MCITP Self-Paced Training Kit (Exam 70-623): Supporting and Troubleshooting Applications on a Windows Vista® Client for Consumer Support Technicians

Anil Desai

To learn more about this book, visit Microsoft Learning at
http://www.microsoft.com/MSPress/books/11229.aspx

9780735624238

Microsoft Press

Table of Contents

Chapter 6

Configuring Windows Vista Security

As a Consumer Support Technician, there's a good chance that you're aware of potential security issues that occur on customers' computers. It's not uncommon to hear complaints related to system slowdowns after visiting an unfamiliar Web site or installing a new application. Cleaning computers that have been infected by viruses or spyware can be a difficult and time-consuming process. The ideal solution is to prevent them from being infected in the first place. That leads to increasing security. Often, it's necessary to reduce the permissions that are granted to users on their own computers.

Security and usability are often at odds: increasing one often decreases the other. This makes the true goal of configuring and managing security settings a balancing act. Imagine, for example, if you were required to enter five different pieces of personal information to log on to a computer. In many ways, this system might be more secure than one that just required a single password. However, it would make the act of using your computer cumbersome and frustrating. You might even resort to writing down the necessary information on a piece of paper that you store near the computer (thereby negating the real benefits of the security itself). The net result would be that the drawbacks of implementing security overshadowed its potential benefits. On the other hand, you cannot simply grant all users full permissions to make changes to all areas of their systems. This often leads to the installation of malicious software or accidental file deletions and operating system changes.

Users rely on your expertise as a Consumer Support Technician to help them ensure that their systems remain secure. They expect to be reasonably protected from malware such as viruses, unwanted third-party applications, and security issues. Customers also expect you to help keep their systems usable and performing well over time.

One of the fundamental design goals Microsoft mandated for Windows Vista was to make the product as secure as possible while retaining compatibility with the vast library of existing programs that have been written for the Windows platform. Numerous features have been designed to meet this goal. In this chapter, you'll learn ways in which you can create, configure, and manage standard and administrator user accounts. Then, you'll learn about the User Account Control (UAC) feature of Windows Vista, including many different options that can be configured to meet users' needs. These are critical aspects of working with a secure operating system, whether in a home or small business environment.

Exam objectives in this chapter:

- Customize and configure user accounts.
- Configure User Account Control.

Lessons in this chapter:

Before You Begin

A basic understanding of computer security issues and concepts such as user accounts and permissions will be helpful as you learn the concepts in this chapter. You should have already installed Windows Vista and created at least one user account. Some of the practice exercises require you to be running Windows Vista Home Premium, Windows Vista Ultimate, or Windows Vista Business. Other editions of Windows Vista (such as Windows Vista Enterprise) will also work, but some of the default security settings might be different from those described in the text.

Lesson 1: Managing User Accounts

Modern operating systems such as Windows Vista have been designed to meet the needs of many different users. Accordingly, the operating system provides a method for creating multiple user accounts on a single installation of Windows Vista. You can configure and customize each user account based on the needs of the individual who will be using it. For example, desktop settings, screen savers, shortcuts, and user-specific data files are all stored separately for each account. In general, give each user of a system his or her own account.

From the standpoint of a consumer—a typical home or small-business user—it's common for a computer to include multiple user accounts. For example, a family of four might have separate accounts for each parent and each child. A small business might have various employees that occasionally use a single shared computer to perform specific tasks.

Regardless of the purpose of a particular user account, there are security-related considerations that should be addressed. In this lesson, you'll learn about the different types of accounts that are available in Windows Vista and how to create and manage them.

After this lesson, you will be able to:

- Describe the differences between standard and administrative user accounts.
- Provide examples of tasks that can be performed by administrative user accounts but not by standard user accounts.
- Create new standard and administrative user accounts.
- View and modify details about a user account.

Estimated lesson time: 45 minutes

Understanding User Account Types

When a user logs on to a computer running Windows Vista, he or she must provide valid credentials that prove his or her identity. Most commonly, a user performs a logon by using a combination of a user name and a password. Each user account has its own collection of settings and permissions. These include the following:

- **User profile** A user profile contains all of the operating system preferences that are defined separately for each user account. Examples include desktop wallpaper options, the Windows Sidebar configuration, and application shortcuts. By default, user profiles are located in the C:\Users folder.
- **Application settings** Each user profile has its own collection of application settings. These settings usually pertain to personal preferences for an application (such as default paths, toolbar layouts, and related details). They are stored either in the user-specific portion of the registry or in configuration files that are stored within the profile.

- **User data folder** Each user has his or her user data storage location on the computer. This enables multiple users of the same computer to keep their files separate from each other.
- **Other user-specific folders** To improve consistency and usability for operating system users, each user profile includes several shortcuts to special folders. Examples include Music, Pictures, Saved Games, Documents, Downloads, and Videos. Each user will have his or her separate shortcuts and storage locations for these default folders.
- **Security privileges and policy settings** Each user account has a set of security-related actions that it can perform. For example, users might have restrictions related to logon hours or installing applications.
- **File system permissions** These are details related to which actions the user can take on which files. For example, a user will be allowed to create and delete documents in his or her own user data folder but will not be able to access another user's data folder.

The two main types of user accounts in Windows Vista are Standard User and Administrator. In this lesson, you'll learn about the purposes of each account type, along with differences in the permissions they are granted. In Lesson 2, "Understanding User Account Control (UAC)," you'll look at details related to how the UAC feature can be used to enable the temporary elevation of privileges.

Standard User Accounts

The default type of user account in Windows Vista is a standard user account. This account is designed to provide basic permissions for completing common daily tasks. It allows users to launch applications, create new documents, and modify basic system configuration settings. In general, these operations affect only the user who is logged on to Windows Vista. They do not include systemwide changes such as the installation of new software.

Administrator User Accounts

Accounts that have Administrator permissions have the capability of performing any operation or task on the system. This includes all of the permissions that are granted to a standard user account plus the ability to make major operating system changes, install new software, and create and modify other user accounts. Administrator accounts also have the ability to set permissions for other users on the system.

There are potential security considerations for users who use an administrative account for daily computer use. The primary issue is that unwanted software can make changes to the operating system or to data without the user's permission. This is because all programs run, by default, using the security permissions of the user who launched them. A related issue is that such users have the ability to perform actions that could lead to operating system instability or corruption. For example, a novice user who is running as an Administrator might accidentally delete critical operating system files or programs, thinking that they are not

needed. These are all reasons why Microsoft designed the UAC feature as a major component of Windows Vista.

Therefore, it is recommended that most users log on to their computers using a standard user account. One potential problem with this approach is that applications often expect to have full permissions on the system. You'll learn about ways in which this situation can be addressed in Lesson 2.

Windows Vista creates a default account called Administrator during the installation process. This account has full permissions on the system and is generally not designed for regular use. For this reason, the default Administrator account is disabled on new installations. For in-place upgrade installations of Windows Vista, the setup process disables the built-in Administrator account only if there are other active Administrator accounts on the system. If there aren't any, the account remains enabled.

The Guest Account

A third type of account that is created with default Windows Vista installations is the Guest account. This account is designed for users who require temporary access to a computer and don't need to store their user-specific profile settings permanently. For example, if a friend is visiting your home and just needs to launch a Web browser to check her e-mail, you can allow her to use the Guest account. Users who log on as a guest have a very limited set of permissions. For example, they cannot access other users' files or perform systemwide tasks such as installing software or hardware.

For security reasons, the built-in Guest account is disabled by default. This prevents users from having an option to log on to the system as Guest.

Comparing User Permissions

When working with standard and Administrator user accounts, it's important to understand which actions each type of user is allowed to perform. Specifically, it's important to understand a list of permissions that are granted to standard user accounts. In this section, you'll learn examples of operations that can be performed by each type of account.

Permissions of Standard User Accounts

The following actions can be performed by a standard user account:

- Perform basic system management tasks. The built-in Windows Vista applications and tools indicate operations that require elevated permissions with a shield icon next to the control.
- Change personal user settings such as passwords, desktop wallpaper, system sounds, and screen savers.

- Access removable media such as memory storage devices and CD/DVD media.
- Create a local area network (LAN) connection.
- Connect to a wireless network.
- Personalize display settings, including desktop resolution and number of colors.
- Use Remote Desktop to connect to remote computers.
- Perform basic configuration settings in Control Panel. For example, a user can change power management settings.
- Enable or disable accessibility options such as the screen magnifier.
- Connect and configure some external devices, such as universal serial bus (USB) storage or Bluetooth devices.

It is important to note that these are the default settings for a standard user account. Administrators can manually change the permissions and privileges of users to meet their requirements. Also, in some cases, a background service or process might perform important tasks that the user cannot perform directly. One example is the disk defragmentation service, which is configured to run under a specific user account.

Permissions of Administrator Accounts

Administrator accounts, as mentioned earlier, have full permissions on a computer system. This includes the ability to change or delete files owned by any user on the system and to make changes to the operating system. Examples of operations that can be performed by an Administrator account but not by a standard user account include the following:

- Installing new software on the computer
- Adding new hardware and installing device drivers on the computer
- Making changes to configuration of the Automatic Updates feature
- Accessing files that are in secure locations, such as the Windows folder and the Program Files folder
- Configuring Windows Firewall (including enabling, disabling, and adding exceptions)
- Performing a complete system backup and restore operation
- Creating new user accounts, removing user accounts, and configuring the user account type
- Managing the behavior of the UAC feature

Again, this is just a sample of the types of operations that a standard user account cannot perform.

Exam Tip Exam 70-623 tests your ability to identify which types of operations require privilege escalation. One great way to learn these is to "poke around" the Windows Vista user interface. Open Control Panel items and Administrative Tools to see the actions you can perform as a standard user and which ones require additional permissions. This will help give you a good idea of the limits of standard user accounts without having to memorize long lists of potential actions.

Managing User Accounts

So far, you have looked at details related to the different types of accounts that are available on a computer running Windows Vista. In this lesson, you'll see how you can use that information to perform actual user account–related tasks. Many of these operations will require you to log on to the computer by using an account that has Administrator permissions.

Adding User Accounts

The Windows Vista Control Panel provides utilities that enable you to create and manage user accounts quickly and easily. To access the relevant settings, you need to have Administrator permissions on the computer. You can open the Manage Accounts window by clicking the Add Or Remove User Accounts link in the User Accounts And Family Safety section of the default Control Panel. Figure 6-1 shows an example of the available options and settings.

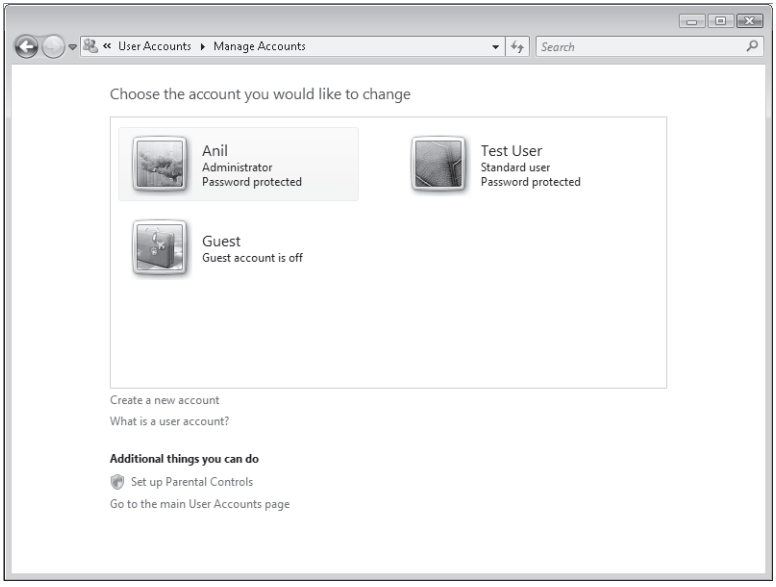

Figure 6-1 Using the Manage Accounts window in Control Panel

The default view shows a list of all of the users who are currently configured on the computer and an overview of their settings. The Create A New Account link starts the process of creating a new user (see Figure 6-2). The details that are required include the name of the new account. Usually, this corresponds to the individual who will be using that logon. The other option is related to whether the account should be created as a standard user (the default option), or as an Administrator.

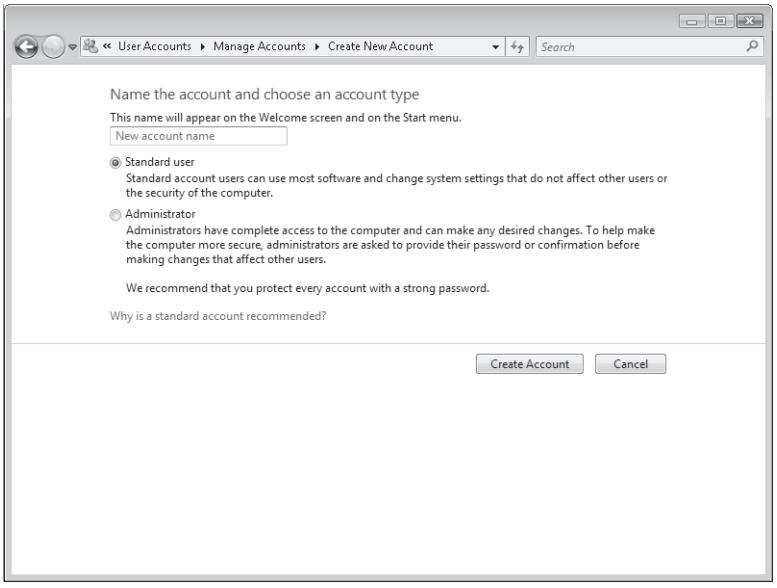

Figure 6-2 Creating a new user account

After you click Create Account, the new account is available for logon. Generally, you will want to configure various properties of the account before you make it available for use by individuals.

Configuring User Accounts

There are several different operations that are commonly performed when managing user accounts. You can access these by clicking the name or icon of an account in the Manage Accounts window. Figure 6-3 shows the options that are available.

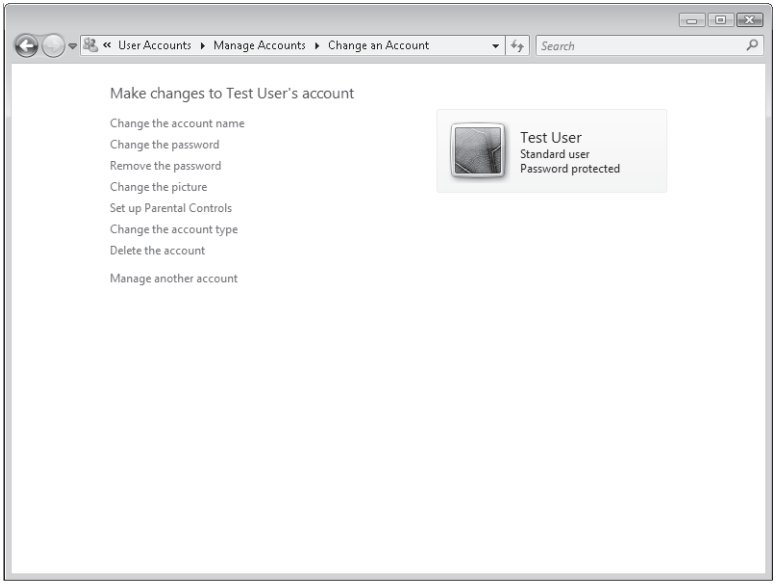

Figure 6-3 Changing settings for an account

The options include the following:

- Change The Account Name
- Change The Password (or Create A Password if the account does not currently have one)
- Remove The Password (if one is currently configured)
- Change The Picture
- Set Up Parental Controls
- Change The Account Type
- Delete The Account

The built-in Guest account has a limited set of options and commands. As mentioned earlier, this account is disabled by default. When you click the Guest account, you have the option of turning it on. If you click the Guest account item when it is turned on, you see the Turn Off The Guest Account link. The only other option that is available for a Guest account is the ability to change the picture that is used.

