

Managing Network Connections

You can view a list of all the connection interfaces (wired and wireless) on a computer by opening Network And Sharing Center and clicking Change Adapter Settings. You can right-click any network connection and select Status. If you click Details on the Local Area Connection Status dialog box, you access the Network Connection Details information box. This was shown in Figure 6-38 earlier in this lesson.

On a small wired network with ICS enabled, a workstation typically has an address on the 192.168.0.0/24 network with its default gateway 192.168.0.1. A WAP is typically not configured with the 192.168.0.1 address but might instead have, for example, the IP address 192.168.123.254. Whatever the settings on your network are, you should take note of them when everything is working correctly. This information is invaluable if something goes wrong.

NOTE **CHANGING NETWORK SETTINGS**

Rather than accept the default ICS settings, many administrators prefer to change them (for example by using the 10.0.10.0/24 network for wired computers and the 192.168.123.0/24 subnet for wireless ones). However, changing default ICS settings is not in the objectives for the 70-680 examination.

When you right-click an adapter and click Properties, this accesses the Local Area Connections Properties dialog box. From this dialog box, you can enable or disable the items shown or install more items (client services, server services or protocols) by clicking Install.

Typically, the Local Area Connection Status dialog box for both wired and wireless connections) might contain the following items:

- Client for Microsoft Networks Enables the computer to access resources on a Microsoft network.
- Quality of Service (QoS) Packet Scheduler Provides traffic control. This can be significant if you have high-bandwidth traffic, such as video streaming, on your network.
- File and Printer Sharing for Microsoft Networks Enables other computers to access resources on your computer in a Microsoft network (and other networks).
- Internet Protocol Version 6 (TCP/IPv6) Permits IPv6 configuration.
- Internet Protocol Version 4 (TCP/IPv4) Permits IPv4 configuration.
- Link-layer Topology Discovery Mapper I/O Driver Discovers and locates other computers, devices and network infrastructure features on the network and determines network bandwidth.
- Link-layer Topology Discovery Responder Allows a computer to be discovered and located on the network.

If an item is configurable, selecting the item activates the Properties button, which you can click to configure the item's properties. You can also configure the adapter itself (for example, updating the driver) by clicking Configure in the Local Area Connections Properties dialog box.

Take note of the items that have been installed and enabled on your computer while it is working correctly. It is probable that all the other computers on a network that you are administering have similar settings (apart from their IP addresses). It is a good idea to check this, possibly by using Remote Desktop. Although you might not change these settings very often, if something goes wrong you can find out what the original settings were.

✓ Quick Check

- From which dialog box can you add a new protocol, server service or client service?

Quick Check Answer

- The Local Area Connections Properties dialog box

You can also right-click a connection in the Network Connections dialog box and select Diagnose. This starts Windows Network Diagnosis, as discussed in Lesson 1 of this chapter.

If you have more than one network connection, you can create a network bridge by selecting two or more connections (click each connection in turn while holding down the Ctrl key) and then right-clicking and selecting Bridge Connections. If you are not logged in as an administrator, you are asked to supply credentials.

A network bridge is software or hardware that connects two or more networks so that they can communicate. If you are managing a network that has different types of networks (for example, wired and wireless), you would typically use a bridge when you want to exchange information or share files among all the computers on those networks. If you use the network bridge software built into Windows 7, you do not need to buy additional hardware.

Troubleshooting Wireless Networks

Lesson 1 discussed basic troubleshooting and resolving connectivity issues. However, connectivity problems exist that are unique to wireless networks and you need to be aware of them and know how to resolve them.

Preventing Your Computer from Switching Between WAPs

When you, or users you support, move around with a mobile wireless-enabled computer, the computer can switch automatically from one wireless network to another to stay connected. This is normal behaviour if automatic switching is enabled. Automatic switching is used, for example, in business premises, hospitals or academic institutions that are too large to be covered by a single network.

However, problems can occur when the same location is within range of several wireless networks and a computer tries to switch among these access points even though the user has not moved his location. This can cause temporary interruptions to the user's connection or the computer might lose the connection entirely.

