The Launch Pad

To: service@launchpadonline.com

Cc: mjordan@launchpadonline.com; mgary@launchpadonline.com; Ralph Wilson; rkrell@launchadonline.com; tfrastack@launchpadonline.com; jortiz@launchpadonline.com; kschrank@launchpadonline.com; gsilver@launchpadonline.com; rjohnson@launchpadonline.com

Subject: Tech Note 2-22-03

We have an exciting product announcement to make. As of December 10th, we are officially an authorized Apple reseller. Whereas previously Apple has been identified with the consumer market, with the release of the first Apple server, the Xserve http://www.apple.com/xserve/, Apple is now positioning itself in the business market. Some of you have probably seen the commercials which are part of the Apple Switch campaign http://www.apple.com/switch/ all part of the marketing blitz unleashed by Apple to try to make a dent in the PC business marketplace. Whether they will succeed remains to be seen. In the meantime they are offering strong channel support for resellers such as The Launch Pad and we will be designing some targeted marketing efforts to break into this market in our region.

Our goal is not only to generally increase sales and our customer base but to be able to tap into markets such as non-profits, print and graphic shops and educational organizations. That means more opportunity for technicians. As of 2003 we are also planning to introduce a bonus program for technicians that sell Apple products to new customers. If you are interested in getting more familiar with the Apple product line and involved in this program, send an e-mail to apple@launchpadonline.com.

Wireless Networking

Also, in 2003 we are going to be promoting and installing more and more wireless networking infrastructures. There are many advantages to wireless networks for small businesses and the technology has improved in both performance and stability. One issue still of concern and something that needs to be addressed with wireless installations is the need for security. Since the predominant router we will be promoting is the Linksys, I am including a security plan that needs to be implemented in wireless installations.

Steps to tighten security on Linksys wireless networks

By default, many wireless devices can leave networks and data open to access, paving the way for practices like war driving, in which someone armed with a wireless network card and a few easily-obtainable hacker tools, can identify a wireless network and connect to it to access company data.

As network consultants, our mission is to provide the convenience of wireless networks in a relatively secure environment. To help you in this effort, here is a list of simple security fixes that will provide additional protection when you're installing a Linksys wireless network access point for your clients.

Equipment used
The options described will be based on use of:

- A Linksys wireless network access point; this device provides access for wireless clients to the wireless network.
- Linksys USB and PCMCIA network adapters for clients.
- A Windows XP operating system.

However, the same techniques can be applied to other access points and OSes.

Stage one: Security configurations for the wireless network access point
In this first stage, you should make sure that the wireless network is running and clients are able to connect. You should note that some of the security configurations that I list here will make it more difficult to isolate network connectivity problems. But, ultimately, the enhanced security is worth the extra connectivity troubleshooting you might have to do down the road.

The configurations for stage one are:

1. Place wireless access point away from windows or exterior walls. The closer an access point is to a window or exterior wall the greater the signal will be outside the building.
2. Change the default settings for the access point. In particular, you should change the default IP address, the default service set identifier (SSID), and the default administrative password. To do so, access the Web-based administration utility on the access point, and then make appropriate changes to the Setup and Password pages. **Figure A** below shows what you'll see, for example, on the Setup page.
   Choose combinations that are complex for the SSID and password, which include letters, numbers, and special characters. The phrases should be at least nine characters long. Although this sounds like basic information, all too many businesses have neglected to perform this simple task and have found their networks compromised because of this oversight.
3. Enable logging. The log tells you which computers (by MAC address) have connected to the network. As with any log, you should do a quick scan on a daily basis to see if there is any unusual activity. To change the log, open the Log Web page within the administration utility. **Figure B** shows you what this screen looks like.