Changing Passwords

A common operation for users is to change their password. By default, standard users can change only their own passwords. It is a good practice for users to change any initial password that has been provided to them by an administrative user. Administrators have the ability to set, remove, or modify the password for any account. Figure 6-4 shows the Change Password dialog box.

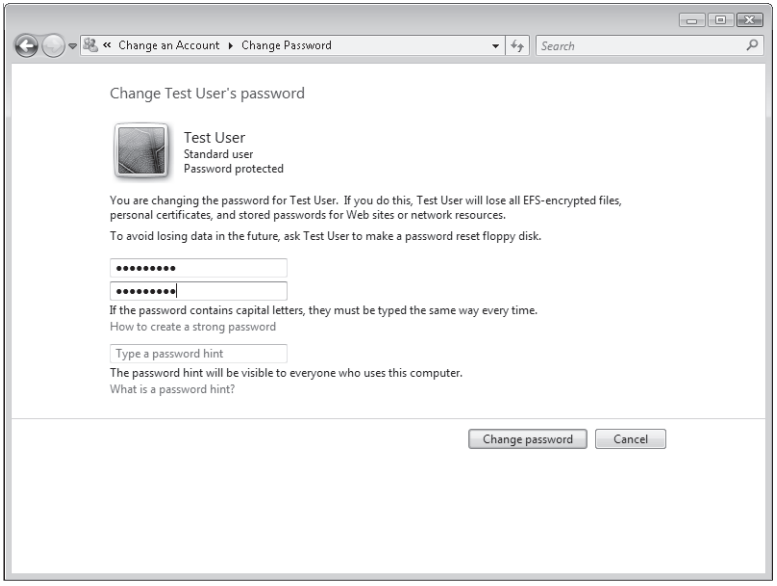

Figure 6-4 Changing an account's password

Passwords are case-sensitive; that is, capital and lowercase letters must be entered exactly as they have been defined. When changing a password, it might be necessary to enter the old password first. This is done to ensure that a user does not simply walk up to a computer to which someone is already logged on and make a change without knowing the original password. To make it easier to remember passwords, you can configure a password hint to be shown to all users who attempt to use the account through the logon screen. For this reason, this hint should be something that will help only the intended user access the system.

Performing Advanced User Account Configuration

The Manage Accounts window has been designed to provide access to the most common account-related operations on a computer running Windows Vista. In some cases, however, you might need to perform advanced operations. You can do this by using Local Users And Groups within the Computer Management console (see Figure 6-5). To access this console, in the Start menu, right-click Computer and choose Manage. Alternatively, if the Administrative Tools program group is available in the Start menu, select Computer Management.

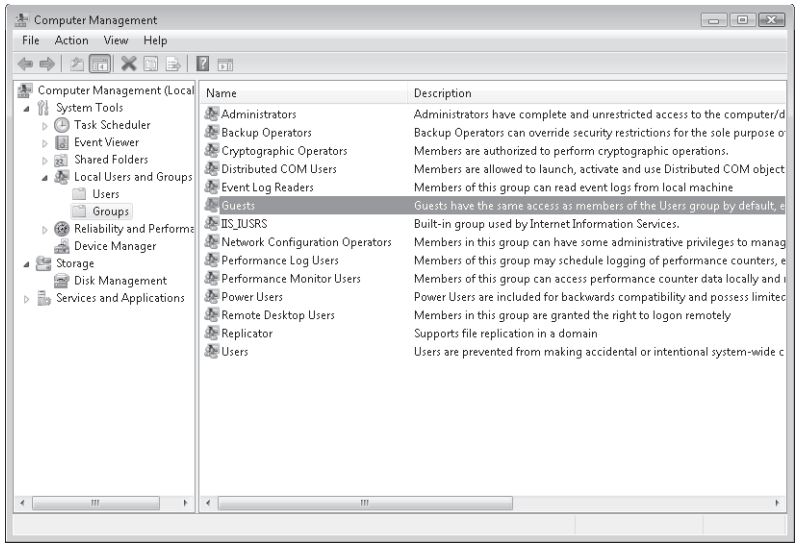

Figure 6-5 Using the Computer Management console to manage user accounts

The two main folders are Users and Groups. The Users folder contains a list of all of the user accounts created on the system. Depending on the software and services you have installed on the computer, it's possible that you'll notice some accounts that might not have been present in the Manage Accounts Control Panel item. Often, these accounts are designed to provide support for special software or services that require particular sets of permissions on the computer. You can view and modify detailed settings for a user by right-clicking the account and selecting Properties. User accounts have several different options, such as those shown in Figure 6-6.

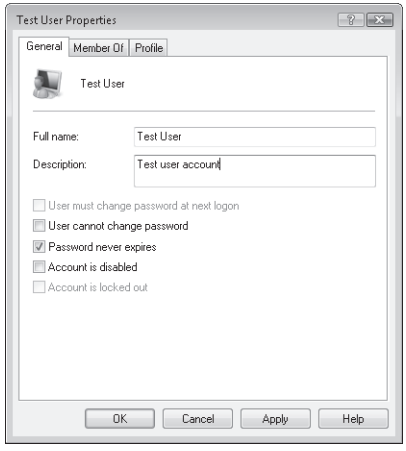

Figure 6-6 Viewing the General properties tab for a Windows user account

The Groups folder within Local Users And Groups displays a list of all of the security groups that are defined on the computer. You use groups to manage permissions for collections of users. A general practice is to place users in groups and then to assign permissions to the groups themselves. Because you can easily change the membership of a group, this simplifies the process of managing permissions.

MORE INFO Centrally managing advanced user settings

Most home and small-business users do not have reasons to configure advanced user settings and permissions manually. In general, you should encourage customers to use the features in Control Panel for managing security settings.

In corporate network environments, many of these options are more important. Most larger organizations have dedicated IT staff that are able to manage such settings centrally, using Windows Active Directory directory service.

In addition to the Administrators and Users groups, there are several other groups that pertain to collections of permissions that might be required for certain types of operations. For example, members of the Remote Desktop Users group are able to access this computer using the Remote Desktop feature, and members of the Backup Operators group can bypass standard file system security for performing a backup operation. Most groups include descriptive text that provides information about their purpose and function.

To view the members of a group, right-click the group name in the list and select Properties. The General tab shows a list of the user accounts that are currently members of the group (see Figure 6-7). The Add button also provides you with the ability to include new members in the group.

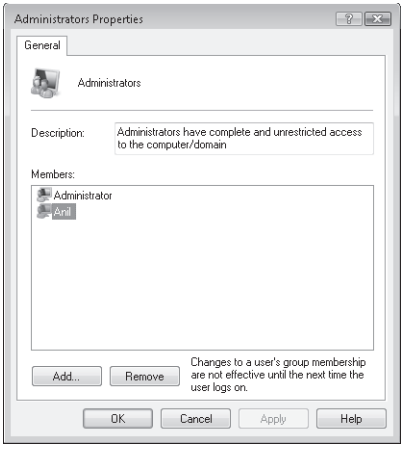

Figure 6-7 Viewing properties of a Windows Vista group

Quick Check

1. What is the recommended type of account to use for daily computer use?
2. Which type of account should you create or enable for a user who requires temporary access to the computer?

Quick Check Answers

1. Use a standard user account for performing common operations on the computer.
2. The Guest account has been designed to allow users temporary access to a computer. It provides a minimal set of permissions for performing common tasks.

Practice: Creating and Managing User Accounts

In this practice exercise, you will work with the user account management tools provided with the Windows Vista operating system.

▶ Practice: Create and Configure New Accounts

This exercise familiarizes you with the process of creating a new user account. To complete this exercise, you need to log on to the computer as an administrator initially.

1. Open Control Panel and click User Accounts And Family Safety. This opens the main window for security and safety-related settings.
2. Under User Accounts, click Add Or Remove User Accounts.

   You now see a list of all of the users who are currently configured on the computer.
3. Click Create A New Account to start the process of adding a new account.
4. Type **Test User** as a user name, and then choose the default Standard User option for the account type. This creates an account that has permissions to accomplish many common tasks, but it will not be able to change system settings.
5. Click Create Account.

   You now see the new user account in the Manage Accounts window.
6. To view and modify the settings of the Test User account, click it.
7. Click Change The Picture and select a different picture for the user account. Click Change Picture to complete the configuration. The picture you select appears on the Windows Vista logon screen.
8. By default, the new user account has not been assigned a password. To increase security, click Create A Password.
9. Type **test!123** in the New Password and Confirm New Password text boxes.

   Note that you can optionally provide a password hint to help the user remember his or her logon information. Remember that this hint is visible to all users of the system

(whether or not they have logged on), so be sure that it is something that is understood only by the user who will be using the account.

10. Click Create Password.
11. Close the Manage Accounts window and close Control Panel.
12. To test the new account, start by logging off the computer.
13. Next, test the new account by using it to log on to the system. You should see the Test User account as an option. Click this account, and then provide the password that you assigned in step 9 to log on to the system. During the first logon, Windows Vista creates a new user profile and sets up the default system settings for new accounts.
14. Try performing several different types of tasks using the new account. Make a note of which types of operations are allowed and which ones require you to type in administrator credentials.
15. When finished, log off the computer. Optionally, you can delete the Test User user account by logging on as an administrator and using the Manage Accounts window.

Lesson Summary

- For security reasons, it is recommended that users run with a minimal set of permissions whenever possible.
- Standard user accounts have limited permissions on the system but are able to perform most common day-to-day tasks.
- Administrator user accounts have full permissions on the computer, but users can run with minimal permissions for most tasks.
- You can enable the Guest account for use by individuals who might need to access the system occasionally.
- The Manage Accounts window in Control Panel enables administrators to create new accounts and modify account settings.
- You can use Local Users And Groups in the Computer Management console to perform advanced security configuration, including group membership.

Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 1, "Managing User Accounts." The questions are also available on the companion CD if you prefer to review them in electronic form.

NOTE Answers

Answers to these questions and explanations of why each answer choice is correct or incorrect are located in the "Answers" section at the end of the book.

---

1. You are a Consumer Support Technician explaining the limitations of a standard user account to a customer. Which of the following operations require the user to provide approval for privilege escalation when running in Admin Approval Mode? (Choose all that apply.)
   - **A.** Changing the user's own password
   - **B.** Installing new device drivers
   - **C.** Installing a new accounting software package
   - **D.** Changing the desktop wallpaper
2. You are a Consumer Support Technician assisting a user with configuring security on his Windows Vista–based laptop. The customer mentions that he often has friends and coworkers that want to use his computer temporarily to perform tasks such as checking stock quotes on a Web site. The customer wants to ensure that users cannot make permanent changes to his system configuration. Which of the following types of accounts are most appropriate for these individuals to use?
   - **A.** Administrator
   - **B.** Guest
   - **C.** Standard User
   - **D.** Power User

Lesson 2: Understanding User Account Control (UAC)

As mentioned earlier, one of the primary design goals for Windows Vista was to make it an extremely secure desktop operating system. This process has involved significant engineering effort in all areas of the Windows platform. Many of these improvements have been performed so that users might not readily notice them. Others, however, do require user interaction.

As a Consumer Support Technician, it's likely that you've heard about the User Account Control (UAC) feature of Windows Vista. The primary purpose of UAC is to ensure that users and applications are granted the lowest level of permission they require to complete their tasks. The benefits include ensuring that people and programs cannot make potentially disastrous changes to their systems. In this lesson, you'll learn about the purpose and function of UAC and how you can configure it based on customers' requirements.

After this lesson, you will be able to:

- Describe common security issues and considerations related to desktop operating systems.
- Describe the purpose and function of a UAC file and registry virtualization and Admin Approval Mode.
- Perform permissions elevations, including answering of prompts for consent and prompts for credentials.
- Enable and disable UAC by using Control Panel.
- Configure the behavior of UAC by using Local Security Policy settings.

Estimated lesson time: 60 minutes

Understanding Common Security Risks and Threats

In the area of computer security, it is often wise to know the methods of the "enemy." That is, it's important to understand ways in which malicious programs or people might be able to perform unwanted actions on your computer. Some of these actions might include the following:

- **Using system resources** Malicious programs might use CPU, memory, disk, and network resources to perform their tasks. In one example, users' computers are used to launch an attack on another site or computer without their knowledge. In those cases, users might notice that their computer appears to be working more slowly than before.
- **Tampering with critical system files or data** In some cases, the data might simply be destroyed. In other cases, it might be transmitted to other computers. Regardless, these changes can cause data loss and instability of the operating system.

- **Attempting to obtain personal information such as credit card numbers, user names, and passwords** Often, this data is then transmitted to a remote computer, where it might be used for actions such as identity theft.
- **Tracking system usage** Software that is commonly referred to as spyware often runs in the background on a computer, unknown to users. It collects information such as Web sites that are visited and then reports this information back to the distributor of the software. Apart from violating security, this can lead to system slowdowns and instability.
- **Displaying unwanted advertisements** It is a common practice for applications to include additional software that is installed with little or no warning to the user. The additional code can perform operations such as automatically loading content from Web sites.

Some of these programs might be designed with a specific purpose in mind (for example, collecting potentially useful personal financial data). In other cases, the programs might have no purpose other than to annoy the user. Regardless of the authors' goals, it's obvious that malware should be prevented from running on desktop computers.

Understanding the Security Goals of Windows Vista

A fundamental principle of managing security is giving users and applications a minimal set of security permissions. This ensures that they can perform the most common operations that they need to accomplish tasks, but it greatly limits the potential damage that a malicious program can cause. For example, users rarely (if ever) need to modify operating system files directly. By preventing them from performing this action, the operating system can avoid the mistaken or malicious deletion of critical components. By default, applications that a user launches inherit all of the permissions of that user. If a user can open a Microsoft Word document, type a letter, and then e-mail it, a program could easily perform the same actions automatically. Therefore, it's important to place restrictions.

Microsoft had two primary goals when designing security for the Windows Vista operating system. The first was to ensure that users and applications were granted a minimal set of permissions for completing common operations. The other goal, however, was to ensure compatibility with earlier applications. In previous versions of Windows, it was very common for programs to assume that they had full access to the computers on which they were running. They could easily perform tasks such as reading and writing files from the file system and making modifications to the system registry. Because developers relied on these capabilities, it was often necessary for users to log on to their systems with accounts that had full administrative permissions. If the permissions were not available, the application might fail to run or might return errors to the user. Based on the two goals of security and compatibility, let's look at some new architectural features in Windows Vista.

Real World

Anil Desai

There's no doubt about it: things would be far simpler for everyone involved if security were not a concern. In the early days of desktop computing, users and programs expected to have full control of their computers. Accordingly, application developers designed their programs under the assumption that they would also have these permissions and rights. Users would be able to perform any action they required on their systems. Unfortunately, having these abilities also increases potential security risks.