With 802.11b or 802.11g routers and access points, the maximum range is up to 150 feet (46 metres) indoors and 300 feet (92 metres) outdoors. With 802.11a routers and access points, the maximum range is 50 feet (15 metres) indoors and 100 feet (30 metres) outdoors. These ranges are for optimal conditions with no interference. If a wireless-enabled computer is (for example) on a desktop that is 50 feet distant from one WAP and 70 feet away from another, problems can occur. You can ask the user to move (usually impractical) or turn off automatic switching in one or both of the network profiles.

You do this by clearing the Connect To A More Preferred Network If Available check box on the network's Wireless Network Properties dialog box, shown earlier in Figure 6-39. You can do this for one or both of the overlapping networks. This action results in a user needing to detect and manually connect to the network she wants to use rather than having the computer attempting to connect to both networks.

WARNING DISABLING AUTOMATIC SWITCHING IS NOT ALWAYS A GOOD IDEA

You can disable automatic switching between preferred networks to solve the problems that occur when a user is working in an overlap area. However, be very cautious about doing this as a matter of course. A doctor working in a hospital does not want to manually connect to another WAP point when she moves from one ward to another. A teacher does not want to change his settings when moving between classes. Always ensure that your users understand the disadvantages of this 'fix.'

Reducing Interference

To reduce interference from devices such as mobile phones and microwave ovens, you can change the channel that your WAP uses. Some channels are less prone to interference than others. To configure a third-party WAP, you follow the manufacturer's instructions. However, you can configure most third-party WAPs through a Web interface from any computer on the network.

If, for example, your WAP has an IPv4 address of 192.168.123.154, then entering **http://192.168.123.254** should access configuration controls similar to those shown in Figure 6-41. This illustration shows the basic setup page for an unidentified third-party WAP with default settings. Whatever the equivalent control looks like on your network, you can log in and change the channel settings. A number of factors determine which channel gives you the least interference; these include your location and the type of devices that are causing interference. You need to experiment with channel settings until you find the best one.

802.11b and 802.11g use the 2.4-GHz frequency. Microwave ovens and cordless phones also use this frequency. 802.11a uses the 5-GHz frequency. Some cordless phones also use this frequency. If these devices cause interference between a computer and the network it is connected to, the computer might try to switch to another nearby network. It is often impractical to ask your friends not to phone or your neighbours not to use their microwaves while you are browsing the Internet.

The screenshot shows a web browser window titled "Wireless Broadband NAT Router Web-Console - Windows Internet Explorer" with the address bar showing "http://192.168.123.254/". The browser's address bar also contains the text "automatic switching". The page content is titled "Wireless Broadband Router 11G". On the left, there is a "User's Main Menu" with "Status" selected. Below it, there is a "System Password" field with a masked password and a "Log in" button. The main content area is titled "System Status" and contains two tables.

Item	WAN Status	Sidenote
Remaining Lease Time	96:37:36	
IP Address	82.40.60.120	
Subnet Mask	255.255.248.0	
Gateway	82.40.56.1	
Domain Name Server	194.168.4.100, 194.168.8.100	
Wireless LAN MAC	00-50-18-4B-F4-64	
WAN MAC Address	00-50-18-4B-F4-63	

Statistics of WAN	Inbound	Outbound
Octets	4046320997	2398170235
Unicast Packets	1877357	4645800
Non-unicast Packets	259708680	5684

FIGURE 6-41 A typical third-party WAP configuration interface

The solution here is to change the WAP settings to use a different wireless channel or to configure the channel to be selected automatically if it is set to a fixed channel number. Check the manufacturer's information that came with your WAP for instructions about how to set the wireless signal channel.

Networks with the Same Service Set Identifier (SSID)

The SSID is the identity of your wireless network. If a network on your list of preferred wireless networks has the same SSID as another network that is in range of your computer, Windows might try to switch between the two WAPs because it considers them to be the same network. Typically, the default SSID of a WAP is named Default. If several people set up wireless networks (for example, in an apartment block or in a building that contains a number of small business offices) and none of them change the default, then problems can occur. In this case, the solution is to give each WAP a unique SSID.

Figure 6-42 shows the wireless setup page for a third-party WAP with default settings. This page lets you specify the channel and change the SSID.

