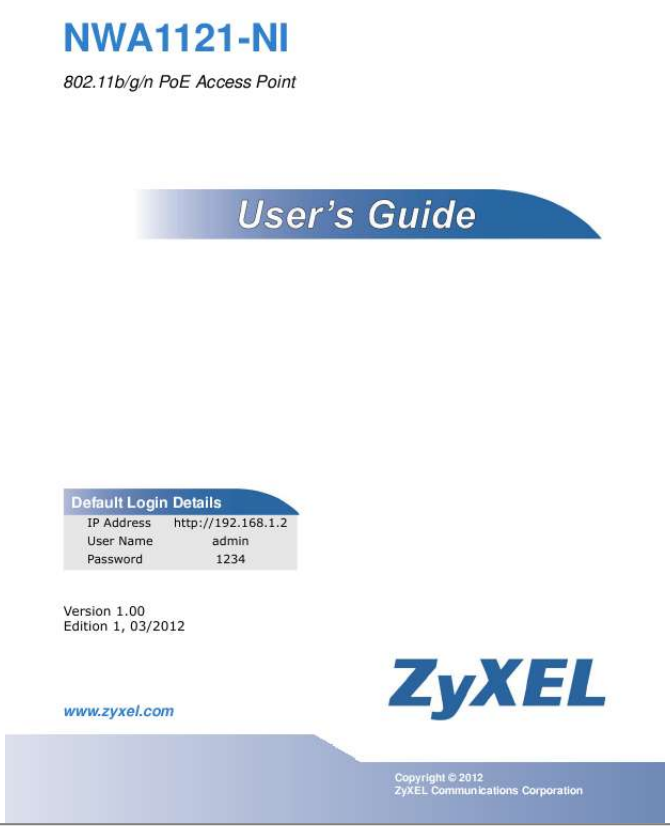

Manual abstract:

@@READ CAREFULLY BEFORE USE. @@@@11 Introducing the Web Configurator ....

.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 115 10.2 What You Can Do in this Chapter ...
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.... 115 10.
3 What You Need To Know .....
.....

.....
.....
.....
.....

.....
.....
...controls network access with MAC address filtering and RADIUS server authentication. It also provides a high level of network traffic security, supporting IEEE 802.
1x, WiFi Protected Access (WPA), WPA2 and WEP data encryption. Its Quality of Service (QoS) features allow you to prioritize time-sensitive or highly important applications such as VoIP. Your NWA1121-NI is easy to install, configure and use. The embedded Web-based configurator enables simple, straightforward management and maintenance. See the Quick Start Guide for instructions on how to make hardware connections. 1.2 Wireless Modes The NWA1121-NI can be configured to use the following WLAN operating modes: OPERATING MODE MBSSID Client Root AP Repeater NUMBER OF SUPPORTED SSID 8 1 5 1 UNIVERSAL REPEATER FUNCTION No No Yes Yes AP FUNCTION Yes No Yes Yes Applications for each operating mode are shown below. 1.2.1 MBSSID A Basic Service Set (BSS) is the set of devices forming a single wireless network (usually an access point and one or more wireless clients).

The Service Set IDentifier (SSID) is the name of a BSS. In NWA1121-NI User's Guide 11 Chapter 1 Introducing the NWA1121-NI Multiple BSS (MBSSID) mode, the NWA1121-NI provides multiple virtual APs, each forming its own BSS and using its own individual SSID profile. You can configure multiple SSID profiles, and have all of them active at any one time. You can assign different wireless and security settings to each SSID profile. This allows you to compartmentalize groups of users, set varying access privileges, and prioritize network traffic to and from certain BSSs. To the wireless clients in the network, each SSID appears to be a different access point. As in any wireless network, clients can associate only with the SSIDs for which they have the correct security settings. For example, you might want to set up a wireless network in your office where Internet telephony (VoIP) users have priority. You also want a regular wireless network for standard users, as well as a 'guest' wireless network for visitors. In the following figure, VoIP_SSID users have QoS priority, SSID01 is the wireless network for standard users, and Guest_SSID is the wireless network for guest users.
In this example, the guest user is forbidden access to the wired Land Area Network (LAN) behind the AP and can access only the Internet. Figure 1 Multiple BSSs 12 NWA1121-NI User's Guide Chapter 1 Introducing the NWA1121-NI 1.2.2 Wireless Client The NWA1121-NI can be used as a wireless client to communicate with an existing network. In the figure below, the printer can receive requests from the wired computer clients A and B via the NWA1121-NI in Client mode (Z).
Figure 2 Wireless Client Application NWA1121-NI User's Guide 13 Chapter 1 Introducing the NWA1121-NI 1.2.3 Root AP In Root AP mode, the NWA1121-NI (Z) can act as the root AP in a wireless network and also allow repeaters (X and Y) to extend the range of its wireless network at the same time. In the figure below, both clients A, B and C can access the wired network through the root AP. Figure 3 Root AP Application On the NWA1121-NI in Root AP mode, you can have multiple SSIDs active for regular wireless connections and one SSID for the connection with a repeater (universal repeater SSID).

Wireless clients can use either SSID to associate with the NWA1121-NI in Root AP mode. A repeater must use the universal repeater SSID to connect to the NWA1121-NI in Root AP mode. When the NWA1121-NI is in Root AP mode, universal repeater security between the NWA1121-NI and other repeater is independent of the security between the wireless clients and the AP or repeater. If you do not enable universal repeater security, traffic between APs is not encrypted. When universal repeater security is enabled, both APs and repeaters must use the same pre-shared key. See Section 6.6 on page 74 for more details. Unless specified, the term "security settings" refers to the traffic between the wireless clients and the AP. At the time of writing, universal repeater security is compatible with the NWA1121-NI only. 1.

2.4 Repeater The NWA can act as a wireless network repeater to extend a root AP's wireless network range, and also establish wireless connections with wireless clients. Using Repeater mode, your NWA1121-NI can extend the range of the WLAN. In the figure below, the NWA1121-NI in Repeater mode (Z) has a wireless connection to the NWA1121-NI in Root AP mode (X) which is connected to a wired network and also has a wireless connection to another NWA1121-NI in Repeater mode (Y) at the same time. Z and Y act as repeaters that forward traffic 14 NWA1121-NI User's Guide Chapter 1 Introducing the NWA1121-NI between associated wireless clients and the wired LAN. Clients A, B and C access the AP and the wired network behind the AP throught repeaters Z and Y. Figure 4 Repeater Application When the NWA1121-NI is in Repeater mode, universal repeater security between the NWA1121-NI and other repeater is independent of the security between the wireless clients and the AP or repeater. If you do not enable universal repeater security, traffic between APs is not encrypted. When universal repeater security is enabled, both APs and repeaters must use the same pre-shared key. See Section 6. 6 on page 74 for more details. Once the security settings of peer sides match one another, the connection between devices is made. At the time of writing, universal repeater security is compatible with the NWA1121-NI only. 1.3 Ways to Manage the NWA1121-NI Use any of the following methods to manage the NWA1121-NI.

