IT Essentials v8

Companion Guide

Networking Academy

IT Essentials v8 Companion Guide

Cisco Press

Step 4. Change the default DHCP IPv4 addresses. It is a best practice to use private IPv4 addressing inside your network. The IPv4 address 10.10.10.1 is used in the example in Figure 6-25, but it could be any private IPv4 address you choose. Search the Internet for "private IP addressing" to learn more.

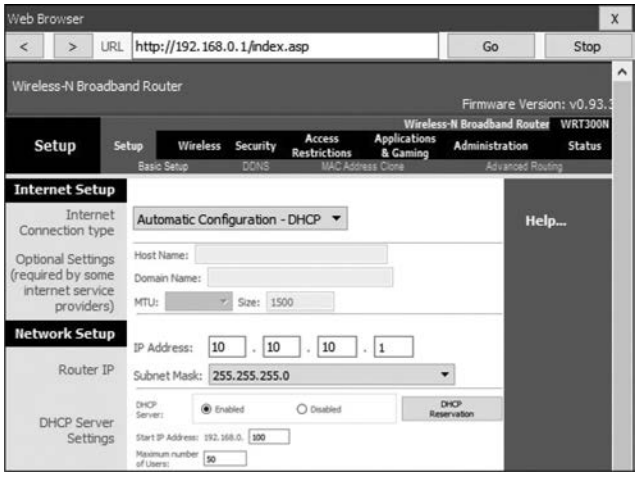

Figure 6-25 Changing the DHCP IPv4 Addresses

Step 5. When you click Save, you temporarily lose access to the wireless router, so renew the IP address. To do so, open a command window and renew your IP address with the **ipconfig /renew** command, as shown in Figure 6-26.

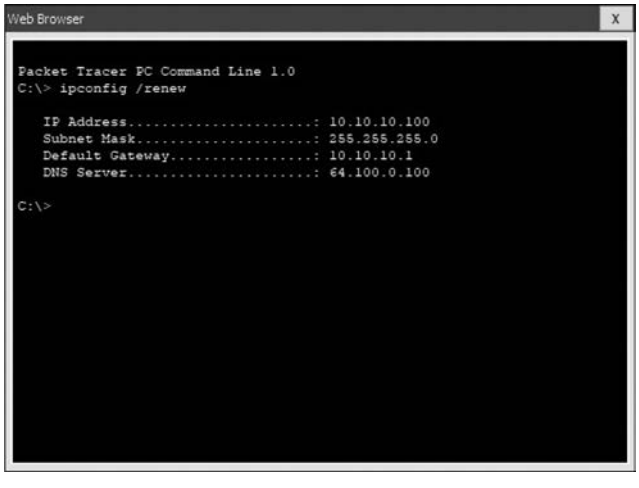

Figure 6-26 Renewing the IP Address

Step 6. Log in at the new IP address by entering the router's new IP address to regain access to the router configuration GUI, as shown in Figure 6-27. You are now ready to continue configuring the router for wireless access.

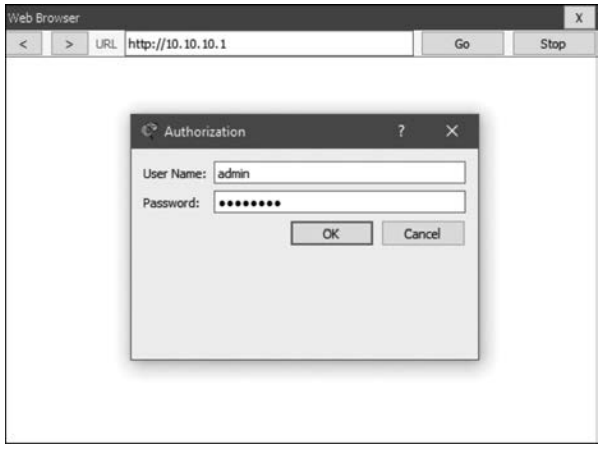

Figure 6-27 Logging in at the New IP Address

Basic Wireless Settings (6.1.3.5)

The basic wireless setup of a network is performed using the following six steps:

Step 1. View the WLAN defaults. Out of the box, a wireless router provides wireless access to devices using a default wireless network name and password. The network name is the *service set identifier (SSID)*. Locate the basic wireless settings for your router to change these defaults, as shown in Figure 6-28.

