# 3.0 Getting Started with OBR3650HP

## 3.1 Before You Begin

The OBR3650HP provides the base station component of the Vecima VistaMAX system. To set up and configure the base station, you require the following:

- One VistaMAX OBR3650HP base station with a stand-alone Power over Ethernet (PoE) or WES800 Ethernet Switch
- One VistaMAX outdoor subscriber station or indoor subscriber station such as the OSR3500C or ISR3510.
- One of the following components to provide the DHCP and TFTP server:
  - Vecima's Network Management 8000
  - A third-party DHCP and TFTP server as per the WiMAX standard. This setup is not covered in this manual.

**Setting up the system using NMS8000**

Using the NMS8000 as the provisioning tool for all OSR subscriber stations and hosts on the VistaMAX system is the most common scenario. The platinum, gold, silver, or bronze VistaMAX starter kits available from Vecima Networks includes an NMS8000.

**NOTE**

If you wish to connect Internet-accessible hosts to the VistaMAX system, you will need to provide a router with a public IP address and a valid DNS server. When you are connecting to Internet-accessible host and using the NMS8000, Vecima recommends connecting one of the NMS8000 Ethernet interfaces on a public routeable IP address.

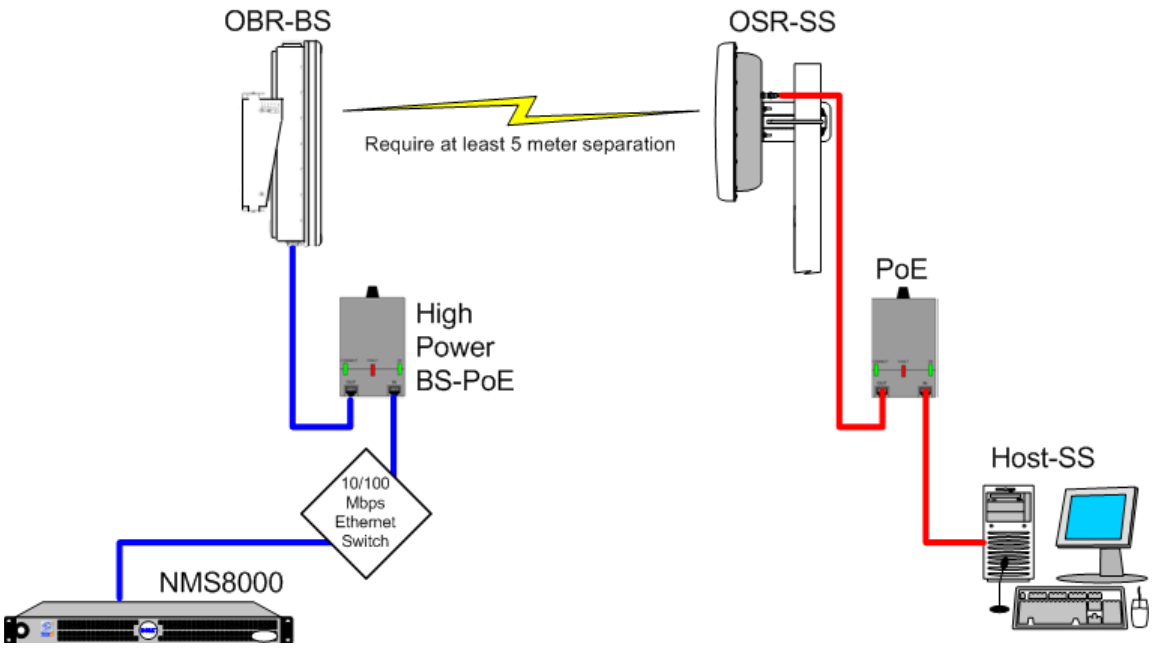



*Figure 3-1 Using NMS8000 to Provision VistaMAX System*

## 3.2 Overview of Configuration

The following steps outline the process for configuring a VistaMAX system. This process assumes that you are using an NMS8000.

**Step 1** Use CAT5 straight-through Ethernet cables to connect the physical components as shown in **Using NMS8000 to Provision VistaMAX System**.

**Step 2** Use the Web-based interface to configure the IP addresses for the base station and subscriber station(s). If necessary, configure the IP addresses for the NMS8000.

**Step 3** Use the Web-based interface to configure the radio parameters for the base station and subscriber station(s).

**Step 4** If necessary, use the Web-based interface for the NMS8000 to add the subscriber stations on the NMS8000.

**Step 5** Establish the link between the base stations and subscriber stations and verify that the subscriber stations are online.

The steps that pertain to the base station are described in more detail below. For more information, refer to the *NMS8000 & NMS8000/SSP Network Management Server Installation and Operation Guide* or related information listed under Finding Related Documentation on page iii.

# 3.3 Using the Web Based Interface

The Web interface of the OBR3650HP system may be viewed with a standard web browser such as Mozilla™ or Internet Explorer™, no additional add-ins are required.

**NOTE**

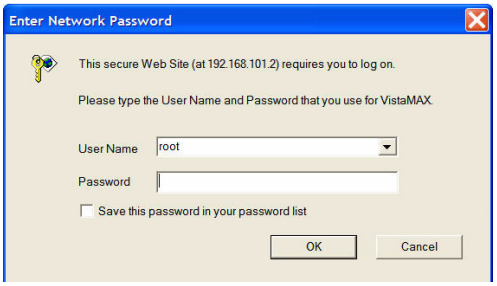
If your Web certificate is invalid or expired, you will be prompted to continue without the certificate or add an exemption to the certificate.

The following are the default log on settings for the Base station Web-based interface:

- Web-based interface access — `https://192.168.101.2`
- subnetwork mask — `255.255.255.0`
- username — `root`
- password — `vistamax`

**To log on to the Web-based interface:**

**Step 1** Open a Web browser and open the Web-based interface by typing `https://192.168.101.2` in the address bar. The Network Password page opens:




**NOTE**

`192.168.101.2` is the default IP address that comes preconfigured from Vecima, but your IP address might be different. If you are not using the default address, contact your system administrator for the IP address.

**Step 2** Type the username `root` and the password `vistamax` to access the web GUI. The log on screen displays:

# 3.4 Configuring the Network

You will need to configure your network to establish communication between the network elements. Figure 3-2 shows an example of a properly configured network. The example shows a network configuration using default values. If you purchased a WiMAX starter kit, these value will already be set.

The VistaMAX Base Station is shipped with a default IP address. However, depending upon your network configuration, you may want to change the IP address of your Base Station.

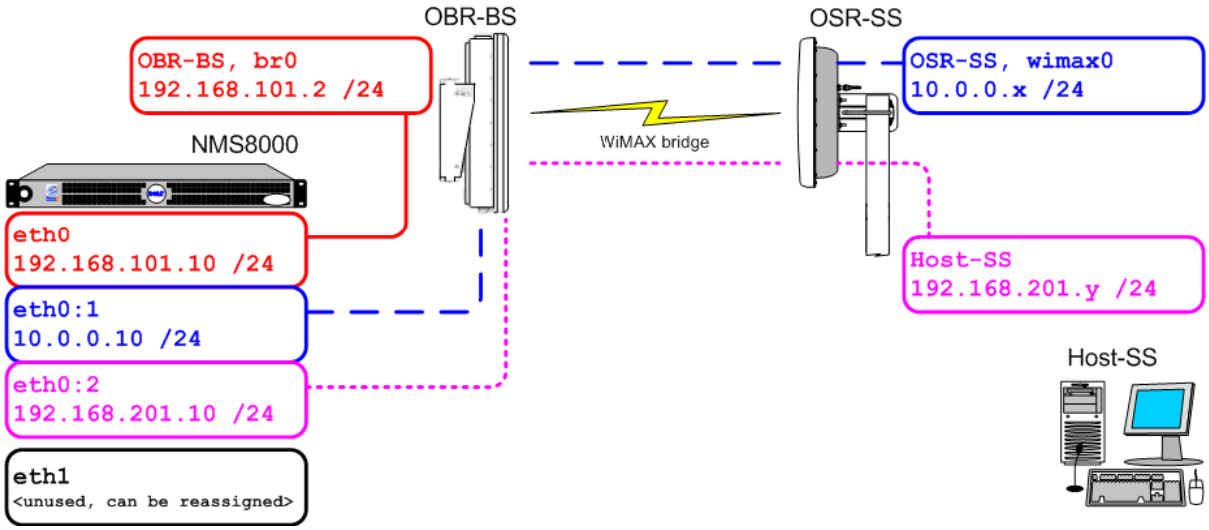



***Figure 3-2 Network Diagram***

As per the WiMAX standard, the subscriber station requires an IP address and TFTP offered to it during network entry. To fulfill this requirement, both a DHCP and TFTP server must be present. It is possible to use a third-party customer-supplied DHCP and TFTP server, but Vecima recommends using the Network Management Server 8000 (NMS8000). Most Vecima starter kits come with an NMS as part of the solution.

**NOTE**

Customers who purchased the basic starter kit or who do not have an NMS must use the WiMAX-out-of-the-box (WOOTB) procedure. For more information about WOOTB, contact the Application Engineering Support at Vecima Networks.

**To configure a network using NMS8000:**

**Step 1** Open the base station graphical user interface (GUI) and click **Configuration > Network Configuration**. The Current Interfaces screen opens displaying the name, IP address, and netmask of the base station's primary interface. The default value is `192.168.101.2`. To modify this value, click **br0** to open the BR0 configuration screen and type the new value in the appropriate field. See "**To change the base station IP address**" below for a detailed description of this Step.

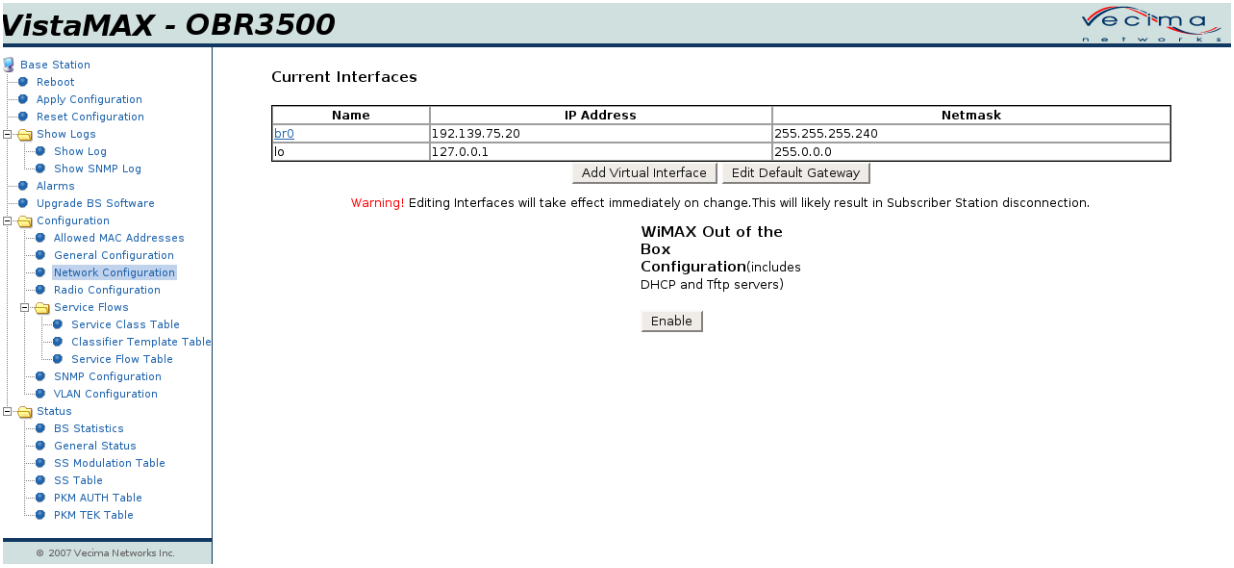
**Step 2** Using the NMS GUI, set up and enable DHCP on the NMS, then configure the subscriber stations and host computers as required.

**NOTE**

For more information see the *NMS8000 & NMS8000/SSP Network Management Server Installation and Operation Guide*.

