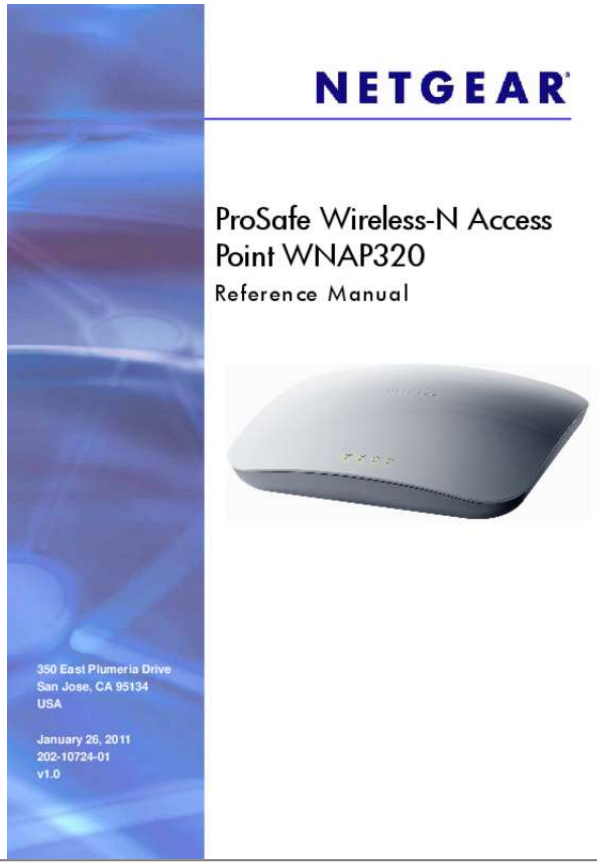

Manual abstract:

@@@@@@Other brand and product names are registered trademarks or trademarks of their respective holders. Statement of Conditions To improve internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use, or application of, the product(s) or circuit layout(s) described herein. 61 Restore the Wireless Access Point to the Factory Default Settings . 62 Reboot the Wireless Access Point without Restoring the Default Configuration . 88 Configure the Wireless Access Point for Repeater Mode . 92 Configure the Wireless Access Point for Client Mode . 99 You Cannot Access the Internet or the LAN from a Wireless-Capable Computer . 99 You Cannot Configure the Wireless Access Point from a Browser . 101 Testing the Path from Your Computer to a Remote Device .

Introduction 1 This chapter introduces the ProSafe Wireless-N Access Point WNAP320 and describes some of the key features. This chapter includes the following sections: •••••About the ProSafe Wireless-N Access Point WNAP320 on this page What Is In the Box? On page 7 System Requirements on page 7 Key Features and Standards on page 7 Hardware Description on page 10 About the ProSafe Wireless-N Access Point WNAP320 The ProSafe Wireless-N Access Point WNAP320 is the basic building block of a wireless LAN infrastructure. It provides connectivity between wired Ethernet networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices. The wireless access point provides wireless connectivity to multiple wireless network devices within a fixed range or area of coverage—interacting with a wireless network interface card (NIC) through an antenna. Typically, an individual in-building wireless access point provides a maximum connectivity area of about a 500-foot radius.

The ProSafe Wireless-N Access Point WNAP320 can support up to 64 users simultaneously in a range of several hundred feet. The ProSafe Wireless-N Access Point WNAP320 acts as a bridge between the wired LAN and wireless clients. Connecting multiple wireless access points through a wired Ethernet backbone can further increase the wireless network coverage. As a mobile computing device moves out of the range of one wireless access point, it moves into the range of another. As a result, wireless clients can freely roam from one wireless access point to another and still maintain seamless connection to the network.

The autosensing capability of the ProSafe Wireless-N Access Point WNAP320 allows packet transmission at up to 300 Mbps, or at reduced speeds to compensate for distance or electromagnetic interference. The product package should contain the following items: ••••••ProSafe Wireless-N Access Point WNAP320 Power adapter and cord (12 VCD, 1. 0A) Straight-through Category 5 Ethernet cable NETGEAR WNAP320 Wireless-N Access Point Installation Guide Resource CD, which includes this manual Wall-mount kit made up of brackets and hardware Contact your reseller or customer support in your area if there are any missing or damaged parts. Asp for the telephone number of customer support in your area. You should keep the Installation Guide, along with the original packing materials, and use the packing materials to repack the wireless access point if you need to return it for repair. To qualify for product updates and product warranty, NETGEAR encourages you to register on the NETGEAR website at http://my. System Requirements Before installing the wireless access point, make sure that your system meets these requirements: ••••••A 10/100/1000 Mbps local area network device such as a hub or switch The Category 5 UTP straight-through Ethernet cable with RJ-45 connector included in the package, or one like it A 100–120V, 50–60 Hz AC power source A Web browser for configuration, such as Microsoft Internet Explorer 6. 0 or later , or Mozilla 1. 5 or later At least one computer with the TCP/IP protocol installed An 802. 11b/g- or 802.

11n/g-compliant device, such as the NETGEAR WNDA3100 wireless adapter Key Features and Standards The ProSafe Wireless-N Access Point WNAP320 is easy to use and provides solid wireless and networking support. The wireless access point complies with the IEEE 802. 11 b/g standards for wireless LANs, and is Wi-Fi certified for 802. The wireless access point provides WPA and WPA2 enterprise-class strong security with RADIUS and certificate authentication as well as dynamic encryption key generation. The WPA-PSK and WPA2-PSK preshared key authentication is without the overhead of RADIUS servers but with all of the strong security of WPA. When a wireless access point is connected to a wired network and a set of wireless stations, it is called a basic service set (BSS). The basic service set identifier (BSSID) is a unique identifier attached to the header of packets sent over a WLAN that differentiates one WLAN from another when a mobile device tries to connect to the network. The multiple BSSID feature allows you to configure up to eight SSIDs on your wireless access point and assign different configuration settings to each SSID. All the configured SSIDs are active, and the network devices can connect to the wireless access point by using any of these SSIDs. • DHCP client support.

DHCP provides a dynamic IP address to PCs and other devices upon request. The wireless access point can act as a client and obtain information from your DHCP server; it can also act as a DHCP server and provide network information for wireless clients. A network of computers that behave as if they are connected to the same network even though they might actually be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, which makes them extremely flexible. VLANs are very useful for user and host management, bandwidth allocation, and resource optimization.