• Web Configurator. This is recommended for everyday management of the NWA1121-NI using a (supported) web browser. • FTP (File Transfer Protocol) for firmware upgrades and configuration backup and restore. • SNMP (Simple Network Management Protocol). The device can be monitored by an SNMP manager.

NWA1121-NI User's Guide 15 Chapter 1 Introducing the NWA1121-NI 1.4 Configuring Your NWA1121-NI's Security Features Your NWA1121-NI comes with a variety of security features. This section summarizes these features and provides links to sections in the User's Guide to configure security settings on your NWA1121-NI. Follow the suggestions below to improve security on your NWA1121-NI and network. 1.4.1 Control Access to Your Device Ensure only people with permission can access your NWA1121-NI. • Control physical access by locating devices in secure areas, such as locked rooms. Most NWA1121-NIs have a reset button. If an unauthorized person has access to the reset button, they can then reset the device's password to its default password, log in and reconfigure its settings.

• Change any default passwords on the NWA1121-NI, such as the password used for accessing the NWA1121-NI's web configurator (if it has a web configurator). Use a password with a combination of letters and numbers and change your password regularly. Write down the password and put it in a safe place. • See Section 11.5 on page 121 for instructions on changing your password. • Configure remote management to control who can manage your NWA1121-NI. See Chapter 9 on page 101 for more information. If you enable remote management, ensure you have enabled remote management only on the IP addresses, services or interfaces you intended and that other remote management settings are disabled. 1.4.

2 Wireless Security Wireless devices are especially vulnerable to attack. Take the following measures to improve wireless security. • Enable wireless security on your NWA1121-NI. Choose the most secure encryption method that all devices on your network support. See Section 6.

6 on page 74 for directions on configuring encryption. If you have a RADIUS server, enable IEEE 802.1x or WPA(2) user identification on your network so users must log in. This method is more common in business environments. • Hide your wireless network name (SSID).

The SSID can be regularly broadcast and unauthorized users may use this information to access your network. See Section 6.5 on page 72 for directions on using the web configurator to hide the SSID. • Enable the MAC filter to allow only trusted users to access your wireless network or deny unwanted users access based on their MAC address. See Section 6.8 on page 89 for directions on configuring the MAC filter. 1.5 Good Habits for Managing the NWA1121-NI Do the following things regularly to make the NWA1121-NI more secure and to manage it more effectively. • Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.

• Write down the password and put it in a safe place. 16 NWA1121-NI User's Guide Chapter 1 Introducing the NWA1121-NI • Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the NWA1121-NI to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the NWA1121-NI. You could simply restore your last configuration. 1.6 Hardware Connections See your Quick Start Guide for information on making hardware connections. 1.7 LED Figure 5 LED Table 1 LED COLOR Amber STATUS On Flashing Off DESCRIPTION There is system error and the NWA1121-NI cannot boot up, or the NWA1121-NI doesn't have an Ethernet connection with the LAN.

The NWA1121-NI is starting up. The NWA1121-NI is receiving power and ready for use. The WLAN is active. The WLAN is active, and transmitting or receiving data. The WLAN is not active.

Green On Blinking Off NWA1121-NI User's Guide 17 Chapter 1 Introducing the NWA1121-NI 18 NWA1121-NI User's Guide C HAPT ER 2 Introducing the Web Configurator This chapter describes how to access the NWA1121-NI's web configurator and provides an overview of its screens. 2.1 Accessing the Web Configurator 1 Make sure your hardware is properly connected and prepare your computer or computer network to connect to the NWA1121-NI (refer to the Quick Start Guide). Launch your web browser. Type "192.

168.1.2" as the URL (default). The login screen appears. Figure 6 The Login Screen 2 3 4 5 Type "admin" as the (default) username and "1234" as the (default) password. Click Login. You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) then click Apply. Alternatively, click Ignore. NWA1121-NI User's Guide 19 Chapter 2 Introducing the Web Configurator Note: If you do not change the password, the following screen appears every time you login.

Figure 7 Change Password Screen You should now see the Dashboard screen. See Chapter 2 on page 19 for details about the Dashboard screen. 2.2 Resetting the NWA1121-NI If you forget your password or cannot access the web configurator, you will need to use the RESET button at the rear panel of the NWA1121-NI. This replaces the current configuration file with the 20 NWA1121-NI User's Guide Chapter 2 Introducing the Web Configurator factory-default configuration file. This means that you will lose all the settings you previously configured. The password will be reset to "1234". Figure 8 The RESET Button 2.2.1 Methods of Restoring Factory-Defaults You can erase the current configuration and restore factory defaults in two ways: Use the RESET button to upload the default configuration file.

Hold this button in for about 3 seconds (the light will begin to blink). Use this method for cases when the password or IP address of the NWA1121-NI is not known. Use the web configurator to restore defaults (refer to Section 11.8 on page 124). NWA1121-NI User's Guide 21 Chapter 2 Introducing the Web Configurator 2.

3 Navigating the Web Configurator The following summarizes how to navigate the web configurator from the Dashboard screen. Figure 9 Status Screen of the Web Configurator A B C As illustrated above, the Web Configurator screen is divided into these parts: • A - title bar • B - navigation panel • C - main window 2.3.1 Title Bar Click Logout at any time to exit the Web Configurator. Click ZAbout to open the about window, which provides information of the boot module and driver versions.

22 NWA1121-NI User's Guide Chapter 2 Introducing the Web Configurator 2.3.2 Navigation Panel Use the menu items on the navigation panel to open screens to configure NWA1121-NI features.

The following tables describe each menu item. Table 2 Navigation Panel Summary LINK Dashboard TAB FUNCTION This screen shows the NWA1121-NI's general device and network status information. Use this screen to access the statistics and client list. Monitor Logs Statistics Association List Channel Usage Configuration Network Wireless LAN Wireless Settings SSID Security RADIUS MAC Filter LAN VLAN System WWW Use this screen to configure the wireless LAN settings and NWA1121NI's operation mode. Use this screen to configure up to eight SSID profiles for your NWA1121-NI. Use this screen to configure wireless security profiles on the NWA1121-NI. Use this screen to configure up to four RADIUS profiles.