Figure A

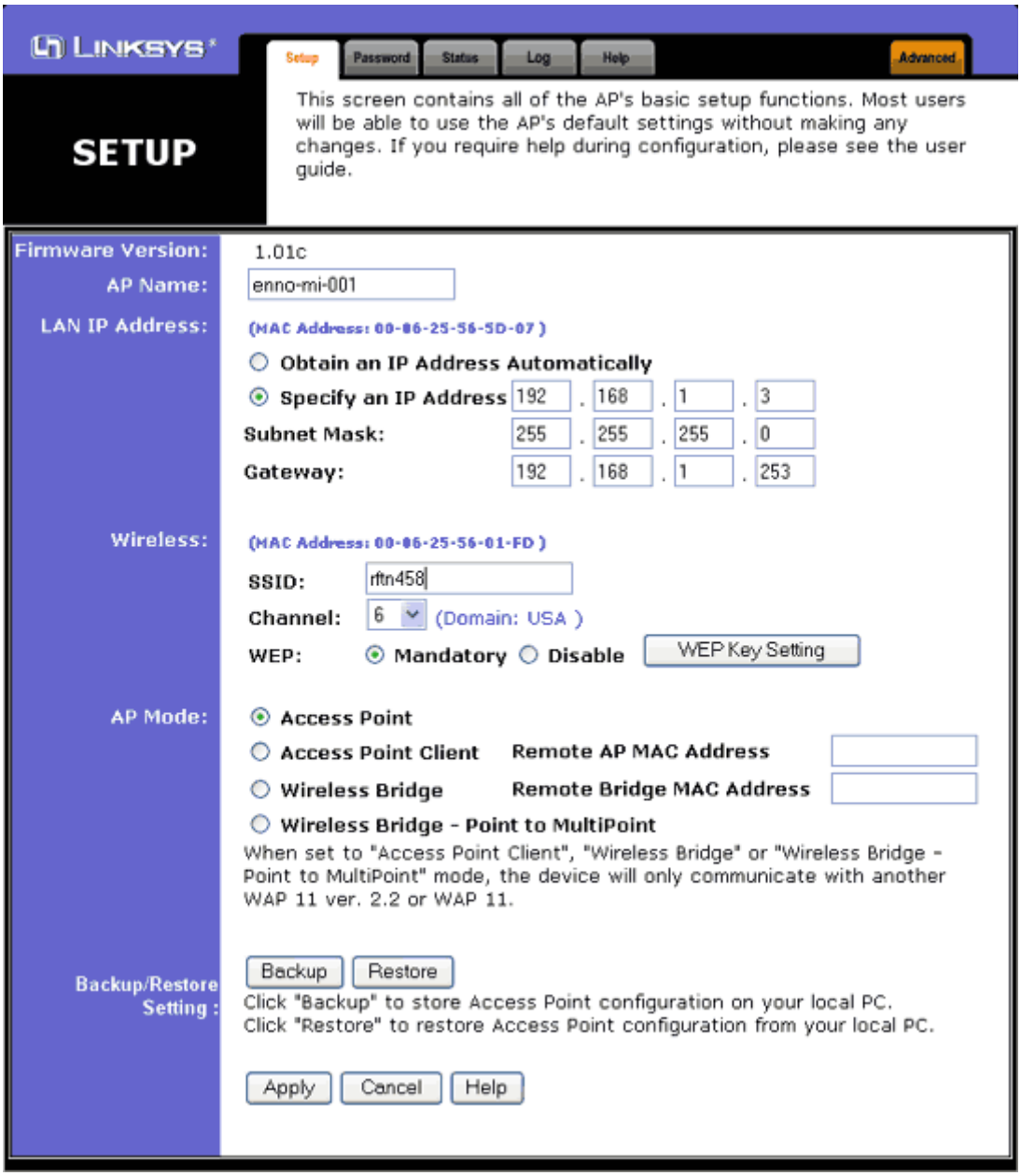
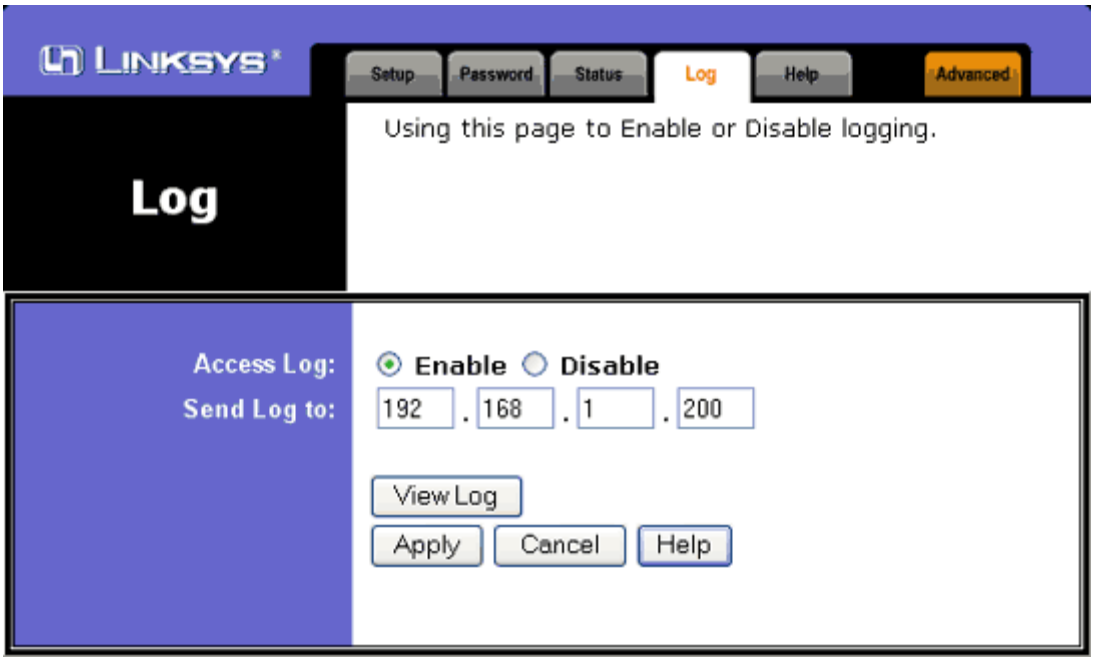

