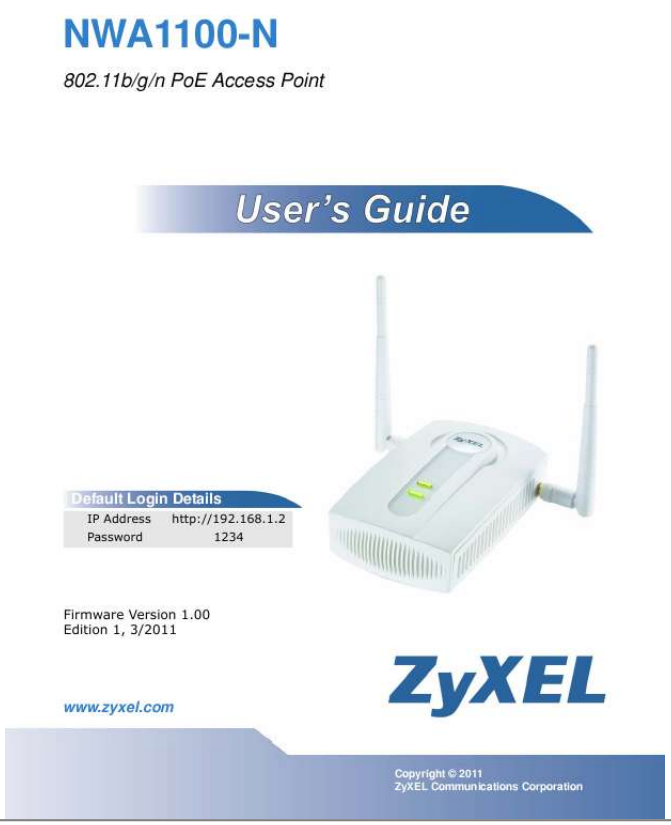

Manual abstract:

This can help you quickly pinpoint the information you require. You can also enter text directly into the toolbar in Reader. · To quickly move around within a page, press the [SPACE] bar. This turns your cursor into a "hand" with which you can grab the page and move it around freely on your screen. · Embedded hyperlinks are actually cross-references to related text. Click them to jump to the corresponding section of the User's Guide PDF. Related Documentation · Quick Start Guide The Quick Start Guide is designed to help you get your NWA up and running right away. @@@@@@@@· Knowledge Base If you have a specific question about your product, the answer may be here. This is a collection of answers to previously asked questions about ZyXEL products. · Forum This contains discussions on ZyXEL products.

Learn from others who use ZyXEL products and share your experiences as well. Customer Support Should problems arise that cannot be solved by the methods listed above, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. See http://www.zyxel.

com/web/contact_us.php for contact information. Please have the following information ready when you contact an office. · Product model and serial number. · Warranty Information.

· Date that you received your device. · Brief description of the problem and the steps you took to solve it. 4 NWA1100-N User's Guide Document Conventions Document Conventions Warnings and Notes These are how warnings and notes are shown in this User's Guide. Warnings tell you about things that could harm you or your NWA. Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations. Syntax Conventions · The NWA1100-N may be referred to as the "NWA", the "device", or the "ZyXEL Device" in this User's Guide. · Product labels, screen names, field labels and field choices are all in bold font. · A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard. · "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.

· A right angle bracket (>) within a screen name denotes a mouse click. For example, Maintenance > Log > Log Setting means you first click Maintenance in the navigation panel, then the Log sub menu and finally the Log Setting tab to get to that screen. · Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on. · "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words". Icons Used in Figures Figures in this User's Guide use the following generic icons.

The NWA icon is not an exact representation of your NWA. Graphics in this book may differ slightly from the product due to differences in operating systems, operating system versions, or if you installed updated firmware/software for your device. Every effort has been made to ensure that the information in this manual is accurate. NWA1100-N User's Guide 5 Document Conventions Table 1 Common Icons NWA Computer Notebook Server Printer Firewall Switch Router Internet Cloud 6 NWA1100-N User's Guide Safety Warnings Safety Warnings · · · · · Do NOT use this product near water, for example, in a wet basement or near a swimming pool. Do NOT expose your device to dampness, dust or corrosive liquids.

Do NOT store things on the device. Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning. Connect ONLY suitable accessories to the device. Do NOT open the device or unit.

Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information. Make sure to connect the cables to the correct ports. Place connecting cables carefully so that no one will step on them or stumble over them. Always disconnect all cables from this device before servicing or disassembling. Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). Do NOT remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet. Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.

Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution. If the power adaptor or cord is damaged, remove it from the device and the power source. Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one. Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning. Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device. Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s). If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

The PoE (Power over Ethernet) devices that supply or receive power and their connected Ethernet cables must all be completely indoors. This product is for indoor use only (utilisation intérieure exclusivement). · · · · · · · · · · · · · · · Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately. NWA1100-N User's Guide 7 Safety Warnings 8 NWA1100-N User's Guide Contents Overview Contents Overview User's Guide ....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

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

. 137 NWA1100-N User's Guide 9 Contents Overview 10 NWA1100-N User's Guide Table of Contents Table of Contents About This User's Guide .....

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

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

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

.....
.....
.. 3 Document Conventions...
.....

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

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

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

..... 5 Safety Warnings.....
.....
.....
.....

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

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

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

..... 7 Contents Overview .....
.....
.....
.....

.....

..... 243 16 NWA1100-N User's Guide PART I User's Guide 17 18 CHAPT E R 1 Introducing the NWA This chapter introduces the main applications and features of the NWA. It also discusses the ways you can manage your NWA. 1.

1 Introducing the NWA Your NWA extends the range of your existing wired network without additional wiring, providing easy network access to mobile users. The NWA 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, Wi-Fi 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 NWA 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 Applications for the NWA The NWA can be configured to use the following WLAN operating modes: 1 2 3 4 5 Access Point Bridge/Repeater AP + Bridge Wireless Client MBSSID Applications for each operating mode are shown below.

NWA1100-N User's Guide 19 Chapter 1 Introducing the NWA 1.2.1 Access Point The NWA is an ideal access solution for wireless Internet connection. A typical Internet access application for your NWA is shown as follows. Stations A, B and C can access the wired network through the NWAs. Figure 1 Access Point Application 1.2.2 Bridge / Repeater The NWA can act as a wireless network bridge and establish wireless links with other APs. In the figure below, the two NWAs (A and B) are connected to independent wired networks and have a bridge connection (A can communicate with B) at the same time. A NWA in repeater mode (C in Figure 3) has no Ethernet connection.

When the NWA is in bridge mode, you should enable Spanning Tree Protocol (STP) to prevent bridge loops. When the NWA is in Bridge / Repeater mode, security between APs (the Wireless Distribution System or WDS) is independent of the security between the wireless stations and the AP. If you do not enable WDS security, traffic between APs is not encrypted. When WDS security is enabled, both APs must use the same pre-shared key. See Section 6.4.2 on page 65 for more details. Once the security settings of peer sides match one another, the connection between devices is made. 20 NWA1100-N User's Guide Chapter 1 Introducing the NWA At the time of writing, WDS security is compatible with other ZyXEL NWA-series access points only. Refer to your other access point's documentation for details.

Figure 2 Bridge Application Figure 3 Repeater Application 1.2.2.1 Bridge / Repeater Mode Example In the example below, when both NWAs are in Bridge mode, they form a WDS (Wireless Distribution System) allowing the computers in LAN 1 to connect to the computers in LAN 2.

Figure 4 Bridging Example Be careful to avoid bridge loops when you enable bridging in the NWA.

Bridge loops cause broadcast traffic to circle the network endlessly, resulting in possible throughput degradation and NWA1100-N User's Guide 21 Chapter 1 Introducing the NWA disruption of communications. The following examples show two network topologies that can lead to this problem: · If two or more NWAs (in bridge mode) are connected to the same hub. Figure 5 Bridge Loop: Two Bridges Connected to Hub · If your NWA (in Bridge mode) is connected to a wired LAN while communicating with another wireless bridge that is also connected to the same wired LAN. Figure 6 Bridge Loop: Bridge Connected to Wired LAN To prevent bridge loops, ensure that you enable STP in the Wireless screen or your NWA is not set to bridge mode while connected to both wired and wireless segments of the same LAN. 1.

2.3 AP + Bridge In AP+Bridge mode, the NWA supports both AP and bridge connection at the same time. In the figure below, A and B use X as an AP to access the wired network, while X and Y communicate in bridge mode. Using AP + Bridge mode, your NWA can extend the range of the WLAN. In the figure below, A and B act as AP + Bridge devices that forward traffic between associated wireless workstations and the wired LAN. 22 NWA1100-N User's Guide Chapter 1 Introducing the NWA When the NWA is in AP+Bridge mode, security between APs (the Wireless Distribution System or WDS) is independent of the security between the wireless stations and the AP. If you do not enable WDS security, traffic between APs is not encrypted. When WDS security is enabled, both APs must use the same pre-shared key. See Section 6.4.