Use this screen to configure MAC filtering profiles. Use this screen to configure the NWA1121-NI's LAN IP address. Use this screen to configure the NWA1121-NI's VLAN settings. Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the NWA1121NI. Use this screen to import or remove a certificate from the NWA1121NI. Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the NWA1121NI. Use this screen to configure the NWA1121-NI for SNMP management. Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to access the NWA1121-NI. Use this screen to change your log settings. View Log Use this screen to view the logs for the categories that you selected.
Use this screen to view port status, packet specific statistics, the "system up time" and so on. Use this screen to view the wireless stations that are currently associated to the NWA1121-NI. Use this screen to know whether a channel is used by another wireless network or not. Certificates Telent SNMP FTP Log Settings Maintenance General Password Time Firmware Upgrade Use this screen to configure your device's name. Use this screen to configure your device's password.
Use this screen to change your NWA1121-NI's time and date. Use this screen to upload firmware to your device. NWA1121-NI User's Guide 23 Chapter 2 Introducing the Web Configurator Table 2 Navigation Panel Summary LINK Configuration File Restart TAB FUNCTION Use this screen to backup and restore your device's configuration (settings) or reset the factory default settings. Use this screen to reboot the NWA1121-NI without turning the power off. 2. 3.3 Main Window The main window displays information and configuration fields. It is discussed in the rest of this document. 24 NWA1121-NI User's Guide C HAPT ER 3 Dashboard The Dashboard screens display when you log into the NWA1121-NI, or click Dashboard in the navigation menu. Use the Dashboard screen to look at the current status of the device, system resources, and interfaces. The Dashboard screens also provide detailed information about system statistics, associated wireless clients, and logs. 3.1 The Dashboard Screen Use this screen to get a quick view of system, Ethernet, WLAN and other information regarding your NWA1121-NI. Click Dashboard. The following screen displays.

Figure 10 The Dashboard Screen NWA1121-NI User's Guide 25 Chapter 3 Dashboard The following table describes the labels in this screen. Table 3 The Dashboard Screen LABEL Refresh Interval Refresh Now System Information System Name WLAN Operating Mode Firmware Version This field displays the NWA1121-NI system name. It is used for identification. You can change this in the Maintenance > General screen's System Name field. This field displays the current operating mode of the wireless module (Root AP, Repeater, Client, or MBSSID). You can change the operating mode in the Configuration > Wireless LAN > Wireless Settings screen. This field displays the current version of the firmware inside the device. It also shows the date the firmware version was created. You can change the firmware version by uploading new firmware in Maintenance > Firmware Upgrade. This field displays the serial number of the NWA1121-NI.
DESCRIPTION Select how often you want the NWA1121-NI to update this screen. Click this to update this screen immediately. Serial Number Ethernet Information LAN MAC Address This displays the MAC (Media Access Control) address of the NWA1121-NI on the LAN. Every network device has a unique MAC address which identifies it across the network. This field displays the current IPv4 address of the NWA1121-NI on the network.
Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks. This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN port. The gateway helps forward packets to their destinations.
This field displays the current IPv6 address(es) of the NWA1121-NI on the network. This is the IPv6 link-local address that the NWA1121-NI generates automatically. This is the NWA1121-NI's IPv6 global address that you specify manually in the Configuration > LAN screen. IPv4 Address Subnet Mask Gateway IP Address IPv6 Address Link Local Global WLAN Information SSID Channel Status Security Mode Summary Statistics Association List View Log System Status System Up Time This field displays the SSID (Service Set Identifier). This is available only when the WLAN operation mode is Client. The channel or frequency used by the NWA1121-NI to send and receive information. This shows the current status of the wireless LAN. This is available only when the WLAN operation mode is Client. This displays the security mode the NWA1121-NI is using. This is available only when the WLAN operation mode is Client.

Click this link to view port status and packet specific statistics. See Section 5.4 on page 50. Click this to see a list of wireless clients currently associated to each of the NWA1121-NI's wireless modules. See Section 5.5 on page 51. Click this to see a list of logs produced by the NWA1121-NI. See Section 5.3 on page 49. This field displays the elapsed time since the NWA1121-NI was turned on.
26 NWA1121-NI User's Guide Chapter 3 Dashboard Table 3 The Dashboard Screen (continued) LABEL Current Date/Time System Resource CPU Usage This field displays what percentage of the NWA1121-NI's processing ability is currently being used. The higher the CPU usage, the more likely the NWA1121-NI is to slow down. This field displays what percentage of the NWA1121-NI's volatile memory is currently in use. The higher the memory usage, the more likely the NWA1121-NI is to slow down. Some memory is required just to start the NWA1121-NI and to run the web configurator.
DESCRIPTION This field displays the date and time configured on the NWA1121-NI. You can change this in the Maintenance > Time screen. Memory Usage Interface Status Interface Status This column displays each interface of the NWA1121-NI.

This field indicates whether or not the NWA1121-NI is using the interface. For each interface, this field displays Up when the NWA1121-NI is using the interface and Down when the NWA1121-NI is not using the interface.

Channel Rate This shows the channel number which the NWA1121-NI is currently using over the wireless LAN. For the LAN port this displays the port speed and duplex setting. For the WLAN interface, it displays the downstream and upstream transmission rate or N/A if the interface is not in use. SSID Status Interface SSID BSSID Security VLAN This section is not available when the WLAN operation mode is Client. This column displays each of the NWA1121-NI's wireless interfaces. This field displays the SSID(s) currently used by each wireless module. This field displays the MAC address of the wireless module. This field displays the type of wireless security used by each SSID. This field displays the VLAN ID of each SSID in use, or Disabled if the SSID does not use VLAN. NWA1121-NI User's Guide 27 Chapter 3 Dashboard 28 NWA1121-NI User's Guide C HAPT ER 4 Tutorial This chapter first provides an overview of how to configure the wireless LAN on your NWA1121-NI, and then gives step-by-step guidelines showing how to configure your NWA1121-NI for some example scenarios.

4.1 How to Configure the Wireless LAN This section illustrates how to choose which wireless operating mode to use on the NWA1121-NI and how to set up the wireless LAN in each wireless mode. See Section 4.1.2 on page 29 for links to more information on each step. 4.1.1 Choosing the Wireless Mode • Use MBSSID (Multiple Basic Service Set Identifier) operating mode if you want to use the NWA1121-NI as an access point with some groups of users having different security or QoS settings from other groups of users. See Section 1.2.

1 on page 11 for details. • Use Client operating mode if you want to use the NWA1121-NI to access a wireless network. See Section 1.2.2 on page 13 for details.

