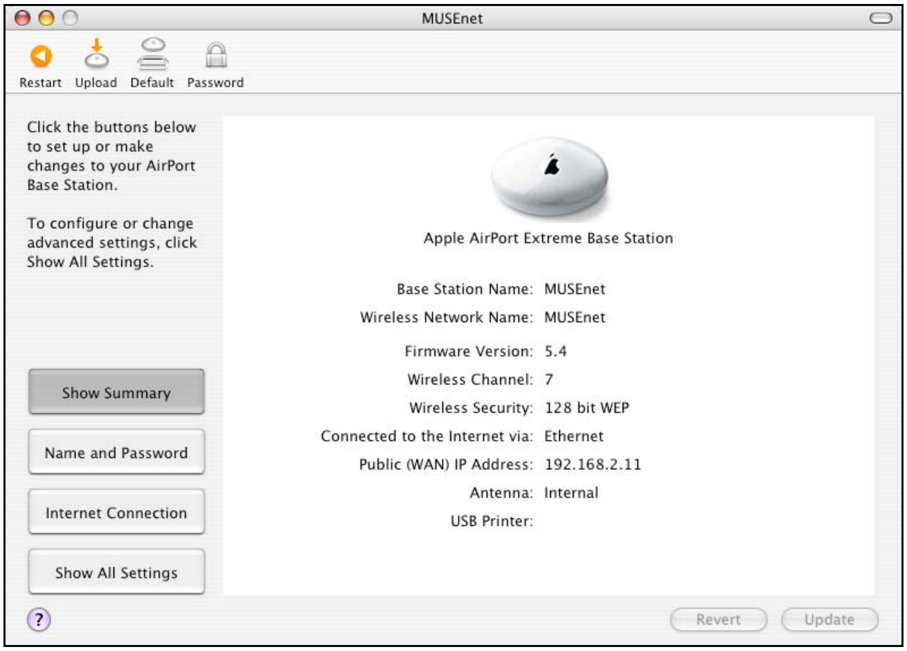
1. APPLE AIRPORT EXTREME

1.1 Product Description

The following are device specific configuration settings for the Apple Airport Extreme. Navigation through the management screens will be similar but may vary across specific products in this vendor's family of routers. See the vendor's website for more information about wireless configuration at www.apple.com/airportextreme/. The following equipment was used in the test case:

Device:	Apple Airport Extreme Base Station V4.0.8
Firmware:	Version 5.4

An administration utility is provided by the manufacturer, which assists the user in configuring the access point. Start the utility and click on the Show All Settings button to begin configuration of the recommended settings as shown in Figures 4-1 and 4-2.



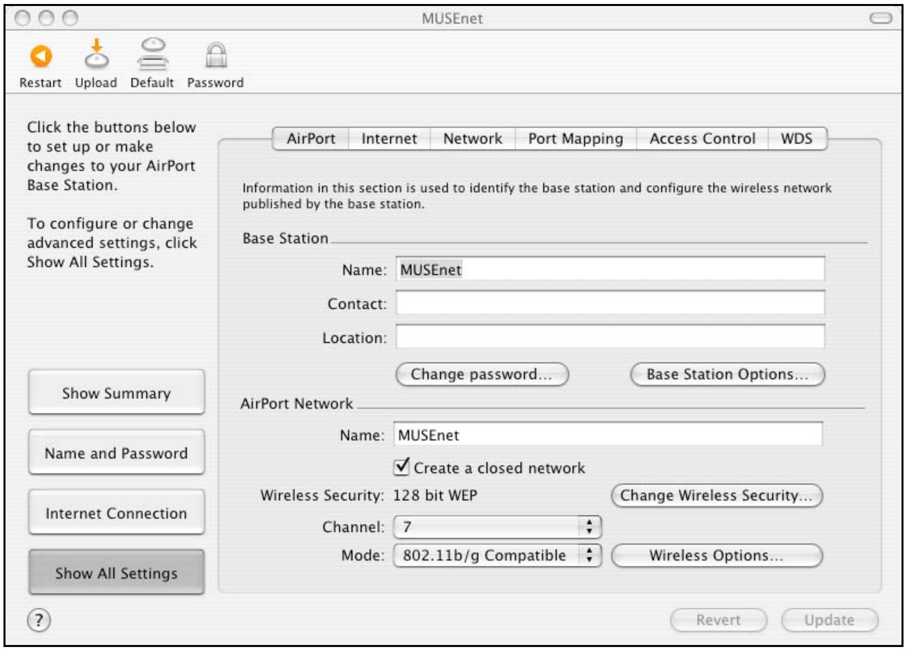
Click the buttons below to set up or make changes to your AirPort Base Station.