It is very important to understand that maintaining complete end-to-end security requires a team effort. It has been said that a chain is only as strong as its weakest link. It's not enough for a few users to follow the rules: all must do so. Application developers, home and business users, and Consumer Support Technicians must all exercise discipline to minimize security issues.

For example, from a network standpoint, having the world's most sophisticated and powerful firewall software won't prevent users from using their initials as their password. A malicious user might easily circumvent all of this protection simply by guessing the password. Similarly, you can easily disable the many security features in Windows Vista with just a few mouse clicks.

So how can you, as a Consumer Support Technician, do your part? Perhaps the most important aspect of ensuring security for the customers you support is to make sure that they understand the importance of features such as UAC. Users often don't see the benefits of limiting what they can easily do on their systems. This can lead them to circumvent or disable the features altogether. When, on the other hand, they see the potential benefits of security, they are much more likely to use best practices. Overall, it's your job to help lead the security team effort.

Understanding the UAC Process

In previous versions of Windows, it was most common for users to log on to their computers by using an account that had Administrator permissions. This meant that the user (and any program that he or she launched) would be able to perform any operation on the computer. This includes reading and writing to critical operating system files and accessing data stored anywhere on the system. In Windows Vista, it is recommended that users log on to the computer, using a limited set of permissions. In Lesson 1, you learned about the details of working with standard and administrative user accounts.

Microsoft designed the UAC feature of Windows Vista to allow users to log on to their computers using a standard user account. They can perform the majority of their tasks using a limited

set of permissions. During the logon process, Windows Explorer (which provides the user interface for Windows Vista) automatically inherits the standard level of permissions. Additionally, any programs that are executed using Windows Explorer (for example, by double-clicking an application shortcut) also run with the standard set of user permissions. Many applications, including those that are included with the Windows Vista operating system itself, are designed to work properly in this way.

Other applications, especially those that were not specifically designed with the Windows Vista security settings in mind, often require additional permissions to run successfully. These types of programs are referred to as *legacy applications*. Additionally, actions such as installing new software, and making configuration changes to programs such as Windows Firewall, require more permissions than what is available to a standard user account. Windows Vista can automatically detect when an application is attempting to use more than standard user privileges.

Understanding Standard User Mode

When a user logs on to Windows Vista by using a standard user account, Windows Explorer and all other processes that are launched run with a minimal set of permissions. In this mode, UAC requires the user to provide credentials to the system whenever an application or operation requires elevated permissions. When an application or process requests access to more permissions, the user is prompted for approval. This process is known as application elevation because it allows Windows Vista to give a program a full set of permissions. Figure 6-8 shows a sample screen. After the credentials are provided and accepted, the program runs with elevated permissions. The user, however, still continues to have only a limited set of permissions.

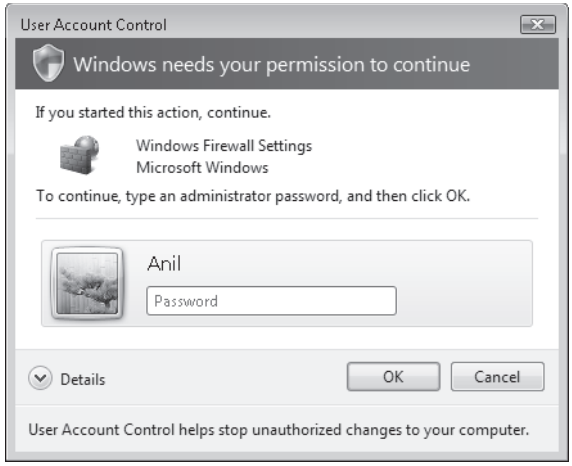

Figure 6-8 Providing administrator credentials for application elevation

In a typical consumer environment, the user might already have knowledge of the user name and password of an Administrator account on the computer. By providing those details, he or she is implying that he or she wishes to allow the program to run in an elevated way. Other users of the computer who do not have these credentials will be unable to perform administrator-level actions.

Another way in which the standard user mode can be used is often called the "over the shoulder" method. In this case, a parent or supervisor might want most users to run under the standard user mode. Whenever there is a need to elevate privileges, this person can provide the necessary credentials. For example, a mother might want her child to log on to the computer as a standard user. Whenever the child needs to perform tasks such as changing system settings or installing new software, the mother must provide the necessary credentials.

Understanding Admin Approval Mode

In some cases, users might want to log on to the computer by using an Administrator account but still have the security benefits of running with minimal permissions. UAC provides this ability by using the Admin Approval Mode. The user account technically has full permissions on the system, but UAC limits which actions the user can perform. This effectively makes the account behave like a standard user account for most operations. Actions that require additional permissions can be performed, but the user must first approve them.

When an application requests elevated privileges, the default prompt Windows Vista shows to the user is one that asks the user to provide consent (see Figure 6-9). This method ensures that the user is aware when an application is attempting to run with elevated privileges. It can also help prevent situations in which malware applications attempt to modify the system. However, by default, it does not require the user to provide credentials for an Administrator account, because the current account already has this ability. Later in this lesson, you'll see how you can change UAC settings to require credentials in Admin Approval Mode.

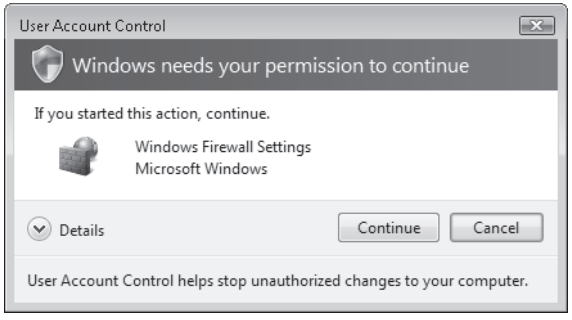

Figure 6-9 Providing consent for an application to run with elevated privileges

Additional Security Features

In addition to the UAC elevation prompts in Windows Vista, there are several other security-related enhancements that have been designed to increase safety and provide compatibility for earlier applications. In this section, you'll learn about how they work.

File System and Registry Virtualization

Two important areas of security-related concerns are the Windows file system and the registry. The file system contains files ranging from operating system components to user data. In the past, applications were designed with the assumption that they would be able to access these files and settings freely. These earlier applications often fail to run properly when they cannot make those changes.

To prevent direct access to secure file system locations (such as the operating system and Program Files folders), Windows Vista uses a technique called virtualization. This method works by monitoring for when applications request direct access to the file system or registry. When this occurs, the operating system automatically redirects the requests to the appropriate location. For example, if a previous program is attempting to write a configuration file to the Program Files folder, Windows Vista automatically intercepts that request and writes the file to a subfolder of the User profile. This is a much safer operation, and it still enables the application to run without modifications.

NOTE Temporary compatibility measures

Microsoft designed file system and registry virtualization technology primarily for compatibility with the vast library of earlier applications that were written for previous versions of Windows. Over time, many applications will be designed and updated to use safer models for file and registry access. Therefore, virtualization is being used as a temporary measure to bridge the gap until that happens. It is not intended to be used as a long-term compatibility solution.

Understanding the Secure Desktop

One method by which malicious applications might attempt to collect sensitive information from the user is by emulating a standard application or window. This is particularly true of the UAC elevation prompt. Users might be prompted for credentials by an unauthorized application that appears to be a standard Windows dialog box. The program collects user names and passwords and then might use this information to compromise security.

To prevent this problem, Windows Vista displays elevation prompts, using a secure desktop. The secure desktop automatically dims the desktop background and prevents all applications from launching any new prompts or windows until the user makes a decision related to the UAC elevation prompt. In this way, the user can be assured that the UAC prompt is coming from the Windows Vista operating system itself.

Identifying Tasks That Require Privilege Elevation

Although you can perform the majority of common tasks in Windows Vista as a standard user, there are various functions that require elevated privileges. Built-in operating system tools and applications use a shield icon next to the appropriate button or link to indicate that privilege elevation is required (see Figure 6-10). This helps users understand when they are performing potentially unsafe actions.

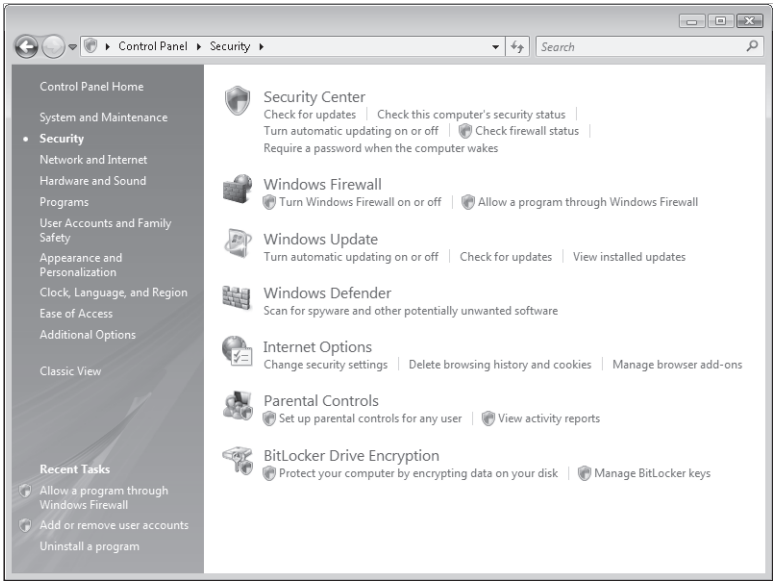

Figure 6-10 Tasks that require administrator permissions are shown with a shield icon

Responding to Elevation Prompts

A common source of security-related and configuration-related issues occurs when users install unknown applications. In some cases, this might be done deliberately, but in other cases, users might be tricked into running a setup program without knowing it. UAC automatically attempts to verify whether an application is a known program or potentially unsafe. Figure 6-11 shows an example of the approval dialog box that is presented to users.

In addition to providing the name of the program and its publisher (if available), the details include the full path to the application. This can help users determine whether they really want to install the program. Options include allowing or disallowing the program to run.

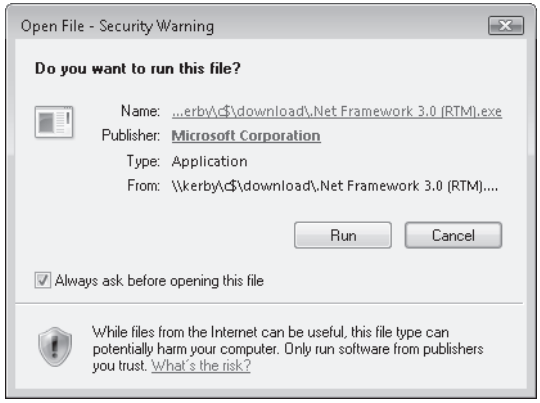

Figure 6-11 A prompt for an unknown application

Running Programs with Elevated Privileges

In some cases, users always want to run a particular program using Administrator permissions. For example, a customer might know that her former accounting software requires elevated permissions, and she does not want a prompt to appear automatically every time she launches the application. Run This Program As An Administrator offers the option to run a program always as an administrator. You can configure this setting on the Compatibility tab of a program or shortcut (see Figure 6-12).

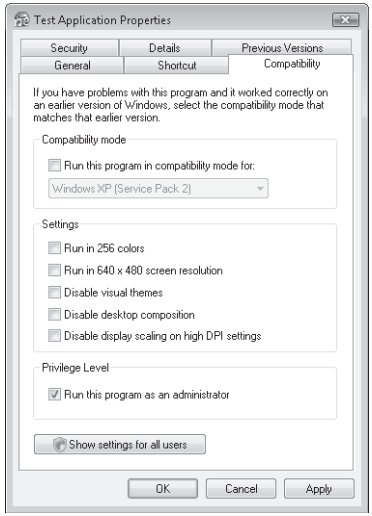

Figure 6-12 Using Compatibility tab settings to run a program as an administrator

In some cases, the Run This Program As An Administrator check box might be disabled. For example, the application might be a built-in program that is included with Windows Vista and might not require elevated credentials. In those cases, the check box is disabled.

Another way to launch a program with elevated permissions is to right-click a program or shortcut and select Run As Administrator. This setting launches the application with Administrator permissions. Unless UAC is disabled, the user is prompted to provide consent or credentials.

Understanding Installer Detection

Perhaps one of the most common tasks that requires elevated privileges is the process of installing new software. Setup programs and installers often need to write directly to secure file system locations (such as the Program Files folder) and make changes to the registry.

Windows Vista uses methods to identify installation programs automatically and automatically prompts for approval of elevation when the application is run. This helps prevent common error messages and issues that users encounter when attempting to install programs, using standard user permissions.

NOTE Choosing new applications

Whenever possible, recommend that customers select software that includes the Certified for Windows Vista logo. This helps ensure that the product has been designed for compatibility with UAC and other security features. More information about various Windows software logos is available in Chapter 1, "Preparing to Install Windows Vista."

Enabling and Disabling UAC

To ensure security of new Windows Vista installations, the UAC feature is enabled by default. When users log on to the computer, they start launching processes under the context of a standard user.

There are several different ways to control the behavior of the UAC feature. In some cases, customers might ask you for information about how to disable the feature altogether. You can access the Use User Account Control (UAC) To Help Protect Your Computer check box from within Control Panel . This check box is available by clicking User Accounts And Family Safety and then clicking User Accounts. You can also access this check box by searching for UAC in Control Panel. As shown in Figure 6-13, the dialog box provides a single check box that determines whether UAC is enabled.

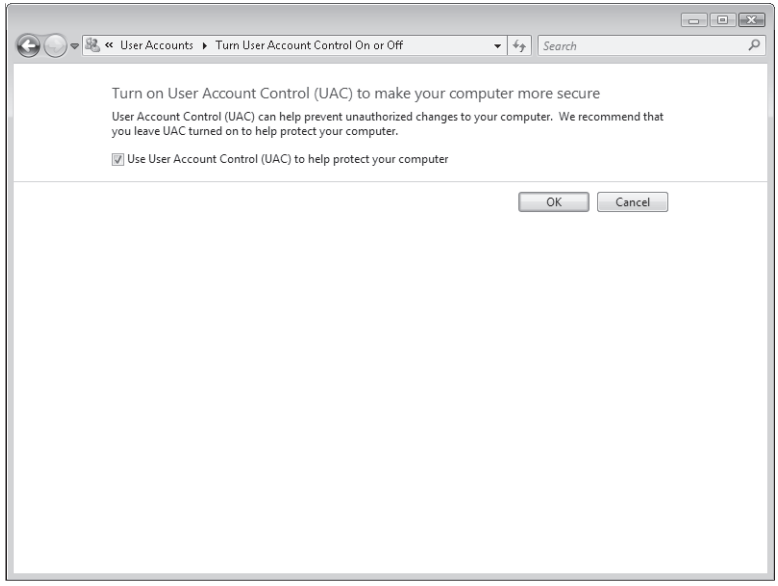

Figure 6-13 Viewing details related to the status of the UAC feature

NOTE Questioning the decision to disable UAC

When a customer asks how he or she can completely disable UAC, it's a good idea to get some more information about why he or she is making this request. Is the customer frustrated with the frequency of elevation and consent prompts? Is he or she having difficulty running certain applications? Often, users don't understand the value of the UAC feature and therefore see it as only an annoyance. As a Consumer Support Technician, explain the purpose and function of UAC, including how it can help prevent security issues and increase system reliability. It's quite likely that customers might decide that disabling the feature completely is too much of a risk and that changing various settings might be a much better overall solution. Remember, your goal should be to strike a balance between security and usability.

