWERTHRELD=30, ANTBITMAP=4T4R,
```

```
PREAMBLEINDEX=66;


/* Add GPS*/

ADD GPS: CN=0, SRN=0, SN=7, DELAY=0;

/*Set GPS*/

SET GPS: DELAY=0;

/*Add clock source*/

ADD CLKSRC: CLKSRC=GPS, PRI=1;

/*Set clock work mode*/

SET CLKMODE: MODE=MANUAL;

/*set time src to GPS*/

SET TIMESRC: TIMESRC=GPS;
```

13.3 Verify Carrier Status and Unblock

Note: Sections 12.3 to 12.10 should be performed after the antenna and diplexer installations are completed.

1. In the command input area enter the following to check the carrier status:

```
DSP CARRIERSTATUS
```

2. This will list the current state of the carriers. If any carriers are blocked. You must unblock them in order to allow RF transmissions and to complete the next sections.

```
DSP CARRIERSTATUS:;
WA-SEA0005
+++    HUAWEI        2009-09-17 20:41:57
O&M    #101632
%%/*57649*/DSP CARRIERSTATUS:;%%
RETCODE = 0  Operation succeeded

CARRIER STATUS INFO
-------------------
SECTORID  CARRIERID  BLOCKFLAG  RESOUCESTATE  OPERTIONSTATUS

2         0          Unblocked  Available     Available
1         0          Unblocked  Available     Available
0         0          Unblocked  Available     Available
(Number of results = 3)
```

```
---    END
```

3. To unblock carriers use the following command with *Block Flag* set to *Unblock* for each blocked carrier.

```
MOD CARRIERBLOCKFLAG
```

13.4 Verify for Rolled Fiber

A fiber run ay be connected to the incorrect port on the RRU, this is termed as "rolled" fiber. Use the following steps to check this condition. Note: This check only applies to a site with a single carrier on the RRU.

1. In the command input area execute the following commands:

```
GET OPTICALPORTINFO: RACKNO=0, SUBRACKNO=20, BOARDNO=0;
```

```
GET OPTICALPORTINFO: RACKNO=0, SUBRACKNO=21, BOARDNO=0;
```

```
GET OPTICALPORTINFO: RACKNO=0, SUBRACKNO=22, BOARDNO=0;
```

2. Check the input power column of the output. Input power should be shown for port index = 0. If input power is zero for port index = 0, then the fiber is "rolled".

```
GET OPTICALPORTINFO: RACKNO=0, SUBRACKNO=20, BOARDNO=0;
HI-HON0063
+++    HUAWEI        2009-09-08 23:07:52
O&M    #11976
%%/*4054*/GET OPTICALPORTINFO: RACKNO=0, SUBRACKNO=20, BOARDNO=0;%%
RETCODE = 0  Operation succeeded

RRU optical port information
----------------------------
OPTICALPORTINDEX  INPOSITIONSTATUS  OPTICALMODULETYPE  VENDORNAME        OPTICALMODE
WAVELENGTH(
nm)  RATING(100Mbps)  LINKLENGTH9M1KU(9micron)  LINKLENGTH9M100U(9micron)
LINKLENGTH50M(50micron)  LINKLENGTH625M(62.5micron)  TEMPERATURE(dedegrees Celsius)
VOLTAGE(mV)  CURRENT(mA)  OUTPUTPOWER(uW)  INPUTPOWER(uW)

0                 INPOSITION        ESFP              AVAGO             MULTIMODE    850
43              0                           0                              15
7                           47                                 3402         5            318
336
1                 INPOSITION        ESFP              AVAGO             MULTIMODE    850
43              0                           0                              15
7                           43                                 3397         6            340
0
(Number of results = 2)


---    END
```

13.5 Verify GPS Status

Follow the next steps to verify sector GPS status.

1. In the command input area enter:

```
DSP CLKSTAT
```

2. This will list the GPS state. Normal operation should appear as Normal and Locked:

```
%%DSP CLKSTAT:;%%
RETCODE = 0  Operation succeeded

System Clock State
------------------
       Current clock source  =  GPS
Current clock source status  =  Normal
            Clock work mode  =  Auto
                 PLL status  =  Locked
                  Center DA  =  31325
                 Current DA  =  31304
                 Initial DA  =  31325
(Number of results = 1)
```

13.6 Verify Clock Source

Follow the next steps to verify the BTS clock source.

1. In the command input area enter:

```
LST TIMESRC
```

2. GPS should be listed as the time source. A valid response should appear as:

```
%%LST TIMESRC:;%%
RETCODE = 0  Operation succeeded

Time Source Information
-----------------------
TIMESOURCE  =  GPS
(Number of results = 1)


---    END
```

13.7 Verify Wimax VSWR

The following steps will verify the VSWR levels for each of the sectors.

1. In the command input area execute the following commands:

```
GET RRUVSWR: RACKNO=0, SUBRACKNO=20, BOARDNO=0;
GET RRUVSWR: RACKNO=0, SUBRACKNO=21, BOARDNO=0;
GET RRUVSWR: RACKNO=0, SUBRACKNO=22, BOARDNO=0;
```

2. Each of these commands checks the VSWR levels for each transmit/receive port. If Wimax is suspected to be causing Expedience interference, this command can be used to identify the port and jumpers that may be causing the interference. This command measures the reflection through the system that may give clues as to the cause. **VSWR values should be equal to or less than 1.7 for non-diplexer installations. For diplexer installations, values should be equal to or less than 2.0.** Higher values may indicate the need to replace jumpers on the offending port. This command must be executed against each RRU.

	Valid VSWR Values
Non-diplexer Installation	17/1.7 or less
Diplexer Installation	20/2.0 or less

```
+++    HUAWEI        2009-06-27 03:50:24
O&M    #25145
%%GET RRUVSWR: RACKNO=0, SUBRACKNO=20, BOARDNO=0;%%
RETCODE = 0  Operation succeeded

RRU VSWR
--------
TXINDEX  VSWR(0.1)

0        11
1        11
2        12
3        10
(Number of results = 4)


---    END
```

13.8 Verify Wimax Noisefloor Levels

The following steps will verify the noisefloor levels for each of the sectors.

1. In the command input area execute the following commands:

```
GET RRURTWP: RACKNO=0, SUBRACKNO=20, BOARDNO=0;
GET RRURTWP: RACKNO=0, SUBRACKNO=21, BOARDNO=0;
GET RRURTWP: RACKNO=0, SUBRACKNO=22, BOARDNO=0;
```

2. Each of these commands checks the interference levels. Each should return a valid response that shows a noise floor near -98 to -100dBm. The response shows 4 samples for our single carrier on the sector.

```
%%GET RRURTWP: RACKNO=0, SUBRACKNO=20, BOARDNO=0;%%
RETCODE = 0  Operation succeeded

RRU RTWP
--------
RXIDDEX  RRU CARRIERINDEX  RTWP(0.1dBm)

0        0                 -986
0        1                 -13486
0        2                 -13486
1        0                 -987
1        1                 -13486
1        2                 -13486
2        0                 -991
2        1                 -13486
2        2                 -13486
3        0                 -986
3        1                 -13486
3        2                 -13486
(Number of results = 12)


---    END
```

13.9 Verify Expedience Noisefloor Post Diplexer Cut

The Expedience noisefloor must also be verified after the diplexer cut in order to identify Wimax induced interference. Use the same steps in section 13.1 for taking post readings for comparison. An increase of more than 10% should be investigated.

13.10 Block Wimax Carriers

When all steps are complete, the Wimax RF transmission should be blocked before leaving the site. Follow the next steps to block RF transmission.

1. In the command input area enter the following command with *Block Flag* set to *Block* for each carrier:

```
MOD CARRIERBLOCKFLAG
```

2. Next enter the following to check the carrier status:

```
DSP CARRIERSTATUS
```

3. This will list the current state of the carriers. All carriers should be *Blocked*.