In this mode, the wireless access point communicates only with another bridge-mode wireless station or wireless access point. Network authentication should be used to protect this communication. point-to-multipoint bridge. Select this only if this wireless access point is the master for a group of bridge-mode wireless stations. the other bridge-mode wireless stations - 8 | Chapter 1.

Introduction ProSafe Wireless-N Access Point WNAP320 Reference Manual send all traffic to this master, and do not communicate directly with each other. Network authentication should be used to protect this traffic. wireless repeater. In this mode, the wireless access point does not function as an access point but communicates only with wireless stations that function in repeater mode, point-to-point bridge mode, and point-to-multipoint-bridge mode. Network authentication should be used to protect this communication. client. In this mode, the wireless access point functions as a client bridge only, and sends all traffic to a remote wireless access point or peer device.

• • Hotspot settings. You can allow all HTTP (TCP, port 80) requests to be captured and redirected to the URL you specify. You can upgrade it easily, using only your Web browser, and you can upgrade it remotely.

You can also use the command-line interface. rogue AP detection. The Rogue AP filtering feature ensures that unknown APs are not given access to any part of the LAN. access control. The Access Control MAC address filtering feature can ensure that only trusted wireless stations can use the wireless access point to gain access to your LAN. security profiles. When using multiple BSSIDs, you can configure unique security settings (encryption, SSID, and so on) for each BSSID. hidden mode. The SSID is not broadcast, assuring only clients configured with the correct SSID can connect. Adjustable power output allows more secure or economical operation.

power over Ethernet. Power can be supplied to the wireless access point over the Ethernet port from any 802. Power/Test, Active, LAN, and WLAN for each radio mode are easily identified. WMM allows wireless traffic to have a range of priorities, depending on the kind of data. Time-dependent information, like video or audio, has a higher priority than normal traffic.

For WMM to function correctly, wireless clients must also support WMM. quality of Service (QoS) support. You can configure parameters that affect traffic flowing from the wireless access point to the client station and traffic flowing from the client station to the wireless access point. The QoS feature allows you to prioritize traffic, such as voice and video traffic, so that packets do not get dropped. vLAN security profiles.

Each security profile is automatically allocated a VLAN ID when the security profile is modified. It provides connectivity between wired Ethernet networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices. Additionally, the wireless access point supports the following wireless features: • • • • • • • • • Aggregation support Reduced InterFrame spacing support Multiple input, multiple output (MIMO) support Distributed coordinated function (CSMA/CA, back-off procedure, ACK procedure, retransmission of unacknowledged frames) RTS/CTS handshake Beacon generation Packet fragmentation and reassembly Auto or long preamble Roaming among wireless access points on the same subnet Autosensing Ethernet Connections with Auto Uplink The ProSafe Wireless-N Access Point WNAP320 can connect to a standard Ethernet network. The Ethernet port automatically senses whether the Ethernet cable plugged into the port should have a "normal" connection such as to a computer or an "uplink" connection such as to a switch or hub. That port then configures itself correctly. This feature also eliminates any concerns about crossover cables, as Auto Uplink accommodates either type of cable to make the right connection. Hardware Description This section describes the top and rear hardware functions of the ProSafe Wireless-N Access Point WNAP320. 10 | Chapter 1. Introduction ProSafe Wireless-N Access Point WNAP320 Reference Manual Top Panel The ProSafe Wireless-N Access Point WNAP320 LEDs are described in the following figure and table: 1 Figure 1. 2 3 4 Table 1.

Top Panel LEDs Item 1 LED Description Power/Test Off On (green) Amber, then blinking green Power is off. power is on. A self-test is running or software is being loaded. During startup, the LED is first steady amber, then goes off, and then blinks green before turning steady green after about 45 seconds. If after 1 minute the LED remains amber or continues to blink green, it indicates a system fault. 2 3 4 5 6 7 The rear panel functions of the ProSafe Wireless-N Access Point WNAP320 are described in the following list: 1. Using a sharp object, press and hold this button for about 5 seconds to reset the wireless access point to factory defaults settings. All configuration settings are lost, and the default password is restored. For more information, see Restore the Wireless Access Point to the Factory Default Settings on page 62. The port has a DB9 male connector and supports the following settings: 9600 K default baud rate, (8) data bits, no (N) parity bit, and one (1) stop bit.

4. 10/100/1000BASE-T Gigabit Ethernet (RJ-45) port with Auto Uplink (Auto MDI-X) with IEEE 802. Cable security lock receptacle for an optional lock. 6. Power socket for a 12 VDC, 1A power adapter.

Introduction ProSafe Wireless-N Access Point WNAP320 Reference Manual Bottom Panel with Product Label The product label on the bottom of the wireless access point's enclosure displays factory default settings, regulatory compliance, and other information: Figure 3. Installation and Basic Configuration 2 This chapter describes how to install and configure your access point for wireless connectivity to your LAN. This basic configuration will enable computers with 802. 11b/g or 802. 11n wireless adapters to connect to the Internet, or access printers and files on your LAN.

In planning your wireless neapter. If this computer is already part of your network, record its TCP/IP configuration settings. Configure the computer with a static IP address of 192. Connect an Ethernet cable from the wireless access point to the computer (point A in the following figure). 4. Securely insert the other end of the cable into the wireless access point's Ethernet port (point B in the following figure). Turn on your computer. 6. Connect the power adapter to the wireless access point. tip: The wireless access point supports Power over Ethernet (PoE).

If you have a switch that provides PoE, you will not need to use the power adapter to power the wireless access point. This can be especially convenient when the wireless access point is installed in a high location far away from a power outlet. The Power/Test LED blinks when the wireless access point is first turned on. (To be exact, during startup, the LED is first steady amber, then goes off, and then blinks green.) After about 45 seconds, the LED should stay lit (steady green). If after 1 minute the Power/Test LED is not lit or is still blinking, check the connections and see if the power outlet is controlled by a wall switch that is turned off. active LED. The Active LED is lit or blinks green when there is Ethernet traffic. lAN LED. The LAN LED indicates the LAN speed: green for 1000 Mbps, amber for 100 Mbps, and no light for 10 Mbps.

If the LAN LED is not lit, make sure that the Ethernet cable is securely attached at both ends. wLAN LED. The WLAN LED is lit or blinks green when the wireless LAN (WLAN) is ready. chapter 2. Installation and Basic Configuration | 17 ProSafe Wireless-N Access Point WNAP320 Reference Manual Log In to the Wireless Access Point The default IP address of your wireless access point is http://192.