• Use Root AP operating mode if you want to allow wireless clients to access your wired network through the NWA1121-NI and also have repeaters communicate with the NWA1121-NI to expand wireleass coverage. See Section 1.2.3 on page 14 for details. • Use Repeater operating mode if you want to use the NWA1121-NI to communicate with the root AP or other repeaters.

See Section 1.2.4 on page 14 for details. 4.1.2 Further Reading Use these links to find more information on the steps: • Choosing 802.11 Mode: see Section 6.4 on page 60. • Choosing a wireless Channel ID: see Section 6.4 on page 60.

• Choosing a Security mode: see Section 6.6 on page 74. • Configuring an external RADIUS server: see Section 6.7 on page 87. • Configuring MAC Filtering: see Section 6.8 on page 89. 4.2 How to Configure Multiple Wireless Networks In this example, you have been using your NWA1121-NI as an access point for your office network. Now your network is expanding and you want to make use of the MBSSID feature (see Section NWA1121-NI User's Guide 29 Chapter 4 Tutorial 6.4.

4 on page 69) to provide multiple wireless networks. Each wireless network will cater to a different type of user. You want to make three wireless networks: one standard office wireless network with all the same settings you already have, another wireless network with high priority QoS settings for Voice over IP (VoIP) users, and a guest network that allows visitors to access only the Internet and the network printer. To do this, you will take the following steps: 1 2 3 4 5 6 Edit the SSID profiles. Change the operating mode from Root AP to MBSSID and reactivate the standard network.

Configure different security modes for the networks. Configure a wireless network for standard office use. Configure a wireless network for VoIP users. Configure a wireless network for guests to your office. The following figure shows the multiple networks you want to set up.

Your NWA1121-NI is marked Z, the main network router is marked A, and your network printer is marked B. B A Z The standard network (SSID01) has access to all resources. The VoIP network (VoIP_SSID) has access to all resources and a high QoS priority. The guest network (Guest_SSID) has access to the Internet and the network printer only, and a low QoS priority. 30 NWA1121-NI User's Guide Chapter 4 Tutorial To configure these settings, you need to know the Media Access Control (MAC) addresses of the devices you want to allow users of the guest network to access. The following table shows the addresses used in this example. Table 4 Tutorial: Example Information Network router (A) MAC address Network printer (B) MAC address 00:AA:00:AA:00:AA AA:00:AA:00:AA:00 4.2.1 Configure the SSID Profiles 1 Log in to the NWA1121-NI (see Section 2.1 on page 19).

Click Wireless LAN > SSID. The SSID screen appears. Click the Edit icon next to the Profile1. 2 3 Rename the Profile Name and SSID as SSID01. Click Apply. 4 Repeat Step 2 and 3 to change Profile2 and Profile3 to VoIP_SSID and Guest_SSID. NWA1121-NI User's Guide 31 Chapter 4 Tutorial 4.2.1.1 MBSSID 1 Go to Wireless LAN > Wireless Settings.

Select MBSSID from the Operation Mode drop-down list box. SSID01 is the standard network, so select SSID01 as the first profile. It is always active. Select VoIP_SSID as the second profile, and Guest_SSID as the third profile. Select the corresponding Active check-boxes.

Click Apply to save your settings. Now the three SSIDs are activated. 2 3 4 32 NWA1121-NI User's Guide Chapter 4 Tutorial 4.2.2 Configure the Standard Network 1 Click Wireless LAN > SSID.

Click the Edit icon next to SSID01. 2 Select SecProfile1 as SSID01's security profile. Select the Hidden SSID checkbox as you want only authorized company employees to use this network, so there is no need to broadcast the SSID to wireless clients scanning the area. Also, the clients on SSID01 might need to access other clients on the same wireless network. Do not select the Intra-BSS Traffic blocking check-box. Click Apply. NWA1121-NI User's Guide 33 Chapter 4 Tutorial 3 Next, click Wireless LAN > Security. Click the Edit icon next to SecProfile1. 4 Since SSID01 is the standard network that has access to all resources, assign a more secure security mode. Select WPA2-PSK-MIX as the Security Mode, and enter the Pre-Shared Key.

In this example, use ThisisSSID01PreSharedKey. Click Apply. 5 You have finished configuring the standard network, SSID01. 4.2.3 Configure the VoIP Network 1 Go to Wireless LAN > SSID. Click the Edit icon next to VoIP_SSID. 2 Select SecProfile2 as the Security Profile for the VoIP network. Select the Hidden SSID checkbox. 34 NWA1121-NI User's Guide Chapter 4 Tutorial 3 Select WMM_VOICE in the QoS field to give VoIP the highest priority in the wireless network.

Click Apply. 4 Next, click Wireless LAN > Security. Click the Edit icon next to SecProfile2. NWA1121-NI User's Guide 35 Chapter 4 Tutorial 5 Select WPA2-PSK as the Security Mode, and enter the Pre-Shared Key.

In this example, use ThisisVoIPPreSharedKey.
Click Apply. 6 Your VoIP wireless network is now ready to use. Any traffic using the VoIP_SSID profile will be given the highest priority across the wireless network. 4.2.
4 Configure the Guest Network When you are setting up the wireless network for guests to your office, your primary concern is to keep your network secure while allowing access to certain resources (such as a network printer, or the Internet). For this reason, the pre-configured Guest_SSID profile has intra-BSS traffic blocking enabled by default. "Intra-BSS traffic blocking" means that the client cannot access other clients on the same wireless network. 1 Click Wireless LAN > SSID. Click the Edit icon next to Guest_SSID. 2 Select SecProfile3 in the Security field. Do not select the Hidden SSID check-box so the guests can easily find the wireless network. Select WMM_BESTEFFORT in the QoS field to give the guest a lower QoS priority. 3 36 NWA1121-NI User's Guide Chapter 4 Tutorial 4 Select the check-box of Intra-BSS Traffic blocking Enabled. Click Apply.