**To change the base station IP address:**

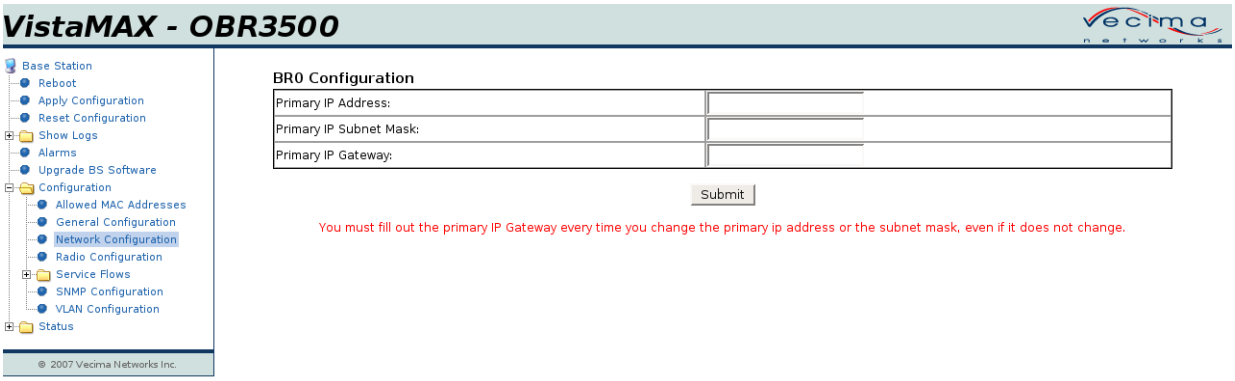
**Step 1** Log on to the Web-based interface and click **Configuration > Network Configuration**. The Current Interfaces table displays showing the primary (**br0**) IP address and virtual addresses (**br0:1 br0:2**, etc) for your base station.




From this page, you can set the following parameters:

| Parameter | Description | Default |
|---|---|---|
| **br0** and Virtual Interfaces | This is where the primary interface (**br0**) and any virtual interfaces (br0:1, br0:2, etc.) will be configured for remote access.<br><br>The primary interface is the IP address for the Base Station. | Dependent on your network design. |
| Gateway | This is where the default gateway will be specified for the **br0**. | Dependent on your network design. |

**Step 2** Click the **br0** link under Name field in the Current Interfaces table. The window will change to this.




•In the **Primary IP Address** field, enter the new IP for the Base Station: `192.168.101.138`

•In the **Primary IP Subnet Mask** field, enter the subnet mask for the Base Station. `255.255.255.0`

•In the **Primary IP Gateway** field, enter the gateway address for your network `192.168.101.3`

**Step 3** Click the **Submit** button. The following message appears:

```
Network saving in progress ....
Network will now be reset.
You should now change your network on your computer so that you will be able to connect to 192.168.101.138.
After the network has been readjusted, You can cancel the reboot by clicking here to make changes permanent.
Otherwise Reverting Changes in 2 minutes.
```

**Step 4** Click the **here** link to make the change permanent.

## NOTE

At this point, you may need to change the IP configuration of the computer which you are using to access the base station.If you have completely changed the domain for the Base Station (*was* `192.168.101.1`, *now* `172.200.26.1`), please ensure the IP of the computer is capable of communicating with the new IP address of the BS. If not, adjust the network configuration of the computer accordingly before moving on to the next step.

The following information displays on the page to indicate the changed IP address:

```
Reboot Cancelled Succesfully.
Permanent IP Config Set
Permanent IP Gateway set
Network Configuration Saved.
Network Saved.

Save Completed.
```

The address on the browser also changes to reflect the new IP address:

`https://192.168.101.138/cgi-bin/index.cgi`

## NOTE

If you were not able to reconnect and click the **here** link to confirm the IP address of the Base Station within 2 minutes, the Base Station will revert to the old IP address and reboot automatically. Please restart the IP address change process by going back to step 1.

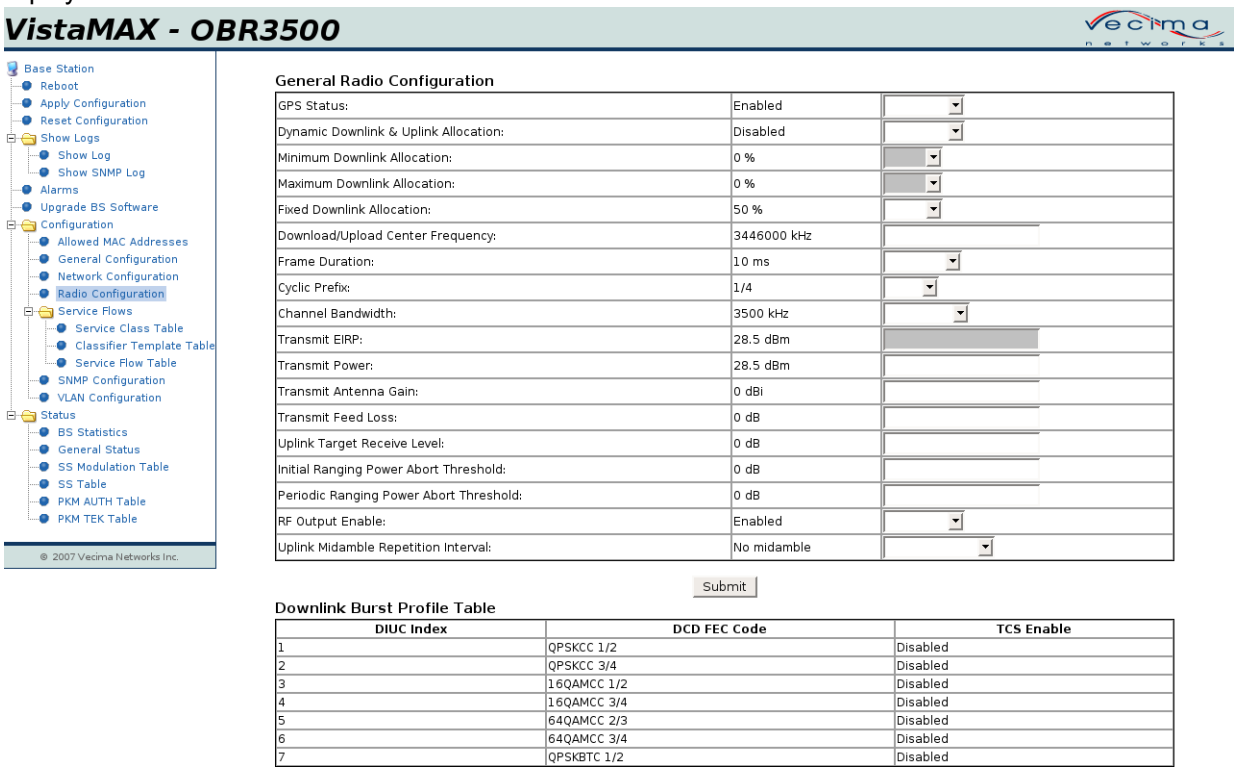
**Step 5** Once you have made the correct configuration settings, click the **Submit** button at the bottom of the window.

**Step 6** To apply the Radio Configuration, click **Apply Configuration** from the menu options. The configuration area displays a list of changes made. Click **Yes** to apply the changes.

# 3.5 Configuring the Radio

**To configure the radio**

**Step 1** Log on to the Web-based interface and click **Configuration > Radio Configuration**. The following page displays:




You can set the following parameters for the base station radio from this page:

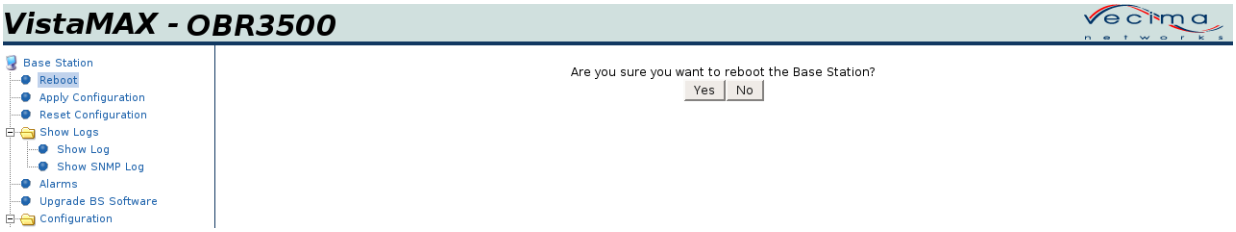
| Parameter | Description | Procedure | Default |
|---|---|---|---|
| Downlink/Uplink center frequency | This is the channel center frequency in KHz | Enter the value into the blank field. | Customer specific |
| Transmit power | The output power level of the Downlink in dBm | Enter the value into the blank field | 28.0 dBm |
| Channel Bandwidth | The available options are 3500 and 7500 kHz | Click the drop-down menu arrow and select the bandwidth | 7000000 kHz |
| Frame Duration | The combined Downlink and Uplink frame length in milliseconds | Click the drop-down menu arrow and select the duration | 10.0 ms |
| Cyclic Prefix | The redundant symbol percentage used to counteract inter-symbol interference | Click the drop-down menu arrow and select the prefix | 1/4 |
| Uplink Target Receive Level | This is the Uplink Rx level which all Subscriber Stations will strive to meet in dB | Enter the value into the blank field | 0 dB |
| Downlink Allocation | This is the percentage of the TDD frame that is dedicated to Downlink data | Click the drop down arrow for the Fixed Downlink Allocation and select the value for the location | 50% |

| Parameter | Description | Procedure | Default |
|---|---|---|---|
| Downlink/Uplink Modulation | This is the modulation scheme used for the DL and UL | Click the drop-down arrow and select the value for the modulation | Adaptive |
| RF Output Enable | This enables or disables the transmitter | Click the drop-down arrow and select the output | Enabled |

**Step 2** Once you have made the correct configuration settings, click the **Submit** button at the bottom of the window.

**Step 3** To apply the Radio Configuration, click **Apply Configuration** from the menu options. The configuration area displays a list of changes made. Click **Yes** to apply the changes.

**Step 4** To save configuration changes to the radio, click **Reboot** from the menu options. The configuration screen displays the following:




Click **Yes** to confirm the reboot.

# 3.6 Establishing a Link

Before you can establish the link between the base station and the subscriber station(s), ensure that the equipment is set up as follows.

- The NMS, base station, subscriber station, and one or more host computers are physically connected and powered up as shown in Figure 3-1.
- If you are using an outdoor base station with an integrated antenna, ensure that the base station is vertically aligned in comparison to its mounting. If you are using a non-integrated antenna, connect an external antenna.
- The base station network and radio have been configured as described in this manual.
- The subscriber station is powered up and connected to the host computers and the Downlink/Uplink frequency is set to the same frequency as the base station transmit frequency.
- Host computers should be assigned static IP addresses.

**NOTE**

For more information about how to set up and configure VistaMAX components, see the Finding Related Documentation on page iii section in the Preface. Documentation is available for download from the FTP site or by contacting Vecima Networks.