```
DSP CARRIERSTATUS:;
WA-SEA0005
+++    HUAWEI        2009-09-17 20:41:57
O&M    #101632
%%/*57649*/DSP CARRIERSTATUS:;%%
RETCODE = 0  Operation succeeded

CARRIER STATUS INFO
-------------------
SECTORID  CARRIERID  BLOCKFLAG  RESOUCESTATE  OPERTIONSTATUS

2         0          Blocked  Available     Available
1         0          Blocked  Available     Available
0         0          Blocked  Available     Available
(Number of results = 3)


---    END
```

14 Offline Acceptance Test

This section of the acceptance test plan is performed on sites that do not have any backhaul connectivity and network entry is not possible. The site acceptance procedures outlined below are a simplified subset of functionality checks that include verification of the following aspects:

- Basic airlink parameter verification (BSID, center frequency etc). Please note that we will be using a canned NECB file with simplified values.
- Identification of swapped sectors.
- Azimuth verification
- Field verification of Main/Diversity branch operation.
- Basic coverage and CINR checks.

14.1 Obtain RF Planning Information

RF engineering will provide the following info.

- RF coverage plot showing best server transmitter information
- BSID and preamble index
- Frequency of operation
- Sector distance limits

This information includes a plot of the best server transmitter information and a map specifying the boundaries of the sector to be driven. Also included are basic airlink parameters to test the validity of which sector/frequency is being tested.

The default BTS configuration will transmit with preamble indexes of 0, 33, 66 for A, B and C respectively.

BSIDs are set to :

Sector 1 = FFAB63000000

Sector 2 = FFAB63000010

Sector 3 = FFAB63000020

These BSID values will be used to verify sector coverage.

14.2 Verify Site Location

This portion of the test procedure requires the basic collection of site identifiers to verify coordinate and structure type information used in internal databases/prediction tools and to ensure that the right site is being tested.

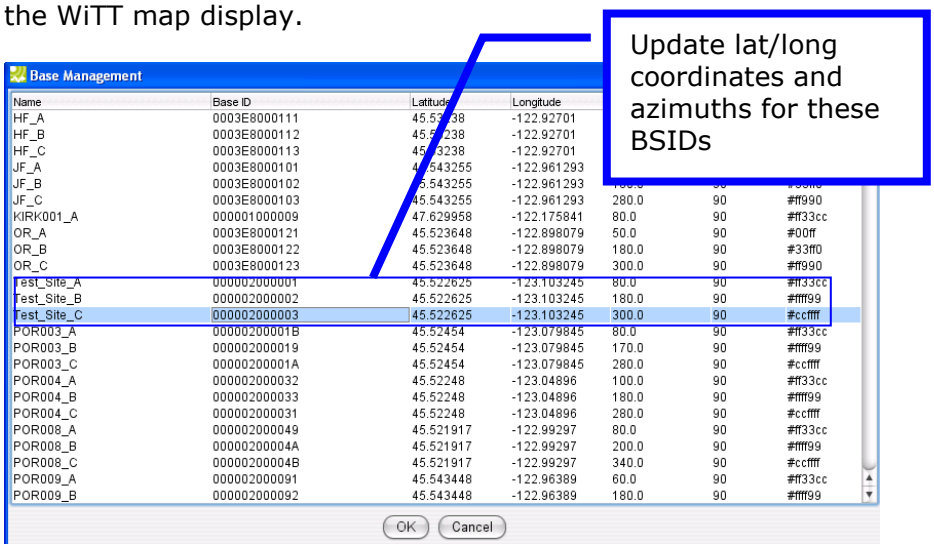
1. Launch WiTT with the GPS.
2. Under *Maps-> Manage Bases*, update these BSIDs

   Sector 1 = FFAB63000000

   Sector 2 = FFAB63000010

   Sector 3 = FFAB63000020

   with the latitudes and longitudes coordinates and azimuths of the site. This will allow correct position and site acquisition on the WiTT map display.



3. From the base of the site, record the following information

   a. Latitude (5 decimal digits ex. 45.45653)

   b. Longitude (5 decimal digits)

   c. Structure Type (Monopole/Rooftop etc)

5. Verify the site location information corresponds with the map information.

14.3 Verify Interference Levels

The following steps will verify the interference levels for each of the sectors.

1. Log into the BTS LMT.

2. In the command input area execute the following commands:

```
GET RRURTWP: RACKNO=0, SUBRACKNO=20, BOARDNO=0;
```

```
GET RRURTWP: RACKNO=0, SUBRACKNO=21, BOARDNO=0;
```

```
GET RRURTWP: RACKNO=0, SUBRACKNO=22, BOARDNO=0;
```

3. Each of these commands checks the interference levels. Each should return a valid response that shows a noise floor near -100dBm. The response shows 4 samples for our single carrier on the sector.

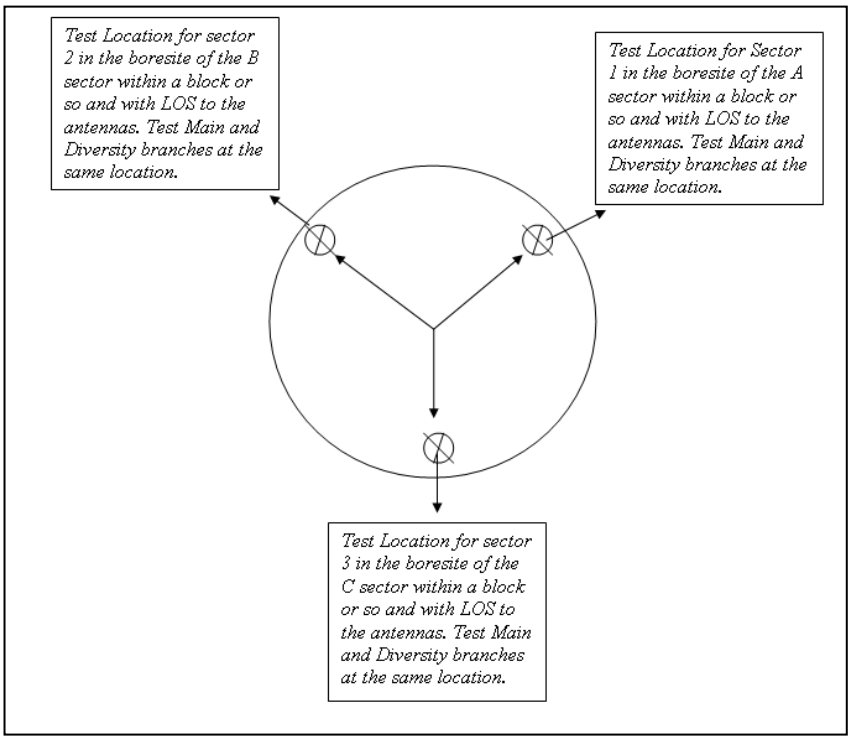
```
%%GET RRURTWP: RACKNO=0, SUBRACKNO=20, BOARDNO=0;%%
RETCODE = 0  Operation succeeded

RRU RTWP
--------
RXIDDEX  RRU CARRIERINDEX  RTWP(0.1dBm)

0        0                 -986
0        1                 -13486
0        2                 -13486
1        0                 -987
1        1                 -13486
1        2                 -13486
2        0                 -991
2        1                 -13486
2        2                 -13486
3        0                 -986
3        1                 -13486
3        2                 -13486
(Number of results = 12)