5 Next, click Wireless LAN > Security. Click the Edit icon next to SecProfile3. 6 Select WPA-PSK in the Security Mode field. WPA-PSK provides strong security that is supported by most wireless clients. Even though your Guest_SSID clients do not have access to sensitive information on the network, you should not leave the network without security. An attacker could still cause damage to the network or intercept unsecured communications or use your Internet access for illegal activities. NWA1121-NI User's Guide 37 Chapter 4 Tutorial 7 Enter the PSK you want to use in your network in the Pre Shared Key field. In this example, the PSK is ThisismyGuestWPApre-sharedkey. Click Apply. 8 Your guest wireless network is now ready to use.
4.2.5 Testing the Wireless Networks To make sure that the three networks are correctly configured, do the following. • On a computer with a wireless client, scan for access points. You should see the Guest_SSID network, but not the SSID01 and VoIP_SSID networks.
If you can see the SSID01 and VoIP_SSID networks, go to its SSID Edit screen and make sure to select the Hidden SSID check-box and click Apply. • Try to access each network using the correct security settings, and then using incorrect security settings, such as the WPA-PSK for another active network. If the behavior is different from expected (for example, if you can access the SSID01 or VoIP_SSID wireless network using the security settings for the Guest_SSID wireless network) check that the SSID profile is set to use the correct security profile, and that the settings of the security profile are correct. 4.3 NWA1121-NI Setup in AP and Wireless Client Modes This example shows you how to restrict wireless access to your NWA1121-NI.
4.3.1 Scenario In the figure below, there are two NWA1121-NIs (A and B) in the network. A is in MBSSID or root AP mode while station B is in wireless client mode. Station B is connected to a File Transfer Protocol (FTP) server. You want only specified wireless clients to be able to access station B. You also want 38 NWA1121-NI User's Guide Chapter 4 Tutorial to allow wireless traffic between B and wireless clients connected to A (W, Y and Z). Other wireless devices (X) must not be able to connect to the FTP server. Figure 11 FTP Server Connected to a Wireless Client 4.3.

2 Configuring the NWA1121-NI in MBSSID or Root AP Mode Before setting up the NWA1121-NI as a wireless client (B), you need to make sure there is an access point to connect to. Use the Ethernet port on NWA1121-NI (A) to configure it via a wired connection. NWA1121-NI User's Guide 39 Chapter 4 Tutorial Log into the Web Configurator on NWA1121-NI (A) and go to the Wireless LAN > Wireless Settings screen. 1 2 3 4 5 Set the Operation Mode to Root AP. Select the Wireless Mode. In this example, select 802.11b/g/n. Select Profile1 as the SSID Profile. Choose the Channel you want NWA1121-NI (A) to use. Click Apply.
40 NWA1121-NI User's Guide Chapter 4 Tutorial 6 Go to Wireless LAN > SSID. Click the Edit icon next to Profile1. 7 8 9 Change the SSID to AP-A. Select SecProfile1 in the Security field. Select the check-box for Intra-BSS Traffic blocking Enabled so the client cannot access other clients on the same wireless network.
10 Click Apply. NWA1121-NI User's Guide 41 Chapter 4 Tutorial 11 Go to Wireless LAN > Security. Click the Edit icon next to SecProfile1. 12 Configure WPA-PSK as the Security Mode and enter ThisisMyPreSharedKey in the PreShared Key field. 13 Click Apply to finish configuration for NWA1121-NI (A).
4.3.3 Configuring the NWA1121-NI in Wireless Client Mode The NWA1121-NI (B) should have a wired connection before it can be set to wireless client operating mode. Connect your NWA1121-NI to the FTP server. Login to NWA1121-NI (B)'s Web Configurator and go to the Wireless LAN > Wireless Settings screen. Follow these steps to configure station B. 42 NWA1121-NI User's Guide Chapter 4 Tutorial 1 Select Client as Operation Mode. Click Apply. 2 Click on the Site Survey button. A window should pop up which contains a list of all available wireless devices within your NWA1121-NI's range.

Find and select NWA1121-NI (A)'s SSID: AP-A. 3 NWA1121-NI User's Guide 43 Chapter 4 Tutorial 4 Go to Wireless LAN > Security to configure the NWA1121-NI to use the same security mode and Pre-Shared Key as NWA1121-NI (A): WPA-PSK/ThisisMyPreSharedKey. Click Apply. Figure 12 4.3.4 MAC Filter Setup One way to ensure that only specified wireless clients can access the FTP server is by enabling MAC filtering on NWA1121-NI (B) (See Section 6.8 on page 89 for more information on MAC Filter). 1 Go to Wireless LAN > MAC Filter. Click the Edit icon next to MacProfile1. 2 Select Allow in the Access Control Mode field.
Enter the MAC addresses of the wireless clients (W, Y and Z) you want to associate with the NWA1121-NI. Click Apply. Now, only the authorized wireless clients (W, Y and Z) can access the FTP server. 44 NWA1121-NI User's Guide Chapter 4 Tutorial 4.3.
5 Testing the Connection and Troubleshooting This section discusses how you can check if you have correctly configured your network setup as described in this tutorial. • Try accessing the FTP server from wireless clients W, Y or Z. Test if you can send or retrieve a file. If you cannot establish a connection with the FTP server, do the following steps. 1 2 3 Make sure W, Y and Z use the same wireless security settings as A and can access A.
Make sure B uses the same wireless and wireless security settings as A and can access A. Make sure intra-BSS traffic is enabled on A. • Try accessing the FTP server from X. If you are able to access the FTP server, do the following. 1 2 Make sure MAC filtering is enabled. Make sure X's MAC address is not entered in the list of allowed devices. NWA1121-NI User's Guide 45 Chapter 4 Tutorial 46 NWA1121-NI User's Guide P ART II Technical Reference The appendices provide general information.

Some details may not apply to your NWA1121-NI. 47 48 C HAPT ER 5 Monitor 5.1 Overview This chapter discusses read-only information related to the device state of the NWA1121-NI.

Note: To access the Monitor screens, you can also click the links in the Summary table of the Dashboard screen to view the wireless packets sent/received as well as the status of clients connected to the NWA1121-NI. 5.2 What You Can Do • Use the Logs screen to see the logs for the categories that you selected in the Configuration > Log Settings screen (see Section 5.3 on page 49). You can view logs in this page. Once the log entries are all used, the log will wrap around and the old logs will be deleted. • use the Statistics screen to view 802.11 mode, channel number, wireless packet specific statistics and so on (see Section 5.4 on page 50). • Use the Association List screen to view the wireless devices that are currently associated to the NWA1121-NI (see Section 5. 5 on page 51). • Use the Channel Usage screen to view whether a channel is used by another wireless network or not. If a channel is being used, you should select a channel removed from it by five channels to completely avoid overlap (see Section 5.6 on page 52). 5. 3 View Logs Use the Logs screen to see the logged messages for the NWA1121-NI. Log entries in red indicate system error logs. The log wraps around and deletes the old entries after it fills. NWA1121-NI User's Guide 49 Chapter 5 Monitor Click Monitor > Logs. Figure 13 Logs The following table describes the labels in this screen.