**To establish the link between the base station and subscriber station:**

**Step 1** Set up and configure your VistaMAX system.

**Step 2** Power up all the units.

**Step 3** The subscriber station should complete network entry and establish a link to the base station in 1-2 minutes.

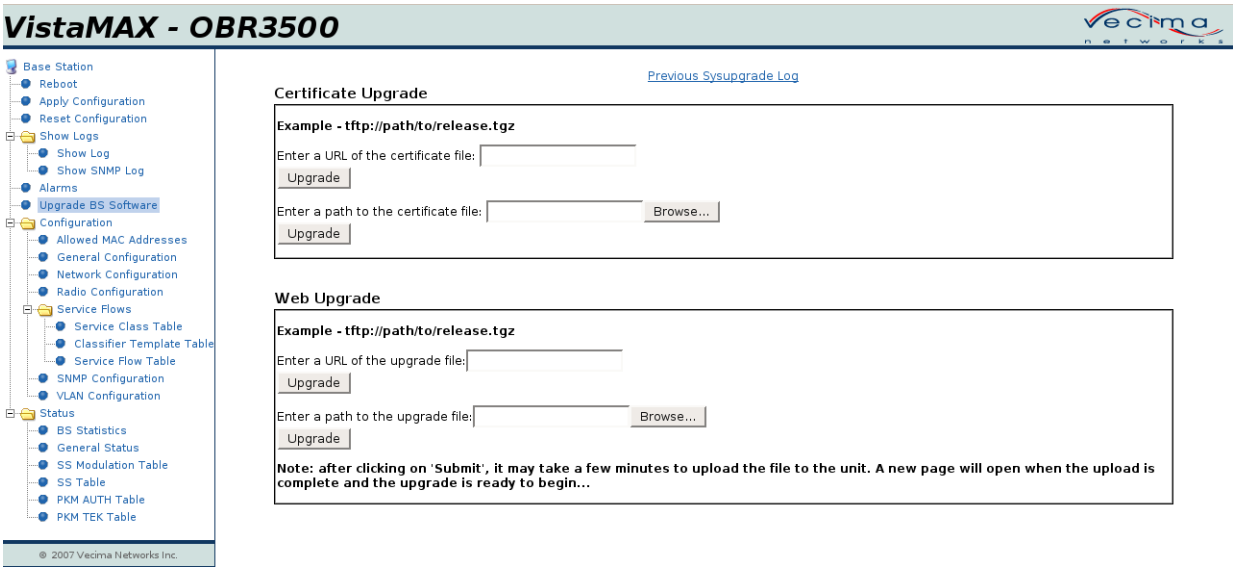
# 3.7 Other Administrative Tasks

## 3.7.1 Upgrading the Base Station

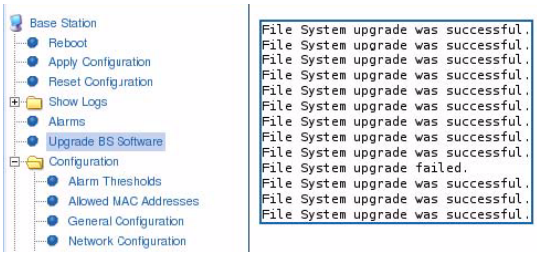
In order to make sure that the Base Station is able to function properly, upgrades may need to be made to the system.

**To upgrade the base station through the Web GUI:**

**Step 1** Log on to the Web-based interface and click **Upgrade BS Software**. The following page displays:

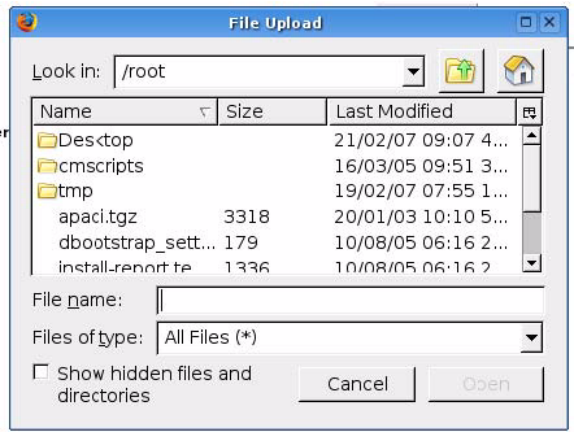



**Step 2** Click **Previous Sysupgrade Log** to verify that the previous upgrade was successful.




**Step 3** Choose one of the following methods to upgrade your base station.

| If | Then |
|---|---|
| The upgrade file is located on a web server | **1)** Enter the address of the web server plus the path to the file in the upgrade line.<br>**1)** Click **Upgrade**. |

| If | Then |
|---|---|
| The upgrade file is located on the tftp server in the tftproot folder. | **1)** Type the URL and path for the certificate. For example:<br>`tftp://<ip of NMS>/<version>/<file>`<br>**2)** Click **Upgrade**. |
| The upgrade file has been downloaded to your computer | **1)** Click the Browse button at the end of the Enter Path Select the file that will be used for the upgrade.<br>  <br>**3)** Click the Open button.<br>**4)** Click **Upgrade**. |

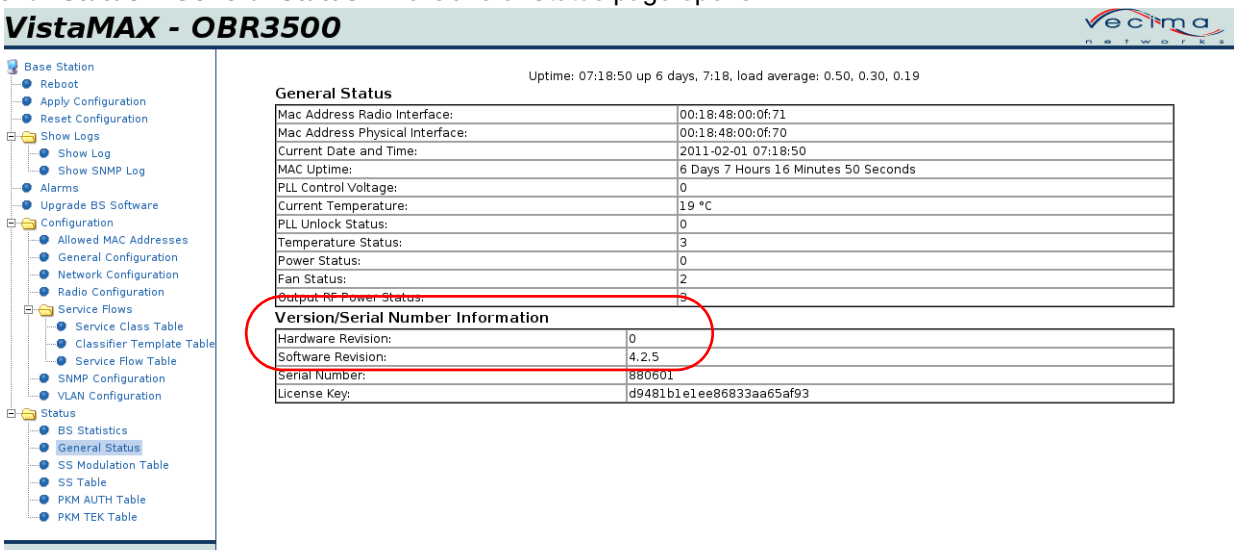


## NOTE

The Base Station upgrade might take about five minutes to complete.

**To verify the upgrade:**

**Step 1** Click **Status > General Status**. The General Status page opens:



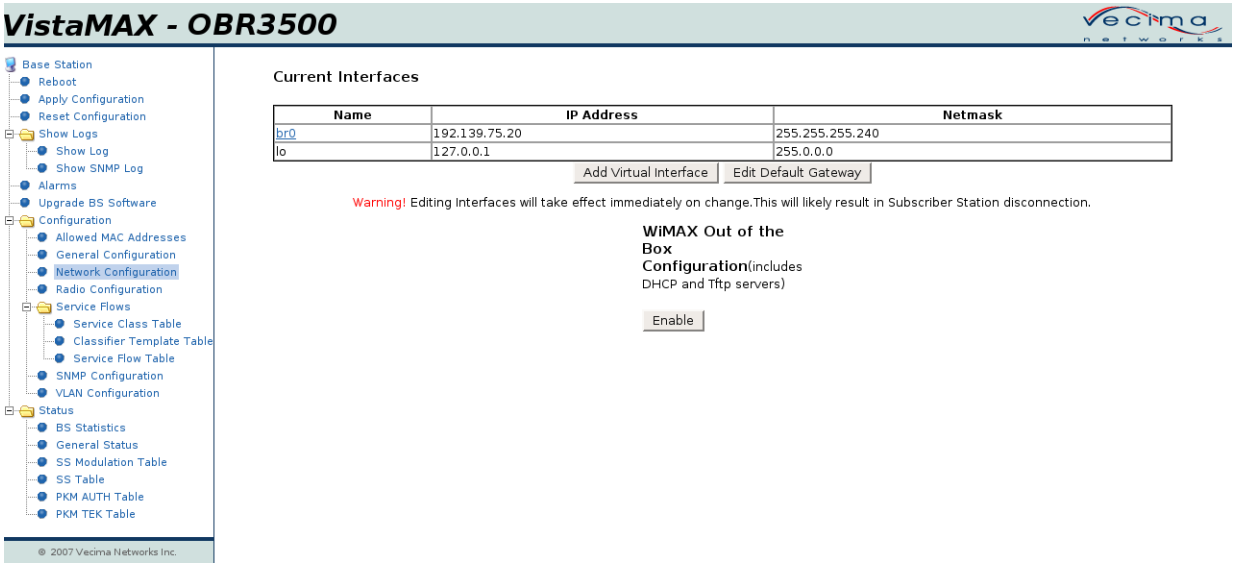

**Step 2** Read the **Versions/Serial Number Information** to ensure the proper version is running.

## 3.7.2 Adding a Virtual IP Address

The ability to define virtual addresses on the Base Station will allow you to access the Base Station from more than one domain. By entering the different IP addresses into the Base Station, you will be able to access the Base Station from various different domains.

**To add a Virtual IP Address:**

**Step 1** Log on to the Web-based interface and click **Configuration > Network Configuration**. The Current Interfaces table displays showing the primary (**br0**) IP address and virtual addresses (**br0:1 br0:2**, etc) for your base station.




**Step 2** Click **Add Virtual Interface**. The Add Virtual Interface page appears.

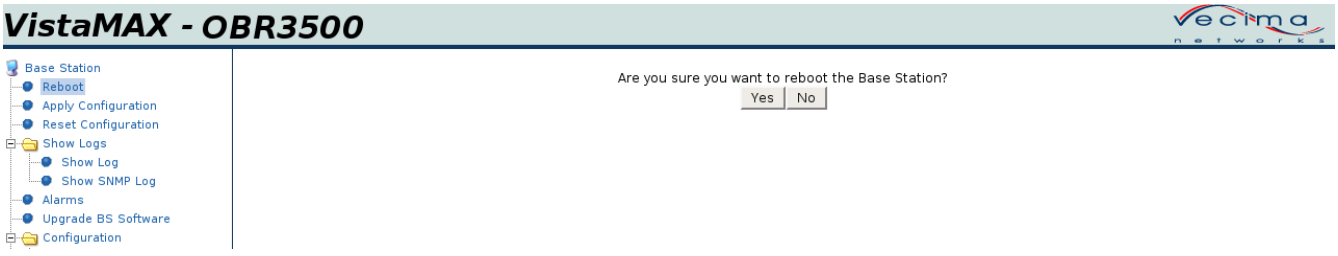
**Step 3** Type the name for the new virtual interface in the **Virtual Interface Name** field. Enter an IP address for the new domain that you wish to add in the **IP Address** field and the subnet address in the **Subnet Mask** field.

**Step 4** Click **Add**.

**Step 5** Repeat steps 2 to 4 until you have added all the virtual addresses that you need.

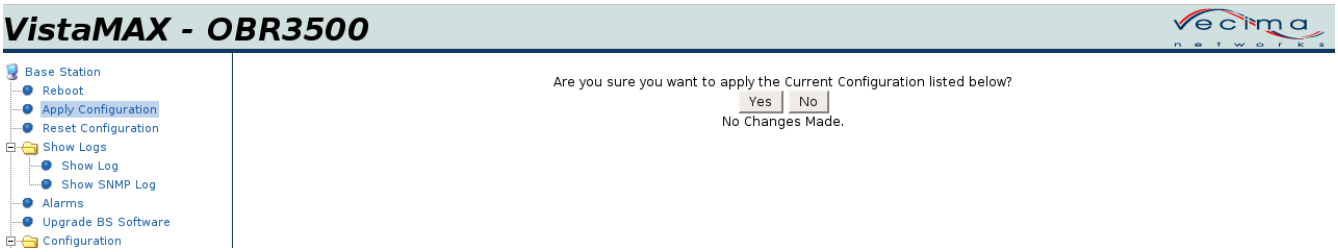
## 3.7.3 Rebooting the system

Select Reboot and click **Yes** to restart the system. If you have made configuration changes, they will be in use after the system restarts.