---    END
```

14.4 Verify Coverage

1. Configure the device to scan on the frequency associated with the first sector to be tested.

2. Configure the device for the private NAP ID FFAB63 by selecting the Private connection manager profile.

3. Select a test location for each sector within a block in the boresite of that sector with unobstructed views (LOS) of the antennas being tested for a total of three locations. (see Fig 6 below). Record the signal strength, CINR , and BSID values. **Verify the BSID is the correct one for the sector being tested.**



4. Based on the best server transmitter plot provided by RF engineering, drive the perimeter of the coverage area as close to the borders of the coverage as possible. This would be any roads close to the null area of the sector and the edge of the sector coverage. In addition drive nearly all the roads in the 0.25 mile buffer area shown by the first red circle on the RF plot.

5. Repeat for the other two sectors.

6. File naming convention at the end of every test before submitting to the RF engineer is "ATP_SectorID_Date.csv".

15 Online Acceptance Test

This section covers field verification of production RF parameters and network entry operation. This acceptance test procedure verifies that the EMS management process was successful by validating the key parameters of the airlink (BSID/Preamble Index and frequency). The following are the key objectives of this test procedure:

- Basic site verification information (latitude, longitude, and structure type)
- Verify site connectivity with backhaul (network entry and basic throughput testing)
- Verify sector level Key airlink parameters (BSID, frequency)
- Coverage verification (identify swapped sectors, azimuth deviations, and down-tilt deviations)
- Handover verification (intra-sector)

15.1 Obtain RF Planning Information

RF engineering will provide the following RF planning information for each sector. Obtain the RF coverage plot showing the best server transmitter. This information will be verifyd in the drive test procedures in the remaining sections.

15.2 Verify Site Location

This portion of the test procedure requires the basic collection of site identifiers to verify coordinate and structure type information used in internal databases/prediction tools and to ensure that the right site is being tested.

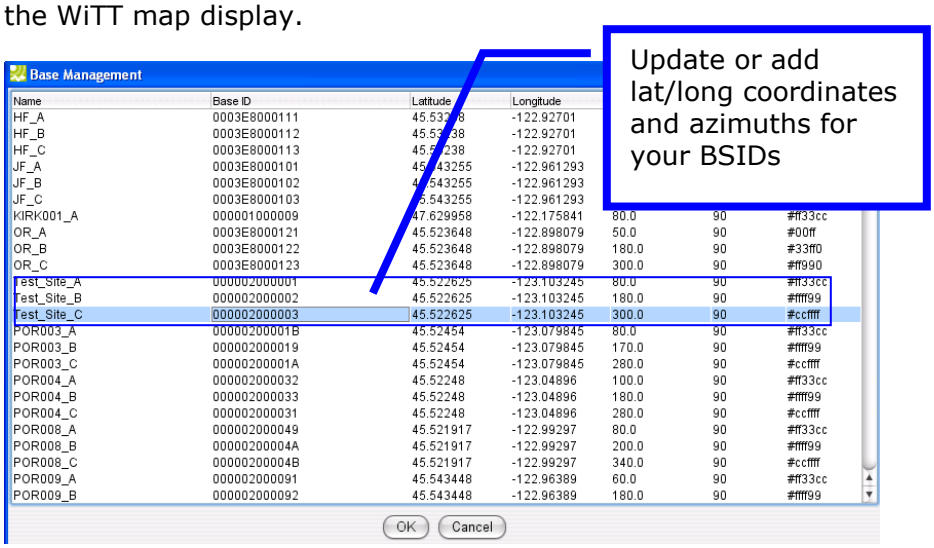
1. Launch WiTT with the GPS.
2. Under *Maps-> Manage Bases*, update or add your BSIDs

   Sector 1 = 00000200000X

   Sector 2 = 00000200000X

   Sector 3 = 00000200000X

with the latitudes and longitudes coordinates and azimuths of the site. This will allow correct position and site acquisition on the WiTT map display.



3. From the base of the site, record the following information

   a. Latitude (5 decimal digits ex. 45.45653)

   b. Longitude (5 decimal digits)

   c. Structure Type (Monopole/Rooftop etc)

4. Verify the site location information corresponds with the map information.

15.3 Verify Interference Levels

The following steps will verify the interference levels for each of the sectors.

1. Log into the BTS LMT.

2. In the command input area execute the following commands:

```
GET RRURTWP: RACKNO=0, SUBRACKNO=20, BOARDNO=0;
GET RRURTWP: RACKNO=0, SUBRACKNO=21, BOARDNO=0;
GET RRURTWP: RACKNO=0, SUBRACKNO=22, BOARDNO=0;
```

3. Each of these commands checks the interference levels. Each should return a valid response that shows a noise floor near -98 to -100dBm. The response shows 4 samples for our single carrier on the sector.

```
%%GET RRURTWP: RACKNO=0, SUBRACKNO=20, BOARDNO=0;%%
RETCODE = 0  Operation succeeded

RRU RTWP
--------
RXIDDEX  RRU CARRIERINDEX  RTWP(0.1dBm)

0        0                 -986
0        1                 -13486
0        2                 -13486
1        0                 -987
1        1                 -13486
1        2                 -13486
2        0                 -991
2        1                 -13486
2        2                 -13486
3        0                 -986
3        1                 -13486
3        2                 -13486
(Number of results = 12)