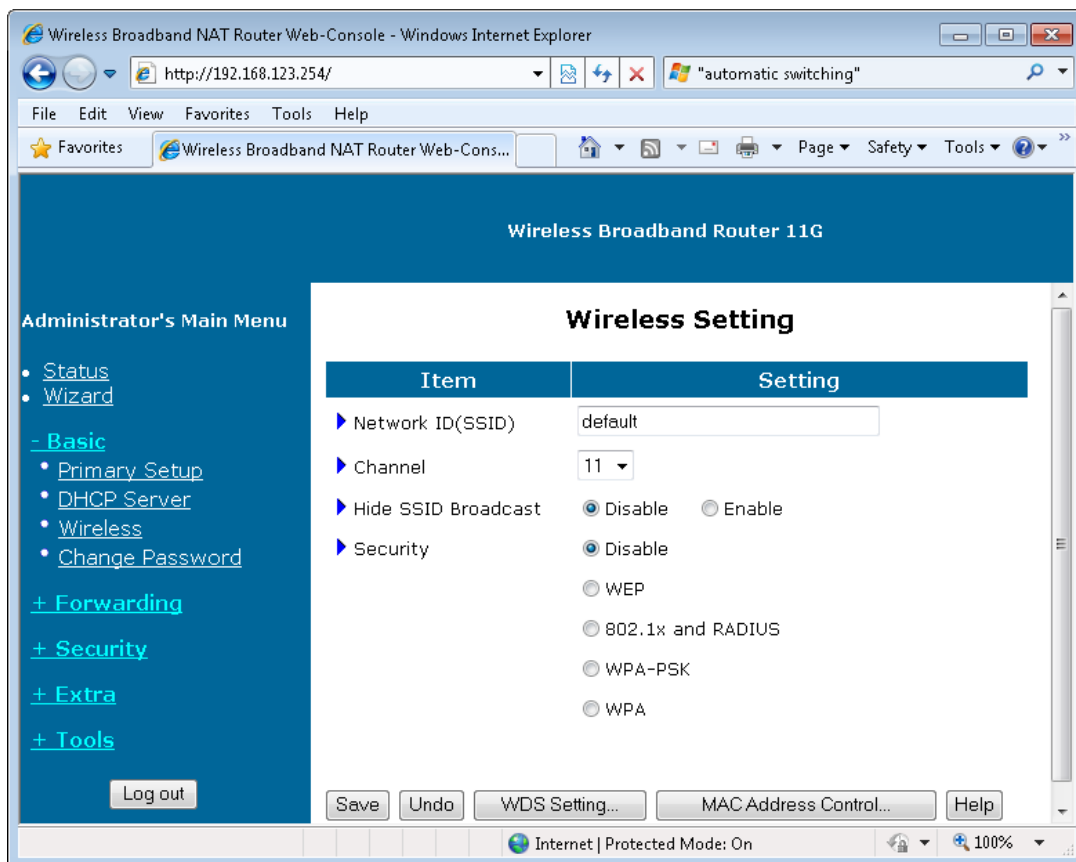


FIGURE 6-42 SSID, channel, SSID broadcast and security settings on a typical third-party WAP

You should always secure a wireless network by changing the SSID and configuring other security settings, as described later in this lesson. If you do not secure your wireless network, a thief no longer needs to break into your home. He or she can sit in an automobile outside your front gate, turn on a wireless-enabled laptop, steal your passwords and empty your bank account. If you are configuring a wireless network for your company and do not secure it, your company could be out of business and you could be out of a job.



REAL WORLD

This actually happened. Some time ago, when wireless home networks were comparatively rare, an employee in the customer support section of a computer equipment retailer received three calls on the same day from customers reporting problems with delays and loss of connectivity in their wireless networks. In one case, the network had been working perfectly for just over a week before the problems occurred. In the other two cases, the networks had been newly installed.

The employee took the precaution of checking the addresses of the customers. They all lived in the same apartment block. Apparently one of them had set up a wireless network and had been so impressed with it that he had invited his immediate neighbours in to have a look at it. They too had been impressed and as a result they purchased exactly the same equipment—with exactly the same defaults.