After selecting to enable or disable UAC, you are prompted to reboot your computer, which is necessary to make the changes effective. When you disable UAC, users receive a notification of this whenever they log on to the computer or access security-related settings in Control Panel. This is done to remind users that they are at risk of potential security issues. You'll look at ways in which you can fine-tune the behavior of UAC later in this lesson.

Managing UAC Settings with Local Security Policy

In addition to the default behavior of UAC, there are several different options that you can use to control the specific way in which this feature works. You define these settings by using policy settings on the computer. To access them, open the Local Security Policy console from the

Start menu. The utility is available in the Administrative Tools program group (if the Start menu options are set to display it) or by searching for Local Security Policy. The default interface shows several different groups of settings, each of which has dozens of available options.

To access the properties of the UAC functionality, expand Local Policies, and then select the Security Options folder. The right side of the console shows all of the available policy options along with their current settings. UAC-related policies are prefixed by the text User Account Control (see Figure 6-14).

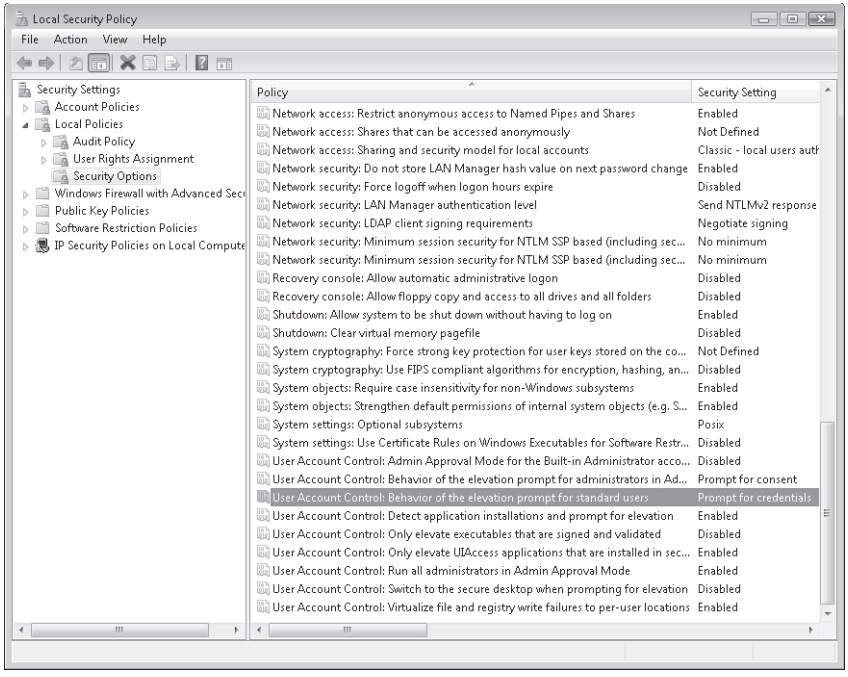

Figure 6-14 Viewing Local Security Policy settings

Each of the settings pertains to some aspect of system behavior or permissions. For example, you can use the Accounts: Guest Account Status option to specify whether the built-in Guest account is enabled. To make changes to a policy setting, double-click the item in the list. For most options, the first tab that is shown, Local Security Setting, provides the options for the setting (see Figure 6-15).

Figure 6-15 Viewing options for a policy setting

It's often difficult to understand the exact purpose of every available option. Fortunately, the Local Security Policy console also includes details about specific options on the Explain tab. The text that is displayed here (see Figure 6-16) provides background information about the policy, along with details about the effects of these settings. Most explanations also include details about the default setting for the option. This can be very helpful in troubleshooting configuration issues. In some cases, links to more information are provided. Overall, this can help you determine the purpose and function of each setting.

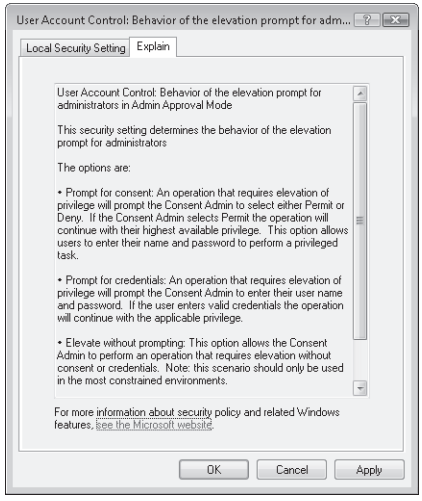

Figure 6-16 Viewing explanatory text for a policy setting

NOTE Resisting the urge to tweak

With all of the options available in the Local Security Policy console, it might be tempting to try to change configuration settings just to see what happens. Although this can be a good method for learning, it's important to make these changes on noncritical systems (such as a test computer). Keep in mind that it is possible to "break" certain functionality with improper settings.

In relation to controlling the behavior of UAC, there are nine different settings that you can configure manually. These are as follows:

- **User Account Control: Run All Administrators In Admin Approval Mode** This setting can be considered a "master switch" that determines whether UAC is enabled on the local computer. The default setting is Enabled. The status of this setting corresponds to the Turn User Account Control (UAC) On Or Off setting in Control Panel. When the status is set to Disabled, Admin Approval Mode, file system and registry virtualization, and all related settings are effectively disabled. It is important to keep in mind that the other settings might appear to be properly configured, but they do not have any effect when this setting is disabled.

  Exam Tip Instead of memorizing the names of each of the UAC-related Group Policy settings, concentrate on the meanings and effects of each. On the exam, you'll be expected to understand how the settings are used, but you won't be tested on the exact wording of each setting.

- **User Account Control: Admin Approval Mode For The Built-In Administrator Account** This setting specifies the UAC options for the built-in Administrator account. By default, this setting is set to Disabled, which means that users who log on with the Administrator account have full permissions on the system. In general, it is recommended that the default Administrator account not be used. If you do have a need to enable the Administrator account, you can add security by enabling this policy setting.
- **User Account Control: Behavior Of The Elevation Prompt For Administrators In Admin Approval Mode** This setting specifies the type of elevation prompt that will be presented to administrative users when a program or process requests additional privileges. The settings include:
  - Prompt For Consent (the default).
  - Elevate Without Prompting.
  - Prompt For Credentials.

  The default setting provides a balance between security and usability. To improve security, you can require that administrators provide a user name and password to elevate permissions. Alternatively, you can choose to eliminate the prompt altogether.

- **User Account Control: Behavior Of The Elevation Prompt For Standard Users** This setting determines how elevation prompts will be shown to standard users. The default setting, Prompt For Credentials, requires the user to provide logon information for an Administrator user every time an application or process requests elevated permissions. In some cases, you might want to prevent elevation from occurring at all. That's the purpose of the Automatically Deny Elevation Requests option.
- **User Account Control: Detect Application Installations And Prompt For Elevation** When users attempt to install an application, Windows Vista automatically attempts to elevate privileges. This is a useful feature, because most setup and installation programs require access to the file system and other protected areas of the computer. The default setting for consumer-focused editions of Windows Vista is for this option to be enabled. This means that users automatically see an elevation prompt whenever they launch an installer. The Disabled option is primarily used in company network environments in which IT staff can control the installation of software, using centralized methods.
- **User Account Control: Only Elevate Executables That Are Signed And Validated** One important potential security risk related to working with applications and software is in trusting the publisher of the application. Malware could easily create a new executable or shortcut that appears to be a familiar application (such as Microsoft Word), but that actually launches malicious code that could damage the system. One way to validate a program is to use a method based on Public Key Infrastructure (PKI) technology. This method allows trusted third parties to validate whether the publisher of the software is who it claims to be.

  This option is set to Disabled, by default, because PKI technology has dependencies on other services such as a Certificate Server. Home and small-business users are unlikely to have the necessary infrastructure to do this.
- **User Account Control: Only Elevate UIAccess Applications That Are Installed In Secure Locations** Some applications might need to run with elevated privileges on Windows Vista. Developers of these applications can create a setting that instructs the operating system to prompt for elevated privileges automatically whenever the program is launched. One potential problem is for malware (such as programs downloaded from the Internet) to request full permissions and then make undesired changes to the system. This setting specifies that only applications that are located within known secure file system locations (such as the Program Files folder and subfolders of the Windows folder) are able to request elevation. This helps ensure that only properly installed programs are able to run with elevated permissions. The setting can be disabled, although this will reduce overall security.
- **User Account Control: Switch To The Secure Desktop When Prompting For Elevation** One method that malware authors have at their disposal is the possibility of tricking a user into providing sensitive information to a program. For example, a program could be designed to look very similar to the standard UAC elevation prompt. A user might

provide a user name and password for privilege escalation, but the application itself is recording or sending this information elsewhere. To help prevent this type of intrusion, the default setting in Windows Vista is to use a secure desktop when an elevation prompt is presented. When this occurs, the entire desktop background is dimmed, and only the prompt is shown. Other applications will be unable to overwrite the prompt or create new windows that take the focus. When you disable this option, the UAC prompt appears like any other window. However, it is then possible for other applications to create a false UAC prompt.

- **User Account Control: Virtualize File And Registry Write Failures To Per-User Locations** This setting is designed to provide compatibility with legacy applications that request direct access to the file system or to the registry. When a program attempts to perform one of these actions, Windows Vista automatically redirects the request to a safe, virtual location. The benefit is that the program can still run successfully, but all write operations occur safely. When you disable this setting, earlier applications are prevented from directly writing to file system and registry locations. In most cases, this means that the applications fail to run correctly.

NOTE Educating customers

When supporting customers who are attempting to understand the purpose of various security settings, you might be tempted just to make various changes on their behalf. It's important, however, that you keep the customer informed of the effects of your modifications. After all, if a security issue or malware infection were to occur on customers' systems due to a change you made, you want to ensure that the user agreed with it. Generally, the more educated customers are with relation to security, the more likely they are to exercise good judgment.

Quick Check

1. What is the default elevation prompt that a user receives when running under Admin Approval Mode?
2. How can you modify UAC to disable the use of the secure desktop?

Quick Check Answers

1. The user is prompted for consent and is not required to provide logon credentials.
2. You can change this setting by using the Local Security Policy console. Specifically, you can set the User Account Control: Switch To The Secure Desktop When Prompting For Elevation option to Disabled.

Practice: Working with UAC

These practice exercises walk you through steps that can be used to configure and customize the behavior of UAC in Windows Vista. The exercises assume that you have created at least one Administrator account and one standard user account (for more information about creating accounts, see Lesson 1).

▶ Practice 1: Configure UAC Behavior

In this exercise, you configure UAC to prevent standard user accounts from performing system-level tasks, even if they have information about administrator credentials on the computer. It is important that you have at least one Administrator account configured on the computer before beginning. This exercise also assumes that all UAC options are set to their default values.

1. Log on to the computer using an Administrator account.
2. From the Start menu, open the Local Security Policy console.
3. Expand the Local Policies folder and select Security Options.
4. Double-click User Account Control: Behavior Of The Elevation Prompt For Standard Users.
5. On the Local Security Setting tab, change the setting to Automatically Deny Elevation Requests.

   This setting specifies that users who log on with a standard user account are not prompted to provide elevation credentials. Therefore, they are unable to run programs with administrator permissions.
6. Log off the computer and log on as a standard user.
7. From the Start menu, open Control Panel and click an item that has a shield next to it.

   Examples include Add Or Remove User Accounts or Allow A Program Through Windows Firewall. Note that you do not receive a UAC elevation prompt. The resulting dialog box states: "This program is blocked by group policy. For more information, contact your system administrator."
8. To change the UAC back to its initial settings, log off the computer and log on again as an administrator. Use the Local Security Policy console to change the User Account Control: Behavior Of The Elevation Prompt For Standard Users setting to Prompt For Credentials.

▶ Practice 2: Run Programs with Administrator Credentials

This practice demonstrates two different methods of running a standard program as an administrator. This exercise assumes that you are logged on to the computer as a member who has administrator permissions with Admin Approval Mode enabled. To complete this exercise, you need to install a program that requires administrator permission on the computer. Place a shortcut to the program on your desktop to follow these steps.

1. Log on to Windows Vista using an Administrator user account.
2. Double-click the program shortcut to open the program.

   You should receive a UAC elevation prompt that asks for approval to run under elevated permissions.
3. Choose Cancel to prevent the program from running.
4. To avoid the elevation prompt, right-click the program shortcut and choose Run As Administrator.

   Note that the program launches and that you do not receive a prompt for UAC elevation.
5. Close the program.
6. To configure the program always to run using administrator credentials, right-click the program shortcut and choose Properties.
7. Click the Compatibility tab, and then select the Run This Program As An Administrator check box. Click OK to save the settings.
8. Double-click the program shortcut and note that you are not prompted for UAC approval.
9. To change the shortcut settings back to the defaults, right-click the shortcut and select Properties. On the Compatibility tab, clear the Run This Program As An Administrator check box. Click OK to save the changes.

Lesson Summary

- Common computer security risks include viruses, adware, and other software that are collectively known as malware.
- For security reasons, users should log on to their computers by using a minimal set of permissions.
- Important design goals for Windows Vista include improving security settings while maintaining compatibility with earlier applications.
- The UAC process allows users to run with minimal permissions and provides prompts when programs require additional permissions.
- In the UAC Standard User Mode, users will be prompted to provide credentials whenever an application requires additional permissions.
- Admin Approval Mode allows a user to log on as an administrator but to run under a minimal set of permissions for most operations.
- File system and registry virtualization prevents direct access to secure operating system locations while still providing for backward compatibility with former applications.
- UAC settings and options can be modified using the Local Security Policy tool.

Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 2. The questions are also available on the companion CD if you prefer to review them in electronic form.

NOTE Answers

Answers to these questions and explanations of why each answer choice is correct or incorrect are located in the "Answers" section at the end of the book.

1. Which of the following Local Security policy options can you set to disable all UAC functionality and options effectively?
   - **A.** User Account Control: Virtualization File And Registry Write Failures
   - **B.** User Account Control: Admin Approval Mode For The Built-In Administrator Account
   - **C.** User Account Control: Only Elevate Executables That Are Signed And Validated
   - **D.** User Account Control: Run All Administrators In Admin Approval Mode
2. You are a Consumer Support Technician assisting a customer with configuring UAC features in Windows Vista. The customer would like to run using a minimal set of permissions but would like to be able to perform privilege escalation without providing credentials. Which of the following settings should you recommend?
   - **A.** An Administrator user account with Admin Approval Mode enabled
   - **B.** An Administrator user account with Admin Approval Mode disabled
   - **C.** A standard user account with the behavior of the elevation prompt set to Prompt For Credentials
   - **D.** A standard user account with the behavior of the elevation prompt set to Automatically Deny Elevation Requests

Chapter Review

To further practice and reinforce the skills you learned in this chapter, you can perform the following tasks:

- Review the chapter summary.
- Review the list of key terms introduced in this chapter.
- Complete the case scenarios. These scenarios set up real-world situations involving the topics of this chapter and ask you to create a solution.
- Complete the suggested practices.
- Take a practice test.

Chapter Summary

- Windows Vista includes standard and Administrator user account types.
- User Account Control (UAC) is designed to help users run with a minimal set of permissions on their computers while still being able to support earlier applications.
- The process of privilege escalation allows standard users to perform tasks and run programs that require Administrator permissions.