Table 5 Logs LABEL Display E-Mail Log Now DESCRIPTION Select a category of logs to view. Select All Log to view logs from all of the log categories that you selected in the Configuration > Log Settings screen. Click E-Mail Log Now to send the log screen to the e-mail address specified in the Log Settings page (make sure that you have first filled in the E-mail Log Settings fields in Configuration > Log Settings). Click Refresh to renew the log screen. Click Clear Log to delete all the logs. This field is a sequential value and is not associated with a specific entry. This field displays the time the log was recorded. This field states the reason for the log. This field lists the source IP address and the port number of the incoming packet. Refresh Clear Log # Time Message Source 5.

4 Statistics Use this screen to view read-only information, including 802.11 Mode, Channel ID, Retry Count and FCS Error Count. Also provided is the "poll interval". The Poll Interval field is configurable and is used for refreshing the screen. 50 NWA1121-NI User's Guide Chapter 5 Monitor Click Monitor > Statistics. The following screen pops up. Figure 14 Statistics The following table describes the labels in this screen. Table 6 Statistics LABEL Description 802.11 Mode Channel ID RX Pkts TX Pkts Retry Count FCS Error Count Poll Interval Set Interval Stop DESCRIPTION This is the wireless interface on the NWA1121-NI. This field shows which 802.

11 mode the NWA1121-NI is using. This shows the channel number which the NWA1121-NI is currently using over the wireless LAN. This is the number of received packets on this port. This is the number of transmitted packets on this port. This is the total number of retries for transmitted packets (TX). This is the total number of checksum error of received packets (RX). Enter the time interval for refreshing statistics. Click this button to apply the new poll interval you entered above. Click this button to stop refreshing statistics. 5.

5 Association List View the wireless devices that are currently associated with the NWA1121-NI in the Association List screen. Association means that a wireless client (for example, your network or computer with a wireless network card) has connected successfully to the AP (or wireless router) using the same SSID, channel and security settings. NWA1121-NI User's Guide 51 Chapter 5 Monitor Click Monitor > Association List to display the screen as shown next. Figure 15 Association List The following table describes the labels in this screen. Table 7 Association List LABEL # MAC Address SSID Association Time Signal Strength Refresh DESCRIPTION This is the index number of an associated wireless device. This field displays the MAC address of an associated wireless device. This field displays the SSID to which the wireless device is associated. This field displays the time a wireless device first associated with the NWA1121-NI's wireless network. This field displays the RSSI (Received Signal Strength Indicator) of the wireless connection. Click Refresh to reload the list.

5.6 Channel Usage Use this screen to know whether a channel is used by another wireless network or not. If a channel is being used, you should select a channel removed from it by five channels to completely avoid overlap. Click Monitor > Channel Usage to display the screen shown next. 52 NWA1121-NI User's Guide Chapter 5 Monitor Wait a moment while the NWA1121-NI compiles the information. Figure 16 Channel Usage The following table describes the labels in this screen. Table 8 Channel Usage LABEL SSID DESCRIPTION This is the Service Set IDentification (SSID) name of the AP in an Infrastructure wireless network or wireless station in an Ad-Hoc wireless network. For our purposes, we define an Infrastructure network as a wireless network that uses an AP and an AdHoc network (also known as Independent Basic Service Set (IBSS)) as one that doesn't. See the chapter on wireless configuration for more information on basic service sets (BSS) and extended service sets (ESS). This is the index number of the channel currently used by the associated AP in an Infrastructure wireless network or wireless station in an Ad-Hoc wireless network.

This field displays the MAC address of the AP in an Infrastructure wireless network. It is randomly generated (so ignore it) in an Ad-Hoc wireless network. This is the IEEE 802.1x standard used by the wireless network. This field displays the strength of the AP's signal.

If you must choose a channel that is currently in use, choose one with low signal strength for minimum interference. This is the wireless security method used by the wireless network to protect wireless communication between wireless stations, access points and the wired network. Click Refresh to reload the screen. Channel MAC Address Wireless Mode Signal Strength Security Refresh NWA1121-NI User's Guide 53 Chapter 5 Monitor 54 NWA1121-NI User's Guide C HAPT ER 6 Wireless LAN 6.1 Overview This chapter discusses the steps to configure the Wireless Settings screen on the NWA1121-NI.

It also introduces the wireless LAN (WLAN) and some basic scenarios. Figure 17 Wireless Mode In the figure above, the NWA1121-NI allows access to another bridge device (A) and a notebook computer (B) upon verifying their settings and credentials. It denies access to other devices (C and D) with configurations that do not match those specified in your NWA1121-NI.

6.2 What You Can Do in this Chapter • Use the Wireless Settings screen to configure the NWA1121-NI's operation mode (see Section 6.4 on page 60). • Uee the SSID screen to configure up to eight SSID profiles for your NWA1121-NI (see Section 6.5 on page 72). • Use the Security screen to choose the wireless security mode for your NWA1121-NI (see Section 6.6 on page 74).

• Use the RADIUS screen if you want to authenticate wireless users using a RADIUS Server and/or accounting server (see Section 6.7 on page 87). • Use the MAC Filter screen to specify which wireless station is allowed or denied access to the NWA1121-NI (see Section 6.8 on page 89). NWA1121-NI User's Guide 55 Chapter 6 Wireless LAN 6.3 What You Need To Know BSS A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP). Intra-BSS traffic is traffic between wireless clients in the BSS. ESS An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS). Operating Mode The NWA1121-NI can run in four operating modes as follows: • Root AP.

The NWA1121-NI is a wireless access point that allows wireless communication to other devices in the network. • Repeater. The NWA1121-NI acts as a wireless repeater and increase a root AP's wireless coverage area. • Client. The NWA1121-NI acts as a wireless client to access a wireless network. • MBSSID. The Multiple Basic Service Set Identifier (MBSSID) mode allows you to use one access point to provide several BSSs simultaneously. Refer to Chapter 1 on page 11 for illustrations of these wireless applications. SSID The SSID (Service Set IDentifier) is the name that identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID.

In other words, it is the name of the wireless network that clients use to connect to it. Normally, the NWA1121-NI acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the NWA1121-NI does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess. This type of security is fairly weak, however, because there are ways for unauthorized wireless devices to get the SSID. In addition, unauthorized wireless devices can still see the information that is sent in the wireless network. Channel A channel is the radio frequency(ies) used by wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. 56 NWA1121-NI User's Guide Chapter 6 Wireless LAN Wireless Mode The IEEE 802.