Configuring Wireless Network Security

Many wireless connection problems are related to security. The precise steps involved in setting up security depend on the type of WAP you have installed on your network. This section discusses the settings available in most WAPs and ways in which you can increase wireless network security. You can take the following steps to increase security in your own or your employer's wireless network:

- **Change the default SSID** Typically, you do this so that nearby networks with default settings do not interfere with your wireless network. Changing a SSID also improves network security because hackers who see a network with a default SSID deduce that it is a poorly configured network and are thus more likely to attack it.
- **Turn on WPA or WEP encryption** All wireless equipment supports some form of encryption that scrambles messages sent over wireless networks so they cannot be easily read if they are intercepted. You should choose the strongest form of encryption that works with your wireless network. However, all wireless devices on your LAN must share the identical encryption settings. Therefore, you need to find the most secure setting that you can configure on both your WAP and your wireless adapters. You configure authentication and encryption settings on your wireless adapters by using the Security tab of the network's Wireless Network Properties dialog box, as described earlier in this lesson.
- **Change default administrator passwords** The Web page interface that allows you to configure a third-party WAP usually presents you with a logon dialog box that requires at least a password (typically *admin*) and sometimes a user name. The default settings are well known to hackers. Change them.
- **Enable MAC address filtering** This is regarded as a fairly complex configuration because MAC addresses—48-bit hexadecimal numbers—look daunting. Many administrators believe they need to go a round all their network devices, enter the `ipconfig /all` command, write down the MAC addresses and then type this information into the WAP configuration Web site interface. In fact, this time-consuming operation is not necessary. ARP resolves IP addresses to MAC addresses and caches the results. So all you need to do is sit at a single station on your network, ping all the network devices (firewalls permitting) and then capture the contents of the ARP cache into a text file from which you can copy and paste them into the WAP interface. Unless you require that other laptops should be able to use a wireless network (in a hotel, for example) you should configure MAC filtering to help secure your network.
- **Disable SSID broadcast** A WAP typically broadcasts its SSID at regular intervals. This feature is designed for businesses and mobile hot spots where wireless clients might come and go. In a home network and many small office networks, this feature is unnecessary and increases the likelihood that a hacker will try to log on. If you know the settings on your WAP, you can connect to it either through Network And Sharing Center or by a *Netsh* command, as described earlier in this lesson.

- Do not auto-connect to open wireless networks Connecting to an unsecured wireless network exposes a computer to security risks. Some network adapters have a setting that prohibits this. This is a setting specific to the adapter, not to Windows 7. Windows Live One-Care, if installed, increases browser and firewall security if a computer connects to an unsecured network.
- Enable firewalls Ensure that Windows Firewall is enabled on wireless computers. If the WAP has a built-in firewall, check that this firewall is enabled.
- Position the WAP centrally Wireless signals normally reach to the exterior of a home or office but you should minimise the outdoor leakage as much as possible. Position the WAP near the centre of the building. Do not put it on your front windowsill.
- Turn off the network during extended periods of nonuse It is often impractical to turn a WAP off frequently but consider doing so during extended periods offline (for example, during holiday closures).
- Consider assigning static IP addresses to wireless clients DHCP makes setup easy and comparatively error-free. However, network attackers can obtain valid IP addresses from a network's DHCP pool. Most WAPs let you disable DHCP. You can then assign private static IP addresses to all your network devices. This increases security, but static setup is inconvenient and error-prone. You should consider this option only in networks where security is a highly critical consideration or your WAP appears to have problems configuring (for example) external DNS settings through DHCP.

Windows 7 Printing Enhancements

Windows 7 introduces location-aware printing, printer driver isolation, configurable default spooler security settings and an improved point-and-print experience for users. These enhancements build upon the features introduced by Windows Vista and are fully supported in Windows 7; they include high-fidelity print output, improved print performance, greater manageability of printers and print servers, integrated support for the new XML Paper Specification (XPS) and the Windows Color System.

On a Windows 7 computer, you can take advantage of integrated support for the new XML Paper Specification (XPS) that describes the content and appearance of paginated documents. The XPS document printing capability supports vector-based graphics that can be scaled up to a high degree without creating jagged or pixellated text. An XPS document is created by default when you print from any application running on Windows 7 and you can print this document without re-rendering to an XPS-capable printer by using Microsoft XPS Document Writer. You can view XPS documents in Internet Explorer by using the Microsoft XPS Viewer.

By default, Windows 7 renders print jobs on the client instead of the print server. This can significantly reduce print processing times when printing to XPS-capable printers. Client-side rendering (CSR) also works on non-XPS printers, diminishes the CPU and memory load on print servers and can reduce network traffic. XPS documents render an image once and reuse the rendered image on multiple pages of a print job.