3 on page 69 for more details. Unless specified, the term "security settings" refers to the traffic between the wireless stations and the NWA. Figure 7 AP + Bridge Application 1.2.4 Wireless Client The NWA 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 NWA in Wireless Client mode. Figure 8 Wireless Client Application NWA1100-N User's Guide 23 Chapter 1 Introducing the NWA 1.2.5 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 Multiple BSS (MBSSID) mode, the NWA provides multiple virtual APs, each forming its own BSS and using its own individual SSID profile. You can configure up to eight SSID profiles, and have up to four 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 9 Multiple BSSs 24 NWA1100-N User's Guide Chapter 1 Introducing the NWA 1.3 Ways to Manage the NWA Use any of the following methods to manage the NWA. · Web Configurator. This is recommended for everyday management of the NWA using a (supported) web browser. · Command Line Interface. Line commands are mostly used for troubleshooting by service engineers. · FTP (File Transfer Protocol) for firmware upgrades. · SNMP (Simple Network Management Protocol). The device can be monitored by an SNMP manager. 1.

4 Configuring Your NWA's Security Features Your NWA 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 NWA. Follow the suggestions below to improve security on your NWA and network. 1.4.1 Control Access to Your Device Ensure only people with permission can access your NWA. · Control physical access by locating devices in secure areas, such as locked rooms. Most NWAs 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 NWA, such as the password used for accessing the NWA'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. · Avoid setting a long timeout period before the NWA's web configurator automatically times out. A short timeout reduces the risk of unauthorized person accessing the web configurator while it is left idle. · See Chapter 5 on page 55 for instructions on changing your password and setting the timeout period.

· Configure remote management to control who can manage your NWA. See Chapter 12 on page 109 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. If your NWA has a wireless function, take the following measures to improve wireless security. · Enable wireless security on your NWA. Choose the most secure encryption method that all devices on your network support. See Section 8.4 on page 87 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. NWA1100-N User's Guide 25 Chapter 1 Introducing the NWA · 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 6.4 on page 62 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 10.4 on page 103 for directions on configuring the MAC filter. 1.5 Good Habits for Managing the NWA Do the following things regularly to make the NWA more secure and to manage it more effectively.

1.6 Hardware Connections See your Quick Start Guide for information on making hardware connections.
26 NWA1100-N User's Guide Chapter 1 Introducing the NWA 1.7 LEDs Figure 10 LEDs Table 2 LEDs LABEL 1 LED SYS COLOR Green Red STATUS On Flashing Off DESCRIPTION The NWA is receiving power and ready for use. There is system error and the NWA cannot boot up. The NWA is not receiving power. The wireless adaptor WLAN is active.
The wireless adaptor WLAN is active, and transmitting or receiving data. The wireless adaptor WLAN is not active. The NWA has a 10/100 Mbps Ethernet connection. The NWA has a 10/100 Mbps Ethernet connection and is sending or receiving data. The NWA has a 1000 Mbps Ethernet connection.
The NWA has a 1000 Mbps Ethernet connection and is sending/receiving data. The NWA does not have an Ethernet connection. 2 WLAN Green On Blinking Off 3 ETHERNET Green On Blinking Yellow On Blinking Off NWA1100-N User's Guide 27 Chapter 1 Introducing the NWA 28 NWA1100-N User's Guide CHAPT E R 2 Introducing the Web Configurator This chapter describes how to access the NWA'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 NWA (refer to the Quick Start Guide). Launch your web browser. Type "192.168.1.2" as the URL (default).