1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. Your NWA1121-NI can support 802.11b/g, 802.11n and 802.11b/g/n. MBSSID Traditionally, you needed to use different APs to configure different Basic Service Sets (BSSs). As well as the cost of buying extra APs, there was also the possibility of channel interference. The NWA1121-NI's MBSSID (Multiple Basic Service Set IDentifier) function allows you to use one access point to provide several BSSs simultaneously. You can then assign varying levels of privilege to different SSIDs.

Wireless stations can use different BSSIDs to associate with the same AP. The following are some notes on multiple BSS. • A maximum of four BSSs are allowed on one AP simultaneously. • You must use different WEP keys for different BSSs. If two stations have different BSSIDs (they are in different BSSs), but have the same WEP keys, they may hear each other's communications (but not communicate with each other).

• MBSSID should not replace but rather be used in conjunction with 802.1x security. Wireless Security Wireless security is vital to your network. It protects communications between wireless stations, access points and the wired network. Figure 18 Securing the Wireless Network In the figure above, the NWA1121-NI checks the identity of devices before giving them access to the network.

In this scenario, Computer A is denied access to the network, while Computer B is granted connectivity. The NWA1121-NI secure communications via data encryption, wireless client authentication and MAC address filtering. It can also hide its identity in the network. NWA1121-NI User's Guide 57 Chapter 6 Wireless LAN User Authentication Authentication is the process of verifying whether a wireless device is allowed to use the wireless network. You can make every user log in to the wireless network before they can use it. However, every device in the wireless network has to support IEEE 802.1x to do this. For wireless networks, you can store the user names and passwords for each user in a RADIUS server. This is a server used in businesses more than in homes. If you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized wireless devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network. The following table shows the relative effectiveness of wireless security methods:. Table 9 Wireless Security Levels SECURITY LEVEL Least Secure SECURITY TYPE Unique SSID (Default) Unique SSID with Hide SSID Enabled MAC Address Filtering WEP Encryption IEEE802.1x EAP with RADIUS Server Authentication Wi-Fi Protected Access (WPA) Most Secure WPA2 The available security modes in your NWA1121-NI are as follows: • None. No data encryption. • WEP. Wired Equivalent Privacy (WEP) encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. • 802.

1x-Only. This is a standard that extends the features of IEEE 802.11 to support extended authentication. It provides additional accounting and control features. This option does not support data encryption.

• 802.1x-Static WEP. This provides 802.1x-Only authentication with a static 64bit or 128bit WEP key and an authentication server. • WPA.

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. • WPA2. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA. • WPA2-MIX. This commands the NWA1121-NI to use either WPA2 or WPA depending on which security mode the wireless client uses. • WPA2-PSK. This adds a pre-shared key on top of WPA2 standard.

• WPA2-PSK-MIX.

This commands the NWA1121-NI to use either WPA-PSK or WPA2-PSK depending on which security mode the wireless client uses. Note: To guarantee 802.11n wireless speed, please only use WPA2 or WPA2-PSK security mode. Other security modes may degrate the wireless speed performance to 802.11g. 58 NWA1121-NI User's Guide Chapter 6 Wireless LAN Passphrase A passphrase functions like a password. In WEP security mode, it is further converted by the NWA1121-NI into a complicated string that is referred to as the "key". This key is requested from all devices wishing to connect to a wireless network. PSK The Pre-Shared Key (PSK) is a password shared by a wireless access point and a client during a previous secure connection. The key can then be used to establish a connection between the two parties.

Encryption Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message. Encryption is the process of converting data into unreadable text. This secures information in network communications.

The intended recipient of the data can "unlock" it with a pre-assigned key, making the information readable only to him. The NWA1121-NI when used as a wireless client employs Temporal Key Integrity Protocol (TKIP) data encryption. EAP Extensible Authentication Protocol (EAP) is a protocol used by a wireless client, an access point and an authentication server to negotiate a connection. The EAP methods employed by the NWA1121-NI when in Wireless Client operating mode are Transport Layer Security (TLS), Protected Extensible Authentication Protocol (PEAP), Lightweight Extensible Authentication Protocol (LEAP) and Tunneled Transport Layer Security (TTLS). The authentication protocol may either be Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2) or Generic Token Card (GTC).

Further information on these terms can be found in Appendix D on page 179. RADIUS Remote Authentication Dial In User Service (RADIUS) is a protocol that can be used to manage user access to large networks. It is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. Figure 19 RADIUS Server Setup NWA1121-NI User's Guide 59 Chapter 6 Wireless LAN In the figure above, wireless clients A and B are trying to access the Internet via the NWA1121-NI. The NWA1121-NI in turn queries the RADIUS server if the identity of clients A and U are allowed access to the Internet. In this scenario, only client U's identity is verified by the RADIUS server and allowed access to the Internet. The RADIUS server handles the following tasks: • Authentication which determines the identity of the users. • Authorization which determines the network services available to authenticated users once they are connected to the network. • Accounting which keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server. You should know the IP addresses, ports and share secrets of the external RADIUS server and/or the external RADIUS accounting server you want to use with your NWA1121-NI. You can configure a primary and backup RADIUS and RADIUS accounting server for your NWA1121-NI. 6.4 Wireless Settings Screen Use this screen to choose the operating mode for your NWA1121-NI. Click Network > Wireless LAN > Wireless Settings. The screen varies depending upon the operating mode you select. 60 NWA1121-NI User's Guide Chapter 6 Wireless LAN 6.4.1 Root AP Mode Use this screen to use your NWA1121-NI as an access point.

Select Root AP as the Operation Mode. The following screen displays. Figure 20 Wireless LAN > Wireless Settings: Root AP NWA1121-NI User's Guide 61 Chapter 6 Wireless LAN The following table describes the general wireless LAN labels in this screen. Table 10 Wireless LAN > Wireless Settings: Root AP LABEL Basic Settings Wireless LAN Interface Operation Mode Wireless Mode Select the check box to turn on the wireless LAN on the NWA1121-NI. Select Root AP from the drop-down list.

Select 802.11b/g to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the NWA1121-NI. The transmission rate of your NWA1121-NI might be reduced.

Select 802.11b/g/n to allow IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the NWA1121-NI. The transmission rate of the NWA1121NI might be reduced. Select 802.11n to allow only IEEE802.11n compliant WLAN devices to associate with the NWA1121-NI. Channel Channel Width Select the operating frequency/channel depending on your particular region from the drop-down list box.

This field displays only when you select 802.11n or 802.11b/g/n in the Wireless Mode field. A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300Mbps. However, not all devices support 40MHz channels. Select the channel bandwidth you want to use for your wireless network. It is recommended that you select 20/40MHz. This allows the NWA1121-NI to adjust the channel bandwidth depending on network conditions. Select 20MHz if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding. Select SSID Profile The SSID (Service Set IDentifier) identifies the Service Set with which a wireless station is associated.