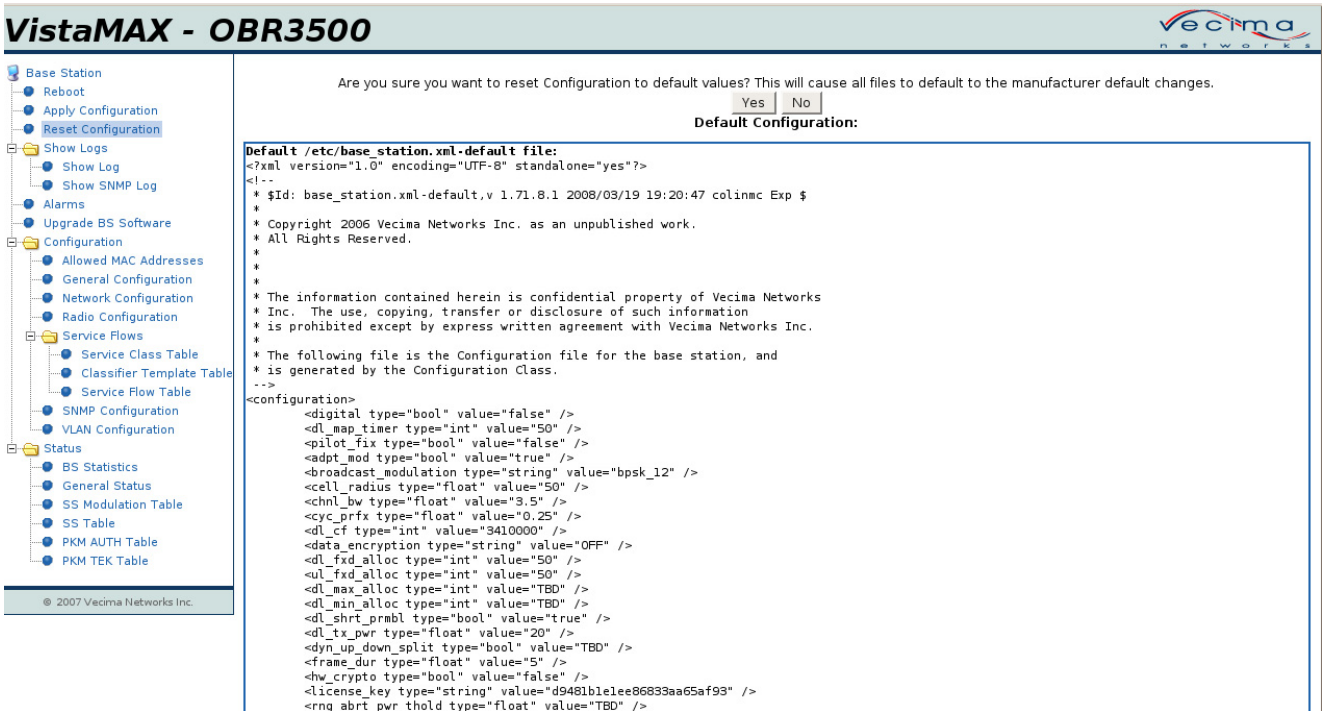
## 3.7.4 Applying Configuration

Select Apply Configuration and click **Yes** to confirm the configuration changes.



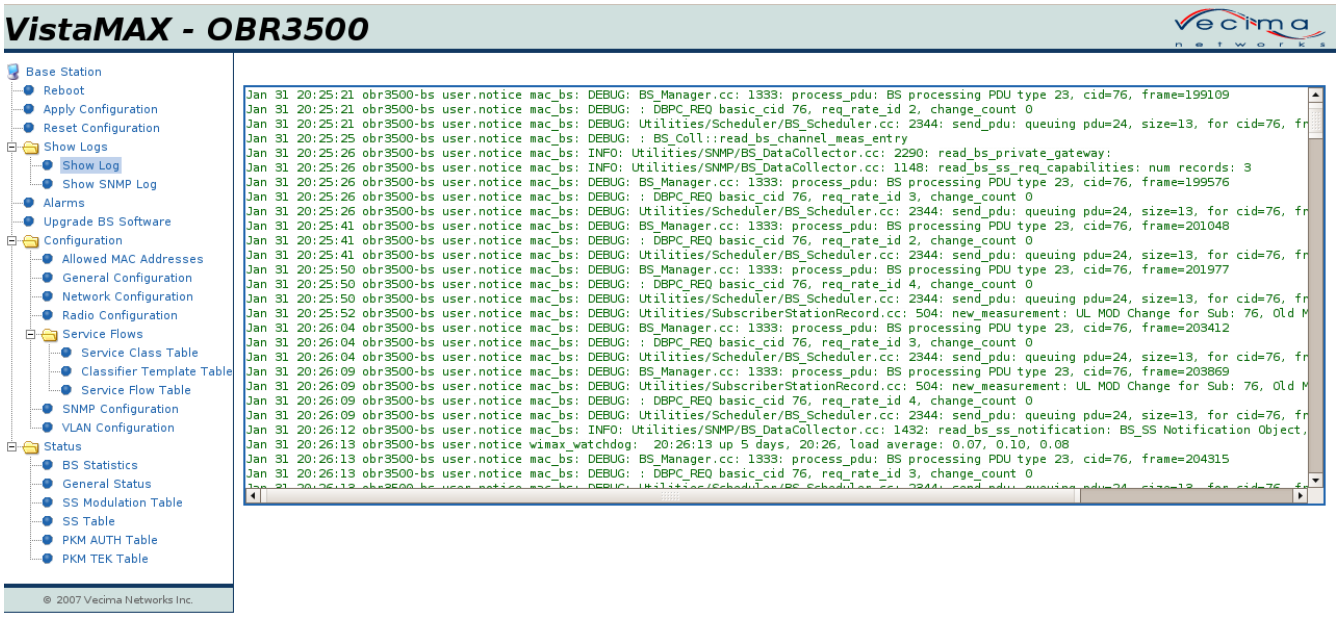

## 3.7.5 Resetting Configuration

Select Reset Configuration to reset the configuration to the basic default configuration. Select **Yes** to confirm the reset.



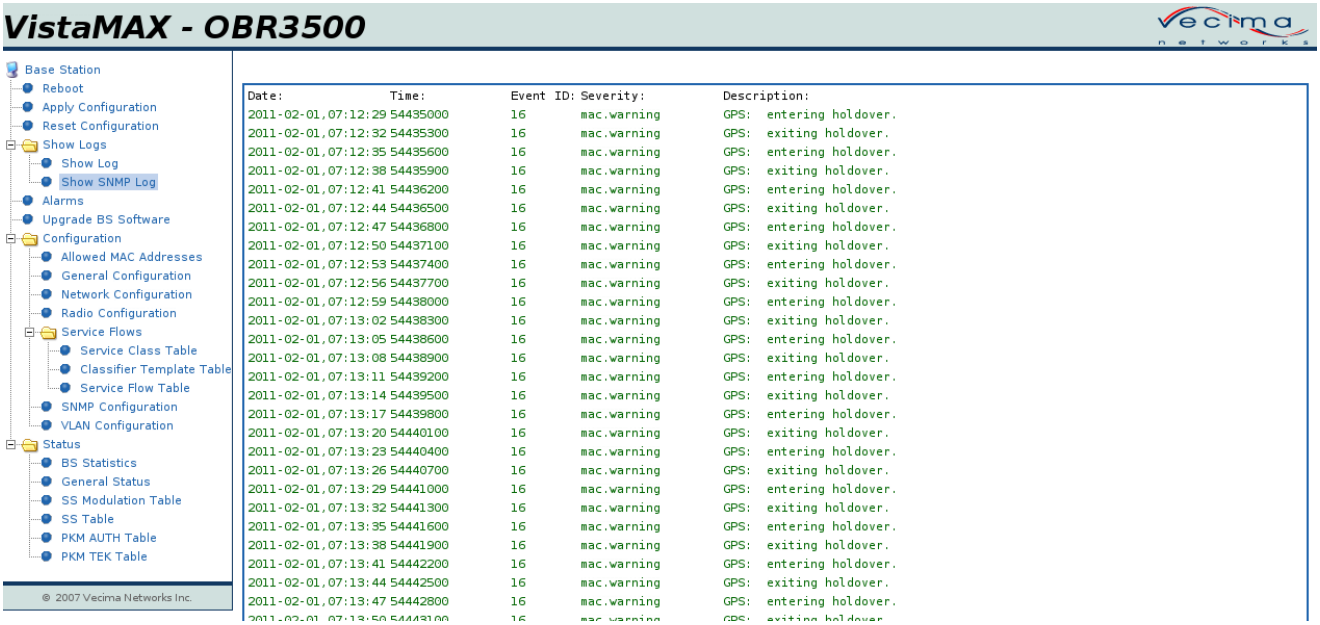
## 3.7.6 Checking Base Station Logs

Select Show Log to display the log activity for the base station.




## 3.7.7 Viewing SNMP Log

Select Show SNMP Log to display the SNMP activity on the base station.



## 3.7.8 Setting Service Flow Information

The service flow is part of the Quality of Service (QoS) feature of the base station. Service flows provide the following functions:

- Service flows specify a multitude of QoS parameters including: traffic priority, sustained and reserved data rates, jitter, maximum latency, and specify security profiles.
- Service flows are setup individually for both uplink and downlink data flows.
- Service flows classify traffic based on Layer 2, 3 or 4 (Ethernet, IP, TCP/UDP/RTP) header information including items such as source and destination addresses, port numbers, 802.1Q VLAN IDs, and Ethernet or IP traffic priority levels.

Before each frame, OBR3650HP examines all of the incoming requests and grants a time to transmit for the subscriber station based on all of the active service flow parameters to guarantee QoS where required. Individual subscriber stations receive aggregate bandwidth grants from the OBR3650HP and must individually manage their own uplink bandwidth usage.

**Setting up a Quality of Service framework:**

**Step 1** Define a service class and set up its parameters.

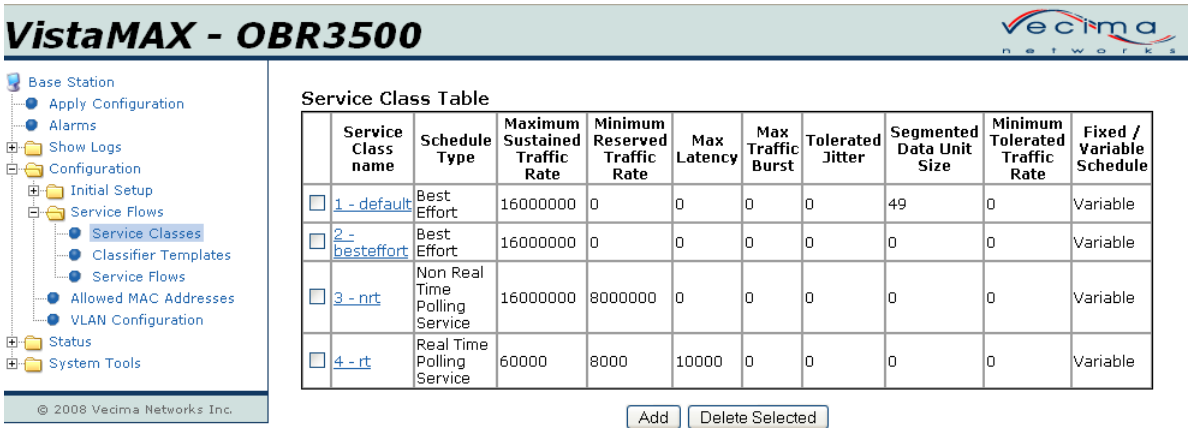
**Step 2** Define a classifier template and set up its rules.

**Step 3** Create service flows and associate them with service classes and classifier templates.

**Step 4** Provision subscriber stations with service flows.

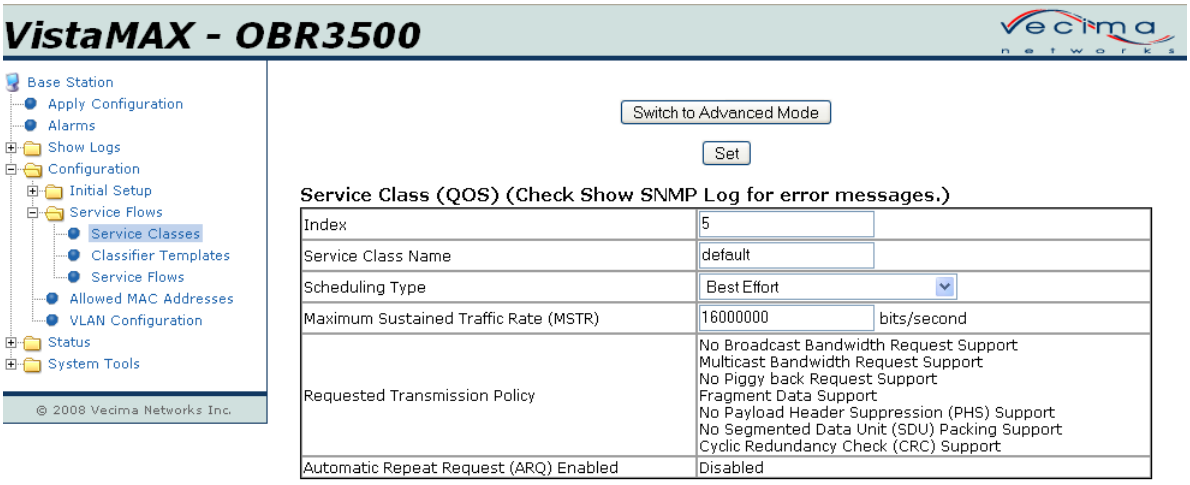
**To define a service class and set up its parameters:**

1) Click **Configuration > Service Flows > Service Class Table** to open the Service Class Table page. This page lists all the default and user defined Service Classes and shows the parameters for each one.