Key Terms

Do you know what these key terms mean? You can check your answers by looking up the terms in the glossary at the end of the book.

- Admin Approval Mode
- consent
- credentials
- elevation prompt
- Local Security Policy
- privilege escalation
- User Account Control (UAC)

Case Scenarios

In the following case scenarios, you apply what you've learned about user accounts and UAC in Windows Vista. You can find answers to these questions in the "Answers" section at the end of this book.

Case Scenario 1: Creating User Accounts Based on Customers' Requirements

You are a Consumer Support Technician assisting a customer in setting up a new Windows Vista–based computer for use by her family. You have asked several questions to determine how you should set up the computer. The customer would like to create four separate user accounts: one for herself, one for her husband, and one for each of her two children. The parents require the ability to install new software and hardware on the computer occasionally. They would like to make this process as simple as possible. The parents also need to run several applications that they know require administrator permissions. The children should not be able to perform advanced system functions unless a parent is present. Overall, the customer wants to minimize risks related to the installation of malicious software or the accidental deletion of important system files.

1. What type of user account should you configure for the parents?
2. What type of user account should you configure for the children?
3. How can the parents specify which applications should be run automatically as an administrator?

Case Scenario 2: Configuring UAC Settings Based on Customers' Requirements

You are a Consumer Support Technician assisting a customer in setting up security in Windows Vista. The customer did not perform the initial configuration of his computer, and he would like to change the behavior of UAC. Specifically, he would like to configure his computer so that he does not need to provide credentials every time he is prompted for privilege elevation. He also wants to ensure that all programs remain visible whenever an approval prompt is displayed. Overall, he wants to achieve these goals without significantly reducing the security of the system.

1. What type of user account should you configure for the customer?
2. Which tool should you access to make changes to the behavior of UAC?
3. Which UAC option should you change to keep desktop applications visible when an elevation prompt is displayed?

Suggested Practices

To help you successfully master the exam objectives presented in this chapter, complete the following tasks. It is recommended that you make security-related changes on a test computer and that you keep a record of the changes you are making so that they can be reversed if necessary.

Practice 1: Working with User Account Types

Create two new user accounts within Windows Vista. The first should be configured as a standard user account, and the second should be an Administrator account. Log on under the standard user account and note which types of actions require you to provide administrator credentials. Then, log on as the administrator and make note of the difference in behavior of the UAC prompts. When finished, delete both user accounts.

Practice 2: Configuring UAC Settings

Use the Local Security Policy console to modify UAC-related settings. Make a note of the initial settings before you make any changes. Verify the results of the settings. For example, you might choose to disable Admin Approval Mode temporarily. Verify that you no longer receive UAC elevation prompts when logging on as an Administrator. Another option is to choose to disable the secure desktop when prompting for elevation. When finished, reset all options to their initial values.

Take a Practice Test

The practice tests on this book's companion CD offer many options. For example, you can test yourself on just one exam objective, or you can test yourself on all the 70-623 certification exam content. You can set up the test so that it closely simulates the experience of taking a certification exam, or you can set it up in study mode so that you can look at the correct answers and explanations after you answer each question.

MORE INFO Practice tests

For details about all the practice test options available, see the "How to Use the Practice Tests" section in this book's introduction.

Chapter 9

Configuring Windows Vista Networking

In the early days of desktop computing technology, it was most common for home and small office computers to be configured to run independently. Although networking technology was available, it was far from a standard option for most environments. Users often shared information by using removable media such as floppy disks. Accessing computers located outside of a home or a small office building was reserved for large corporations.

Now, most of us take network connectivity for granted. We expect to be able to access the Internet from our homes, offices, and even while traveling. We also rely on the ability to share media such as photos, music, and video between computers on our home networks. The underlying technologies that make this possible have changed and evolved over time, but the basic requirements for networking have remained the same. The goals include simplified setup of connections and maintenance of adequate security. Especially when using public networks such as the Internet, it's important that only authorized users are able to access information from a remote location. Convenience has significantly increased by wireless networking options, and it's usually just as easy for people to access Web sites from a coffee shop as it is for them to do so from home.

One of the major design goals for Windows Vista was to simplify the process of creating network connections. For a variety of reasons, there are significant complexities involved in creating secure wired and wireless connections. In this chapter, you'll learn details related to setting up and managing network connections in Windows Vista. Lesson 1, "Managing Network Protocols and Client Network Services," covers details of understanding and managing network protocols and services. Lesson 2, "Configuring Wireless Networking," focuses on configuring wireless network connections.

Exam objectives in this chapter:

- Configure and troubleshoot network protocols.
- Configure and troubleshoot network services at the client.
- Configure and troubleshoot wireless networking.
- Configure and troubleshoot Windows Vista by using the Network And Sharing Center.

Lessons in this chapter:

Before You Begin

It will be helpful for you to have a basic understanding of network connections and how they're used in typical home, home office, and small-business environments. Additionally, to complete the exercises in Lesson 1, you will need a network connection (either wired or wireless) correctly configured to access other computers or the Internet. You might also have a wired or wireless Internet router configured to enable multiple computers to share a single Internet connection. To complete the exercises in Lesson 2, you need to have installed a wireless network adapter that is compatible with Windows Vista.

Lesson 1: Managing Network Protocols and Client Network Services

When two people meet and need to communicate with each other, the first step is to determine a common language to use. When talking with friends and family members, you already know the best method to use. In the world of computers, there are several important standards that are commonly used to enable computers to communicate. By far, the most popular network protocol in the world is Transmission Control Protocol/Internet Protocol (TCP/IP). This protocol is the standard that is used on the public Internet, and it is the primary method of setting up network connections in wired and wireless homes and small businesses.

Customers expect you, as a Consumer Support Technician, to be able to explain to them the various standards and protocols that are available for communications. Furthermore, you need to be familiar with how you can set up and configure appropriate settings in Windows Vista, based on their requirements. In this lesson, you'll learn about networking improvements in Windows Vista, along with important protocols and settings. You'll also learn how to configure and troubleshoot network connections. Because all of the information in this lesson focuses on network protocols and services, it applies equally to both wired and wireless connections. Examples and exercises, however, are based on the use of wired network connections. In Lesson 2, you'll learn about information specific to setting up and managing wireless network connections.

After this lesson, you will be able to:

- Describe new features in the Windows Vista Next Generation TCP/IP Stack.
- List configuration information related to the IPv4 protocol, including IP address, subnet mask, default gateway, and DNS servers.
- Describe the benefits of the IPv6 protocol.
- Describe and manage DNS and DHCP settings on client computers running Windows Vista.
- Create and manage network connections using the Network And Sharing Center.
- Troubleshoot network connections.

Estimated lesson time: 60 minutes

Understanding the Next Generation TCP/IP Stack

Most operating system users rely on the ability to access public networks (such as the Internet) and to communicate with other computers in homes and offices. Because networking is such a critical part of common operations, Windows Vista includes numerous enhancements to the primary networking features of the operating system. The foundation of this

functionality is the networking stack, a set of interrelated components that enable communication on the network.

As mentioned earlier, the most commonly used networking protocol is TCP/IP. Windows Vista includes a feature called the Next Generation TCP/IP stack. This term refers to a collection of technologies embedded in the core networking architecture of the operating system. All network-enabled applications, services, and features rely on this stack in one way or another. Although previous versions of Microsoft Windows include support for TCP/IP, Windows Vista includes numerous enhancements, including the following:

- **Automatic configuration** One of the most difficult parts of setting up a new computer (especially for novice users and customers) is configuring network settings. Microsoft designed Windows Vista to perform configuration options automatically wherever possible to avoid end-user confusion.
- **Performance enhancements** New TCP/IP components have been designed to support enhanced features that enable more efficient transfer of data based on a variety of different network conditions.
- **Extensibility** The Next Generation TCP/IP stack has been designed with the ability to add enhancements and new functionality in mind. Components of the network stack are segmented into logical divisions, making it easier for vendors and software developers to install updates.
- **Dynamic reconfiguration** Especially on modern notebook and portable computers, it's common to connect and reconnect frequently to various networks throughout the day. Microsoft designed the Windows Vista network stack to adapt to various configuration environments without requiring a reboot of the operating system.
- **Diagnostic features** Due to the complexity of network configuration, it's possible for various problems to prevent users from successfully connecting to other computers or to the Internet. When these problems occur, it can often be difficult to pinpoint the true source of the problem. The Windows Vista network stack includes diagnostic capabilities that can make it easier to diagnose and troubleshoot common problems.
- **Improved security** With the ability to connect to computers located around the world over the Internet come some potential security risks. Problems such as malware and malicious users can cause downtime, reduced performance, data loss, and security violations. The Next Generation TCP/IP stack has been designed to protect against common types of network-based attacks.
- **Support for multiple versions of the Internet Protocol (IP)** The networking features in Windows Vista enable support for current and future networking technologies based on the TCP/IP standard. Specifically, it provides support for both Internet Protocol version 4 (IPv4) and IP version 6 (IPv6), both of which you'll learn about in the next section. It also provides features to ease the transition between the protocols.

For the most part, all of these features work automatically whenever you create network connections. In typical use, you rarely have a reason to make modifications directly to the network stack. Now that you have an idea of the purpose and function of the basic network foundation, you can look at the different available protocols.

Understanding IPv4

The purpose of a network protocol is to specify the communications format and conventions that computers use when two or more networked devices need to send messages to each other. As mentioned earlier, Windows Vista supports two major protocol types: IPv4 and IPv6. In this section, you'll learn about the details of configuring IPv4. Specifically, you'll learn about the following settings:

- IP address
- Subnet mask
- Default gateway
- DNS server addresses

Exam Tip Although network protocols other than TCP/IP are available, they're outside the scope of Exam 70-623 and the contents of this book. When taking the exam, you can safely assume that computers are configured to use TCP/IP. Keep in mind, however, that they might not be configured correctly, and you might need to determine how to resolve connection problems.

IP Addresses

By far, the most common version of IP in use at the time of the release of Windows Vista is IPv4 (usually pronounced "IP version 4"). This protocol is a portion of the TCP/IP standard that computers use to communicate on a local area network (LAN) and on the public Internet. A fundamental feature of networking is that each computer on a network must have a unique network address. IPv4 network addresses use a series of four numbers separated by dots. Each number must be between 0 and 254 (inclusive). The following are some examples of IP addresses:

- 10.0.1.1
- 192.168.0.10
- 207.46.232.182

Subnets

In some network environments, it's common for administrators to divide networks into smaller sections known as subnets. To identify which portion of the IP address refers to the

network and which portion refers to the computer's address, computers use a subnet mask. Examples of commonly used subnet masks include the following:

- 255.255.255.0
- 255.255.0.0
- 255.0.0.0

Designing and calculating subnet details is beyond the scope of Exam 70-623, but it is important to understand that, in general, all of the computers that are required to be able to communicate with each other should be located on the same subnet. This means that they should all share the same subnet mask. Also, each computer should have a unique network address that is part of the same subnet. For example, the following computers will all be able to communicate with each other (assuming that other network settings are properly configured):

- 10.10.0.1 / 255.255.255.0
- 10.10.0.20 / 255.255.255.0
- 10.10.0.30 / 255.255.255.0

Note that in these examples, all of the subnet masks are identical, and each computer's host address is unique and located on the same subnet.

Default Gateways

Because you can place computers on separate isolated networks, it is often necessary for them to be able to communicate with each other. For example, if you launch Microsoft Internet Explorer and attempt to connect to *www.microsoft.com*, the specific computers that you are trying to access are obviously not located on your subnet. Your computer must then determine how to access that particular Web site.

This is the purpose of the default gateway setting. The default gateway is an IP address value that specifies the network address to which your computer sends all traffic if the traffic is not destined for the local subnet. For most home and small-business users, the default gateway address is the IP address of the router. A computer can use information from its own IP address and subnet mask together to determine whether a requested resource is on another network. If it is, the computer sends the network request to the default gateway. It is then the default gateway's responsibility to route the packets to another network to enable communications. For example, the infrastructure of the Internet is based on a large group of network devices that have the ability to send traffic to each other.

A valid default gateway address must be located on the same subnet as the computer that plans to use it. Typically, the default gateway is an Internet router when used in a home or small-business environment. This device is able to take network requests from computers on the LAN and forward them to other network devices on the Internet.

Managing IPv4 Settings

In most network environments, IP addresses, subnet masks, and default gateway settings are automatically assigned. For example, you can configure most home Internet routers to assign appropriate values automatically for computers on the network. The benefit is that users typically do not need to be concerned with managing the settings manually. You'll learn about how this is done later in this lesson.

Exam Tip If you're relatively new to managing networking settings, you have probably noticed that there is a lot of information to know. You might be wondering how important it is to understand the underlying technical details of network protocols. In general, Windows Vista is designed to configure network settings whenever possible. However, when configuration or connection problems occur, it can be very useful to have a solid understanding of the actual communications mechanisms themselves. As with most technical topics, practicing common troubleshooting tasks can help you learn this information quickly and easily. If you've seen a particular networking problem before, you'll be well prepared to answer network-related questions when taking Exam 70-623.

Understanding IPv6

A newer version of the IP standard, IPv6, has been created to improve network-based communications. Although IPv4 has been able to adapt to widespread use throughout the Internet, it was never designed to support many millions of different types of devices. There are numerous limitations of the protocol, and it will eventually need to be replaced. Windows Vista includes full support for the IPv6 protocol, but it is important to note that the transition to the new version requires upgrades to all areas of networks and to the Internet before it is complete, a process that is expected to take many years.

MORE INFO What happened to IPv5?

IP standards are defined by the Internet Engineering Task Force (IETF). This organization reviews submissions and ideas for future versions of network protocols, including IPv4 and IPv6. The standards themselves are named Request for Comments (RFC). You might wonder why there is little mention of the version that should come in between those. Initially, IPv5 was intended to be a new network protocol, but it was never made a widespread standard. For all practical purposes, IPv6 is the successor to IPv4. Although you won't be tested on these details on the exam, you can get more background information from the IETF Web site at *http://ietf.org/*.

The primary advantages of IPv6 include the following:

- **Support for more addresses** The total number of possible IPv6 addresses is enough to accommodate all of the network devices in the world for the foreseeable future. This expanded capacity allows literally every device in the world to have its own unique network address.

- **Simplified configuration** Numerous network techniques are required to make IPv4 networks meet the needs of large networks such as the Internet. IPv6 simplifies the process of addressing devices and determining subnets.
- **Performance enhancements** IPv6 includes features that enable it to adapt to a wide variety of different types of networks and workloads. It can automatically adjust the size of network packets and other settings to improve performance.
- **Security improvements** A fundamental concern when transferring information over large networks is ensuring security. Only authorized computers should be able to access information during transit. To achieve the necessary encryption and authentication support, IPv6 includes a feature known as IPSecurity (IPSec).

The primary issue with using IPv6 is that computers and network devices must support this protocol to gain these advantages. In addition, operating system tools and software applications might need updates to use the newer version of the protocol. For these reasons, full-scale upgrades to IPv6 (especially on the public Internet) will take several years.