LINKSYS
Setup
Password
Status
Log
Help
Advanced
SETUP
This screen contains all of the AP's basic setup functions. Most users will be able to use the AP's default settings without making any changes. If you require help during configuration, please see the user guide.
Firmware Version:
1.01c
AP Name:
enno-mi-001
LAN IP Address:
(MAC Address: 00-06-25-56-5D-07)
Obtain an IP Address Automatically
Specify an IP Address
192 . 168 . 1 . 3
Subnet Mask:
255 . 255 . 255 . 0
Gateway:
192 . 168 . 1 . 253
Wireless:
(MAC Address: 00-06-25-56-01-FD)
SSID:
rftn458
Channel:
6
(Domain: USA)
WEP:
Mandatory
Disable
WEP Key Setting
AP Mode:
Access Point
Access Point Client
Remote AP MAC Address
Wireless Bridge
Remote Bridge MAC Address
Wireless Bridge - Point to MultiPoint
When set to "Access Point Client", "Wireless Bridge" or "Wireless Bridge - Point to MultiPoint" mode, the device will only communicate with another WAP 11 ver. 2.2 or WAP 11.
Backup/Restore Setting :
Backup
Restore
Click "Backup" to store Access Point configuration on your local PC.
Click "Restore" to restore Access Point configuration from your local PC.
Apply
Cancel
Help