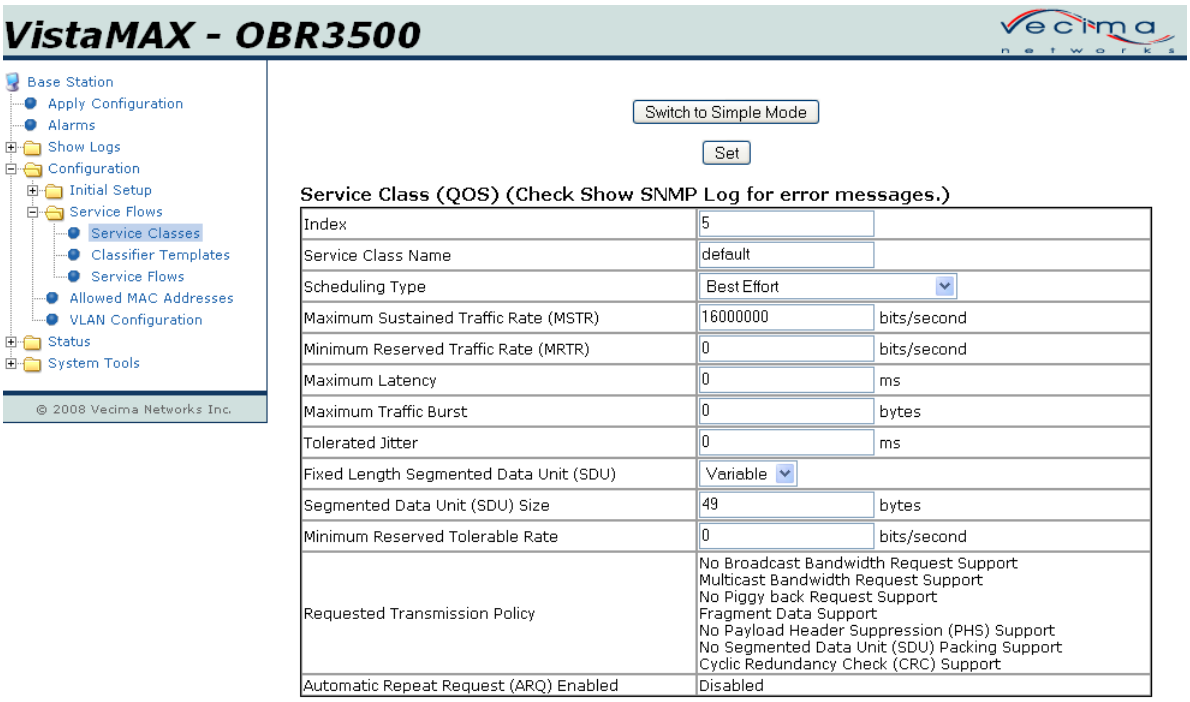

| | Service Class name | Schedule Type | Maximum Sustained Traffic Rate | Minimum Reserved Traffic Rate | Max Latency | Max Traffic Burst | Tolerated Jitter | Segmented Data Unit Size | Minimum Tolerated Traffic Rate | Fixed / Variable Schedule |
|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | 1 - default | Best Effort | 16000000 | 0 | 0 | 0 | 0 | 49 | 0 | Variable |
| ☐ | 2 - besteffort | Best Effort | 16000000 | 0 | 0 | 0 | 0 | 0 | 0 | Variable |
| ☐ | 3 - nrt | Non Real Time Polling Service | 16000000 | 8000000 | 0 | 0 | 0 | 0 | 0 | Variable |
| ☐ | 4 - rt | Real Time Polling Service | 60000 | 8000 | 10000 | 0 | 0 | 0 | 0 | Variable |

**2)** Click **Add** to open a page displaying the Service Class (QoS). Use this page to define the service class parameters.



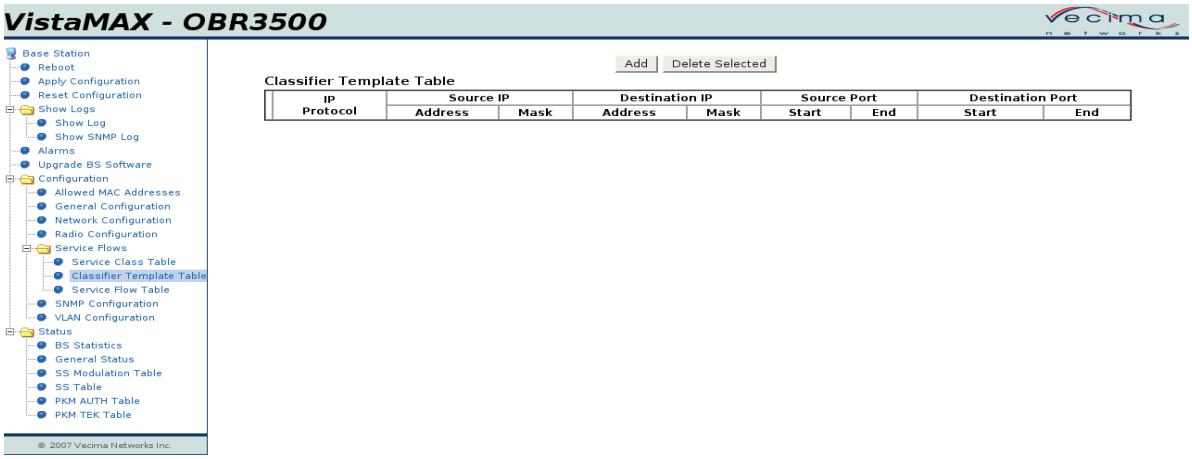

**3)** Enter values in the fields and click **Set** to save the changes and return to the Service Class Table page. **Index**, **Service Class Name**, and **Maximum Sustained Traffic Rate** are required fields.

**4)** Click **Switch to Advanced Mode** to open another page where you can set more parameters.

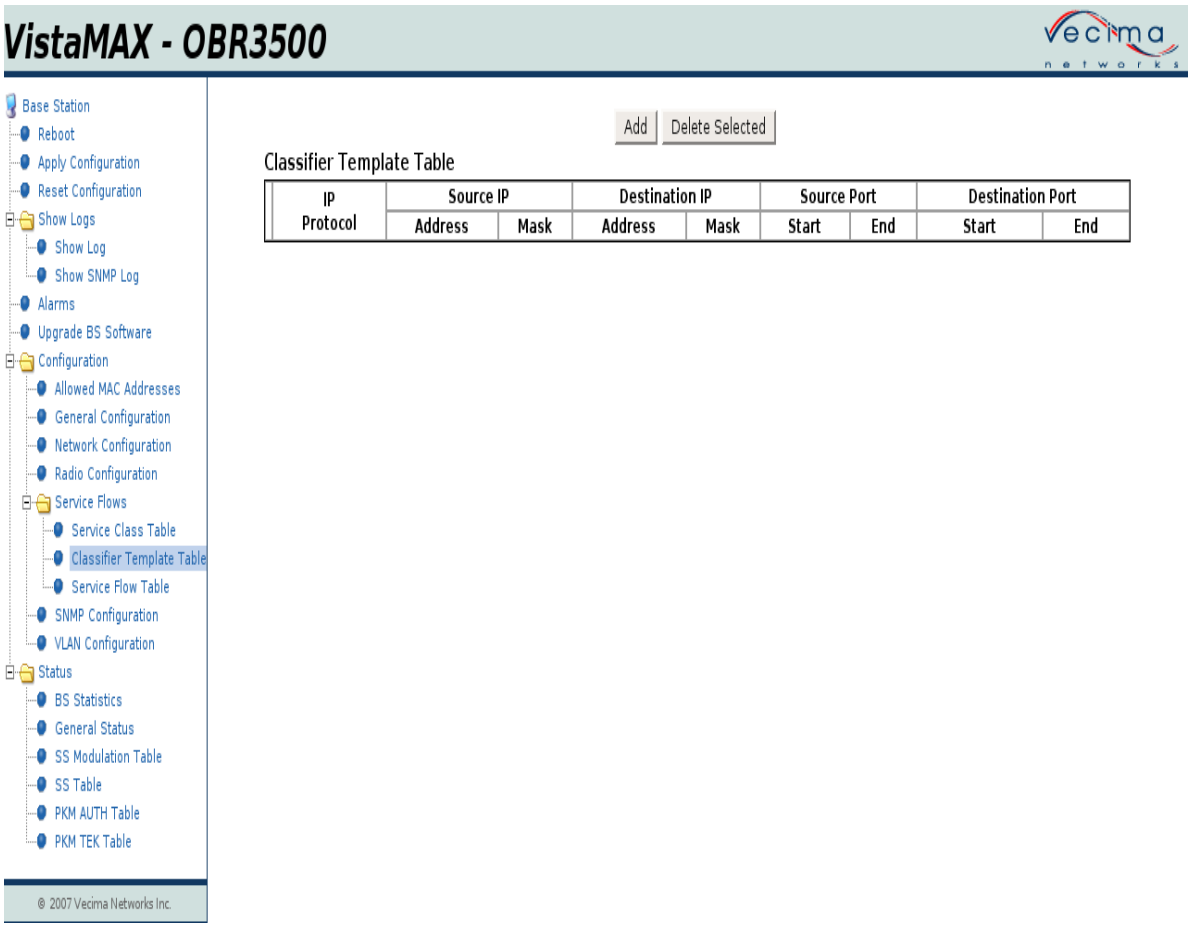


**To define a classifier template and set up its rules.**

1) Click **Configuration > Service Flows > Classifier Templates** to open the Classifier Template Table page. Use this page to define the classifier templates.



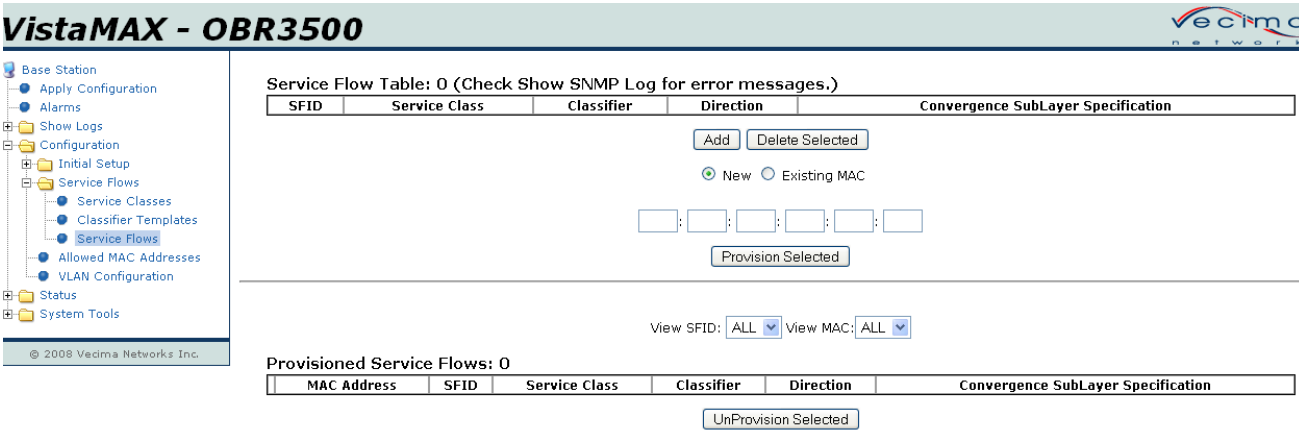

2) Click **Add** to open the Classifier Rule Entry page and set up classifier templates for later use.