To configure or change advanced settings, click Show All Settings.

Apple AirPort Extreme Base Station

Base Station Name:	MUSEnet
Wireless Network Name:	MUSEnet
Firmware Version:	5.4
Wireless Channel:	7
Wireless Security:	128 bit WEP
Connected to the Internet via:	Ethernet
Public (WAN) IP Address:	192.168.2.11
Antenna:	Internal
USB Printer:	

Figure 1-1. Apple: Configuration Summary Screen



Click the buttons below to set up or make changes to your AirPort Base Station.

To configure or change advanced settings, click Show All Settings.

Information in this section is used to identify the base station and configure the wireless network published by the base station.

Base Station

Name: MUSEnet

Contact:

Location:

AirPort Network

Name: MUSEnet

☑ Create a closed network

Wireless Security: 128 bit WEP

Channel: 7

Mode: 802.11b/g Compatible

Figure 1-2. Apple: Show All Settings Screen

1.2 Configuration of Recommended Security Policies

2.3.1.010	Use layer 2 or 3 encryption with AES
Not available in tested product.	

2.3.1.020	Choose products that support a network level security management solution.
Set SNMP and VLAN setting as described in policy 2.3.1.030.	

2.3.1.030	Disable management ports on network devices when not in use.
In its simplest configuration, the services screen should be configured as follows: - Telnet/SSH: Enabled – Enables secure shell tunneling to AP for management purposes (CLI). For secure deployments, SSH should be enabled and Telnet should be disabled. - CDP: Disable Cisco Discovery Protocol. CDP can be disabled, but may adversely impact Power over Ethernet negotiation with the AP, as well as limit the ability for Switch port shutdown of rogue AP's. - Filters: Enabled (optionally, these can be individually enabled if needed). Filters/Access lists can be enabled on the AP to only allow critical services such as DHCP, DNS and VPN services to further control traffic. - CDP: Disable Cisco Discovery Protocol. - Filters: Enabled (optionally, these can be individually enabled if needed). - SNMP: Enabled – Allows network management and monitoring devices to access the AP (but over an OOB management VLAN described later). - VLAN: Enabled – Allows multiple virtual LANs to be configured to the AP from network. - Hot Standby: Disabled - DNS: Disabled - HTTP: Enabled – Allows browser access to the AP for configuration. Caution, this access should only be allowed over a secure channel, since the communication is not HTTPS. - QoS: Disabled (unless applications require this feature) - NTP: Enable – for network Managements best practice – this will provide a way to help correlate events if the need arises for Network Troubleshooting. - ARP Caching: Disabled (enable to decrease wireless broadcast traffic and increase security)	

2.3.1.040	Use OOB management across a specially configured VLAN for network administration/management
Set VLAN setting as described in policy 2.3.1.030.	

2.3.1.050	WLAN must have session timeout capability and must be set to 15 min or less
No setting available on this AP. Must be set on client devices.	

2.3.1.060	Set AP transmit power to lowest possible to attain signal strength required
- From the **Show All Settings, Airport** menu tab (Figure 4-2) - Select the **Wireless Options** button. - Select the best combination of **Interface Robustness, Multicast Rate** and **Transmit Power** that reaches to the furthest required point of the WLAN. This process will require repeated testing using a secured client.	