The Print Management MMC snap-in has been enhanced to allow administrators to configure default security settings for print servers and printer driver isolation settings. Custom filter capabilities have also been extended with additional filter criteria to make filtering more powerful.

The Network Printer Installation Wizard is easier to use than the Add Printer Wizard (which is still available in Windows 7) and has new capabilities, making it easier for users to connect to remote printers and to local printers that are not Plug and Play. Standard users can install printers without requiring administrative privileges.

Improved Colour Facilities

The new Windows Color System (WCS) provides a richer colour-printing experience and supports wide-gamut printers (that is, inkjet printers that use more than four ink colours). To improve print quality on an installed printer, carry out the following procedure:

1. On the Start menu, click Devices And Printers.
2. Double-click a printer. You can see what is printing; change the name, security settings and other properties of your printer; or change colour, layout and paper settings.
3. Double-click Adjust Print Options. The Advanced tab of the Printer Preferences dialog box, shown in Figure 6-43, lets you specify colour settings and enhance print quality and greyscale. The icons at the top right of the tab let you specify duplex printing (if available), set a watermark, specify page settings and set device options.

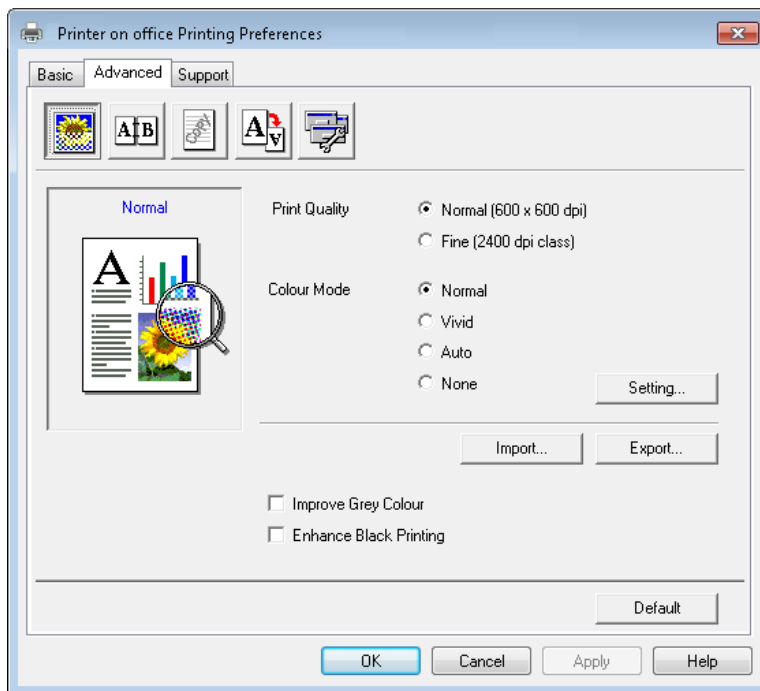


FIGURE 6-43 The Advanced tab of the Printer Preferences dialog box

Location-Aware Printing

Windows Vista enables you to assign printers based on location by using Group Policy and linking Group Policy Objects to sites in Active Directory Domain Services (AD DS). When mobile users move to a different site, Group Policy updates their printer connections for the new location; when the users return to their primary site, their original default printers are restored.

Windows 7 extends this idea and introduces location-aware printing. This allows mobile computer (for example, laptop) users to set a different default printer for each configured network location. Note, however, that location-aware printing is not the same as assigning printers based on their AD DS site.

Microsoft introduced location-aware printing in response to the increasing importance of mobile computers in enterprises. A typical scenario is as follows:

- Don Hall, an employee of the A. Datum Corporation is issued with a company laptop for use in the office and at home. While at work, he connects to a laser printer via the Add Printer Wizard. The printer is automatically set as the default for the A. Datum Corporation network.

- On returning home, Don adds a Plug-and-Play USB inkjet printer. The printer is automatically set as the default for his home network. However, when Don goes back to work the following day and connects to his corporate network, the A. Datum Corporation laser printer is automatically set as his default printer. When he returns home, connects to his home network and plugs in his inkjet printer, the inkjet printer is once again the default.
- Whenever Don is at work, his work printer is his default printer and whenever he is at home, his home printer is his default printer. Don does not need to specify a new default printer every time he switches networks, as in previous versions of Windows. He does not need to set up or configure anything as he moves from network to network.