3) Enter values in the fields and click **Set** to save the changes. **Priority**, **Destination Port Start**, and **Destination Port End** are required fields.

**To create service flows and associate them with service classes and classifier templates.**

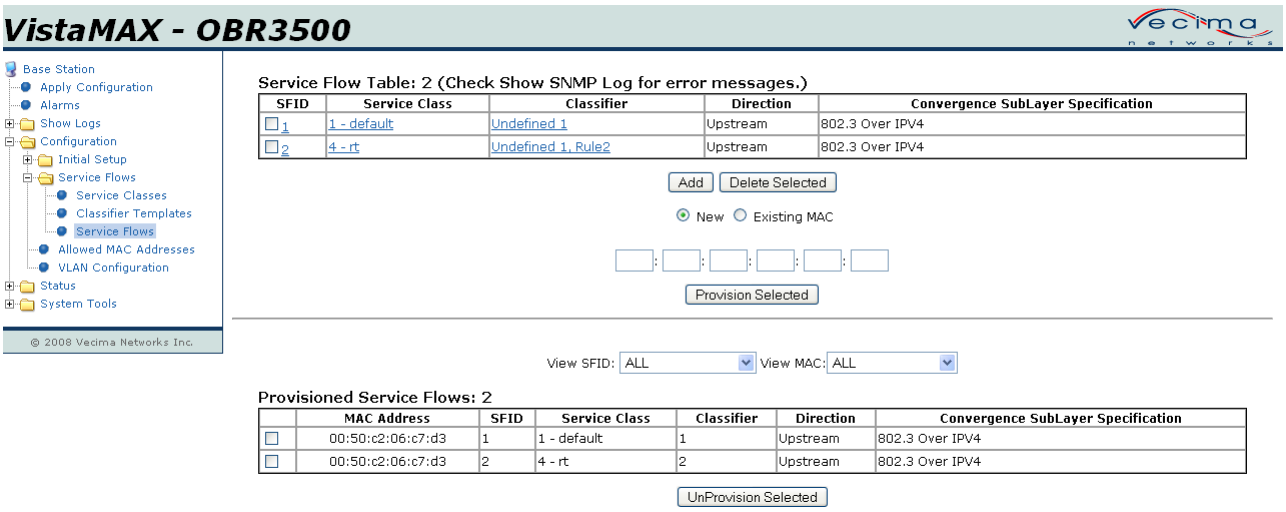
1) Click **Configuration > Service Flows > Service Flows** to open a page displaying the predefined service flows. Use this page to provision subscriber stations with service flows according to their MAC addresses.




2) Click **Add**. A new page opens displaying the Add Service Flow table. Use this page to set up the service flow parameters.
3) Type a number in the **SFID** field to identify the service flow.
4) Select **UpStream** or **DownStream** from the **Direction** drop list to indicate the direction of the data to which the service flow will apply.
5) Select a specification from the **Convergence SubLayer Specification** drop list to indicate the protocol that the service flow uses. The default is IPv4 over Ethernet.
6) Select the State of the service flow: **Authorized**, **Admitted**, or **Active**.
7) Select a service class to include with the service flow.
8) Select a classifier template to include with the service flow.
9) Click **Add**. This saves the service flow and returns you to the Service Flow Table page where the new service flow is displayed. You can then use this service flow to provision subscriber stations.

**To provision a subscriber station:**

1) Type a MAC address in the field provided or select one from the list of that appears when you select **Existing MAC**.
2) Choose the service flows that you want to assign to the selected MAC address by clicking the **SFID** check boxes that correspond to the predefined service flows.
3) Click **Provision Selected**. The new MAC address appears in the Provisioned Service Flows table with the associated service flow.

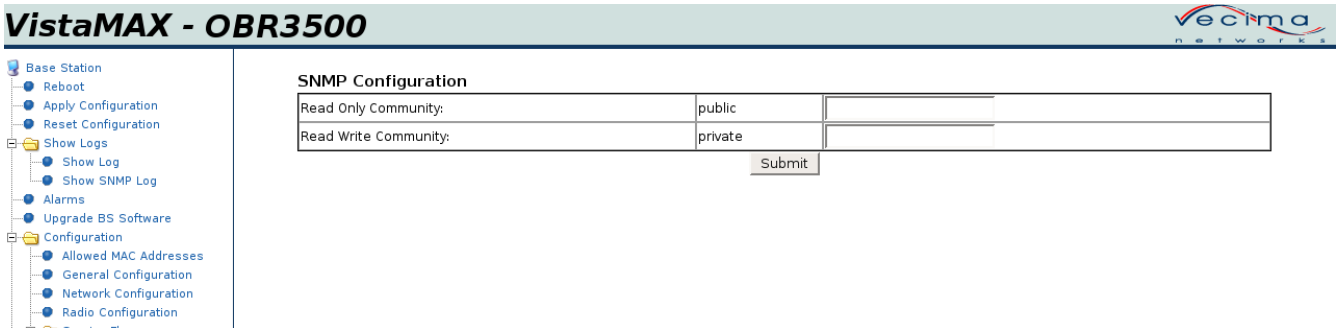



**To remove the service flow from a subscriber station:**

1) Select a MAC Address from the Provisioned Service Flows table by selecting the corresponding check box.
2) Click **UnProvision Selected** to remove the provisioned service flow from the subscriber station.

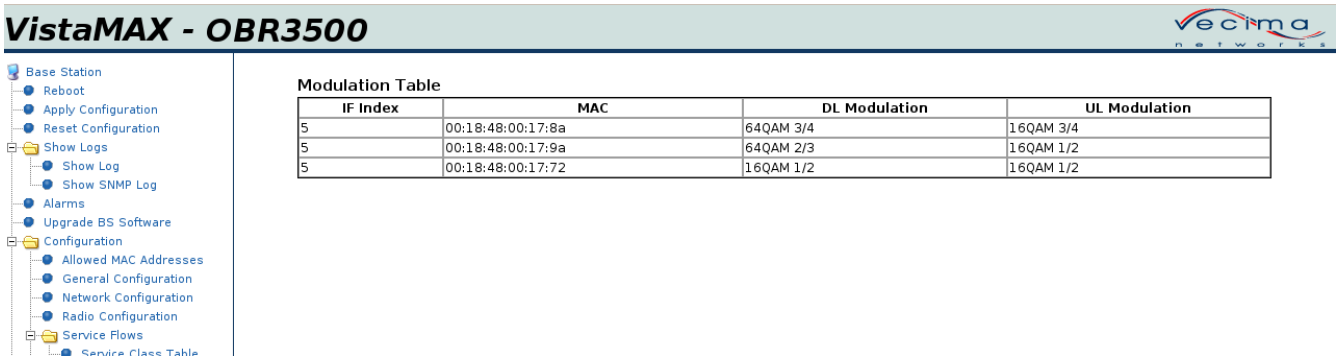
## 3.7.9 SNMP Configuration

Select **SNMP Configurations** to define the SNMP community strings. Currently, setting the SNMP is the only way that the base station can communicate.



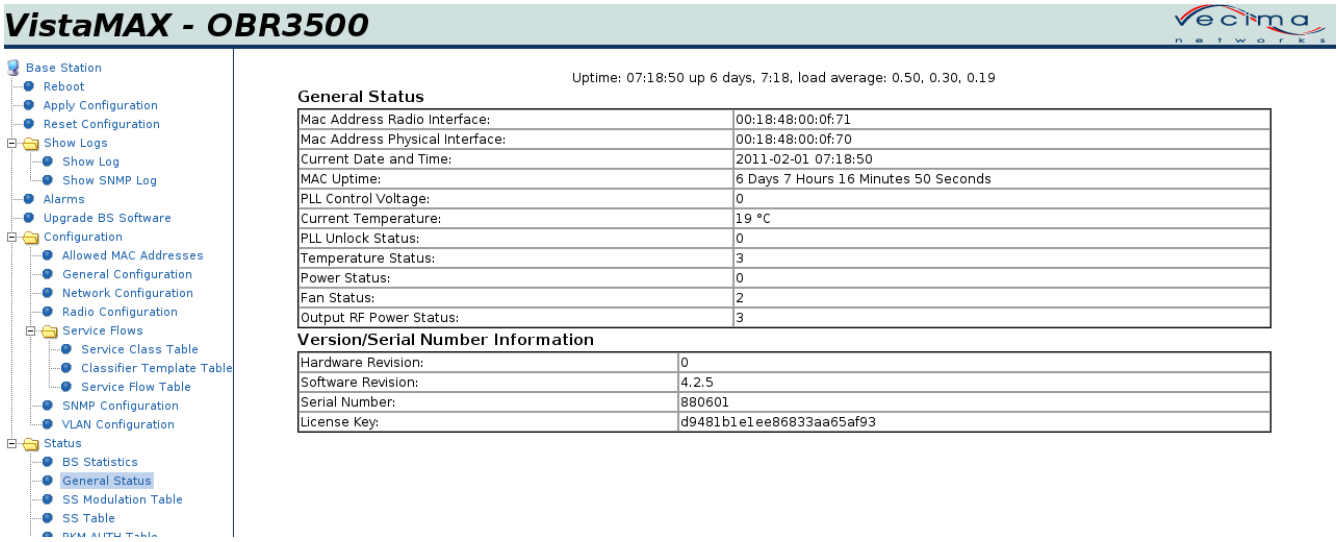

## 3.7.10 Subscriber Station Modulation Table

Select **SS Modulation Table** to show the current downlink and uplink modulations for all registered SS.



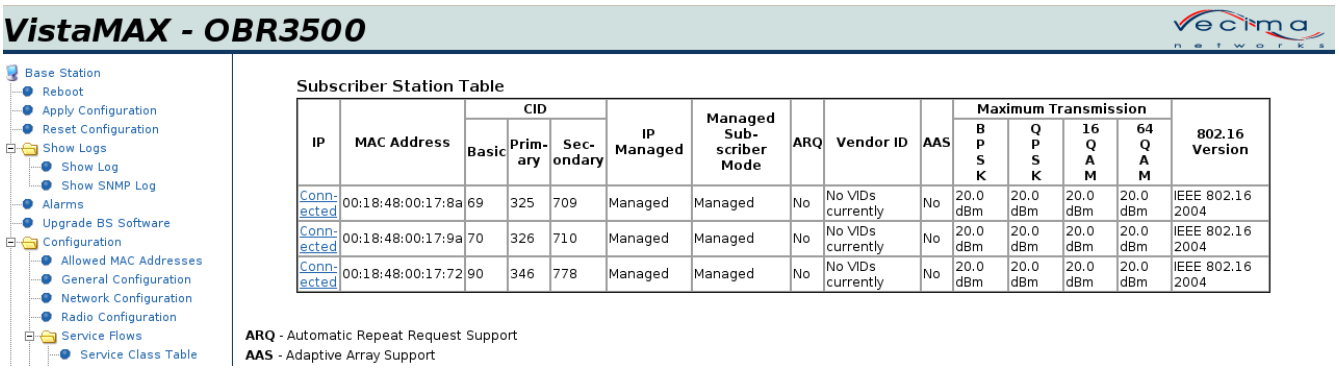

## 3.7.11 Checking Base Station Status

Select **General Status** to display the statistics of a base station.



## 3.7.12 SS Table

Select **SS Table** to display the status of subscriber stations that are connected to the base station.