The wireless access point is set, by default, for the DHCP client to be disabled. Connect to the wireless access point by entering its default address of http://192.

Enter the default user name of admin and the default password of password. The Web browser displays the basic General system settings screen under the Configuration tab of the main menu as shown in Figure 8 on page 19. Web Management Interface The navigation tabs across the top of the Web Management Interface provide access to all the configuration functions of the wireless access point, and remain constant.

The menu items in the blue bar change according to the navigation tab that is selected. Installation and Basic Configuration ProSafe Wireless-N Access Point WNAP320 Reference Manual The bottom right corner of all screens that allow you to make configuration changes show the Apply and Cancel buttons, and on several screens the Edit button. figure 7. These buttons have the following functions: • • • Edit. Allows you to edit the existing configuration. cancel. Cancels all configuration changes that you made on the screen. apply. Saves and applies all configuration changes that you made on the screen. Configure Basic General System Settings and Time Settings Note: After you have successfully logged in to the wireless access point, the basic General system settings screen displays.

Specify the fields as explained in the following table: Table 2. basic General System Settings Field Access Point Name Description This unique name is the wireless access point NetBIOS name. The name is printed on the rear label of the wireless access point. The default is netgearxxxxxx, where xxxxxx represents the last 6 digits of the wireless access point MAC address. You can replace the default name with a unique name up to 15 characters long. The access point name can be retrieved through SNMP. From the Country/Region drop-down list, select the country where the wireless access point is installed. Note: It might not be legal to operate this wireless access point in a region other than one of those identified in this field. Specify the fields as explained in the following table: Table 3. Time System Settings Field Time Zone Current Time NTP Client Description Select the time zone to match your location.

This is a nonconfigurable field that displays the current date and time. Enable the Network Time Protocol (NTP) client to synchronize the time of the wireless access point with an NTP server. Time System Settings (Continued) Field Use Custom NTP Server Description Select this check box to If you want to use a custom NTP server. Note: You must have an Internet connection to use an NTP server that is not on your local network. Hostname / IP Address Enter the host name or IP address of the custom NTP server.

Specify the fields as explained in the following table: Table 4. iP Settings Field DHCP Client Description By default , the Dynamic Host Configuration Protocol (DHCP) client is disabled. If you have a DHCP server on your LAN and you select the Enable check box, the wireless access point will receive its IP address, subnet mask, and default gateway settings automatically from the DHCP server on your network when you connect the wireless access point to your LAN. Enter the IP address of your wireless access point. The default IP address is 192.

To change the address, enter an unused IP address from the address range used on your LAN, or enable DHCP the server. IP Settings (Continued) Field IP Subnet Mask Description Enter the network number portion of an IP address. Unless you are implementing subnetting, enter 255. Enter the IP address of the ISP's router to which the wireless access point will connect. Enter the IP address of the primary and secondary DNS servers. A DNS server is a host on the Internet that translates Internet names (such as www. Typically your ISP transfers the IP address of one or two DNS servers to your wireless access point during login. If the ISP does not transfer an address, you must obtain it from the ISP and enter it manually in this field. Select this check box to validate that the upstream link is active before allowing wireless associations. The wireless access point provides a built-in DHCP server for wireless clients only, which can be especially useful in small networks.

When the DHCP server is enabled, the wireless access point provides preconfigured TCP/IP configurations to all connected wireless stations. Specify the fields as explained in the following table: Table 5. LAN Settings Field Description DHCP Server Select the DHCP Server check box to enable the DHCP server. Use the default settings or specify the pool of IP addresses to be assigned by setting the starting IP address and ending IP address. These addresses should be part of the same IP address subnet as the wireless access point's LAN IP address. dHCP Server VLAN ID Enter the DHCP server VLAN ID. The VLAN ID range is between 1 and 4094. Enter the first address in the range of IP addresses to be assigned to DHCP clients. The default address is 192. Enter the last address in the range of IP addresses to be assigned to DHCP clients.

The default address is 192. Enter the subnet mask to be used by DHCP clients. Enter the IP address of the default routing gateway to be used by DHCP clients. The default address is 192. Enter the IP address of the primary Domain Name Server (DNS) server available to DHCP clients.

Starting IP Address Ending IP Address Subnet Mask Gateway IP Address Primary DNS Address Secondary DNS Address Enter the IP address of the secondary DNS server available to DHCP clients. Primary WINS Server Secondary WINS Server Enter the IP address of the primary WINS server for the network. Enter the IP address of the secondary WINS server for the network. Enter the period that the DHCP server grants to DHCP clients to use the assigned IP addresses. The default time is 1 day.

Configure Basic Wireless Settings For proper compliance and compatibility between similar products in your coverage area, you must correctly configure 802. 11b/g/n wireless adapter settings , including the operating channel and country. The basic wireless network settings must be set correctly for wireless devices to connect to your network. For other wireless features, including wireless security, see Chapter 3, Wireless Configuration and Security. If you configure the wireless access point from a wireless computer and you change the wireless access point's SSID, channel, or wireless security settings, you will lose your wireless connection when you click Apply. You must then change the wireless settings of your computer to match the wireless access point's new settings. (The following figure shows the 11ng setting. Specify the fields as explained the following table: Table 6. Basic Wireless Settings Field Wireless Mode Descriptions Select the wireless operating mode that you want to use by selecting one of the following radio buttons: • 11b. This is the default setting.

the radio is enabled by default. To turn off the radio, clear the Turn Radio On check box. Doing so disables access through the wireless access point, which can be helpful for configuration, network tuning, or troubleshooting activities.

Enter a 32-character (maximum) service set identifier (SSID); the characters are case-sensitive. the default is NETGEAR_11ng. The SSID assigned to a wireless device must match the wireless access point's SSID for the wireless device to communicate with the wireless access point. If the SSIDs do not match, you will not get a wireless connection to the wireless access point. This is a nonconfigurable field that show the status of the wireless scheduler. For more information, see Schedule the Wireless Radio on page 52. Select the Yes radio button to enable the wireless access point to broadcasts its SSID, allowing wireless stations that have a null (blank) SSID to adopt the wireless access point's SSID.