---    END
```

15.4 Verify Network Entry and Throughput Performance

This portion of the test procedure will test connectivity through the backhaul by using the connection manager utility and throughput testing.

1. Begin by performing network entry at cell-core.

2. Configure the device for the commercial NAP ID 2 by selecting the Clear connection manager profile.

3. Launch Connection manager to verify that Network entry is successful and the BSID of the sector being tested is displayed. This may involve moving away from the cell core to a LOS location within the boresite of the sector being tested to ensure that we get onto the proper sector.

4. Run a standard throughput test and record Downlink (DL) and uplink (UL) throughput values using www.speedtest.net or http://www.internetfrog.com/myinternet/voip/ websites. Perform this test on each of the sectors near cell-core. Throughput guidelines for a device configured with unlimited bandwidth QoS are show in the following table.

Table 1: Throughput Guidelines

CINR (dB)	DL Throughput (bps)	UL Throughput (bps)
30-35	10,000-16,000	2,000-2,500
27-29.9	8,500-9,999	1,750-1,999
24-26.9	7,000-8,499	1,500-1,749
21-23.9	6,000-6,999	1,200-1,499

5. Record the DL and UL throughput values, RTD (Round trip delay) and Ping times.

6. Also record the CINR and RSSI values at the location where the throughput values were collected.

15.5 Verify Coverage and Key Airlink Parameters

The RF parameters from will be verified on the device side using WiTT. With WiTT, the following will be verified for each sector:

- Frequency
- BSID

1. Begin by performing network entry at cell-core.

2. Launch WiTT with GPS.

3. Start WiTT monitoring and logging in advanced mode.

4. Verify the Base ID and Frequency to ensure you are on the correct sector.

5. Drive from cell-core to cell-edge until handover or network drop. A network drop would be acceptable if it is known that additional coverage is not provided by a neighboring sector.

6. Once handover or network drop occurs, stop WiTT logging.

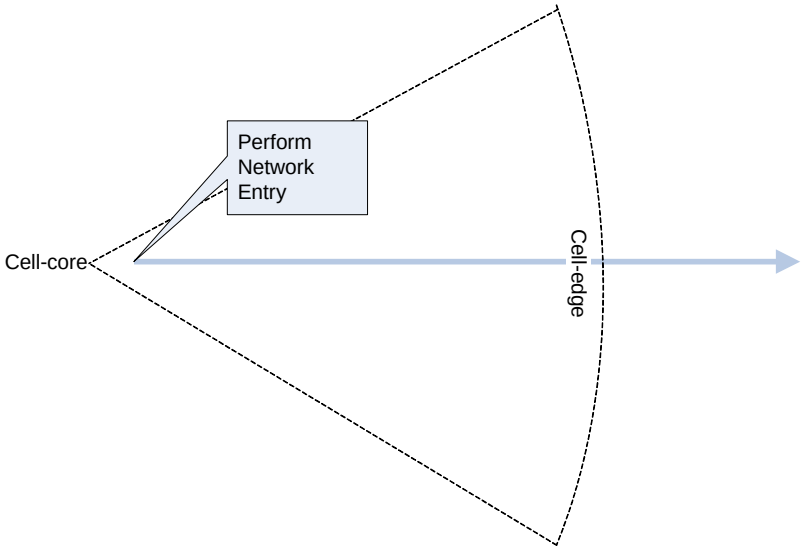
7. Verify if the loss of coverage coincides with the RF coverage plot.

8. Save the WiTT map view image.

9. Rename the WiTT CSV log file to include the site and sector identifiers. (Naming Convention: *SiteID _SectorLabel*_Coverage_date)