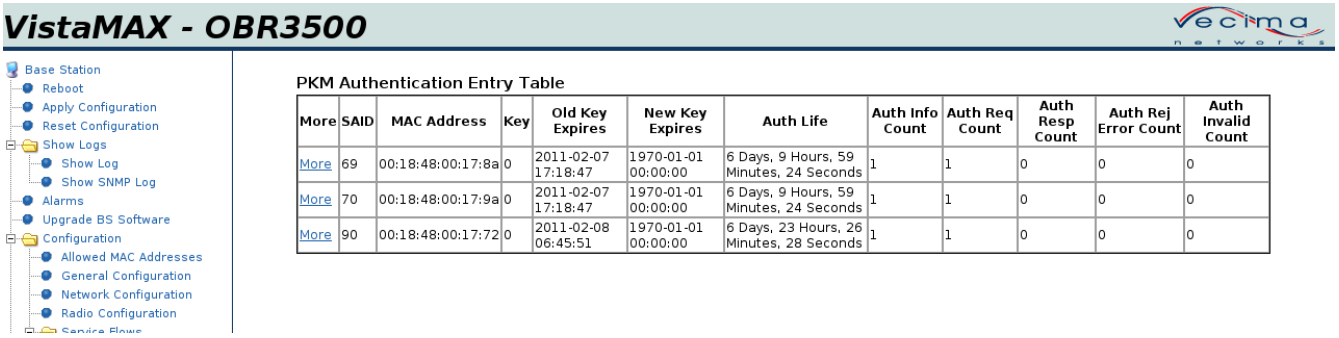



| IP | MAC Address | CID | | | IP Managed | Managed Sub-scriber Mode | ARQ | Vendor ID | AAS | Maximum Transmission | | | | 802.16 Version |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Basic | Prim-ary | Sec-ondary | | | | | | BPSK | QPSK | 16QAM | 64QAM | |
| Conn-ected | 00:18:48:00:17:8a | 69 | 325 | 709 | Managed | Managed | No | No VIDs currently | No | 20.0 dBm | 20.0 dBm | 20.0 dBm | 20.0 dBm | IEEE 802.16 2004 |
| Conn-ected | 00:18:48:00:17:9a | 70 | 326 | 710 | Managed | Managed | No | No VIDs currently | No | 20.0 dBm | 20.0 dBm | 20.0 dBm | 20.0 dBm | IEEE 802.16 2004 |
| Conn-ected | 00:18:48:00:17:72 | 90 | 346 | 778 | Managed | Managed | No | No VIDs currently | No | 20.0 dBm | 20.0 dBm | 20.0 dBm | 20.0 dBm | IEEE 802.16 2004 |

**ARQ** - Automatic Repeat Request Support
**AAS** - Adaptive Array Support

## 3.7.13 PKM AUTH Table

Select PKM AUTH Table to display Privacy and Key Management (PKM) and authentication information.

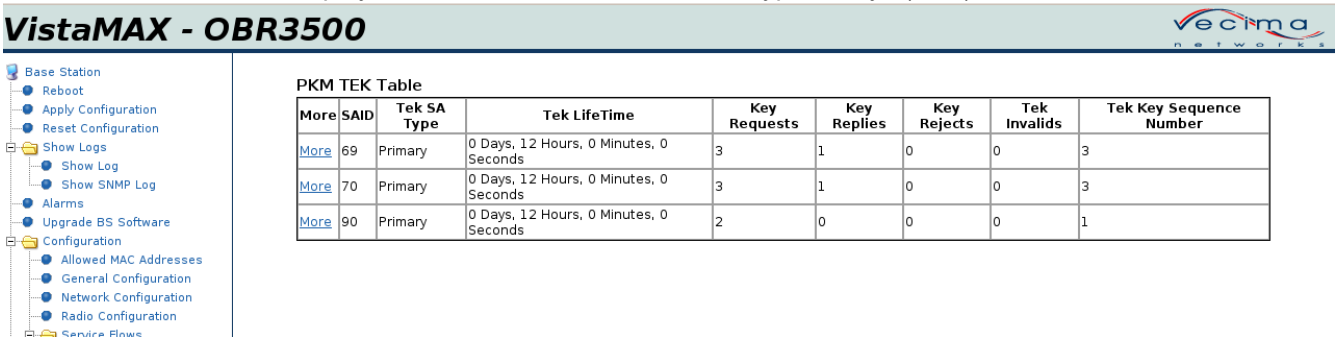



| More | SAID | MAC Address | Key | Old Key Expires | New Key Expires | Auth Life | Auth Info Count | Auth Req Count | Auth Resp Count | Auth Rej Error Count | Auth Invalid Count |
|---|---|---|---|---|---|---|---|---|---|---|---|
| More | 69 | 00:18:48:00:17:8a | 0 | 2011-02-07 17:18:47 | 1970-01-01 00:00:00 | 6 Days, 9 Hours, 59 Minutes, 24 Seconds | 1 | 1 | 0 | 0 | 0 |
| More | 70 | 00:18:48:00:17:9a | 0 | 2011-02-07 17:18:47 | 1970-01-01 00:00:00 | 6 Days, 9 Hours, 59 Minutes, 24 Seconds | 1 | 1 | 0 | 0 | 0 |
| More | 90 | 00:18:48:00:17:72 | 0 | 2011-02-08 06:45:51 | 1970-01-01 00:00:00 | 6 Days, 23 Hours, 26 Minutes, 28 Seconds | 1 | 1 | 0 | 0 | 0 |

This page shows the Security Association ID (SAID) number for MAC Addresses and displays Private Key information for those MAC addresses.

## 3.7.14 PKM TEK Table

Select **PKM TEK Table** to display information about the traffic-encryption keys (TEK).




| More | SAID | Tek SA Type | Tek LifeTime | Key Requests | Key Replies | Key Rejects | Tek Invalids | Tek Key Sequence Number |
|---|---|---|---|---|---|---|---|---|
| More | 69 | Primary | 0 Days, 12 Hours, 0 Minutes, 0 Seconds | 3 | 1 | 0 | 0 | 3 |
| More | 70 | Primary | 0 Days, 12 Hours, 0 Minutes, 0 Seconds | 3 | 1 | 0 | 0 | 3 |
| More | 90 | Primary | 0 Days, 12 Hours, 0 Minutes, 0 Seconds | 2 | 0 | 0 | 0 | 1 |

This page shows the Security Association ID (SAID) number and the traffic-encryption keys (TEK) information.

**This page intentionally left blank**

# A1 Molex® Backshell Installation

A defect was detected with the Ethernet terminating end of the Molex®backshell packaged with the OBR3650HP. The terminating modular plug allowed the shielding wire to be improperly grounded, thus making the cable susceptible to radiated interference. Without proper grounding, the presence of interfering radiation can cause the loss of data packets between the OBR base station and the WES800.

To fix this problem, Vecima recommends reworking the termination of the Ethernet cable using the JMRJ45S-15 modular plug and properly grounding the cablefeed. The cable termination can be repaired in the field at the tower site. Once the Ethernet cable termination is repaired, the cable feed will no longer be susceptible to interfering radiation and the data will be secured.

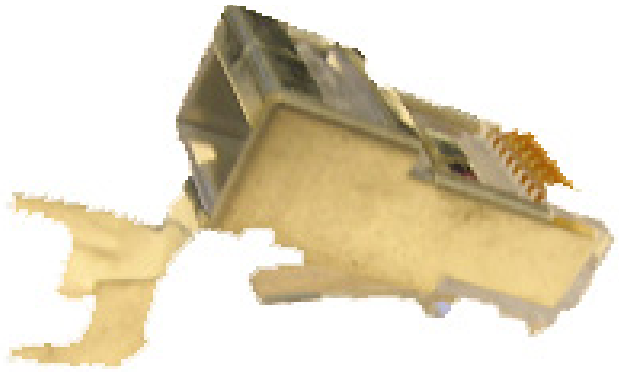


***Figure A-1 JMRJ45S-15 Modular Plug***

**NOTE**

Other than the risk of data loss due to interfering radiation, there is no safety issues concerning the connector that came with the OBR3650HP. Where loss of data due to the radiating interference is not a concern, reworking the terminating end with the JMRJ45S-15 is only necessary as a precaution.

If using a pre-made cable assembly (such as a CAT5CABLE/OD/25, CAT5CABLE/OD/50, CAT5CABLE/OD/75 or CAT5CABLE/OD/100 from Vecima Networks), then the process described in this document is not necessary

**CAUTION**

**Before attaching the backshell, it is highly recommended that the user read through this entire appendix to become familiar with all of the steps involved to ensure that none are missed.**

# A1.1 Molex® Backshell Components

Figure A-2 shows the items that make up the Molex® backshell included with the OBR3650HP. The Ethernet modular plug shown is the JMRJ45S-15 that must be substituted for the plug that comes with the package.


***Figure A-2 Molex® Backshell Elements***

Molex® backshell component parts:

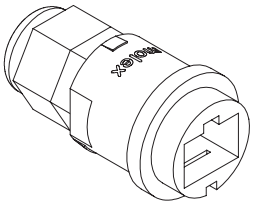
1. Coupling ring
2. Cable seal assembly – might already be threaded to into part 3
3. Plug holder
4. Basket seal
5. JMRJ45S-15 modular plug
6. Loading sleeve
7. Retainer wedge

**NOTE**

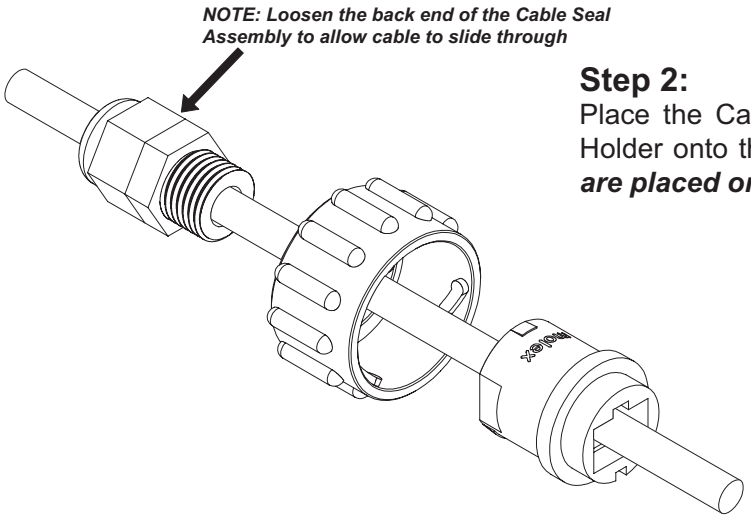
The CAT5E cable is not included with the OBR3650HP. Vecima Networks strongly recommends using CAT5E, outdoor rated cable with stranded conductors (Example: CommScope ICAT5E 2002).

# A1.2 Initial Placement of the Backshell

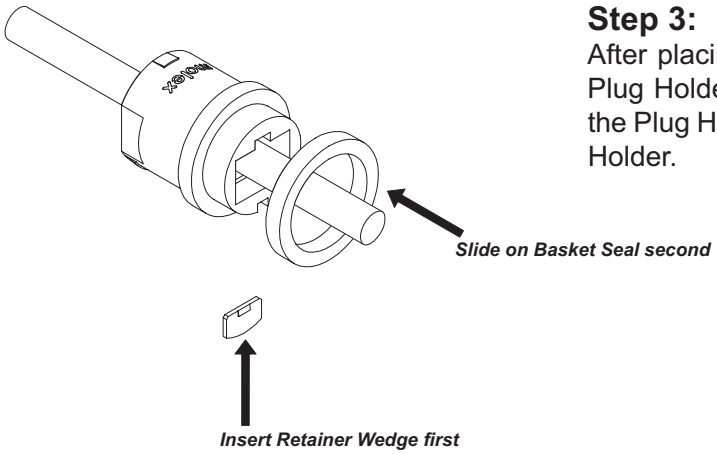
shows the steps necessary to initially place the backshell on the cable.



**Step 1:**
Separate the Cable Seal Assembly from the Coupling Ring (if they came threaded together in the package)




**Step 2:**
Place the Cable Seal Assembly, Coupling Ring and Plug Holder onto the cable as shown. ***It is vital that the items are placed on the cable in the correct order.***




**Step 3:**
After placing the Cable Seal Assembly, Coupling Ring and Plug Holder onto the cable, insert the Retainer Wedge into the Plug Holder and then slide the Basket Seal onto the Plug Holder.

***Figure A-3 Placing the Molex Backshell on***

# A1.3 Attaching the RJ45 Connector

## Assembling the JMRM45S-15 Ethernet Terminating End

**Step 1** Carefully cut about 1.5 inches (approximately 4 cm) of the jacket. Be careful not to cut the foil that encases the wires. Vecima recommends that you use an exacta knife to score the length of jacket that you are removing, then use your needle-nose pliers to carefully split the jacket. If you happen to take off all the foil, simply remove more of the jacket. When complete, 0.65 inches (or 1.7 cm) of intact foil should be exposed and the wires should extend another 0.85 inches (or 2.2 cm) beyond that. See Figure Figure A-4.