<table>
<tr><th>2.3.1.070</th><th>Password-protect AP beyond manufacturer’s default setting</th></tr>
<tr><td colspan="2">- From the <b>Show All Settings, Airport</b> menu tab (Figure 4-2)
- Click the <b>Change password</b> button
- In the popup window that appears, change the base station password
- Use sound password policies such as minimum 8 characters, one digit, one capital letter, and one special character
- To check the strength of your password, you may use the Apple Keychains application, which features a built-in strength tester that provides a password strength score</td></tr>
</table>

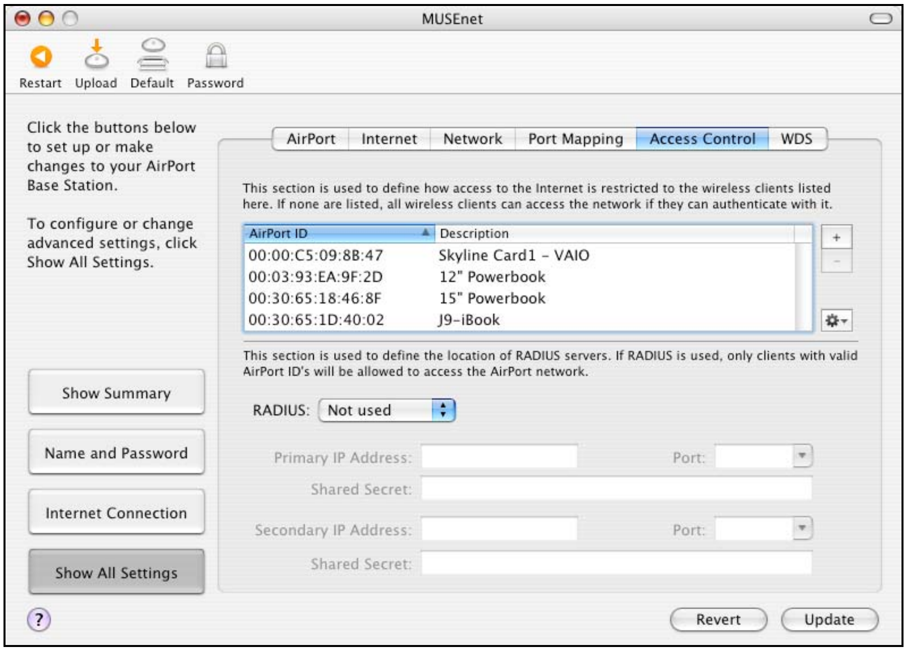
<table>
<tr><th>2.3.1.080</th><th>Change default SSID</th></tr>
<tr><td colspan="2">From the <b>Show All Settings, Airport</b> menu tab (Figure 4-2)
Under the <b>AirPort Network</b> section, in the field labeled <b>Name</b>, type a name for the base station. This will be the SSID of the base station

<b>NOTE</b>: The <b>Base Station, Name</b> field also listed on this screen, is for administration purposes only and will not set the SSID.</td></tr>
</table>

<table>
<tr><th>2.3.1.090</th><th>Disable SSID broadcast mode</th></tr>
<tr><td colspan="2">Not tested.</td></tr>
</table>

2.3.1.100	Enable MAC address filtering

- From the **Show All Settings** menu (Figure 4-2),
- Select the **Access Control** tab (Figure 4.4). Note the window where client Airport IDs (MAC addresses) and client descriptions can be entered
- Click on the + button to the right of this window to add clients
- Exporting this list to other Airport Extreme base stations is a simple process



Click the buttons below to set up or make changes to your AirPort Base Station.

To configure or change advanced settings, click Show All Settings.

This section is used to define how access to the Internet is restricted to the wireless clients listed here. If none are listed, all wireless clients can access the network if they can authenticate with it.

AirPort ID	Description
00:00:C5:09:8B:47	Skyline Card1 – VAIO
00:03:93:EA:9F:2D	12" Powerbook
00:30:65:18:46:8F	15" Powerbook
00:30:65:1D:40:02	J9-iBook

This section is used to define the location of RADIUS servers. If RADIUS is used, only clients with valid AirPort ID's will be allowed to access the AirPort network.