Yes is the default setting. To prevent the SSID from being broadcast, select the No radio button. From the drop-down list, select the channel you wish to use on your wireless LAN. The wireless channels to use in the United States and Canada are 1 to 11; for Europe and Australia, 1 to 13. the default setting is Auto. Note: It should not be necessary to change the wireless channel unless you experience interference (indicated by lost connections or slow data transfers). Should this happen, you might want to experiment with different channels to see which is the best. For more information, see the guidelines following this table. 11ng mode only MCS Index / Data From the drop-down list, select a Modulation and Coding Rate Scheme (MCS) index and transmit data rate for the wireless network. the default setting is Best.

For a list of all options that you can select from in 11ng mode, see Factory Default Settings in Appendix A. channel Width From the drop-down list , select a channel width. The options are Dynamic 20/40 MHz, 20 MHz, or 40 MHz. A wider channel improves the performance, but some legacy devices can operate only in either 20 MHz or 40 MHz. When you select a channel width of Dynamic 20/40 MHz or 40 MHz, you also need to select protection spacing for the extension channel from the Ext Protection Spacing drop-down list. In addition to the default value Auto, you can also select a value of 20 or 25. Turn Radio On Wireless Network Name (SSID) Scheduler Status Broadcast Wireless Network Name (SSID) Channel / Frequency Note: For most networks, the default settings will work fine. Basic Wireless Settings (Continued) Field 11ng mode only (continued) Descriptions Ext Channel Offset When you select a channel width of Dynamic 20/40 MHz or 40 MHz, you also need to select the offset for the extension channel from the Ext Channel Offset drop-down list. In addition to the default value Auto, you can also select Upper or Lower. From the drop-down list, select the guard interval to protect transmissions from interference.

In addition to the default value Auto, you can also select Long - 800 ns. Some legacy devices can operate only with a long guard interval. From the drop-down list, select the transmit data rate of the wireless network. the default setting is Best. For a list of all options that you can select from in 11b mode and 11bg mode, see Factory Default Settings in Appendix A. Guard Interval 11b and 11bg modes only Data Rate Output Power From the drop-down list, select the transmission power of the wireless access point. the default is Full. Note: Increasing the power improves performance, but if two or more wireless access points are operating in the same area, on the same channel, it can cause interference. Note: Make sure that you comply with the regulatory requirements for total radio frequency (RF) output power in your country. channel Bonding This drop-down list lets you to specify channels to bond.

The available options are 20 MHz, 20/40 MHz, and 40 MHz. 3. If you have changed the wireless mode and selected the Turn Radio On check box, a popup window appears: click OK to confirm your change. You should not need to change the operating frequency (channel) unless you notice interference problems, or are setting up the wireless access point near another wireless access point. Observe the following guidelines: • Wireless access points use a fixed channel. You can select a channel that provides the least interference and best performance. In the United States and Canada, 11 channels are available. If you are using multiple wireless access points, it is better if adjacent wireless access points use different channels to reduce interference. The recommended channel spacing between adjacent wireless access points is 5 channels (for example, use channels 1 and 6, or 6 and 11). in infrastructure mode , wireless stations normally scan all channels , looking for a wireless access point.

If more than one wireless access point can be used, the one with the strongest signal is used. This can happen only when the wireless access points use the same SSID. Installation and Basic Configuration ProSafe Wireless-N Access Point WNAP320 Reference Manual Note: For more information about wireless channels, see the article "Wireless Networking Basics" available on the NETGEAR website. A link to this article and other articles of interest can be found in Related Documents in Appendix A. Note: For information about how to configure advanced wireless settings, see Configure Advanced Wireless Settings on page 79. Test Basic Wireless Connectivity After you have configured the wireless access point as explained in the previous sections, test your computers for wireless connectivity before you position and mount the wireless access point at its permanent position. 11n wireless adapters of your computers so that they all have the same SSID and channel that you have configured on the wireless access point. 2. Verify that your computers have a wireless link to the wireless access point, and if you have enabled the DHCP server on the wireless access point, verify that your computers are able to obtain an IP address through DHCP from the wireless access point. 5 or later to browse the Internet, or check for file and printer access on your network.

Note: If you have trouble connecting to the wireless access point, see Chapter 6, Troubleshooting. wARNING! Before you deploy the wireless access point in your network, set up wireless security and other wireless features as described in Chapter 3, Wireless Configuration and Security. In addition to wireless security and other wireless features, before you deploy the wireless access point in your network, configure any additional features as described in Chapter 4, Management and Chapter 5, Advanced Configuration. chapter 2. Installation and Basic Configuration | 27 ProSafe Wireless-N Access Point WNAP320 Reference Manual After you have completed the configuration of the wireless access point, you can reconfigure the computer that you used for this process back to its original TCP/IP settings. Mount the Wireless Access Point This section includes the following subsections: • • • Ceiling Installation on this page Wall Installation on page 30 Desk Installation on page 33 Ceiling Installation To install the wireless access point using the ceiling installation kit: 1.

Verify the package content of the ceiling installation kit. mounting plate Clamp with screws 2. Detach the mounting plate from the wireless access point. Attach the clamp to the ceiling rail.

4. Attach the mounting plate to the clamp. 5. Connect the cables to the wireless access point. Attach the wireless access point to the mounting plate. 7. Attach the cover to the wireless access point. Wall Installation To install the wireless access point using the wall installation kit: 1. Verify the package content of the wall installation kit. Detach the mounting plate from the wireless access point.

3. Attach the mounting plate to the wall. 4. Connect the cables to the wireless access point. Attach the wireless access point to the mounting plate. 6. Attach the cover to the wireless access point. 32 | Chapter 2. Installation and Basic Configuration ProSafe Wireless-N Access Point WNAP320 Reference Manual Desk Installation To install the wireless access point on a desk, attach the rubber feet to the holes in the bottom of the wireless access point. Wireless Configuration and Security 3 This chapter describes how to configure the wireless features of your ProSafe Wireless-N Access Point WNAP320.