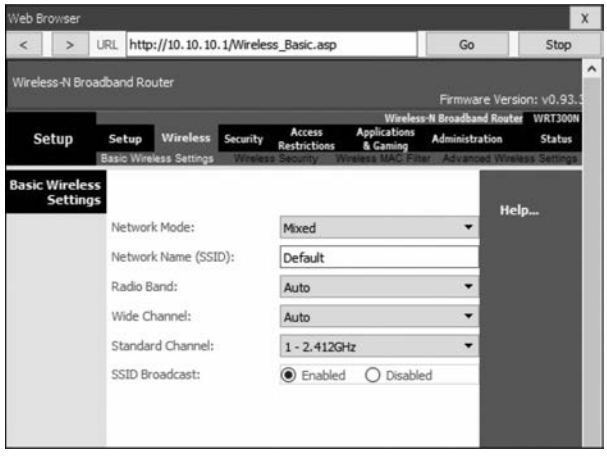

Figure 6-28 Viewing the WLAN Defaults

Step 2. Change the network mode. Some wireless routers allow you to select which *802.11 standard* to implement. The example in Figure 6-29 shows that Mixed has been selected. This means wireless devices connecting to the wireless router can have a variety of wireless radios installed. Today's wireless routers that are configured for mixed mode most likely support 802.11a, 802.11n, and 802.11ac NICs.

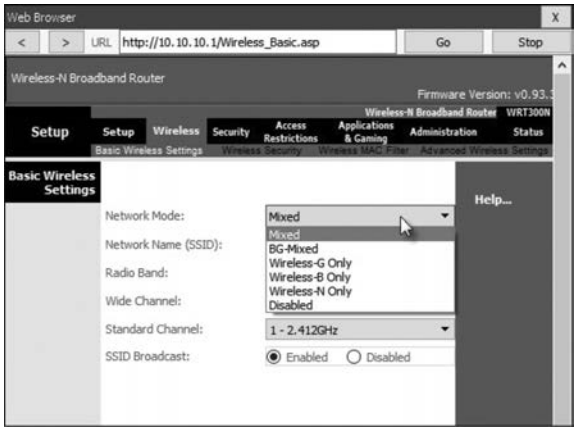

Figure 6-29 Changing the Network Mode

Step 3. Assign an SSID to the wireless LAN (WLAN), as shown in Figure 6-30. OfficeNet is used in this example. The wireless router announces its presence by sending broadcasts advertising its SSID. This allows wireless hosts to automatically discover the name of the wireless network. If the SSID broadcast is disabled, you must manually enter the SSID on each wireless device that connects to the WLAN.

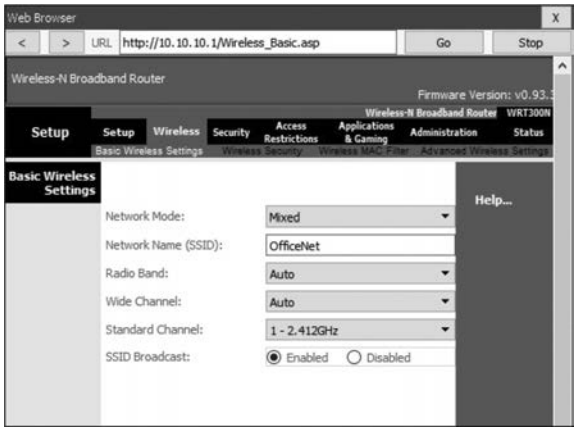

Figure 6-30 Configuring the SSID

Step 4. Configure the channel, as shown in Figure 6-31. Devices configured with the same channel within the 2.4 GHz band may overlap and cause distortion, slowing down the wireless performance and potentially breaking network connections. The solution to avoid interference is to configure non-overlapping channels on the wireless routers and access points that are near each other. Specifically, channels 1, 6, and 11 are non-overlapping. In the example in Figure 6-31, the wireless router is configured to use channel 6.