The login screen appears. Figure 11 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. Note: If you do not change the password, the following screen appears every time you login. Figure 12 Change Password Screen NWA1100-N User's Guide 29 Chapter 2 Introducing the Web Configurator You should now see the Status screen. See Chapter 2 on page 29 for details about the Status screen. Note: The management session automatically times out when the time period set in the Administrator Inactivity Timer field expires (default five minutes).
Simply log back into the NWA if this happens. 2.2 Resetting the NWA 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 NWA. This replaces the current configuration file with the factorydefault configuration file. This means that you will lose all the settings you previously configured.
The password will be reset to "1234". Figure 13 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 10 seconds (the lights will begin to blink).
Use this method for cases when the password or IP address of the NWA is not known. Use the web configurator to restore defaults (refer to Section 15.7 on page 133). 2.3 Navigating the Web Configurator The following summarizes how to navigate the web configurator from the Status screen. 30 NWA1100-N User's Guide Chapter 2 Introducing the Web Configurator Check the status bar at the bottom of the screen when you click Apply or OK to verify that the configuration has been updated. Figure 14 Status Screen of the Web Configurator · Click the links on the left of the screen to configure advanced features such as SYSTEM (General, Password and Time), WIRELESS (Wireless Settings, SSID, Security, RADIUS, MAC Filter), IP, REMOTE MGNT (Telnet, FTP, WWW and SNMP), CERTIFICATES, and LOGS (View Log and Log Settings). · Click MAINTENANCE to view information about your NWA or upgrade configuration and firmware files. Maintenance features include Association List, Channel Usage, F/W (firmware) Upload, Configuration File (Backup, Restore and Default) and Restart. · Click LOGOUT at any time to exit the web configurator.

NWA1100-N User's Guide 31 Chapter 2 Introducing the Web Configurator 32 NWA1100-N User's Guide CHAPT E R 3 Status Screens The Status screens display when you log into the NWA, or click Status in the navigation menu. Use the Status screens to look at the current status of the device, system resources, and interfaces. The Status screens also provide detailed information about system statistics, associated wireless clients, and logs. 3.1 The Status Screen Use this screen to get a quick view of system, Ethernet, WLAN and other information regarding your NWA. Click Status. The following screen displays. Figure 15 The Status Screen The following table describes the labels in this screen. Table 3 The Status Screen LABEL Automatic Refresh Interval Refresh Now System Information DESCRIPTION Select how often you want the NWA to update this screen. Click this to update this screen immediately.
NWA1100-N User's Guide 33 Chapter 3 Status Screens Table 3 The Status Screen (continued) LABEL Device Name WLAN Operation Mode DESCRIPTION This field displays the NWA system name. It is used for identification. You can change this in the System > General screen's Device Name field. This field displays the current operating mode of the first wireless module (Access Point, Bridge/Repeater, AP+Bridge, Wireless Client, or MBSSID). You can change the operating mode in the Wireless > 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 > F/W Upload. This field displays the date and time configured on the NWA. You can change this in the System > Time Setting screen.
Firmware Version Current Date Time Ethernet Information LAN MAC Address This displays the MAC (Media Access Control) address of the NWA on the LAN. Every network device has a unique MAC address which identifies it across the network. This field displays the current IP address of the NWA 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. IP Address Subnet Mask Gateway IP Address WLAN Information SSID Channel Status Security Mode System Resources System Up Time CPU Usage This field displays the elapsed time since the NWA was turned on. This field displays what percentage of the NWA's processing ability is currently being used.

The higher the CPU usage, the more likely the NWA is to slow down.

This field displays what percentage of the NWA's volatile memory is currently in use. The higher the memory usage, the more likely the NWA is to slow down. Some memory is required just to start the NWA and to run the web configurator. This field displays the SSID (Service Set Identifier). This is available only when the WLAN Operation Mode is Wireless Client. The channel or frequency used by the NWA to send and receive information. This shows the current status of the wireless LAN. This is available only when the WLAN Operation Mode is Wireless Client. This displays the security mode the NWA is using. Memory Usage Interface Status Interface Status This column displays each interface of the NWA. This field indicates whether or not the NWA is using the interface. For each interface, this field displays Up when the NWA is using the interface and Down when the NWA is not using the interface. Channel Rate Click this to see which wireless channels are currently in use in the local area. See Section 15.

5 on page 130. 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. 34 NWA1100-N User's Guide Chapter 3 Status Screens Table 3 The Status Screen (continued) LABEL LAN DESCRIPTION This field displays the number of wireless clients currently associated to the first wireless module. Each wireless module supports up to 32 concurrent associations.

This field displays the number of wireless clients currently associated to the second wireless module. Each wireless module supports up to 32 concurrent associations. WLAN System Status Statistics Association List View Log Click this link to view port status and packet specific statistics. See Section 3.1.1 on page 35. Click this to see a list of wireless clients currently associated to each of the NWA's wireless modules. See Section 15.4 on page 129. Click this to see a list of logs produced by the NWA.