The chapter includes the following sections: • • • • • • Wireless Data Security Options on this page Security Profiles on page 36 Configure RADIUS Server Settings on page 48 Restrict Wireless Access by MAC Address on page 50 Schedule the Wireless Radio on page 52 Configure Basic Wireless Quality of Service on page 52 Before you set up wireless security and additional wireless features that are described in this chapter, connect the wireless access point, get the Internet connection working, and configure the 802. 11b , 11bg , or 11ng wireless settings as described in Chapter 2 , Installation and Basic Configuration. The wireless access point should work with an Ethernet LAN connection, and wireless connectivity should have been verified before you set up wireless security and additional wireless features. In planning your wireless network, consider the level of security required. wARNING! If you are configuring the wireless access point from a wireless computer and you change the wireless access point's SSID, channel, or wireless security settings, you will lose your wireless connection when you click Apply. You must then change the wireless settings of your computer to match the wireless access point's new settings. Typically, a wireless access point inside a building works best with devices within a 100 foot radius. Such distances can allow for others outside your immediate area to access your network. chapter 3. Wireless Configuration and Security | 34 ProSafe Wireless-N Access Point WNAP320 Reference Manual Unlike wired network data, your wireless data transmissions can extend beyond your walls and can be received by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The wireless access point provides highly effective security features that are covered in detail in this chapter. Deploy the security features appropriate to your needs. figure 13. There are several ways you can enhance the security of your wireless network: • Use multiple BSSIDs combined with VLANs.

You can configure combinations of VLANS and BSSIDs with stronger or less restrictive access security according to your requirements. For example, visitors could be given wireless Internet access but be excluded from any access to your internal network. For information about how to configure BSSIDs, see Configure and Enable Security Profiles on page 39. restrict access based by MAC address. You can allow only trusted PCs to connect so that unknown PCs cannot wirelessly connect to the wireless access point.

Restricting access by MAC address adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed. For information about how to restrict access by MAC address, see Restrict Wireless Access by MAC Address on page 50. Turn off the broadcast of the wireless network name (SSID). If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network discovery feature of some products, such as Windows XP, but the data is still exposed. For information about how to turn of broadcast of the SSID, see Configure and Enable Security Profiles on page 39. WEP shared key authentication and WEP data encryption block all but the most determined eavesdropper. this data encryption mode has been superseded by WPA-PSK and WPA2-PSK. For information about how to configure WEP, see Configure and Enable Security Profiles on page 39 and Configure an Open System with WEP or Shared Key with WEP on page 43. Wi-Fi Protected Access (WPA) data encryption provides strong data security with Temporal Key Integrity Protocol (TKIP) encryption.

The very strong authentication along with dynamic per frame rekeying of WPA make it virtually impossible to compromise. wPA uses RADIUS-based 802. 1x authentication; for more information, see Configure and Enable Security Profiles on page 39 and Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS on page 45. WPA-PSK uses a pre-shared key (PSK) for authentication; for more information, see Configure and Enable Security Profiles on page 39 and Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK on page 46. • WPA2 and WPA2-PSK (AES). Wi-Fi Protected Access version 2 (WPA2) data encryption provides strong data security with Advanced Encryption Standard (AES) encryption. The very strong authentication along with dynamic per frame rekeying of WPA2 make it virtually impossible to compromise. wPA2 uses RADIUS-based 802. 1x authentication; for more information, see Configure and Enable Security Profiles on page 39 and Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS on page 45. WPA2-PSK uses a pre-shared key (PSK) for authentication; for more information, see Configure and Enable Security Profiles on page 39 and Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK on page 46.

• WPA & WPA2 and WPA-PSK & WPA2-PSK mixed modes. These modes support data encryption either with both WPA and WPA2 clients or with both WPA-PSK and WPA2-PSK clients and provide the most reliable security. wPA & WPA2 uses RADIUS-based 802. 1x authentication; for more information, see Configure and Enable Security Profiles on page 39 and Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS on page 45. WPA-PSK & WPA2-PSK uses a pre-shared key (PSK) for authentication; for more information, see Configure and Enable Security Profiles on page 39 and Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK on page 46.

Security Profiles Security profiles let you configure unique security settings for each SSID. The wireless access point supports up to eight BSSIDs that you can configure on the individual Edit Wireless Network screens that are accessible from the Edit Security Profile screen (see Configure and Enable Security Profiles on page 39).

36 | Chapter 3. Wireless Configuration and Security ProSafe Wireless-N Access Point WNAP320 Reference Manual To set up a security profile you select its network authentication type, data encryption, wireless client security separation, and VLAN ID: • Network authentication The wireless access point is set by default as an open system with no authentication. When you configure network authentication, bear in mind that not all wireless adapters support WPA or WPA2.

Windows XP, Windows 2000 with Service Pack 3, and Windows Vista do include the client software that supports WPA. However, client software is required on the client. Consult the product documentation for your wireless adapter and WPA or WPA2 client software for instructions on configuring WPA2 settings. For information about the types of network authentication that the wireless access point supports, see Configure and Enable Security Profiles on page 39. □ Data encryption Select the data encryption that you want to use. The available options depend on the network authentication setting described earlier (otherwise, the default is None). The data encryption settings are explained in Configure and Enable Security Profiles on page 39. Wireless client security separation If enabled, the associated wireless clients (using the same SSID) will not be able to communicate with each other. This feature is useful for hotspots and other public access situations. by default , wireless client separation is disabled.

For more information, see Configure and Enable Security Profiles on page 39. VLAN ID If enabled and if the network devices (hubs and switches) on your LAN support the VLAN (802. 1Q) standard, the default VLAN ID for the wireless access point will be associated with each profile. The default VLAN ID must match the IDs that are used by the other network devices. For more information, see Configure and Enable Security Profiles on page 39. □ • Some concepts and guidelines regarding the SSID are explained in the following list: • • • • A basic service set (BSS) is a group of wireless stations and a single wireless access point, all using the same service set identifier (BSSID) An extended service set (ESS) is a group of wireless stations and multiple wireless access points, all using the same identifier (ESSID). Different wireless access points within an ESS can use different channels. To reduce interference, adjacent wireless access points should use different channels. Roaming is the ability of wireless stations to connect wirelessly when they physically move from one BSS to another within the same ESS. The wireless station automatically changes to the wireless access point with the least interference or best performance. chapter 3. Wireless Configuration and Security | 37 ProSafe Wireless-N Access Point WNAP320 Reference Manual Before You Change the SSID, WEP and WPA Settings , For a new wireless network, print or copy this form and fill in the settings. For an existing wireless network, the network administrator can provide this information. Be sure to set the Country/Region correctly as the first step. Store this information in a safe place.

□ SSID: The service set identification (SSID) identifies the wireless local area network. You can customize it by using up to 32 alphanumeric characters. Write your SSID on the line. SSID: _____ Note: The SSID in the wireless access point is the SSID you configure in the wireless adapter card. All wireless nodes in the same network must be configured with the same SSID.