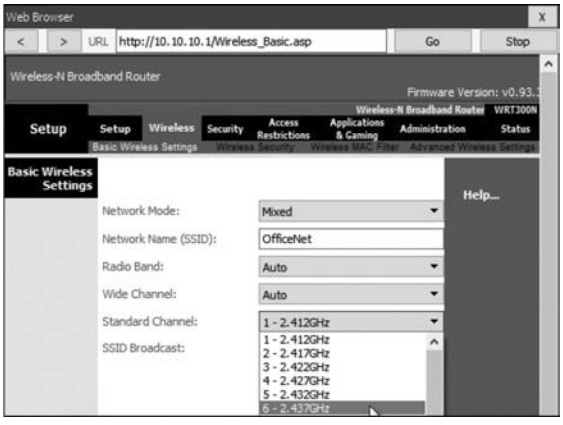

Figure 6-31 Configuring the Channel

Step 5. Configure the security mode. Out of the box, a wireless router may have no WLAN security configured. In the example shown in Figure 6-32, the personal version of Wi-Fi Protected Access version 2 (WPA2 Personal) is selected. WPA2 with Advanced Encryption Standard (AES) is currently the strongest security mode.

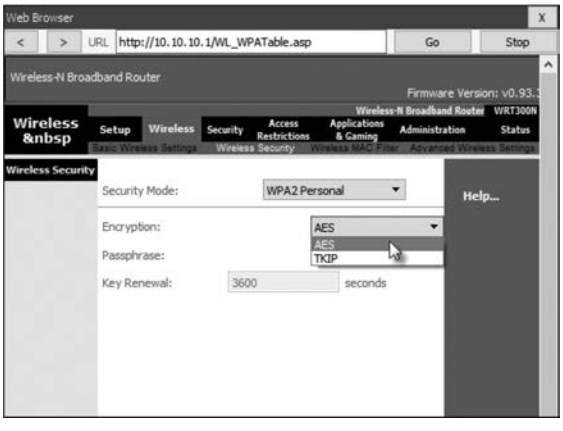

Figure 6-32 Configuring the Security Mode

Step 6. Configure the passphrase, as shown in Figure 6-33. WPA2 Personal uses a passphrase to authenticate wireless clients. WPA2 Personal is easier to use in a small office or home environment because it does not require an authentication server. Larger organizations implement WPA2 Enterprise and require wireless clients to authenticate with a username and password.

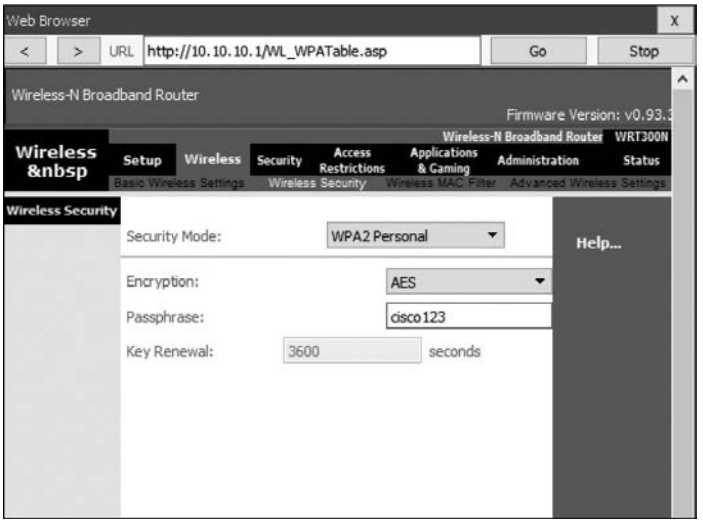

Figure 6-33 Configuring the Passphrase

Configure a Wireless Mesh Network (6.1.3.6)

In a small office or home network, one wireless router may suffice to provide wireless access to all the clients. However, if you want to extend the range beyond approximately 45 meters indoors or 90 meters outdoors, you can add wireless access points. In the wireless mesh network in Figure 6-34, two access points are configured with the same WLAN settings from our previous example. Notice that the channels selected are 1 and 11 so that the access points do not interfere with the wireless router, which was previously configured to channel 6.