Understanding IPv6 Support in Windows Vista

Microsoft included full support for the IPv6 standard as part of the Windows Vista Next Generation TCP/IP stack. In addition to providing support for the newer version of IP, the stack is able to provide support for IPv4 at the same time. Therefore, a single computer can use IPv6 to communicate with computers that support it (such as other computers running Windows Vista) and use IPv4 to communicate with other computers and devices. Microsoft also provides support for the IPv6 protocol in Windows XP Service Pack 1 and in Microsoft Windows Server 2003. All future versions of the Windows client and server operating systems will support the protocol.

Although supporting IPv6 is an important feature, most of the network-related tools and application features of Windows Vista have been designed to work with the new protocol. For example, the Windows Vista networking features include graphical tools for configuring IPv6 details. You'll learn about specific examples later in this lesson.

Real World

Anil Desai

When IPv4 was initially developed (decades ago), it was not designed to sustain a worldwide network in which millions of computers require access. Through a variety of different technologies such as Network Address Translation (NAT), network administrators have been able to overcome some of these challenges. However, security, performance, and scalability needs are important considerations for moving forward.

The IPv6 protocol provides solutions to many of these problems, but it will not be a quick migration from IPv4. The primary reason for this is that many types of network devices and their interdependencies must be considered. The Windows Vista operating system is one example. Microsoft included full support for both the older and newer versions of IP in Windows Vista. Overall, however, Internet service providers (ISPs) and managers of networks throughout the world will need either to support IPv6 or implement methods to enable backward compatibility.

How does all of this affect you, as a Consumer Support Technician? First, you're likely to hear questions from customers about support for IPv6. The good news is that, for the most part, the default settings in Windows Vista are the most appropriate. It uses IPv4 when necessary and IPv6 when possible. In the future, however, it is important to keep an eye on the transition to IPv6 and to understand when new IPv6-enabled products are introduced. For recent updates, see the Microsoft IPv6 Web site at *http://www.microsoft.com/technet/network/ipv6/default.mspx*.

Understanding IPv6 Addresses

IPv6 network addresses appear significantly more complicated than their IPv4 counterparts. The primary reason for this is that each network address must be unique, and a greater number of character combinations are required to make this possible. An example of an IPv6 network address is 2001:0:4136:e37a:2074:22b5:f5f5:ff99. Note that colons separate portions of the address. For most users, IPv6 network addresses and settings are configured automatically, and there is no need to configure them manually.

Exam Tip The technical details of how IPv6 works can be complicated. For the sake of Exam 70-623, it's most important to understand the purpose and function of this protocol, along with how you can configure network settings in Windows Vista. For more detailed information about IPv6, see the Microsoft TechNet IPv6 Web site at *http://www.microsoft.com/technet/network/ipv6/default.mspx*. Throughout the remainder of this chapter, the terms related to IP addresses focus on the IPv4 standard because this is the most commonly used version of the protocol and the one that is most emphasized on Exam 70-623.

Understanding Client Network Services

So far, you've learned about the basic rules for setting up network addresses for computers that are connected. In some ways, the basic rules are fairly simple: Each computer must have a unique IP address on the network and generally is located on the same subnet, which means that each computer must have the same network address as others on the same subnet. In some home and small-business environments, managing one or a few computers manually

might be reasonable. However, when supporting additional computers, some automated methods for managing network services will be very helpful.

In this section, you'll learn how several network-related features of Windows Vista can help you manage settings such as IP addresses. Later in this chapter, you'll see how these settings can be defined when creating and managing network connections.

Exam Tip This section and the corresponding Exam 70-623 objective that it covers mention the term *client*. With respect to Windows Vista, this term refers to desktop or notebook computers that are primarily used by individuals. In larger networked environments, it's common to refer to computers as either clients or servers. Because the focus of Exam 70-623 is on supporting Windows Vista for consumers, you will generally focus on the client side of network settings. Windows Vista includes the ability to use services such as Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) but not to function as a server for those protocols. Keep in mind, however, that the network services described here also have server-side components that must be configured properly for these features to be available. Additionally, most home and small-business routers also include built-in DHCP and DNS features. For more information, consult the product's documentation.

DHCP

When working in networked environments, users are able to provide custom IP addresses for their environments. As mentioned earlier, each computer must have a unique IP address and must be configured with other settings such as the subnet mask and default gateway address. Most consumers find it difficult to keep track of these settings. For example, a customer might need to write down the settings, and every time a friend or family member needs to add a new computer, he or she will have to provide the correct information. If two computers are accidentally configured with the same address, one or both might be unable to communicate on the network. Add in the requirement to support a virtually limitless number of wireless computers, and it can be very time-consuming to manage IP addressing. Clearly, there's room for improvement in this situation.

DHCP is designed to provide appropriate TCP/IP network addresses and related information automatically to computers when they first attempt to connect to a network. The process involves four main steps:

- **Discovery** When a computer first initializes itself on the network, it does not have a valid network address. To obtain one, it sends a broadcast (a network message to all computers on the network) requesting an IP address.
- **Offer** A DHCP server receives the broadcast request and responds by providing an IP address offer to the new computer. The specific address chosen is based on the configuration of the DHCP server's database. Most commonly, a range of IP addresses is configured for use on the network. Other details, such as the subnet mask and the IP address of the DHCP server, are also included.

- **Request** After the client receives the offer, it makes a request for the same IP address to the DHCP server. This step is required to ensure that the client actually needs to reserve the specific request. In some cases, for example, if the computer has received responses from more than one DHCP server, it might not need to make the request. Generally, DHCP clients make a request to the first DHCP server that has responded to a request.
- **Acknowledge** The DHCP server receives the request from the DHCP client and records that the offered TCP/IP address is now in use on the network. This address will be unavailable for assignment to other computers until it expires.

The assignment of a DHCP address is known as a lease, and there is typically a maximum amount of time that can elapse before the lease expires. For example, a typical DHCP server setting is to allow IP address leases to last for up to eight days. As the expiration of the lease approaches, the client computer sends a request to renew the address to the DHCP server. If the DHCP server approves the request, the client can continue using the address. This method helps ensure that computers that are no longer on the network are not taking up allocated IP addresses in the DHCP server's database.

The customers that you support as a Consumer Support Technician will generally enable DHCP services on their Internet router or other device. The specific administration methods and configuration options will vary based on the brand and model of the device, but the general process allows for enabling the DHCP server and configuring a valid range of addresses to assign. Some small business environments might include server computers that provide DHCP services. One example is Windows Server 2003, which includes a DHCP Server component. In these environments, it's simplest to configure only a single DHCP server to be active. If two are required, you must configure each with a different set of IP addresses to avoid potential duplication. Finally, if an environment does not have any DHCP server, users need to configure IP address settings on each networked computer manually.

Domain Name System

From a networking standpoint, the concept of unique IP addresses makes a lot of sense. One can quickly look at the number and determine details about which network it is using. However, when dealing with many computers, it can be difficult to remember which computers have which network addresses. When the millions of servers that are accessible over the Internet are taken into account, it's virtually impossible to keep track of the correct IP values.

Domain Name System (DNS) is designed to provide mappings between TCP/IP addresses and friendly DNS names. DNS names have multiple parts that are separated by a period (.) character. Examples of DNS addresses include the following:

- www.microsoft.com
- technet.microsoft.com
- MyComputer.local

You might recognize these names as similar to what you use to connect to public Web sites. The public structure of the Internet is configured with certain top-level domain names that identify computers that you can access from anywhere in the world. Several third-party service providers are able to make changes to the addresses used in the database. Due to the number of addresses, it's important for public DNS databases to be able to send requests to each other. When a client attempts to connect to another computer using a DNS name, the request is sent to one of the DNS servers that is configured as part of the IP addressing parameters on the client. The DNS server then attempts to resolve the requested name to its IP address by querying other DNS servers. After the IP address for the requested name is determined, it is returned to the client so that it can be used for transferring data. To improve performance, the client makes a temporary record of the address and uses it for subsequent requests.

Exam Tip DNS is a standard on which the entire Internet is based. On the server side, there are many complexities and details that must be addressed to make this system work. For the sake of preparing for Exam 70-623, focus on troubleshooting client-side issues related to DNS. For example, a home computer might be able to connect to other computers on the local network and with an Internet router but not directly with Internet sites using a DNS address. In this case, it's likely that the DNS server IP information is incorrect.

Overall, the use of DNS names is a vital process for connecting to computers and services that are located on the Internet. It allows users to focus on meaningful computer and server names rather than difficult-to-remember IP addresses.

Firewalls

If there were no other restrictions placed on network traffic, it would be easy for all computers to communicate with each other. In some cases, this might be helpful. For example, many home and small-business users have more than one computer and want to share data such as documents, photos, and videos among them. A problem arises, however, when insecure or public networks are included. For example, when connecting to the Internet, it's helpful to be able to connect to any computer in the world through a device such as a router. However, for security and privacy reasons, you would not want unauthorized users and computers on the Internet to be able to access your private computers.

The purpose of a firewall is to divide networks by placing restrictions on communications between computers. In some cases, all traffic between two or more networks can be blocked. More commonly, most protocols are blocked while certain types of communications are allowed. For example, you can configure Windows Firewall to allow applications such as Internet Explorer to connect to Web sites using an outbound connection but to prevent other computers from using the same communications ports to connect to the local computer. For more details about working with the Windows Firewall feature in Windows Vista, see Chapter 7, "Using Windows Security Center."

In a typical home or small business environment, it's common for customers to use an Internet router or similar device that provides firewall functionality. Usually, the default settings of these devices enable computers to make outbound connections but prevent Internet-based users and computers from detecting local computers. The specific configuration steps and settings vary between devices from various brands and manufacturers, so it's important to consult the relevant documentation when assisting customers with setting up firewalls.

Configuring Network Connections

So far, the focus of this lesson has been on learning about IP addresses and related client network services. Understanding this information is important when creating, configuring, and managing network connections in Windows Vista. Generally, if you understand the basic concepts behind network protocols, you'll be able to make appropriate choices and resolve any issues that might arise. In this section, you'll learn how to configure network connections in Windows Vista.

Managing Network Settings

Windows Vista includes several different ways to access network-related settings and tools. One starting point is by clicking Network And Internet in Control Panel. As shown in Figure 9-1, various tasks and operations are available. From here, users can view details about current network settings and devices and set up and manage new connections.

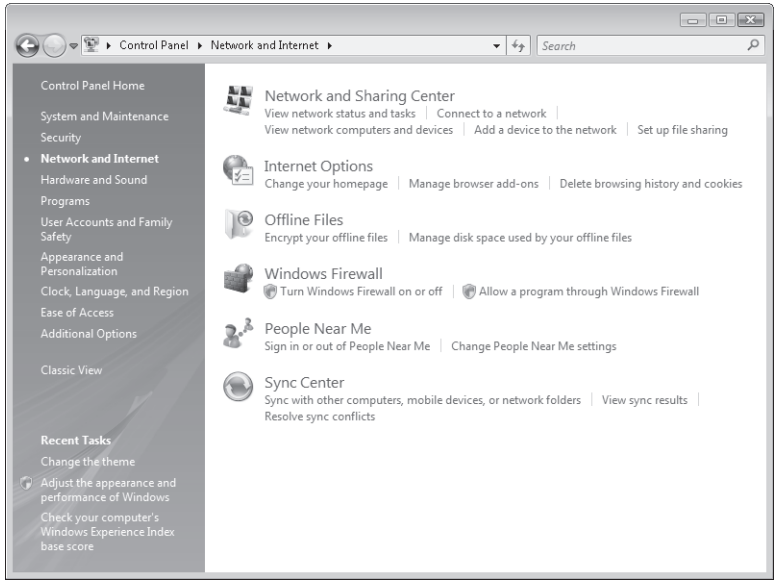

Figure 9-1 Viewing options in the Control Panel Network And Internet group

You configure the majority of options by using Network And Sharing Center. This utility provides a central location from which users can view details about the local network. Figure 9-2 provides an example of the default view of the Network And Sharing Center section.

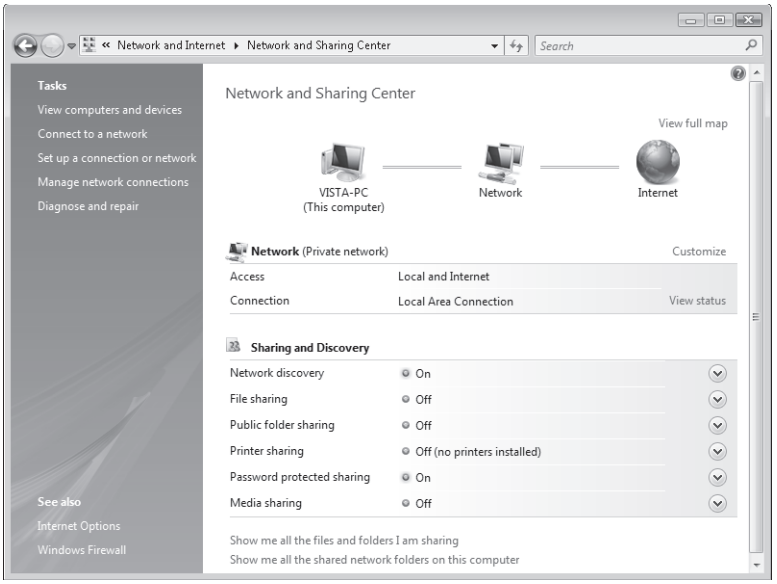

Figure 9-2 Using the Network And Sharing Center to view details about network connections

MORE INFO Sharing network resources

The focus of this chapter is on creating and managing network connections to enable computers to communicate with each other. For more information about sharing network resources such as files, printers, and media, see Chapter 10, "Managing Network Sharing."

Viewing Network Information

When managing and troubleshooting network connections, it's often helpful to get an overview of current connections and how they're configured. Because network connections (and their relationships) can be confusing to customers, the Network And Sharing Center offers a Network Map feature. By clicking View Full Map, users can see the relationships between various network devices and services. Figure 9-3 shows an example. If the computer is connected to multiple networks (for example, a wired network and a wireless network), a drop-down list enables the user to choose which network is shown in the map.

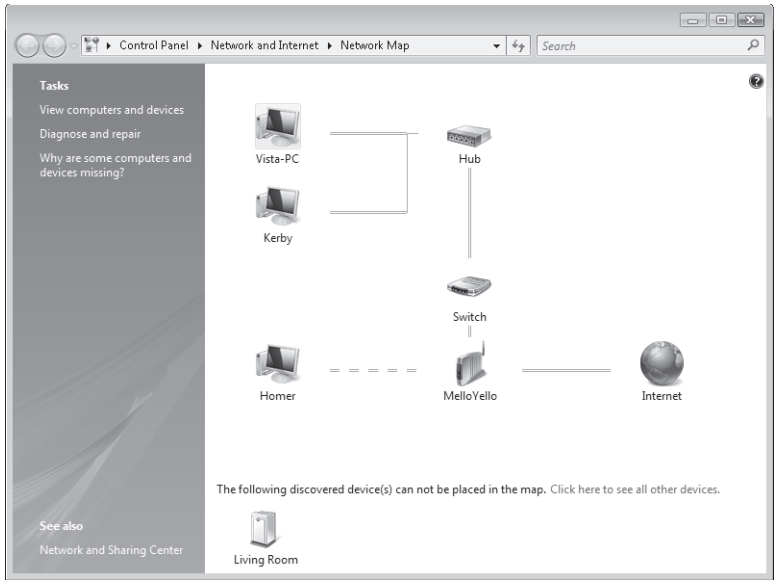

Figure 9-3 Viewing a network map on a desktop computer

You can view and modify information about various items in the network map by right-clicking them and viewing the list of available options. The type of network device determines which actions you can take. For example, you can access settings for a standard Windows Vista–based computer or view configuration details for a computer router or gateway device.