See Chapter 14 on page 123. 3.1.1 System Statistics Screen 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. The fields in this screen vary according to the current wireless mode of each WLAN adaptor. Click Status > Statistics. The following screen pops up.

Figure 16 System Status: Statistics The following table describes the labels in this screen. Table 4 System Status: Show Statistics LABEL Description 802.11 Mode Channel ID RX PKT TX PKT Retry Count FCS Error Count Poll Interval Set Interval Stop DESCRIPTION This is the wireless LAN adaptor. This field shows which 802.11 mode the NWA is using.

Click this to see which wireless channels are currently in use in the local area. See Section 15.5 on page 130. 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 ratio percentage showing the total number of checksum error of received packets (RX) over total 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. NWA1100-N User's Guide 35 Chapter 3 Status Screens 36 NWA1100-N User's Guide CHAPT E R 4 Tutorial This chapter first provides an overview of how to configure the wireless LAN on your NWA, and then gives step-by-step guidelines showing how to configure your NWA 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 NWA and how to set up the wireless LAN in each wireless mode. See Section 4.1.

3 on page 38 for links to more information on each step. 4.1.1 Choosing the Wireless Mode · Use Access Point operating mode if you want to allow wireless clients to access your wired network, all using the same security and Quality of Service (QoS) settings. See Section 1.2.1 on page 20 for details. · Use Bridge / Repeater operating mode if you want to use the NWA to communicate with other access points. See Section 1.2.

2 on page 20 for details. · Use AP + Bridge operating mode if you want to use the NWA as an access point (see above) while also communicating with other access points. See Section 1.2.3 on page 22 for details.

· Use Wireless Client operating mode if you want to use the NWA to access a wireless network. See Section 1.2.4 on page 23 for details. The NWA is a bridge when other APs access your wired Ethernet network through the NWA.

· Use MBSSID (Multiple Basic Service Set Identifier) operating mode if you want to use the NWA as an access point with some groups of users having different security or QoS settings from other groups of users. See Section 1.2.5 on page 24 for details. 4.1.2 Wireless LAN Configuration Overview The following figure shows the steps you should take to configure the wireless settings according to the operating mode you select. Use the Web Configurator to set up your NWA's wireless network NWA1100-N User's Guide 37 Chapter 4 Tutorial (see your Quick Start Guide for information on setting up your NWA and accessing the Web Configurator). Select the WLAN Adaptor you want to configure. Select Operation Mode.

Access Point Bridge / Repeater AP + Bridge Wireless Client MBSSID Select Wireless Mode, SSID Profile, and Channel. Select Wireless Mode, SSID Profile, and Channel. Select Wireless Mode, SSID Profile, and Channel. Select the AP you want to connect to. Select Wireless Mode and SSID Profile. Configure RADIUS authentication (optional). Configure RADIUS authentication (optional). Configure RADIUS authentication (optional). Configure Security Settings. Configure the selected SSID Profiles.

Configure MAC Filter (optional). Configure MAC Filter (optional). Configure Security Settings. Configure RADIUS authentication (optional). Configure MAC Filter (optional).

Check your settings and test. 4.1.3 Further Reading Use these links to find more information on the steps: · Selecting a WLAN Adaptor: see Section 6.4.

1 on page 63. · Choosing 802.11 Mode: see Section 6.4.1 on page 63. · Choosing a wireless Channel ID: see Section 6.4.1 on page 63. · Choosing a Security mode: see Section 8.4.

1 on page 89. · Configuring an external RADIUS server: see Section 9.4 on page 100. · Configuring MAC Filtering: see Section 10.1 on page 102. 38 NWA1100-N User's Guide Chapter 4 Tutorial 4.2 How to Configure Multiple Wireless Networks In this example, you have been using your NWA as an access point for your office network (See your Quick Start Guide for information on how to set up your NWA in Access Point mode). Now your network is expanding and you want to make use of the MBSSID feature (see Section 8.

2.4 on page 139) 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 Access Point 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 NWA is marked Z, the main network router is marked A, and your network printer is marked B.

B A Z NWA1100-N User's Guide 39 Chapter 4 Tutorial 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. 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 5 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 NWA (see Section 2.2 on page 35). Click Wireless > SSID.