□ WEP Key Size, Key Format Passphrase, and Authentication Choose the key size by circling one: 64, 128, or 152 bits. choose the key format by circling one: ASCII or HEX. Choose the authentication type by circling one: Open or Shared. Passphrase: _____ Note: If you select shared key, the other devices in the network will not connect unless they are set to shared key and have the same keys in the same positions as those in the wireless access point. □ WPA-PSK (Pre-Shared Key) and WPA2-PSK Record the WPA-PSK passphrase: WPA-PSK Passphrase: _____ Record the WPA2-PSK passphrase: WPA2-PSK Passphrase: _____ • WPA RADIUS Settings For WPA, record the following settings for the primary and secondary RADIUS servers: Server Name/IP Address: Primary _____ Secondary _____ Port: _____ Shared Secret: _____ • WPA2 RADIUS Settings For WPA2, record the following settings for the primary and secondary RADIUS servers: Server Name/IP Address: Primary _____ Secondary _____ Port: _____ Shared Secret: _____ 38 | Chapter 3. The Profile Settings screen displays, showing eight wireless security profiles: Figure 14. The following table explains the fields of the Profile Settings screen: Table 7. Profile Settings Screen Field Profile Name Description The unique name of the wireless security profile that makes it easy to recognize the profile. The wireless network name (SSID) for the wireless security profile. The configured wireless authentication method for the wireless security profile.

The default VLAN ID that is associated with the wireless security profile. The check box that lets you select the wireless security profile so you can enable it by clicking Apply. sSID Security VLAN Enable 2. To configure or edit a wireless security profile, select the corresponding radio button to the left of the wireless security profile. The Edit Security Profile screen opens for the selected wireless security profile (see the following figure). The first section on the screen is the Profile Definition section; the second section is the Authentication Settings section. These sections are explained separately. Specify the settings of the Profile Definition section of the Edit Security Profile screen as explained in the following table: Table 8. Profile Definition Settings of the Edit Security Profile Screen Field Profile Name Description Enter a unique name of the wireless security profile that makes it easy to recognize the profile. The default names are NETGEAR, NETGEAR-1, NETGEAR-2, and so on through NETGEAR-7.

You can enter a value of up to 32 alphanumeric characters. The wireless network name (SSID) for the wireless security profile. The default names are NETGEAR_11ng, NETGEAR_11ng-1, NETGEAR_11ng-2, and so on through NETGEAR_11ng-7. Select the Yes radio button to enable the wireless access point to broadcasts its SSID, allowing wireless stations that have a null (blank) SSID to adopt the wireless access point's SSID. Yes is the default setting. To prevent the SSID from being broadcast, select the No radio button. wireless Network Name (SSID) Broadcast Wireless Network Name (SSID) 4. Specify the settings of the Authentication Settings section of the Edit Security Profile screen as explained in the following table.

When you configure network authentication, bear in mind the following: • If you are using access point mode (which is the default mode if you did not enable wireless bridging), then all options are available. In other modes such as bridge mode, some options might be unavailable.

Not all wireless adapters support WPA or WPA2. Windows XP, Windows 2000 with Service Pack 3, and Windows Vista do include the client software that supports WPA. However, client software is required on the client. Consult the product documentation for your wireless adapter and WPA or WPA2 client software for instructions on configuring WPA2 settings. • Table 9. Authentication Settings of the Edit Security Profile Screen Field Network Authentication and Data Encryption Description Open System This is the default setting. You can use an open system without any encryption or with WEP encryption. See Configure an Open System with WEP or Shared Key with WEP on page 43. You must use WEP encryption and enter at least one shared key. See Configure an Open System with WEP or Shared Key with WEP on page 43.

You must configure the RADIUS server settings to use this option. You must configure the RADIUS server settings to use this option. See Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS on page 45. Shared Key Note: The data encryption fields that are displayed on screen depend on you selection from the Network Legacy 802. 1x Authentication drop-down list. WPA with RADIUS WPA2 with RADIUS Select this setting only if all clients support WPA2. If selected, you must use AES encryption and configure the RADIUS server settings. See Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS on page 45. WPA and WPA2 with RADIUS Select this setting to allow clients to use either WPA (with TKIP) or WPA2 (with AES). If selected, you must use TKIP + AES encryption and configure the RADIUS server settings.

See Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS on page 45. You must use TKIP or TKIP + AES encryption and enter a WPA passphrase (network key). Authentication Settings of the Edit Security Profile Screen (Continued) Field Network Authentication and Data Encryption (continued) Description WPA2-PSK Select this only if all clients support WPA2. If selected, you must use AES and TKIP + AES encryption and enter a WPA passphrase (network key). see Configure WPA-PSK , WPA2-PSK , and WPA-PSK & WPA2-PSK on page 46.

Select this setting to allow clients to use either WPA (with TKIP) or WPA2 (with AES). If selected, you must use TKIP + AES encryption and enter a WPA passphrase (network key). see Configure WPA-PSK , WPA2-PSK , and WPA-PSK & WPA2-PSK on page 46. WPA-PSK and WPA2-PSK Wireless Client Security Separation If you enable wireless client security separation by selecting Enable from the drop-down list, the associated wireless clients are not be able to communicate with each other. by default , Disable is selected from the drop-down list.

This feature is intended for hotspots and other public access situations. From the drop-down list, select how VLANs operate by making one of the following selections: • Disable. disables dynamic VLANs , and enables static VLANs. This is the default setting. • Optional. Enables dynamic VLANs but if a RADIUS server does not return a VLAN ID, the wireless station is still allowed to connect to the wireless access point. If a RADIUS server does not return a VLAN ID, the wireless station is not authenticated and cannot connect to the wireless access point. For dynamic VLANs to operate (that is, the selection is Optional or Required), the following is required: • The hubs and switches on your LAN must support the VLAN (802. 1Q) standard. The authentication is set to any RADIUS type authentication: either the network authentication in the wireless security profile or the remote MAC address database authentication for the MAC Authentication feature can be used.

Enter the default VLAN ID that must be associated with this wireless security profile. the default VLAN ID is 1. The VLAN ID must match the VLAN ID that is used by the other devices in your network. Authentication Settings of the Edit Security Profile Screen (Continued) Field Access Control Description Note: Access control functions only when static VLANs are enabled, that is, you select Disable from the Dynamic VLAN drop-down list. The Access Control radio buttons let you enable or disable access control through a RADIUS server for the wireless security the profile: • Disable. access control is disabled. This is the default setting. • Enable. Access control is enabled, and wireless stations are authenticated through a RADIUS server; either the network authentication in the wireless security profile or the remote MAC address database authentication for the MAC Authentication feature must be enabled. Access Control Policy Note: Access control policy functions only when static VLANs are enabled, that is, you select Disable from the Dynamic VLAN drop-down list, and when you select the Enable Access Control radio button.