When location-aware printing is available on a computer running Windows 7, an additional control named Manage Default Printers is displayed on the toolbar of the Devices and Printers dialog box. By clicking this control, you open the Manage Default Printers dialog box, shown in Figure 6-44, in which you can configure default printers for each connected network.

When Change My Default Printer When I Change Networks is selected, you can choose each network in turn by clicking the Select Network drop-down box. You can then choose a printer as the default for this network from the Select Printer drop-down box. If a user installs a printer on a network and selects it as the default, these settings are automatically configured in the Manage Default Printers dialog box. You can disable location-aware printing by selecting Always Use The Same Printer As My Default Printer in the Manage Default Printers dialog box.

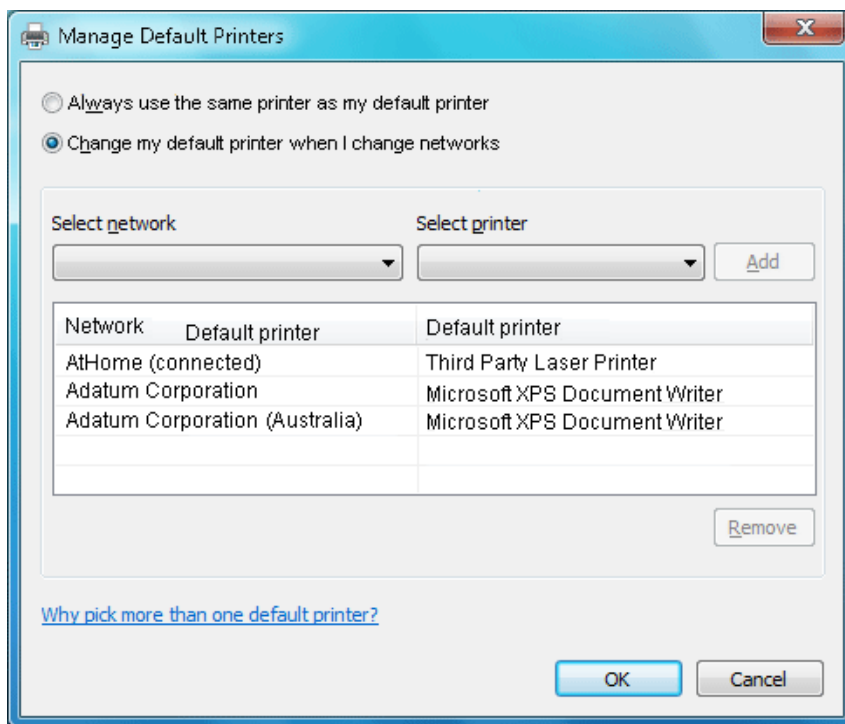


FIGURE 6-44 The Manage Default Printers dialog box

PRACTICE Creating an Ad Hoc Network

In this practice, you create an ad hoc network linking the Aberdeen and Canberra computers. This requires that both computers have wireless adapters and is therefore an optional exercise.

EXERCISE Creating an Ad Hoc Network

In this exercise, you create an ad hoc network while logged on to the Aberdeen computer with the Kim_Akers administrator-level account. You then log on to the Canberra computer with a standard (nonadministrative) account and join the ad hoc network. You created standard accounts earlier in this course—for example the Don Hall account you created in Chapter 4 in Book 1. If you do not have a standard account on Canberra, create one before you start the exercise.

To create an ad hoc network, proceed as follows:

1. Disconnect the Ethernet connection between the two computers and ensure that both computers have their wireless adapters switched on.
2. Log on to the Aberdeen computer with the Kim_Akers account.
3. Create a folder called Test on the Aberdeen computer.
4. Right-click the Test folder and choose Properties.
5. On the Sharing tab, click Advanced Sharing and share the folder. Ensure that the Everyone group has Read permission.
6. Open Network And Sharing Center.
7. Click Set Up A New Connection Or Network.
8. Select Set Up A Wireless Ad Hoc (Computer To Computer) Network, as shown in Figure 6-45. Click Next.