The SSID screen appears. Select the Profile1 check-box and click Edit. 2 3 Rename the Profile Name as SSID01. Click Save. 4 Repeat Step 2 and 3 to change Profile2 and Profile3 to VoIP_SSID and Guest_SSID. 40 NWA1100-N User's Guide Chapter 4 Tutorial 4.2.1.1 MBSSID 1 Go to Wireless > Wireless Settings. Select MBSSID from the Operating 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 NWA1100-N User's Guide 41 Chapter 4 Tutorial 4.2.2 Configure the Standard Network 1 Click Wireless > SSID. Select SSID01 and click Edit.

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 Enable Intra-BSS Traffic blocking check-box. Click Save. 42 NWA1100-N User's Guide Chapter 4 Tutorial 3 Next, click Wireless > Security. Select SecProfile1 and click Edit. 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 > SSID. Select VoIP_SSID and click Edit. NWA1100-N User's Guide 43 Chapter 4 Tutorial 2 Select SecProfile2 as the Security Profile for the VoIP network. Select the Hidden SSID checkbox. Select WMM-Voice in the QoS field to give VoIP the highest priority in the wireless network. Click Save.

3 4 Next, click Wireless > Security. Select SecProfile2 and click Edit. 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. 44 NWA1100-N User's Guide Chapter 4 Tutorial 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 > SSID. Select Guest_SSID and click Edit. 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-best effort in the QoS field to give the guest a lower QoS priority. Select the check-box of Enable Intra-BSS Traffic blocking. Click Save. 3 4 NWA1100-N User's Guide 45 Chapter 4 Tutorial 5 Next, click Wireless > Security.

Select SecProfile3 and click Edit. 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. 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. 7 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 Save.

· 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. 46 NWA1100-N User's Guide Chapter 4 Tutorial 4.3 NWA Setup in AP and Wireless Client Modes This example shows you how to restrict wireless access to your NWA. 4.

3.1 Scenario In the figure below, there are two NWAs (A and B) in the network. A is in Access Point (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 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 17 FTP Server Connected to a Wireless Client 4.3.2 Configuring the NWA in Access Point Mode Before setting up the NWA as a wireless client (B), you need to make sure there is an access point to connect to.

Use the Ethernet port on NWA (A) to configure it via a wired connection. NWA1100-N User's Guide 47 Chapter 4 Tutorial Log into the Web Configurator on NWA (A) and go to the Wireless > Wireless Settings screen. 1 2 3 4 5 Set the Operation Mode to Access Point. Select the Wireless Mode. In this example, select 802.11b/g. Select Profile1 as the SSID Profile. Choose the Channel you want NWA (A) to use. Click Apply. 48 NWA1100-N User's Guide Chapter 4 Tutorial 6 Go to Wireless > SSID.

Select Profile1 and click Edit. 7 8 9 Change the SSID to AP-A. Select SecProfile1 in the Security field. Select the check-box for Enable Intra-BSS Traffic blocking so the client cannot access other clients on the same wireless network. 10 Click Save.

11 Go to Wireless > Security. Select SecProfile1. Click Edit. NWA1100-N User's Guide 49 Chapter 4 Tutorial 12 Configure WPA-PSK as the Security Mode and enter ThisisMyPreSharedKey in the PreShared Key field. 13 Click Apply to finish configuration for NWA (A).

4.3.3 Configuring the NWA in Wireless Client Mode The NWA (B) should have a wired connection before it can be set to wireless client operating mode. Connect your NWA to the FTP server. Login to NWA (B)'s Web Configurator and go to the Wireless > Wireless Settings screen. Follow these steps to configure station B. 1 Select Wireless Client as Operation Mode. Click Apply. 2 Click on the Site Survey tab. A window should pop up which contains a list of all available wireless devices within your NWA's range.

50 NWA1100-N User's Guide Chapter 4 Tutorial 3 Find and select NWA1100-N-A's SSID: NWA-1100-A. Click Selected. 4 Go to Wireless > Security to configure the NWA to use the same security mode and Pre-Shared Key as NWA1100-N-A: WPA-PSK/ThisisMyPreSharedKey. Click Apply. Figure 18 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 NWA (B) (See Chapter 10 on page 102 for more information on MAC Filter). 1 Go to Wireless > MAC Filter. Select MacProfile1 and click Edit. NWA1100-N User's Guide 51 Chapter 4 Tutorial 2 Select Allow Listed in the Access Control Mode field.