The Access Control Policy radio buttons let you enable or disable the access control policy for wireless stations: • Disable. If a RADIUS server does not return a (static) VLAN ID, the wireless station is still allowed to connect to the wireless access point. • Enable. If a RADIUS server does not return a (static) VLAN ID, the wireless station is not authenticated and cannot connect to the wireless access point. If you use a wireless computer to configure wireless security settings, you will be disconnected when you click Apply.

Reconfigure your wireless computer to match the new settings, or access the wireless access point from a wired computer to make further changes. For more information about wireless security options, see the Wireless Networking Basics document that you can access from Related Documents in Appendix A. Configure an Open System with WEP or Shared Key with WEP Wether you use an open system with WEP or shared key with WEP, specify the fields that are explained in the following table. Open System with WEP An open system can function without any encryption or with pre-shared WEP key encryption without RADIUS authentication. The security level of static WEP is not very strong.

chapter 3. Wireless Configuration and Security | 43 ProSafe Wireless-N Access Point WNAP320 Reference Manual When you select Open System from the Network Authentication drop-down list and any selection other than None from the Data Encryption drop-down list, the screen expands to display the WEP fields: Figure 16. Shared Key with WEP Shared key provides pre-shared WEP key encryption without RADIUS authentication. The security level of static WEP is not very strong. When you select Shared Key from the Network Authentication drop-down list, the screen expands to display the WEP fields: Figure 17. table 10. WEP Encryption Settings Field Data Encryption Descriptions Select the encryption key size from the drop-down list: • 64-bit WEP.

This mode functions only with other wireless station that support this mode. enter a passphrase. The passphrase length must be between 8 and 63 characters (inclusive).

The secret passphrase allows you to automatically generate the keys by clicking Generate Keys. the default passphrase is sharedsecret. You can display the actual passphrase by selecting the Show Passphrase in Clear Text radio button. WEP Encryption Settings (Continued) Field Encryption Key (Key1–Key4) Descriptions Either manually enter a key or allow the key to be automatically generated by clicking Generate Key. For ASCII format, depending on the key size selected, the manually entered encryption key must have a length of 5 (64-bit WEP), 13 (128-bit WEP), or 16 (152-bit WEP) characters. For HEX format, depending on the key size selected, the manually entered or automatically generated encryption key must have a length of 10 (64-bit WEP), 26 (128-bit WEP), or 32 (152-bit WEP) characters. Note: Wireless stations must use the key to access the wireless access point. Note: Not all wireless adapters support passphrase key generation. Show Passphrase in Select the Yes radio button to display the actual passphrase in the Passphrase field. 1X security, you must define RADIUS server settings.

For information about RADIUS servers, see Configure RADIUS Server Settings on page 48. when you select Legacy 802. 1X from the Network Authentication drop-down list, the Data Encryption drop-down list becomes nonoperational (it shows None only). You need to define the RADIUS servers only to use legacy 802. Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS WPA, WPA2, and WPA & WPA2 security requires RADIUS-based 802.

1x authentication, so you also must define RADIUS server settings. For information about RADIUS servers, see Configure RADIUS Server Settings on page 48. The selections that are available from the Data Encryption drop-down list depend on the type of WPA authentication that you select from the Network Authentication drop-down list and are shown in the following table. WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS Settings Field TKIP Descriptions Temporal Key Integrity Protocol (TKIP) is the standard encryption method used with WPA. You can also use TKIP with WPA2.

note: TKIP provides only legacy (slower) rates of operation. NETGEAR recommends WPA2 authentication with AES encryption if you want to use the 11n rates and speed. AES Advanced Encryption Standard (AES) is the standard encryption method used with WPA2. Note: Although some wireless clients might support AES with WPA, the WNAP320 wireless access point does not support WPA with AES. For unicast (point-to-point) transmissions, WPA clients use TKIP, and WPA2 clients use AES. For the WPA & WPA2 mixed mode, TKIP + AES is the only supported data encryption method. Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK WPA-PSK, WPA-PSK, and WPA-PSK & WPA2-PSK authentication use a pre-shared key (PSK) and do not require authentication from a RADIUS server. The selections that are available from the Data Encryption drop-down list depend on the type of WPA-PSK authentication that you select from the Network Authentication drop-down list and are shown in the following table. WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK Settings Field Data Encryption Descriptions TKIP Temporal Key Integrity Protocol (TKIP) is the standard encryption method used with WPA. You can also use TKIP with WPA2.

note: TKIP provides only legacy (slower) rates of operation. NETGEAR recommends WPA2 authentication with AES encryption if you want to use the 11n rates and speed. AES Advanced Encryption Standard (AES) is the standard encryption method used with WPA2. Note: Although some wireless clients might support AES with WPA, the WNAP320 wireless access point does not support WPA with AES. For unicast (point-to-point) transmissions, WPA clients use TKIP, and WPA2 clients use AES. For the WPA & WPA2 mixed mode, TKIP + AES is the only supported data encryption method. The passphrase length must be between 8 and 63 characters (inclusive). the default passphrase is sharedsecret. You can display the actual passphrase by selecting the Show Passphrase in Clear Text radio button. Show Passphrase Select the Yes radio button to display the actual passphrase in the Passphrase field.

the default setting is No. In Clear Text Configure RADIUS Server Settings For authentication, accounting, or both authentication and accounting using RADIUS, you must configure primary servers and optional secondary servers. These RADIUS server settings can apply to all devices that are connected to the wireless access point. (The following figure shows some examples. Specify the settings as explained in the following table: Table 13.

RADIUS Server Settings Field Descriptions RADIUS Server Settings Primary IP Address Authentication Server Enter the IP address of the primary RADIUS server for authentication. Authentication Enter the UDP port number of the wireless access point that is used Port to access the primary RADIUS server for authentication. The default port number is 1812. Secret Enter the shared key that is used between the wireless access point and the primary RADIUS server during authentication. Enter the IP address of the secondary RADIUS server for authentication.