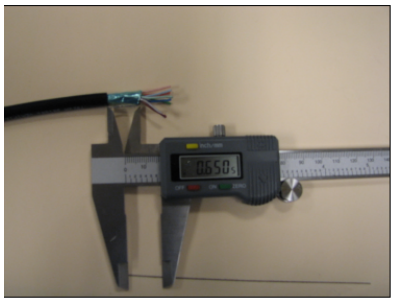


***Figure A-4 Stripped jacket***

**Step 2** Untwist the wire pairs and separate them. Fold the stranded wire back over the foil. See Figure A-5 below for a picture of wires prepared for insertion into the connector sleeve.

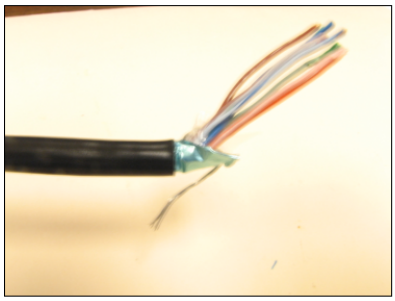
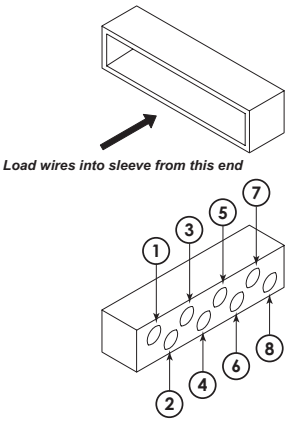


***Figure A-5 Preparing the wires for insertion in connector sleeve***

**Step 3** Insert each wire through the loading sleeve in the precise order shown in Figure A-6. Ensure that the foil is closed around the wires and that the loading sleeve is pushed as far back on the cable as possible so that it is close to the foil. Be sure to insert the wires into the open end of the loading sleeve. Trim the wires so that the they extend from the foil by 0.4 inches (1 cm). Figure Figure A-7 shows the completed assembly before crimping.




1. White/Orange (Pair 2, TX Data +)
2. Orange (Pair 2, TX Data)
3. White/Green (Pair 3, RX Data +)
4. Blue (Pair 1, +48VDC)
5. White/Blue (Pair 1, +48VDC)
6. Green (Pair 3, RX Data -)
7. White/Brown (Pair 4, DC Return)
8. Brown (Pair 4, DC Return)

**Color Coding shown is EIA/TIA 568B**

***Figure A-6 Inserting wires in loading sleeve***

*Figure A-7 Cable ready for crimping*

**Step 4** Before installing into the connector bend back the metal strain relief along the cable length. The metal strain relief should fit just after the jacket and cover the foil.

Check the following before crimping:

1) The wires are in the correct order. See Figure A-6
2) You can see the copper ends of the wires. If the wires are not snug against the connector end, the connection will be intermittent.

After ensuring that the cable is prepared correctly, crimp the cable using a WT1144 or WT1145 crimping tool as shown in Figure A-8. The crimped cable is shown in Figure A-9.

**NOTE**

If no crimping tool is available, use a pair of pliers to crimp the shield to the cable. Ensure that the shield is securely attached to the cable.

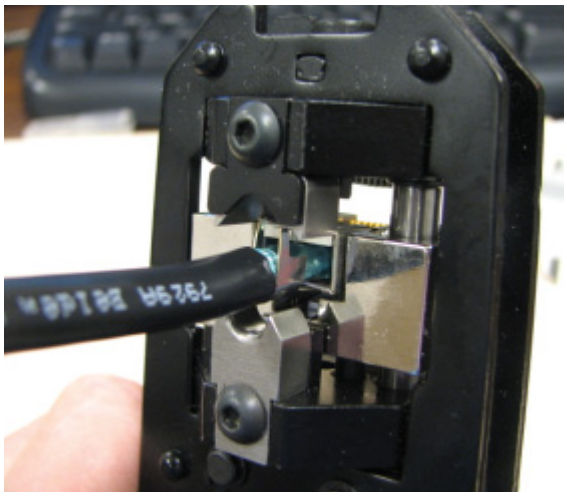


*Figure A-8 Crimping the cable*

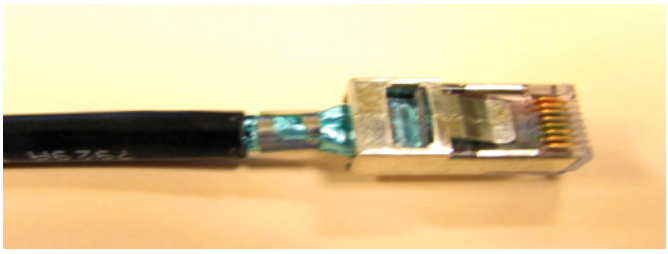


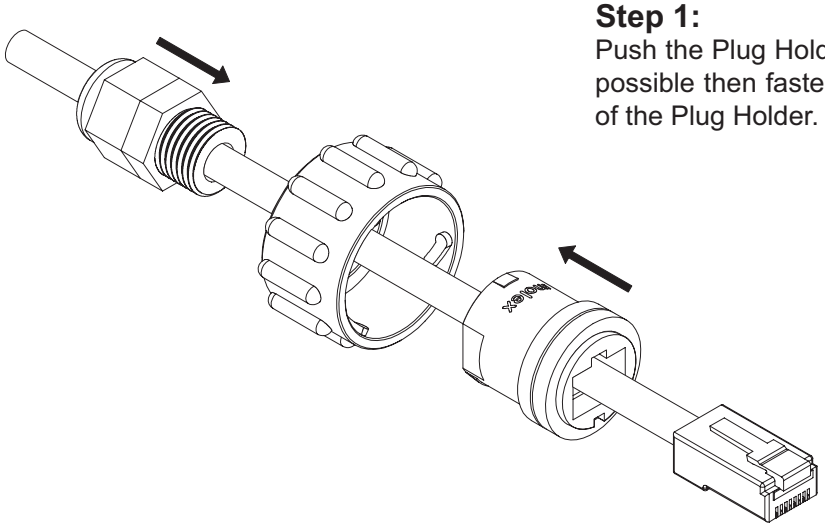
*Figure A-9 Assembled cable terminating end*

**Step 5** After crimping the cable, cut a two inch piece of ZTHS.50-01 heat-shrunk protective sheath and place it over the connector and a leading piece of cable. See Figure A-10.

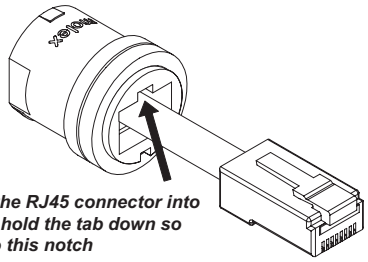
***Figure A-10 Connector wrapped in ZHTHS.50-01 sheath***

# A1.4 Completing the Backshell Installation

Figure A-11 shows the steps necessary to compete the installation of the backshell on the cable.



**Step 1:**
Push the Plug Holder as far back into the Coupling Ring as possible then fasten the Cable Seal Assembly into the rear of the Plug Holder.

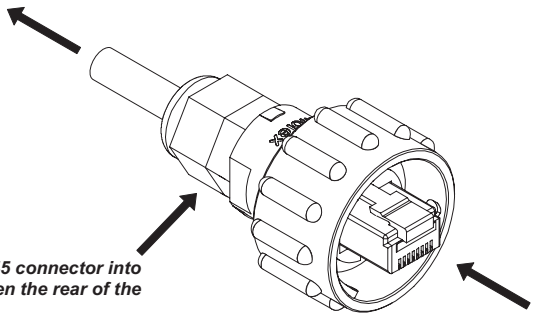


*When inserting the RJ45 connector into the Plug Holder, hold the tab down so that it slides into this notch*

**Step 2:**
Push the RJ45 connector into the Plug Holder until it is snug against the Reatainer Wedge and then tighten the rear of the Cable Seal Assembly to hold the cable in place.

***When pushing the RJ45 connector into the Plug Holder, be sure to hold the tab down so that it slides into the slot as indicated***.

This prevents the RJ45 connector tab from locking since there is no access to push down the tab once it is inside the Coupling Ring. The Coupling Ring takes care of locking the RJ45 connector in place via its bayonet  locking mechanism.



*After pushing the RJ45 connector into the Plug Holder, tighten the rear of the Cable Seal Assembly*

***Figure A-11 Attaching the RJ45 Connector***

**This page intentionally left blank**

# B1 Installing the Antenna - Points to Consider

Improperly installed antennas will add cost, time, and frustration to your operation. Taking some time to plan a proper installation will have long term benefits.

## B1.1 Planning the Installation

Consider the following points when planning an installation:

- The antenna should support proper grounding and lightning protection.

  It is usually far easier to bring the coax into the building where the AC power enters the building; because this is the easiest and cheapest way to properly bond the cable entrance to the AC ground (coax is easier and cheaper to work with than #6 AWG copper). Any lightning energy coming in on the coax will be also shared and spread over to the AC ground system, and there will be no voltage differential between the two ground systems.

- The antenna should be able to send and receive a strong signal.

  The simplest method is to presurvey the proposed location with an antenna and transceiver that are connected via a temporary string of coaxial cable to a power inserter. The assembly can be mounted to any pole and hand–held to determine the presence of signal using the integrated beeper.

- The antenna should support your plan for cableruns.

  Cableruns that are too long might decrease the efficiency of signal transmission. Cableruns should be able to support proper grounding and surge protection. Make sure that you have determined the entire wiring route & needs before drilling holes in the structure and attaching mounting hardware.

**CAUTION**

**To comply with RF exposure requirements, the integrated antenna or any external antenna which is connected to an OBR3650HP requires a minimum distance of 1.5 meters between it and all persons.**

## B1.2 Safety Considerations

Before you begin your installation, read all critical safety warnings.

- Do not put the antenna under a power line. The power line can cause interference, and also exposes the Installation to unnecessary site hazards.
- All Installations must meet building and electrical codes. Note that some municipalities have restrictions or community covenants regarding towers and antenna structures. Check first.
- Do not install the antenna in high winds or in stormy weather, particularly if lightning is present.
- Remember to assemble the antenna hardware at a safe location before climbing up to the antenna mount.
- Depending on your location, you may need two or more people to install the antenna and mount.

## B1.3 Evaluating the Mounting Location

You can mount the antenna to a variety of surfaces.

- The antenna should have a clear line-of-sight to the subscriber station. Do not put the antenna where it will be blocked by people, animals or vehicles.

  Consider how time and the season will affect the line-of-sight. For example, will foilage from growing trees interfere with the line-of-sight? Will wind or ice add strain to the mounting assembly?

- The simple arm supplied with the integrated antenna assembly can be mounted to the side of the house if you can locate the structural studding.

  The simple arm can also be attached to brick or cinder blocks. If mounting to brick, be sure to put the anchors in the brick only, as anchors will not hold in joint mortar. If mounting to cinder blocks, use toggle bolts that go into the hollow space in the block.

- The rooftop will often be another spot to fasten to. This usually is the best location for obstruction clearance. Locating underlying truss structure can be done with stud finders, looking for nail fasteners through the fascia board, standard sounding techniques, or from the underside of the roof. To prevent the roof from leaking, you should caulk the holes with silicone sealant around the holes and at the bottom of the antenna foot where it contacts the surface. Apply the sealant before you bolt the foot down tight. Be sure to caulk all holes to prevent leaks.
- An independent radio tower can also be used, but the Installation of these towers is beyond the scope of this document, usually involving professional structural engineering. Metal towers can provide some of the best lightning protection since the large metallic structural elements will best carry lightning energy straight to ground.
- Wooden poles are NOT recommended, because the insulating properties of the wooden pole mean that a large percentage of a lightning stroke will follow the coax towards the terminal end, even when substantial grounding conductors are used. Also, wooden poles will sway in the wind putting the antenna beam in and out of alignment in high wind conditions. By the time the pole is re-guyed to minimize the sway; a properly engineered metal tower could have been installed.
- Wind considerations. The integrated antenna has been engineered to operate in 160 Km (100MPH) winds, and survive in 220 Km (135 MPH) winds, but these forces will generate several hundred Kg. of load to the supporting mast. At this point, the mounting structure needs to be very secure.
- The Installation should be accessible year round. Ice might build up in the winter or early spring time.

**TIP**

When the primary coaxial cable is placed, leave approximately 24” of coaxial cable with a 4” to 6” diameter loop where the antenna will be installed. This will allow for the required flexibility for adjustment and future servicing.