Enter the MAC addresses of the wireless clients (W, Y and Z) you want to associate with the NWA. Click Apply. Now, only the authorized wireless clients (W, Y and Z) can access the FTP server. 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. 52 NWA1100-N User's Guide PART II Technical Reference The appendices provide general information. Some details may not apply to your NWA. 53 54 CHAPT E R 5 System Screens 5.1 Overview This chapter provides information and instructions on how to identify and manage your NWA over the network.

Figure 19 NWA Setup In the figure above, the NWA connects to a Domain Name Server (DNS) server to avail of a domain name. It also connects to an Network Time Protocol (NTP) server to set the time on the device. 5.2 What You Can Do in this Chapter · Use the System > General screen to specify the System Name and Ethernet Data Rate value (see Section 5.4 on page 57) . · Use the System > Password screen to manage the password for your NWA (see Section 5.4.1 on page 57). · Use the System > Time Setting screen to change your NWA's time and date. This screen allows you to configure the NWA's time based on your local time zone (see Section 5.

5 on page 58). 5.3 What You Need To Know IP Address Assignment Every computer on the Internet must have a unique IP address. If your networks are isolated from the Internet, for instance, only between your two branch offices, you can assign any IP addresses NWA1100-N User's Guide 55 Chapter 5 System Screens to the hosts without problems. @@Table 6 Private IP Address Ranges 10.

0.0.0 172.16.0.

0 192.168.0.0 10.255.255.255 172.31.255.255 192.

168.255.255 You can obtain your IP address from the IANA, from an ISP or have it assigned by a private network. @@On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses. Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space. IP Address and Subnet Mask Similar to the way houses on a street share a common street name, computers on a LAN share one common network number. Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask. If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established.

The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.

168.1.1 to 192.168.1.

254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network. Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.2, for your device, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the device unless you are instructed to do otherwise. 56 NWA1100-N User's Guide Chapter 5 System Screens 5.

4 General Screen Use the General screen to identify your NWA over the network. Click System > General. The following screen displays. Figure 20 System > General The following table describes the labels in this screen. Table 7 System > General LABEL System Settings System Name Type a descriptive name to identify the NWA in the Ethernet network. This name can be up to 15 alphanumeric characters long. Spaces are not allowed, but dashes "-" are accepted. Ethernet Data Rate Ethernet Data Rate Apply Cancel Select an Ethernet port speed and duplex mode from the drop-down list. Select Auto if you would like to have the system configure this automatically. Click Apply to save your changes.
Click Cancel to reload the previous configuration for this screen. DESCRIPTION 5.4.1 Password Screen Use this screen to control access to your NWA by assigning a password to it. Click System > Password.
The following screen displays. Figure 21 System > Password NWA1100-N User's Guide 57 Chapter 5 System Screens The following table describes the labels in this screen. Table 8 System > Password LABEL Current Password New Password Retype to Confirm Apply Reset DESCRIPTIONS Type in your existing system password. Type your new system password (max 19 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype your new system password for confirmation. Click Apply to save your changes. Click Reset to reload the previous configuration for this screen. 5.5 Time Screen Use this screen to change your NWA's time and date, click System > Time. The following screen displays. Figure 22 System > Time The following table describes the labels in this screen. Table 9 System > Time LABEL Current Time and Date Current Date Current Time This field displays the last updated date from the time server. This field displays the time of your NWA. Each time you reload this page, the NWA synchronizes the time with the time server (if configured).

Time and Date Setup Enable NTP client update NTP server Select this to have the NWA use the predefined list of Network Time Protocol (NTP) servers. Select an NTP server from the drop-list box. DESCRIPTION 58 NWA1100-N User's Guide Chapter 5 System Screens Table 9 System > Time (continued) LABEL Manual IP Time Zone Setup Time Zone Apply Refresh Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT). Click Apply to save your changes. Click Refresh to reload the previous configuration for this screen. DESCRIPTION Enter the IP address or URL of your time server. Check with your ISP/ network administrator if you are unsure of this information. 5.6 Technical Reference This section provides some technical information about the topics covered in this chapter.
5.6.1 Pre-defined NTP Time Servers List When you turn on the NWA for the first time, the date and time start at 2000-01-01 00:00:00. When you select Auto in the System > Time Setting screen, the NWA then attempts to synchronize with one of the following pre-defined list of NTP time servers. The NWA continues to use the following pre-defined list of NTP time servers if you do not specify a time server or it cannot synchronize with the time server you specified.
Table 10 Default Time Servers ntp1.cs.wisc.edu ntp1.gbg.
netnod.se ntp2.cs.wisc.edu tock.usno.navy.mil ntp3.cs.wisc.