The secondary RADIUS server is used when the primary RADIUS server is not available. Secondary IP Address Authentication Server Authentication Enter the UDP port number of the wireless access point that is used Port to access the secondary RADIUS server for authentication. The default port number is 1812. Secret Enter the shared key that is used between the wireless access point and the secondary RADIUS server during authentication. Enter the IP address of the primary RADIUS server for accounting. Primary Accounting Server IP Address Authentication Enter the UDP port number of the wireless access point that is used Port to access the primary RADIUS server for accounting. The default port number is 1813. Secret Enter the shared key that is used between the wireless access point and the primary RADIUS server during the accounting process. Enter the IP address of the secondary RADIUS server for accounting. The secondary RADIUS server is used when the primary RADIUS server is not available.

Secondary Accounting Server IP Address Authentication Enter the UDP port number of the wireless access point that is used Port to access the secondary RADIUS server for accounting. The default port number is 1813. Secret Enter the shared key that is used between the wireless access point and the secondary RADIUS server during the accounting process. Authentication Settings Reauthentication Time (Seconds) The interval in seconds after which the supplicant is reauthenticated with the RADIUS server. The default interval is 3600 seconds (1 hour). enter 0 to disable reauthentication. Select the check box to allow the global key update, and enter the interval in seconds.

The check box is selected by default, and the default interval is 1800 seconds (30 minutes). Clear the check box to prevent the global key update. Wireless Configuration and Security | 49 ProSafe Wireless-N Access Point WNAP320 Reference Manual Restrict Wireless Access by MAC Address For increased security, you can restrict access to an SSID by allowing access to only specific computers or wireless stations based on their MAC addresses.

You can restrict access to only trusted computers so that unknown computers cannot wirelessly connect to the wireless access point. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed. Note: For wireless adapters, you can usually find the MAC address printed on the wireless adapter. Select the Turn Access Control On check box to enable the access control feature. 3. From the Select Access Control Database drop-down list, select one of the following database options: • Local MAC Address Database. The wireless access point uses the local MAC address database for access control. This is the default setting. • Remote MAC Address Database. The wireless access point uses the MAC address database on an external RADIUS server on the LAN for access control.

If you select this database, you first must configure the RADIUS server settings (see Configure RADIUS Server Settings on page 48). The wireless access point places the MAC addresses of the attached wireless stations in this table. 5. Populate the Trusted Wireless Stations table by one of the following methods: • Select MAC addresses from the Available Wireless Stations table: a. Select individual check boxes for MAC addresses, or select all MAC addresses by selecting the check box in the heading. b. Click Move to transfer the MAC addresses from the Available Wireless Stations table to the Trusted Wireless Stations table. enter MAC addresses manually: a. Enter a MAC address directly in the Trusted Wireless Stations table. To delete a MAC address from the Trusted Wireless Stations table, select individual check boxes for MAC addresses, or select all MAC addresses by selecting the check box in the heading, and then click Delete.

Now, only devices in the Trusted Wireless Stations table are allowed to wirelessly connect to the wireless access point. wARNING! When configuring the wireless access point from a wireless computer whose MAC address is not in the access control list, you will lose your wireless connection when you click Apply. You must then access the wireless access point from a wired computer or from a wireless computer which is on the access control list to make any further changes. • Chapter 3. Wireless Configuration and Security | 51 ProSafe Wireless-N Access Point WNAP320 Reference Manual Schedule the Wireless Radio Scheduled Wireless On/Off is a green feature that allows you to turn off the wireless radio during scheduled vacations, office shutdowns, on evenings, or on weekends. Specify the settings as explained in the following table: Table 14. Schedule Wireless Radio On/Off Settings Field Description Schedule Wireless on-off Select the On radio button to enable the timer. by default , the Off radio button is selected. Radio off schedule Select check boxes to specify the days when you want to schedule the radio to be turned off. by default , Saturday and Sunday are selected.

Fill in the time that you want the radio to be turned back on. Use 24-hour time format. Fill in the time that you want the radio to be turned off. Use 24-hour time format. WMM allows wireless traffic to have a range of priorities, depending on the type of data.

time-dependent information , such 52 | Chapter 3. Wireless Configuration and Security ProSafe Wireless-N Access Point WNAP320 Reference Manual as video or audio, has a higher priority than normal traffic. For WMM to function correctly, wireless clients must also support WMM. By enabling WMM, you allow Quality of Service (QoS) control for upstream traffic flowing from a wireless station to the wireless access point and for downstream traffic flowing from the wireless access point to a wireless station. WMM defines the following four queues in decreasing order of priority: • • • • Voice.

The highest priority queue with minimum delay, which makes it ideal for applications like VoIP and streaming media. video. The second highest priority queue with low delay is given to this queue. Video applications are routed to this queue. best Effort. The medium priority queue with medium delay is given to this queue. Low priority queue with high throughput. Applications, such as FTP, that are not time-sensitive but require high throughput can use this queue. The WMM Powersave feature saves power for battery-powered equipment by increasing the efficiency and flexibility of data transmission. Note: For information about how to configure advanced wireless QoS, that is, to configure specific Enhanced Distributed Channel Access (EDCA) settings, see Configure Advanced QoS Settings on page 81.

To enable this feature, select the Enable radio button, which is the default setting. Select the Disable button to disable the feature. • WMM Powersave. To enable this feature, select the Enable radio button, which is the default setting. Select the Disable button to disable the feature. Management 4 This chapter describes how to use the management and monitoring features of your ProSafe Wireless-N Access Point WNAP320. This chapter includes the following sections: • • • • • • • Enable Remote Management on this page Upgrade the Wireless Access Point Software on page 58 Manage the Configuration File or Reset to Factory Defaults on page 60 Change the Administrator Password on page 64 Enable the Syslog Server on page 65 Monitor the Wireless Access Point on page 66 Enable Rogue AP Detection and Monitor Access Points on page 72 Enable Remote Management Both SNMP and the remote console Secure Shell (SSH) are enabled by default, which allows for remote management of the wireless access point from a client running SNMP management software, as well as from a secure shell (SSH) client. Specify the settings as explained in the following table: Table 15. SNMP Settings Field SNMP Description Select the Enable radio button to allow the SNMP network management software, such as HP OpenView, to manage the wireless access point through SNMPv1/v2 protocol. by default , the Disable radio button is selected.

Read-Only Community Name Enter the community string to allow the SNMP manager to read the wireless access point's Management Information Base (MIB) objects. the default is public. Read-Write Community Name Enter the community string to allow the SNMP manager to read and write the wireless access point's MIB objects. The IP address of the SNMP manager to receive traps sent from the wireless access point. The port number of the SNMP manager to receive traps sent from the wireless access point.