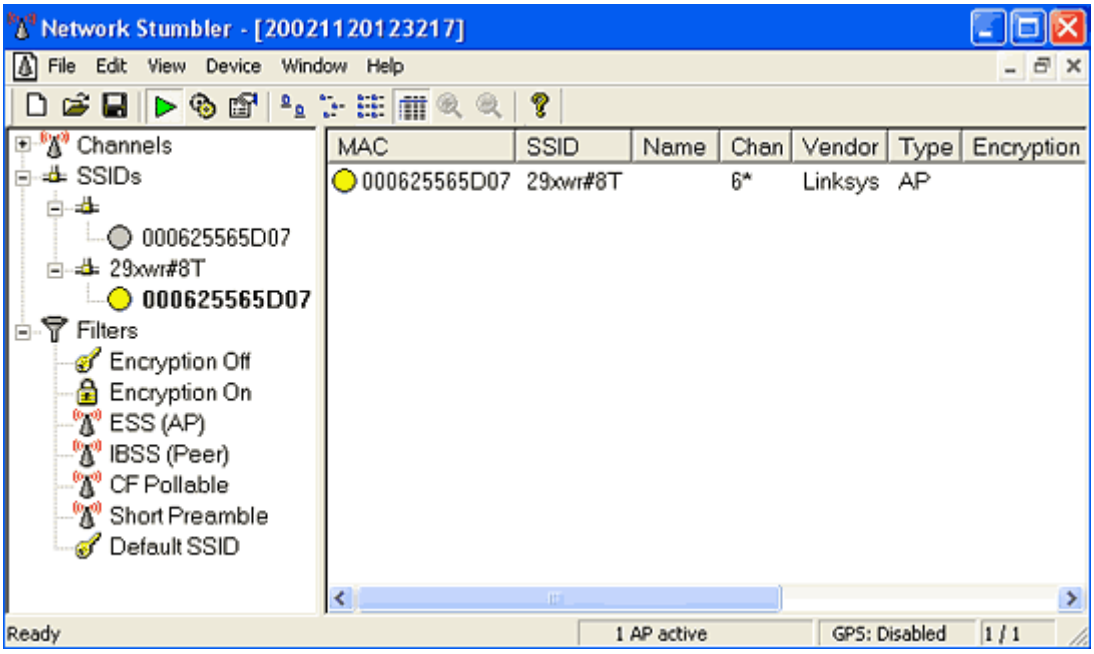
Figure B



You can also have the log sent to another computer and view it using the Log Viewer utility provided by Linksys. I prefer this method because I can centralize my log files. Unfortunately, the Log Viewer is only available by sending an e-mail to Linksys Web site's support desk.

Once you have completed these configurations, make sure all clients can connect successfully. You also should see what type of information is normally accessible by wireless network analyzers. A simple, free tool for this task is NetStumbler. **Figure C** highlights information accessible on a wireless network using NetStumbler.