RADIUS: Not used

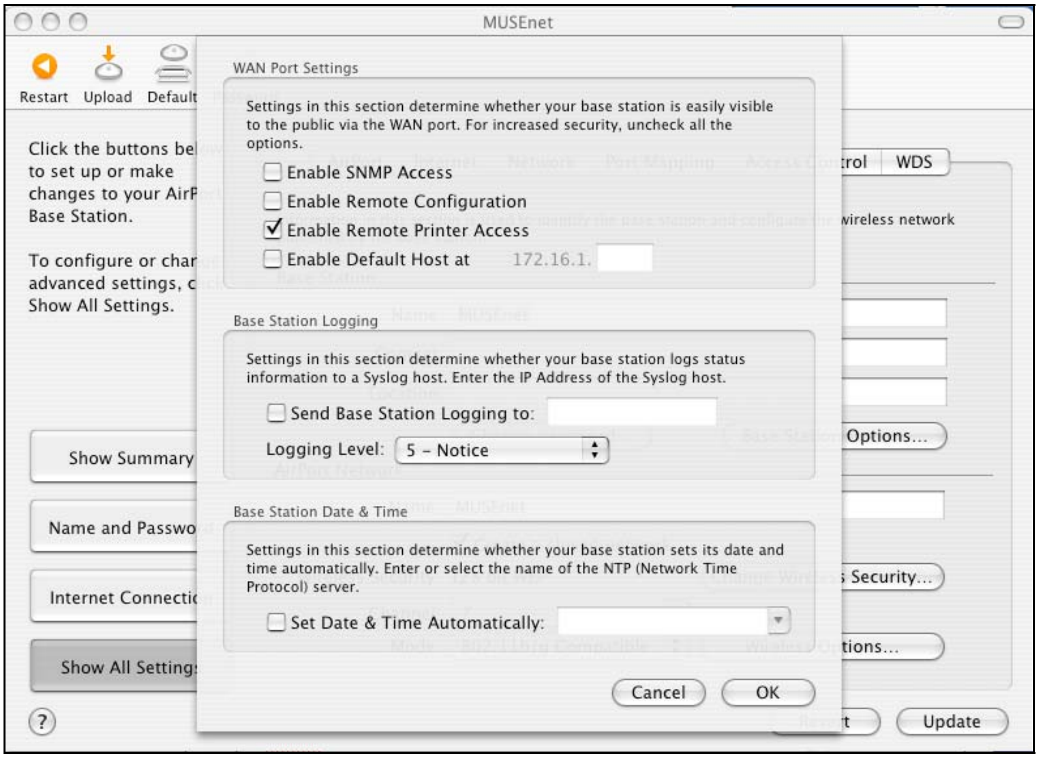
Figure 1-3. Apple: MAC Address Filtering

2.3.1.110	Backup system configuration settings
Not tested. See vendor website.	

2.3.1.120	Enable Wireless Client Isolation
Not tested	

2.3.1.130	Enable and configure logging

- From the **Show All Settings, Airport** tab (Figure 4-2)
- Click the **Base Station Options** button
- Select **Logging Level 5** from the drop down menu (default)
- Click the **Send Base Station Logging** checkbox
- Enter the IP address of the device you wish to receive the Syslog stream



Click the buttons bel to set up or make changes to your AirP Base Station.

To configure or char advanced settings, c Show All Settings.

WAN Port Settings

Settings in this section determine whether your base station is easily visible to the public via the WAN port. For increased security, uncheck all the options.

□ Enable SNMP Access
□ Enable Remote Configuration
☑ Enable Remote Printer Access
□ Enable Default Host at 172.16.1.

Base Station Logging

Settings in this section determine whether your base station logs status information to a Syslog host. Enter the IP Address of the Syslog host.

□ Send Base Station Logging to:

Logging Level: 5 - Notice

Base Station Date & Time

Settings in this section determine whether your base station sets its date and time automatically. Enter or select the name of the NTP (Network Time Protocol) server.

□ Set Date & Time Automatically:

Figure 1-4. Apple: Logging