In addition to the Network Map feature, you can also view details about a particular network connection. The View Status link in Network And Sharing Center provides information about a particular network connection. Figure 9-4 shows an example.

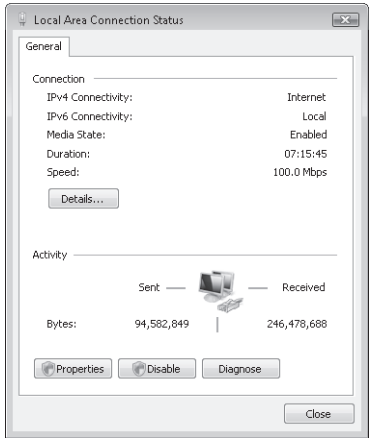

Figure 9-4 Viewing status information about a wired network connection

The basic details specify whether the computer is currently connected to a network, whether the connection is enabled, how long the connection has been active, and the speed of the connection. In addition, the Activity section shows the number of bytes that have been sent by and received from the network connection. This information provides a good overview of the status of the connection.

In some cases, it can be helpful to view more details such as the specific TCP/IP configuration of the connection. You can click Details to open a dialog box that shows this information (see Figure 9-5). Specific information includes the network address, subnet mask, and information about DHCP and DNS servers. If the computer used a DHCP server to obtain the address information, details about the duration of the lease are also available.

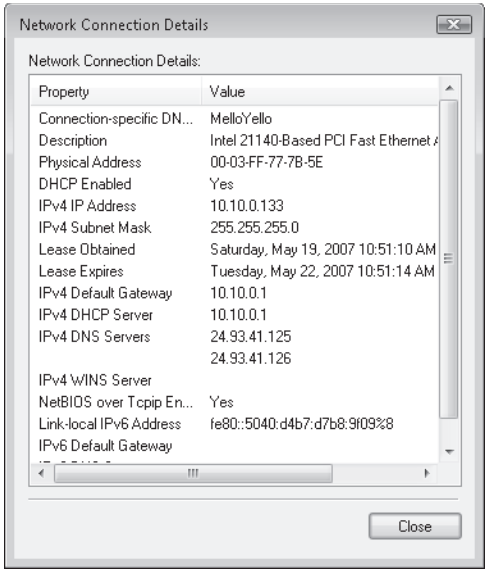

Figure 9-5 Viewing details for a network connection

Modifying Network Settings

The vast majority of networks today run a standard set of protocols and services. In most cases, Windows Vista is able to configure the appropriate setting for a network connection automatically. In some cases, however, it might be necessary to configure settings such as the IP address, subnet mask, default gateway, and DNS servers for a computer manually. It's most common to use a manual configuration when a DHCP server is either unavailable or not providing the correct information.

To access the properties of a network connection, open Network And Sharing Center and click View Status next to the relevant network connection. Then, click Properties (see Figure 9-6).

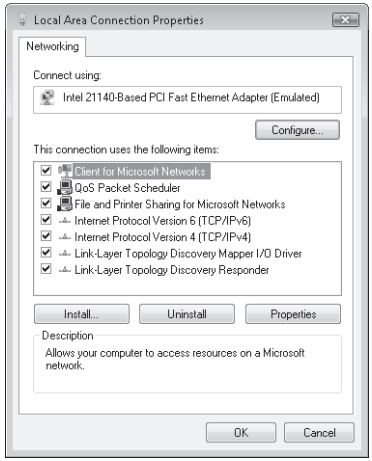

Figure 9-6 Viewing properties for a wired network connection

The specific list of items shown might vary based on the enabled services and protocols for the network. By default, new network connections include settings for both IPv4 and IPv6. You can uninstall or disable most of the items in the list. In general, it is recommended that you use the default options because they are required for certain types of functionality. For example, if you remove the File And Printer Sharing For Microsoft Networks feature, users will not be able to share or access files on other computers. It is also possible to install new services or protocols manually if they are required.

In addition to adding and removing services for a network connection, the primary settings that you can modify are related to the network connection and protocols. Clicking Configure in the Properties dialog box displays the details of the associated network adapter used by the connection. Most of the available properties are related to the settings for the hardware device itself. Many network adapters include advanced options that you can also modify if necessary (see Figure 9-7).

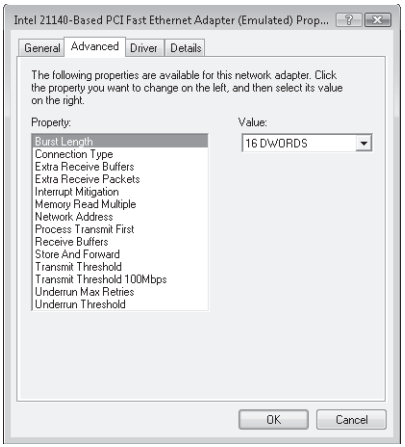

Figure 9-7 Viewing the Advanced tab of the Properties dialog box of a network adapter

Setting Network Location Details

Networked computers often have different security requirements based on the type of network to which they are connected. For example, within a typical home environment, it's likely that computers need to share information. Because the network is usually limited to authorized users and computers, it's safe to do this. When you connect the same computer to a public or insecure network (such as in an airport or other public place), it is recommended that you limit access to the computer. You can configure these settings by clicking Customize next to a network connection in the Network And Sharing Center. Figure 9-8 shows the typical options that are available.

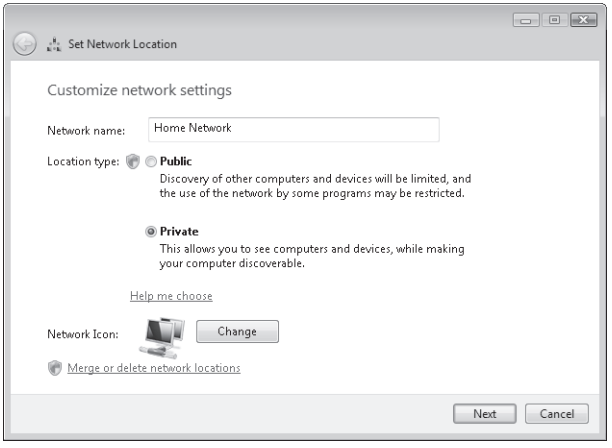

Figure 9-8 Customizing network settings using the Network And Sharing Center

In addition to switching between the Public and Private options for network connection types, you can also change the name of the network. Windows Vista uses this setting to help you quickly identify the type of network that you are using. It is also possible to change the network icon. Finally, it is possible to merge or delete network connections. This option is useful when, for example, multiple network connections are defined on the computer that all use similar settings.

Manually Configuring TCP/IP Settings

The most commonly modified network connection settings are those related to the IPv4 and IPv6 network protocols. To access these settings, in the Properties dialog box for a network connection, select the appropriate protocol and click Properties. Figure 9-9 shows the properties that are available for the IPv4 protocol.

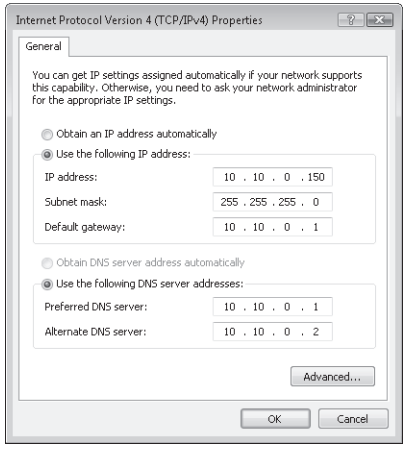

Figure 9-9 Manually configuring settings for the IPv4 protocol

By default, new network connections are designed to use DHCP for automatic assignment of settings. Using the Properties dialog box, however, you can manually specify information for several settings as follows:

- **IP Address** The unique TCP/IP address of this computer
- **Subnet Mask** The subnet mask that is used by all computers on the local subnet
- **Default Gateway** The IP address of a router or other device that enables communications outside the local network
- **DNS Servers** The IP addresses of a preferred and alternate DNS server

If DHCP is enabled, users also see an Alternate Configuration tab that enables them to define a second set of IP address information (see Figure 9-10). This information is most commonly used when you would like to leave the automatic settings to use DHCP, but you want to provide rules for which addresses should be used if a DHCP server is unavailable. The options

include using an automatic private IP address (which is generated automatically by Windows Vista) or to provide specific IP address settings. This tab is also useful when a network connection is used at multiple locations. For example, if a customer uses a laptop computer at work and at home, he or she might need to assign different addresses for each environment manually.

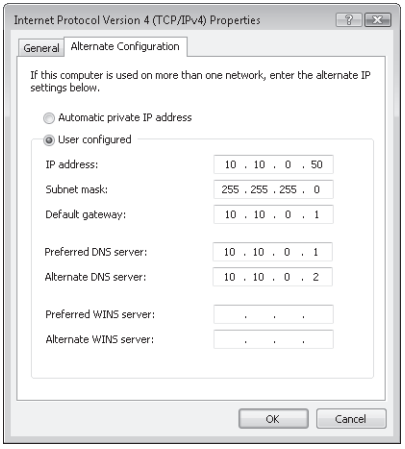

Figure 9-10 Specifying alternate configuration options for a network connection

On the General tab of the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box, the Advanced button enables further configuration of network details. Although these settings are not common for most consumers, it is possible to configure a single network adapter to use multiple IP addresses and subnet masks and to configure multiple gateways (see Figure 9-11).

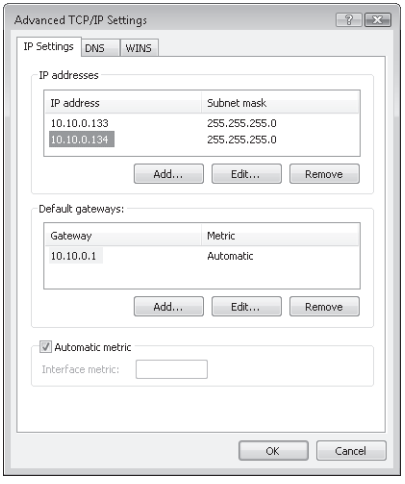

Figure 9-11 Configuring advanced TCP/IP settings for a network connection

In addition, there are advanced configuration options for DNS and Windows Internet Naming Service (WINS). Most home and small-business users use the default settings. In some business network environments, however, it might be helpful to change the default behavior of these protocols.

By default, the Properties dialog box of a network connection also includes details about the IPv6 protocol. As with IPv4 settings, the defaults are appropriate for most users. You can configure manual IPv6 addresses and other details by accessing the Properties dialog box of the protocol (see Figure 9-12).

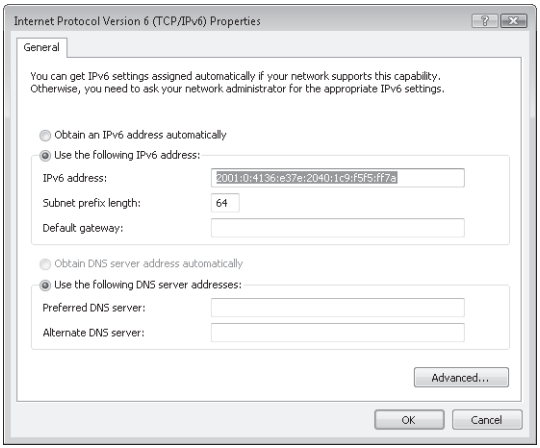

Figure 9-12 Configuring properties of the IPv6 protocol

Another method of configuring network settings is by clicking Manage Network Connections in the Network And Sharing Center. The resulting display shows all of the available network connections on the computer and enables the user to change the settings manually. This view is similar to the one that you see in previous versions of Windows such as Windows XP and Microsoft Windows 2000 Professional.

Creating a New Network Connection

The process of creating a new network connection is simple and can be performed by starting at the Network And Sharing Center. Clicking the Set Up A Connection Or Network link launches a dialog box that enables you to select the type of connection to create (see Figure 9-13).

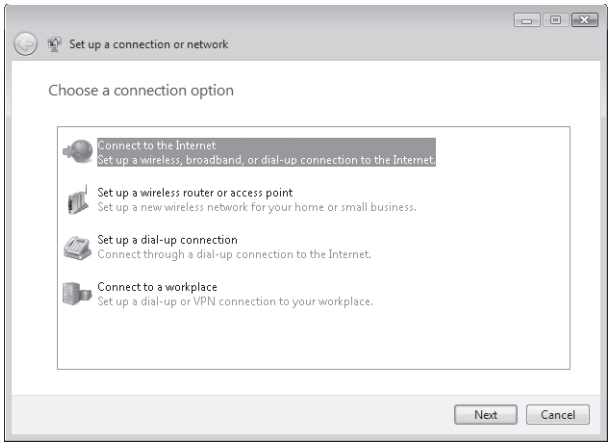

Figure 9-13 Setting up a new network connection by using the Network And Sharing Center

There are several different options, each of which provides a description of a typical usage scenario. For home and small-business users, the most common option is usually Connect To The Internet. The other network types include connecting to a workplace by using a virtual private network (VPN), creating a dial-up connection, or configuring a wireless router or access point. Each step of the process walks users through available options. The specific details are based on the type of network connection, whether other similar network connections have been defined, and the security requirements.

Troubleshooting Network Connections

As a Consumer Support Technician, you are likely to be asked for assistance with configuring customers' wired and wireless network connections. Common problems include having incorrectly configured IP address settings or trying to access remote resources when a network connection is disabled. Because the process of troubleshooting these types of problems usually follows a sequence of steps, Windows Vista includes an automatic method for resolving the most common issues.

Understanding the Network Diagnostics Framework

The process of troubleshooting network-related problems can be complicated, especially for customers with limited knowledge of the technical details. One of the most common errors that a user will report is receiving a "Page cannot be displayed" error in Internet Explorer. The root cause of the problem could be one of many different issues. For example, a network cable might be unplugged, or the computer might have failed to obtain a valid IP address from a DHCP server.

Windows Vista includes the Network Diagnostics Framework (NDF) to provide a method to determine the cause of a particular network problem automatically. It can then present options for resolving the issue, such as enabling a network adapter that is disabled. Behind the scenes, the NDF functionality looks at many different details related to network settings and uses a set of steps for determining the cause and potential resolution for the issue. The specific details might vary, for example, for wired and wireless network connections. This frees users and support staff from having to check multiple configuration settings to resolve the issue.

Diagnosing and Repairing a Connection

There are several ways to start the process of automatic troubleshooting for a particular network connection. One method is to right-click the system tray icon for the network connection (if it is available) and select Diagnose And Repair. Other options are to select the Diagnose And Repair option in the Status dialog box of a network connection or to use the Diagnose And Repair link in the Network And Sharing Center. Regardless of the method used, this starts the automatic repair process (see Figure 9-14).