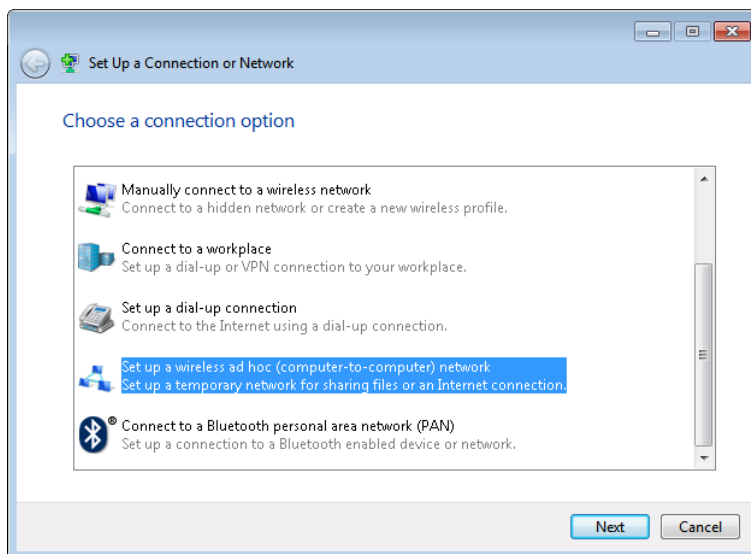


FIGURE 6-45 Selecting the Set Up A Wireless Ad Hoc (Computer To Computer) Network option

9. Click Next to clear the Set Up A Wireless Ad Hoc Network message box.
10. Specify a Network Name called **MyAdHoc**, specify WEP as the Security Type and enter **P@ss1** as the Security Key, as shown in Figure 6-46. Click Next.

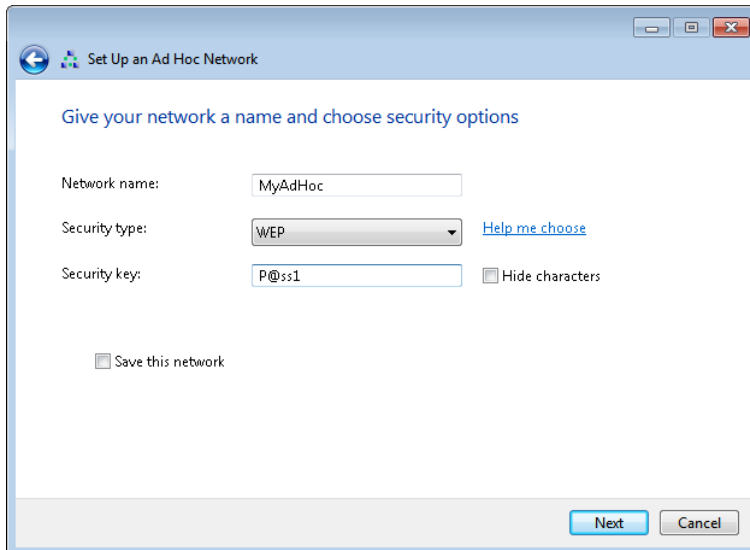


FIGURE 6-46 Specifying ad hoc network parameters

11. Click Close.
12. In Network And Sharing Center, click Connect to a Network. The MyAdHoc network displays with the message Waiting For Users.
13. Log on to the Canberra computer with a nonadministrative account.
14. Click the Wireless Network icon at the bottom left section of your screen.
15. Right-click MyAdHoc and click Connect.
16. Enter the security key (**P@ss1**).
17. In the Search box on the Start menu, enter **\\Aberdeen**. Check that you can see the shared Test folder.
18. Click the Wireless Network icon at the bottom left section of your screen.
19. Right-click MyAdHoc and click Disconnect. If the Canberra computer was previously connected to another network, reconnect it.
20. On the Aberdeen computer, disconnect from the MyAdHoc network. Check that the network is no longer listed on either computer.

Lesson Summary

- Problems with wireless connectivity can occur if a computer is within range of two preferred networks or two networks that have the same SSID. Interference from domestic devices can also cause problems. You can change the channel that a WAP uses to reduce interference.
- Using an unsecured wireless network can create significant security risks. If you configure a wireless network, always ensure that it is secure.
- You can connect to a wireless network, manage wireless networks and enable or disable a wireless adapter through the Network And Sharing Center. You can also use the *Netsh wlan* command-line utility to manage wireless networks.
- Windows 7 configures the default printer that you specify on a particular network to be the default whenever you connect to that network. Thus, when you switch networks, you shift default printers seamlessly. You can configure location-aware printing and specify default printers for specific networks.