edu ntp.cs.strath.ac.uk ntp1.sp.se time1.stupi.se tick.stdtime.
gov.tw tock.stdtime.gov.tw time.
stdtime.gov.tw When the NWA uses the pre-defined list of NTP time servers, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then the NWA goes through the rest of the list in order from the first one tried until either it is successful or all the pre-defined NTP time servers have been tried. NWA1100-N User's Guide 59 CHAPT E R 6 Wireless Settings Screen 6.
1 Overview This chapter discusses the steps to configure the Wireless Settings screen on the NWA. It also introduces the wireless LAN (WLAN) and some basic scenarios. Figure 23 Wireless Mode In the figure above, the NWA 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 NWA. 6.2 What You Can Do in this Chapter Use the Wireless > Wireless Settings screen to configure the NWA's operation mode (see Section 6.4 on page 62). NWA1100-N User's Guide 60 Chapter 6 Wireless Settings Screen 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 NWA can run in four operating modes as follows: · AP (Access Point). The NWA is wireless access point that allows wireless communication to other devices in the network. · Bridge/Repeater. The NWA acts as a wireless network bridge and establishes wireless links with other APs. You need to know the MAC address of the peer device, which also must be in bridge mode. The NWA can establish up to five wireless links with other APs. · AP+Bridge. The NWA functions as a bridge and access point simultaneously.
· Wireless Client. The NWA acts as a wireless client to access a wireless network. · MBSSID Mode. 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 19 for illustrations of these wireless applications. SSID 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. Normally, the NWA acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the NWA 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 IEEE 802.11a/b/g 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. NWA1100-N User's Guide 61 Chapter 6 Wireless Settings Screen 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 NWA can support 802.

11b/g 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 NWA'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. 6.4 Wireless Settings Screen Use this screen to choose the operating mode for your NWA.

Click Wireless > Wireless Settings. The screen varies depending upon the operating mode you select. 62 NWA1100-N User's Guide Chapter 6 Wireless Settings Screen 6.4.1 Access Point Mode Use this screen to use your NWA as an access point.

Select Access Point as the Operation Mode. The following screen displays. Figure 24 Wireless > Wireless Settings: Access Point The following table describes the general wireless LAN labels in this screen. Table 11 Wireless > Wireless Settings: Access Point LABEL Basic Settings Operation Mode Wireless Mode Select Access Point from the drop-down list. Select 802.11b/g to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the NWA. The transmission rate of your NWA might be reduced. Select 802.

11b/g/n to allow IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the Device. The transmission rate of the NWA might be reduced. DESCRIPTION NWA1100-N User's Guide 63 Chapter 6 Wireless Settings Screen Table 11 Wireless > Wireless Settings: Access Point (continued) LABEL SSID Profile DESCRIPTION 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. Select an SSID Profile from the drop-down list box. Note: If you are configuring the NWA from a computer connected to the wireless LAN and you change the NWA'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 NWA's new settings.

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 802.11 b/g/n in the 802.11 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 20/40 (20/40 MHz). This allows the NWA to adjust the channel bandwidth depending on network conditions. Select 20 MHz if you want to lessen radio interference with other wireless devices in your neighborhood.

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 NWA in this field. If there is a high density of APs in an area, decrease the output power of the NWA to reduce interference with other APs. Select one of the following Full (Full Power), 50%, 25%, 12.5% or Min (Minimum).

See the product specifications for more information on your NWA'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. DTIM Interval Output Power Preamble Type Fragmentation 64 NWA1100-N User's Guide Chapter 6 Wireless Settings Screen Table 11 Wireless > Wireless Settings: Access Point (continued) LABEL Rates Configuration DESCRIPTION This section controls the data rates permitted for clients.

For each Rate, select an option from the Configuration list. The options are: · · · Basic (1~11 Mbps only): Clients can always connect to the access point at this speed. Optional: Clients can connect to the access point at this speed, when permitted to do so by the AP. Disable: Clients cannot connect to the access point at this speed. MCS Table The MCS Rate table is available only when 802.

11 b/g/n is selected in the 802.11 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 Enable (default) to have the NWA use the data rate. Select Disable if you do not want the NWA to use the data rate. Apply Cancel Click Apply to save your changes. Click Cancel to begin configuring this screen afresh.