10. Package up the map view image file and CSV log file for each sector and provide these to RF planning.

11. Report any failures of discrepancies to the field supervisor.



.

Figure 32: Drive Route for Validation of Coverage and Key Airlink Parameters

15.6 Verify Intra-Sector Handovers

The coverage verification drive entails driving a route from cell-core to cell-edge as depicted in Figure 31 to test and ensure inter-sector handover functionality. In addition to this, a loop drive route at approximately 0.25 to 0.5 miles away from the site will be needed to ensure intra-sector handover capability

1. Begin by performing network entry at a location in the middle of the sector.

2. Launch Connection manager to verify that Network entry is successful and the BSID of the sector being tested is displayed.

3. Launch WiTT with GPS.

4. Start WiTT monitoring and logging in advanced mode.

5. Drive a circular route around the site as depicted in Figure 31. Verify successful handover between each sector.

6. Once the route is complete, save the WiTT map view image.

7. Rename the WiTT CSV log file to include the site and sector identifiers. (Naming Convention: *SiteID* _Intra_HO_date)

8. Package up the map view image file and CSV log file for each sector and provide these to RF planning.

9. Report any failures of discrepancies to the field supervisor.

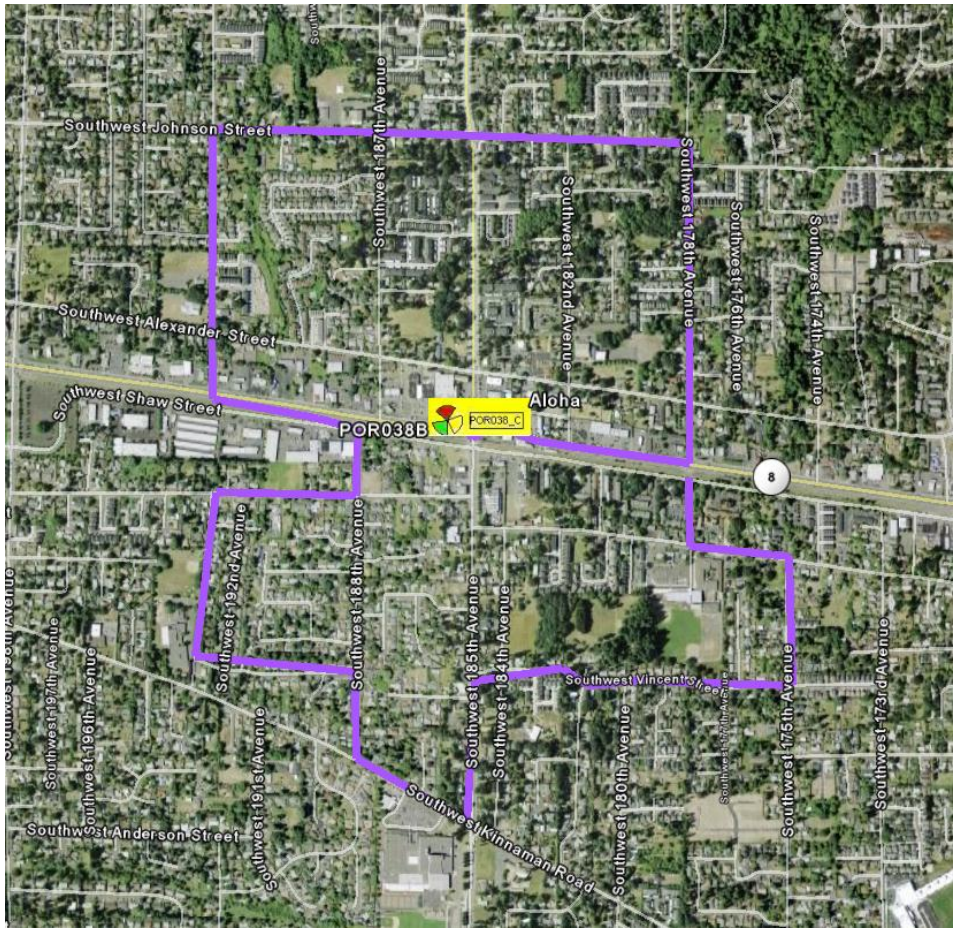


Figure 33: Sample Intra-sector Handover Route

Appendix A Useful BTS MML Commands

The following commands may be useful for troubleshooting via the BTS LMT. Additional command information is provided on the Help tab of the LMT when the command is selected.

Command	Description
GET RRUVSWR	Reports the system VSWR from the RRU.
DSP BRDVER	Displays the bootrom and application software for the individual boards. Also displays hardware version.
LST ALMAF	Lists the active alarms (Same as the Alarm window).
LST SOFTWARE	List the main software package on the BTS.
LST RRU	Lists the number of RRU and their subrack assignments.
LST BRD	Lists BBU chassis slot assignments.
MOD CARRIERBLOCKFLAG	Used to enable/disable transmission of a sector or carrier.
PING	Used to ping from the BTS.
ULK USR	If the LMT user is locked out due to too many failed login attempts, this command can be used to unlock the user.