Figure C



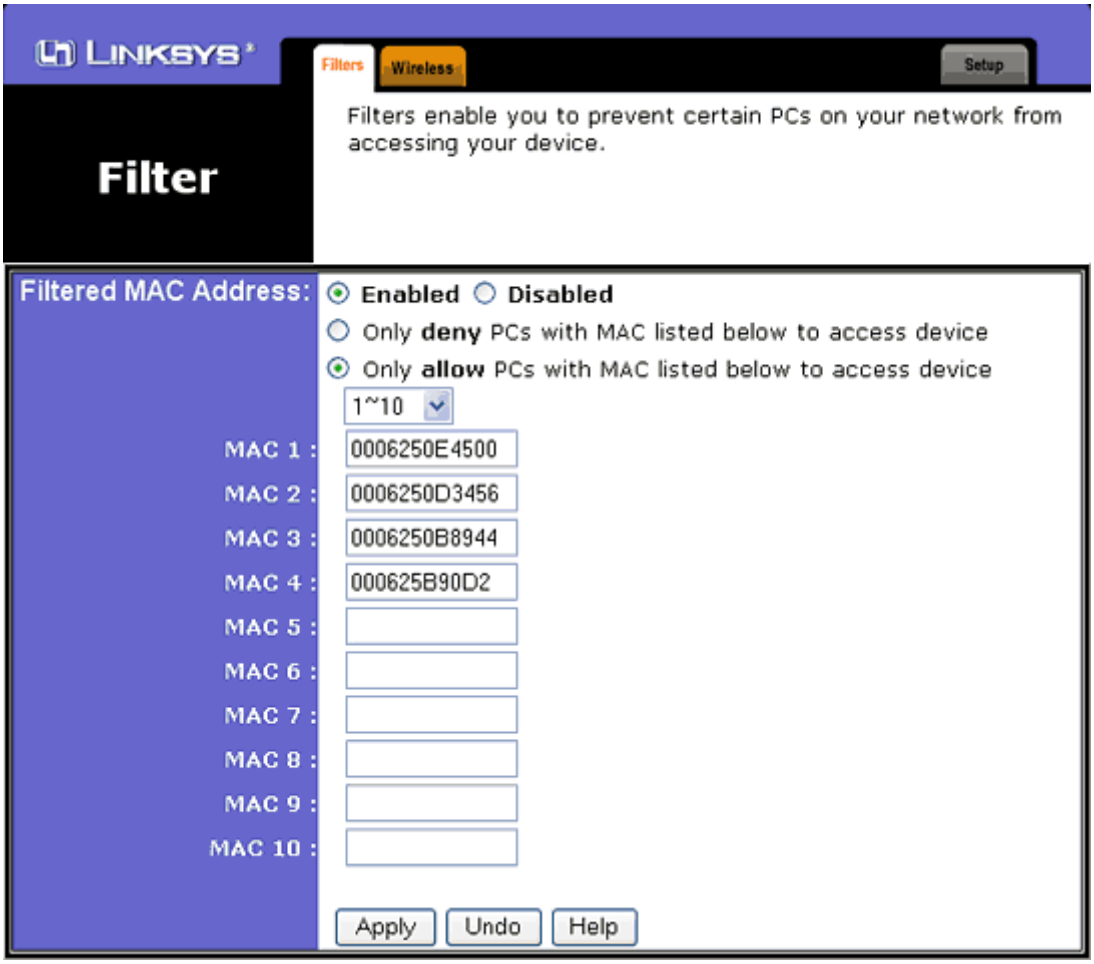
Notice that NetStumbler identifies the access point, its maker, and the SSID. With this type of information, a person can connect to your wireless network. Therefore, it's now time to talk about how to reduce the likelihood that others will discover information about your network, connect to the network, and pull data from it.

Stage two: Security configurations
There are several methods for enhancing security on a wireless network, including the following:

Enable MAC filtering
With this method, you list the network adapters that are allowed to connect to the network by MAC address. The MAC address on a Linksys wireless network adapter is located on the bottom of the device. You can also get the MAC address by typing the command*ipconfig /all (WINDOWS NT/2000/XP)* at the command prompt while the wireless network adapter is installed on the computer.

The MAC address is listed as the Physical Address with this command. Once you have the MAC addresses, you can enable MAC filtering and list MAC addresses for clients you want to connect to the network. To access this page, you have to go to the Advanced tab in the Web-based administration utility for the access point (see **Figure D)**.