Extending a WLAN in a small office or home has become increasingly easy. Manufacturers have made creating a ***wireless mesh network (WMN)*** simple through smartphone apps. You buy a system, disperse the access points, plug them in, download the app, and configure your WMN in a few steps. Search the Internet for "best Wi-Fi mesh network system" to find reviews of current offerings.

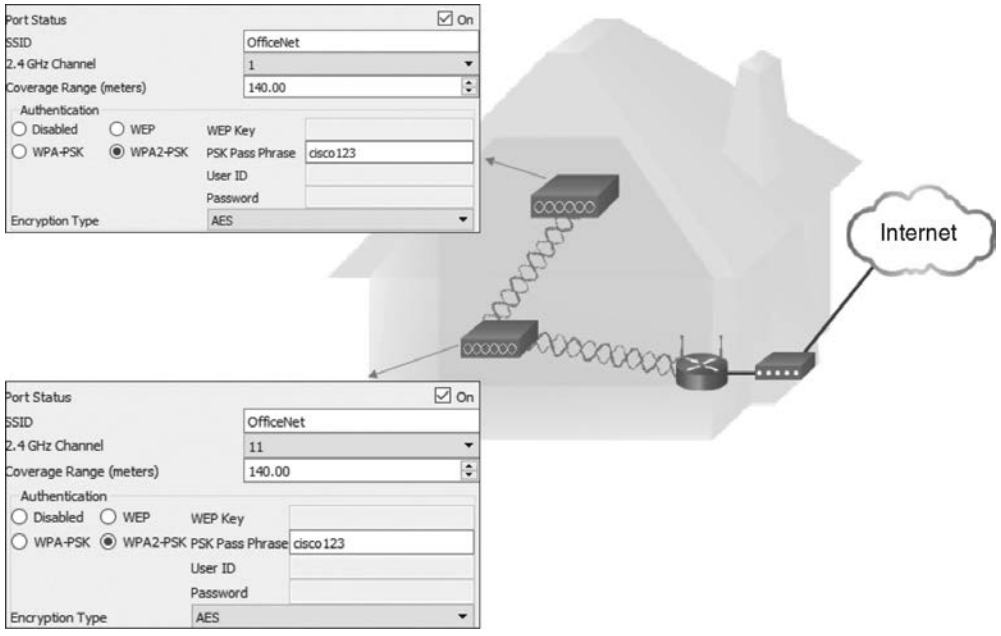

Figure 6-34 Wireless Mesh Network in a Home

NAT for IPv4 (6.1.3.7)

On a wireless router, if you look for a page like the Status page shown in Figure 6-35, you will find the IPv4 addressing information that the router uses to send data to the Internet. Notice that the IPv4 address 209.165.201.11 is a different network than the 10.10.10.1 address assigned to the router's LAN interface. All the devices on the router's LAN will be assigned addresses with the 10.10.10 prefix.

The 209.165.201.11 IPv4 address is publicly routable on the Internet. Any address with 10 in the first octet is a private IPv4 address and cannot be routed on the Internet. With the 10.10.10.1 address, the router will use a process called ***Network Address Translation (NAT)*** to convert private IPv4 addresses to Internet-routable IPv4 addresses. With NAT, a private (local) source IPv4 address is translated to a public (global) address. The process is reversed for incoming packets. The router is able to translate many internal IPv4 addresses into public addresses by using NAT.