Wireless stations associating to the access point (AP) must have the same SSID. You can have up to four SSIDs active at the same time. DESCRIPTION Note: If you are configuring the NWA1121-NI from a computer connected to the wireless LAN and you change the NWA1121-NI's SSID or security settings, you will lose your wireless connection when you press Apply to confirm. You must then change the wireless settings of your computer to match the NWA1121-NI's new settings. # Activve Profile This is the index number of each SSID profile.

Select the check box to enable an SSID profile. Otherwise, clear the check box. Select an SSID Profile from the drop-down list box. Universal Repeater Settings The Universal repeater function allows the NWA1121-NI in root AP or repeater mode to set up a wireless connection between it and another NWA1121-NI in root AP or repeater mode. Note: Universal repeater security is independent of the security settings between the NWA1121-NI and any wireless clients.

Local MAC Address Universal Repeater SSID Profile Local MAC Address is the MAC address of your NWA1121-NI. Select the SSID profile you want to use for universal repeater connections. Note: You can only configure None, WPA-PSK or WPA2-PSK security mode for the SSID used by a universal repeater connection. 62 NWA1121-NI User's Guide Chapter 6 Wireless LAN Table 10 Wireless LAN > Wireless Settings: Root AP (continued) LABEL Advanced Settings Beacon Interval When a wirelessly network device sends a beacon, it includes with it a beacon interval.

This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in lowpower mode before waking up to handle the beacon. A high value helps save current consumption of the access point. Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Active Power Management mode. A high DTIM value can cause clients to lose connectivity with the network. Set the output power of the NWA1121-NI in this field.

If there is a high density of APs in an area, decrease the output power of the NWA1121-NI to reduce interference with other APs. Select one of the following Full (Full Power), 50%, 25%, or 12.5%. See the product specifications for more information on your NWA1121-NI's output power. Select Dynamic to have the AP automatically use short preamble when wireless adapters support it, otherwise the AP uses long preamble. Select Long if you are unsure what preamble mode the wireless adapters support, and to provide more reliable communications in busy wireless networks. RTS/CTS Threshold (Request To Send) The threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to its smallest value (1) turns on the RTS/CTS handshake.
The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. You can use CTS to self or RTS-CTS protection mechanism to reduce conflicts with other wireless networks or hidden wireless clients. The throughput of RTS-CTS is much lower than CTS to self. Using this mode may decrease your wireless performance.
This field is available only when 802.11 b/g/n is selected as the Wireless Mode. Select to enable A-MPDU aggregation. Message Protocol Data Unit (MPDU) aggregation collects Ethernet frames along with their 802.11n headers and wraps them in a 802.
11n MAC header. This method is useful for increasing bandwidth throughput in environments that are prone to high error rates. Short GI This field is available only when 802.11 b/g/n is selected as the Wireless Mode. Select Enabled to use Short GI (Guard Interval). The guard interval is the gap introduced between data transmission from users in order to reduce interference. Reducing the GI increases data transfer rates but also increases interference. Increasing the GI reduces data transfer rates but also reduces interference. The MCS Rate table is available only when 802.11 b/g/n is selected in the Wireless Mode field.

IEEE 802.11n supports many different data rates which are called MCS rates. MCS stands for Modulation and Coding Scheme. This is an 802.11n feature that increases the wireless network performance in terms of throughput. For each MCS Rate (0-15), select either Enabled to have the NWA1121-NI use the data rate. Clear the Enabled check box if you do not want the NWA1121-NI to use the data rate. Turn on the Auto option to have the NWA1121-NI set the data rates automatically to optimize the throughput. DESCRIPTION DTIM Interval Output Power Preamble Type Fragmentation Extension Channel Protection Mode A-MPDU Aggregation MCS Rate Note: You can set the NWA1121-NI to use up to four MCS rates at a time. Apply Cancel Click Apply to save your changes.
Click Cancel to begin configuring this screen afresh. NWA1121-NI User's Guide 63 Chapter 6 Wireless LAN 6.4.2 Repeater Mode Use this screen to have the NWA1121-NI act as a wireless repeater. You need to know the MAC address of the peer device, which also must be in Repeater or Root AP mode.
Figure 21 Wireless LAN > Wireless Settings: Repeater The following table describes the bridge labels in this screen. Table 11 Wireless LAN > Wireless Settings: Repeater LABEL Basic Settings Wireless LAN Interface Operation Mode Select the check box to turn on the wireless LAN on the NWA1121-NI. Select Repeater from the drop-down list. DESCRIPTION 64 NWA1121-NI User's Guide Chapter 6 Wireless LAN Table 11 Wireless LAN > Wireless Settings: Repeater (continued) LABEL Wireless Mode DESCRIPTION Select 802.11b/g to allow both IEEE802.
11b and IEEE802.11g compliant WLAN devices to associate with the NWA1121-NI. The transmission rate of your NWA1121-NI might be reduced. Select 802.11b/g/n to allow IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the NWA1121-NI. The transmission rate of the NWA1121NI might be reduced. Select 802.

11n to allow only IEEE802.11n compliant WLAN devices to associate with the NWA1121-NI. Channel Channel Width Select the operating frequency/channel depending on your particular region from the drop-down list box. This field displays only when you select 802.11n or 802.11b/g/n in the Wireless Mode field. A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300Mbps. However, not all devices support 40MHz channels. Select the channel bandwidth you want to use for your wireless network. It is recommended that you select 20/40MHz.
This allows the NWA1121-NI to adjust the channel bandwidth depending on network conditions. Select 20MHz if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding. Universal Repeater Settings The Universal repeater function allows the NWA1121-NI in root AP or repeater mode to set up a wireless connection between it and another NWA1121-NI in root AP or repeater mode. Note: Universal repeater security is independent of the security settings between the NWA1121-NI and any wireless clients. Local MAC Address Universal Repeater SSID Profile Local MAC Address is the MAC address of your NWA1121-NI.
Select the SSID profile you want to use for universal repeater connections with an AP or repeater or regular wireless connections with wireless clients. Note: You can only configure None, WPA-PSK or WPA2-PSK security mode for the SSID used by a universal repeater connection. Root MAC Address Advanced Settings Beacon Interval When a wirelessly network device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in lowpower mode before waking up to handle the beacon.
A high value helps save current consumption of the access point. Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Active Power Management mode. A high DTIM value can cause clients to lose connectivity with the network. Set the output power of the NWA1121-NI in this field. If there is a high density of APs in an area, decrease the output power of the NWA1121-NI to reduce interference with other APs.