Figure D



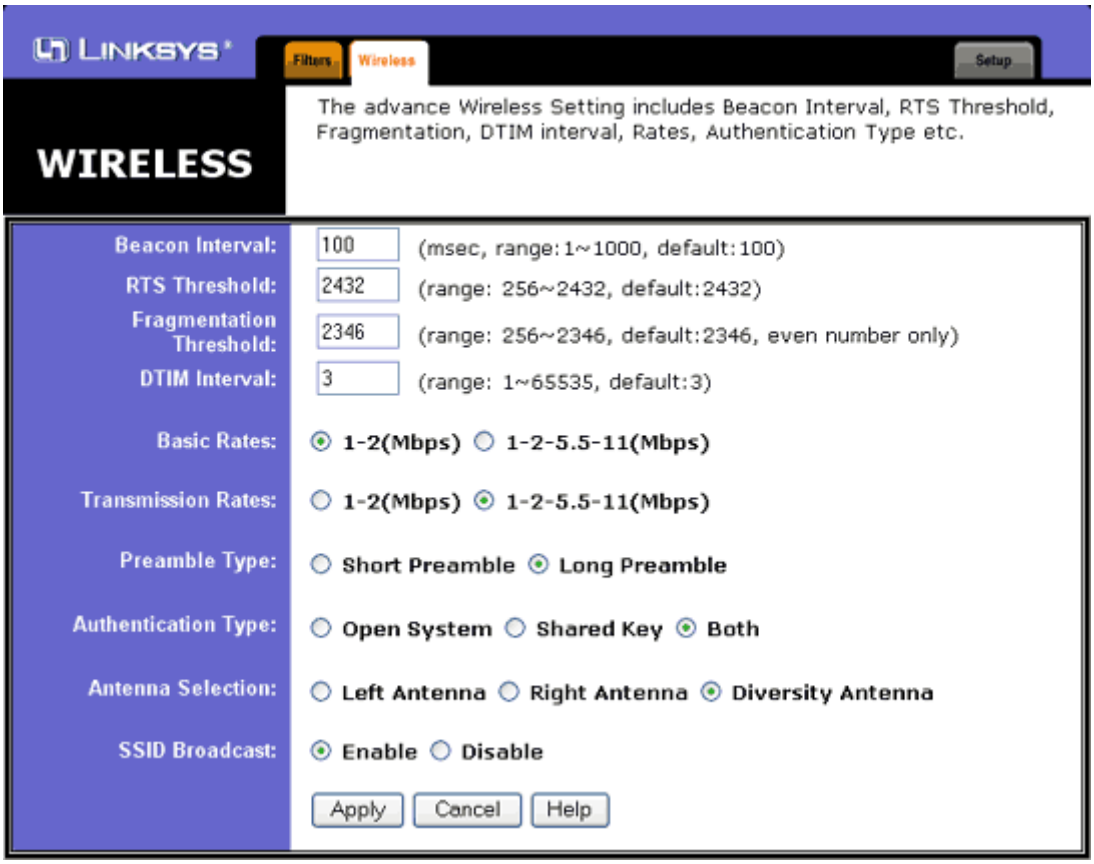
Enable wired equivalent protocol (WEP)
This method keeps outsiders from viewing data transmitted on your wireless network. Although WEP has come under fire because the protocol can be hacked, understand that your network is still more secure with WEP than without. The key is to change the WEP encryption key regularly. I recommend doing it once a week, but many of you will feel this is too much work.

My advice is to balance the need for security with the administrative load. For those of you who are comfortable with scripting, you can create a script that will change the WEP passphrase (upon which the encryption keys are generated) and automatically update clients. More expensive wireless network equipment may have features built-in to do this. To set these features, you will use the Setup page to make WEP mandatory. Then use the WEP Setting page to generate the encryption keys in the Web-based administration utility for the access point.

Set encryption for 128-bit encryption. The higher the encryption, the more difficult it is to compromise it. Some wireless network devices provide 256-bit encryption as well, but both the access point and client network adapters need to support it.

Disable SSID broadcasting
Without the SSID being broadcast, your network is more difficult to locate. To set this option, go to the Wireless page under the Advanced tab in the Web-based administration utility for the access and choose Disable in the SSID Broadcast field (see **Figure E**).

Figure E



Final check
After having done all of this, you can run NetStumbler again to see what type of information is accessible. You should find that none of your wireless network devices are located. Note that when WEP is enabled and SSID broadcasting remains enabled, the access point—including the MAC address—will still be visible; however, the name of the SSID will not appear.