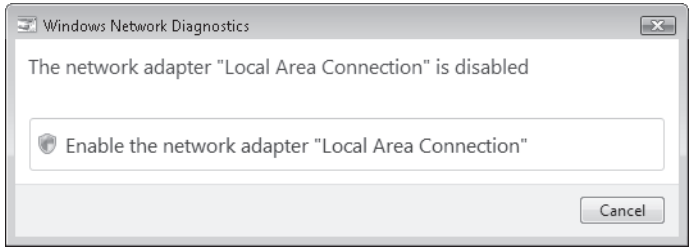

Figure 9-14 Automatically diagnosing and repairing a network connection

If a problem is detected, Windows Vista automatically attempts to resolve it. For example, if the computer is not currently configured with valid TCP/IP information, Windows Vista automatically attempts to release the current DHCP lease (if there is one) and obtain new IP address details. In some cases, Windows Vista might notify users that manual configuration changes might be required. Overall, the *Diagnose And Repair* function can help automatically resolve the most common types of connection problems without requiring expertise from users.

Using Network Troubleshooting Tools

When diagnosing and troubleshooting network connections, there are several different tools and techniques you can use to verify connectivity. In this section, you'll learn about several of the most commonly used tools. You run all of them from a command prompt, and they can return or change configuration details. For more information about a particular command, you can type the command followed by /?.

Windows IP Configuration

The Windows IP configuration (IPCONFIG) command provides a simple way to view and modify information for a network adapter. To view network details, you can use the command without any arguments or type **IPCONFIG /ALL** to view complete details about the configuration of the network connection and various protocol settings (see Figure 9-15).

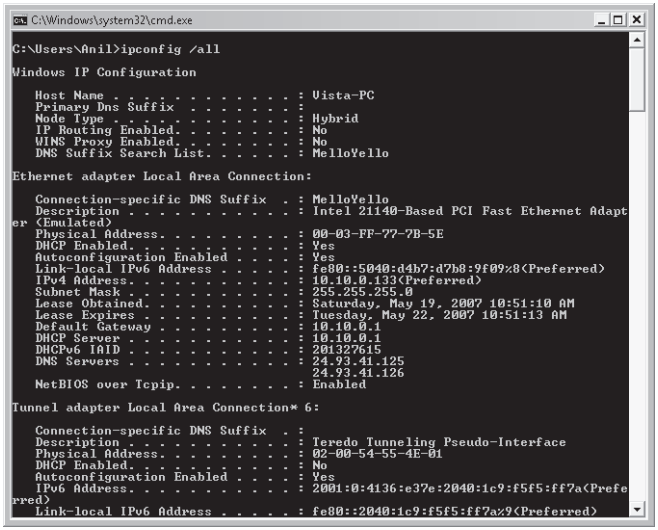

Figure 9-15 Viewing network configuration details by using IPCONFIG

In addition to viewing information about network connections, you can also release and renew DHCP addresses and perform DNS troubleshooting, using the IPCONFIG utility. Type **IPCONFIG /?** for more details on the specific command-line options.

PING

Often, when troubleshooting network connections, you want to test whether computers are able to communicate with each other without having to share files, printers, or other objects. The PING utility is designed to send a simple TCP/IP request to a remote computer and to return the response. Figure 9-16 provides an example.

In addition to determining whether another computer is reachable, the PING command returns the amount of time it took for a response to be received. Although this information is not intended to be used for performance monitoring, it does provide an indication of the speed of the network.

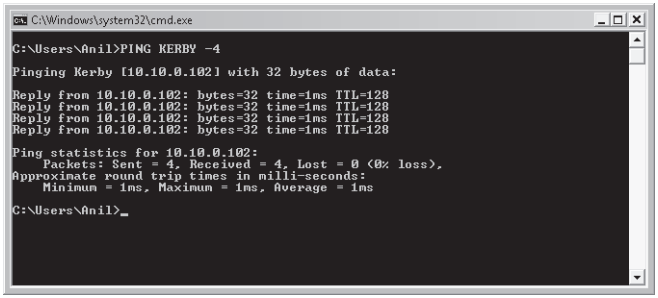

Figure 9-16 Performing a PING to verify IPv4 connectivity

NETSH

The NETSH command launches an interactive command-line application that enables viewing and modifying many different types of network settings. You can access the list of NETSH commands by typing **?** at the NETSH prompt. Common operations include viewing and modifying settings for a particular network interface, making firewall changes, and configuring protocol settings.

Quick Check

1. You would like to get a quick overview of the number and types of devices that are available on a customer's home network. What is the easiest way to do this?
2. What are the most important protocol settings related to an IPv4 connection?

Quick Check Answers

1. The Network Map feature that is available from within the Network And Sharing Center provides a graphical overview of all of the network devices that are present in the environment.
2. An IPv4 connection should include an IP address, a subnet mask, a default gateway, and DNS server addresses.

Practice: Configuring Network Settings

In these exercises, you will configure network settings in Windows Vista. The exercises assume that you currently have a wired network connection on a computer running Windows Vista and that you are able to access the Internet. It also assumes that you have obtained valid TCP/IP network information through a DHCP server. Internet access can be provided through a LAN, a home-based broadband router, or a direct broadband connection (using, for example, a DSL modem or cable modem). The steps in the exercise might result in temporary loss of your Internet connection.

▶ Practice 1: Manually Configure IPv4 Settings

In this exercise, you manually configure TCP/IP settings for a computer running Windows Vista. You use the current DHCP-assigned IP address information as a basis for determining the manually assigned address for the computer.

1. Open the Network And Sharing Center by right-clicking the system tray icon for your wired network connection and selecting Network And Sharing Center.
2. In the Network section of the user interface, click View Status for the wired network connection on the computer.

   You see details such as the speed of the connection, the duration of the connection, and the amount of activity for the adapter.
3. Click Details to view TCP/IP-related information for the network connection. Make a note of the following configuration settings:
   - ❑ IPv4 IP Address: _____
   - ❑ IPv4 Subnet Mask: _____
   - ❑ IPv4 Default Gateway: _____
   - ❑ IPv4 DNS Server (primary): _____
   - ❑ IPv4 DNS Server (secondary): _____
4. Click Close to close the details of the network connection.
5. Click Properties to access information about the wired Internet connection.
6. In the list of network components, select Internet Protocol Version 4 (TCP/IPv4), and then click Properties.
7. On the General tab of the Properties dialog box, choose to assign TCP/IP information by selecting the appropriate options manually. Type the information you recorded in step 3 and then click OK to save the settings.
8. Click Close to close the network Properties dialog box, and then click Close again to return to the Network And Sharing Center.
9. Open Internet Explorer and browse to *http://www.microsoft.com* to verify that your Internet connection is working.
10. To return the system to its original configuration, click View Status for the wired network in the Properties dialog box of the TCP/IP connection. Access the Properties dialog box for IPv4 and specify that all information should be obtained from a DHCP server.
11. Close all open windows and close the Network And Sharing Center.

▶ Practice 2: Diagnose and Repair a Connection

In this practice exercise, you use the automatic network diagnostics of Windows Vista to troubleshoot a common network connection issue.

1. Right-click the system tray icon for your wired network connection and select Network And Sharing Center.
2. Click View Status next to the item for the wired connection.
3. Click Disable to disable the wired network adapter.
4. Open Internet Explorer and attempt to connect to *http://www.microsoft.com*. You should receive an error page stating "Internet Explorer cannot display the Web page."
5. On the Internet Explorer error page, click Diagnose Connection Problems. The Windows Network Diagnostics tool analyzes the connection.
6. The Windows Network Diagnostics dialog box shows that the network adapter is disabled. Click the relevant button to enable the network adapter. Click Close to verify the summary information.
7. Use Internet Explorer to attempt to connect to the same Web site you used in step 4. Verify that the page loads properly.
8. When finished, close Internet Explorer and close Network And Sharing Center.

Lesson Summary

- Windows Vista includes the Next Generation TCP/IP stack, which provides for improved performance, better security, and support for both IPv4 and IPv6.
- The IP address of a computer should be unique on a network.
- The subnet mask determines which addresses are part of a network.
- IPv6 provides a much larger range of addresses than IPv4, along with performance, security, and reliability enhancements.
- The Dynamic Host Configuration Protocol (DHCP) is used to assign TCP/IP settings to client computers automatically.
- The Domain Name System (DNS) is used to resolve friendly hierarchical names such as www.microsoft.com to TCP/IP addresses.
- The Network And Sharing Center can be used to create, configure, manage, and troubleshoot network connections.
- Additional TCP/IP troubleshooting tools include IPCONFIG, PING, and NETSH.

Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 1, "Managing Network Protocols and Client Network Services." The questions are also available on the companion CD if you prefer to review them in electronic form.

NOTE Answers

Answers to these questions and explanations of why each answer choice is correct or incorrect are located in the "Answers" section at the end of the book.

1. You are a Consumer Support Technician assisting a home computer user with troubleshooting a network-related problem. The user reports that he can connect to other computers on his network to share files, but one computer is unable to access the Internet. Which of the following IPv4 settings is most likely misconfigured?
    1. IP address
    2. Subnet mask
    3. Default gateway
    4. Network name
2. You are a Consumer Support Technician assisting a small-business owner with setting up a network for four Windows Vista–based computers. She would like to simplify the addition of new computers to the network and is unfamiliar with managing TCP/IP addresses. You have recommended that she purchase a network router for use in her office. Which of the following networking features will help the user meet her goal?
    1. DHCP
    2. DNS
    3. PING
    4. IPCONFIG

Lesson 2: Configuring Wireless Networking

In recent years, the thought of using a computer without access to the Internet has become hard to imagine for many consumers. Users rely on the ability to access information stored on their own networks or on computers located across the world quickly and easily. Although it is common to find network jacks in office locations, they are less likely to be found in home environments and some types of businesses. This makes the act of connecting to the Internet difficult and inconvenient. Fortunately, there's a better way.

In Lesson 1, you looked at details related to network protocols with a focus on managing wired network connections. The focus of this lesson is on examining the details of working with the convenience of wireless networks. For the most part, all of the information you learned in Lesson 1 applies equally to wired and wireless networks.

Although there are numerous benefits of using wireless technology, there are also some additional security and configuration-related concerns. As a Consumer Support Technician, you'll often be responsible for assisting users with configuring their wireless network adapters for use with Windows Vista. In this lesson, you'll learn about the basics of working with wireless networks, along with the details related to ensuring that these networks remain secure.

After this lesson, you will be able to:

- Describe potential security issues with using wireless network connections.
- Identify commonly used wireless network protocols.
- Describe the features and benefits of network security protocols such as WEP and WPA.
- Use the Network And Sharing Center to create and manage wireless network connections.
- Troubleshoot issues with wireless network connections.

Estimated lesson time: 45 minutes

Working with Wireless Networks

The benefits of using wireless networks are probably apparent to most end users and technical professionals. Not having to find and connect a network cable to a jack is a huge benefit in environments ranging from homes to public locations such as airports and restaurants. There are, however, several potential drawbacks to using wireless connections instead of wired ones.

First, there's the issue of physical security. With wired connections, it's often easy to determine who is connected to the network and to restrict access to a specific building. Due the nature of wireless communications, on the other hand, it is possible for users to connect to a network without having physical access to a building. Simply by enabling their wireless

network adapters, it is possible to view network activity originating from other computers. The potential for intercepting data is high.

Additionally, there are technical issues such as finding the correct wireless network (especially in environments where multiple networks exist) and providing the proper security credentials to access it. Finally, there are numerous available standards and protocols related to wireless networks. This can make the process of selecting and configuring various devices complicated. Although standards are designed to provide for compatibility, there is still some potential for connection problems.

Understanding Typical Wireless Configurations

In most home and small-business environments, there are several required components that are necessary to create and use a wireless network. The first requirement is for a computer to have a wireless network adapter. Like a physical network adapter, a wireless adapter can be built into a computer (which is most common with portable devices such as notebook computers), or it can be added as a peripheral. Common examples of wireless network adapter types include universal serial bus (USB) and PC card–based devices. Desktop computer expansion cards are also available (for more information on installing new hardware devices, see Chapter 11, "Managing and Troubleshooting Devices."

The network adapter provides the computer-side connection to the wireless network. Most commonly, the network itself is created by using a wireless router or access point. These devices can provide the ability to connect multiple computers through wireless connections. They usually include standard wired connection ports for supported standard LAN connections and for connecting to the Internet.

Other types of wireless networking hardware products are also available. For example, because the range of wireless devices is limited based on the strength of the signal, you can use network devices called repeaters to relay the signal to more distant locations.

Understanding Wireless Network Protocols

Regardless of the types of devices that are used, they generally must support the same wireless networking standards. The most commonly used wireless standards include 802.11a, 802.11b, 802.11g, and 802.11n. Each of these protocols differs in terms of the frequencies that are used, the data rate (speed), and the range. Table 9-1 provides a comparison of these values.

Table 9-1 Summary of 802.11 Networking Standards

Protocol	Initial Availability	Frequency Range	Data Rate (Typical)	Data Rate (Maximum)	Range (Indoor)
802.11a	1999	2.4–2.5 GHz	25 Mbit/s	54 Mbit/s	~50 meters

Table 9-1 Summary of 802.11 Networking Standards

Protocol	Initial Availability	Frequency Range	Data Rate (Typical)	Data Rate (Maximum)	Range (Indoor)
802.11b	1999	~5.0 GHz (multiple ranges)	6.5 Mbit/s	11 Mbit/s	~100 meters
802.11g	2003	2.4–2.5GHz	11 Mbit/s	54 Mbit/s	~100 meters
802.11n	2006 (draft)	2.4 GHz or 5 GHz	200 Mbit/s	540 Mbit/s	~250 meters

Exam Tip When preparing for Exam 70-623, it's not necessary to memorize the different performance characteristics and details of various network protocols. Although the variations can have a significant effect on the types of products you recommend to customers, you configure all of the standard wireless networking features of Windows Vista similarly regardless of the network type.

In general, newer standards offer improved performance and improved range. Because the process of upgrading to newer standards often requires the replacement of numerous routers and network adapters, many wireless networking products support multiple protocols.

Understanding Wireless Security Options

As mentioned earlier, one of the security-related issues of transmitting information over a wireless connection is the risk of data interception by third parties. For example, if you are transmitting a document through e-mail while using a wireless connection in an airport, another wireless user might be able to collect this data without your knowledge. Also, in a home environment, the range of a wireless router or access point might make it possible for neighbors to connect to your network and access resources such as home computers or your Internet connection.

To address these concerns, you can protect data by using encryption technologies. The purpose of encryption is to scramble data into a format that is decipherable by only the intended recipient of the communication. Even if data is intercepted, it will be unusable by anyone who does not know the encryption key. There are several different methods by which you can implement encryption. The most common method is by using a shared secret, a password, or other information that is known only to authorized users of the network. In this section, you'll look at different ways in which you can help increase security.

Using Wired Equivalent Privacy

The oldest common wireless security method is known as the Wired Equivalent Privacy (WEP) standard. As its name implies, the goal of this security mechanism is to allow only authorized users to connect to a wireless network. Home and small-business users typically create a WEP key when they initially configure their routers and network adapters. The length

of the key affects the level of security. More characters in the key make the system more difficult to compromise from a security standpoint. Key lengths are typically measured in bits, with some common strengths being 128-bit and 256-bit.

Using WEP security is clearly better than using no encryption, but this security protocol does have well-known vulnerabilities. Specifically, it is possible for unauthorized users to determine mathematically the value of the WEP key simply by monitoring a sufficient amount of networking traffic. Programs are available for automatically performing this task, and it can often be accomplished very quickly. Longer WEP keys make the process more difficult, but eventually, a knowledgeable user can break through the encryption.

Another security challenge is related to sharing WEP keys with authorized users. Although the problem is not specific to WEP, users must have a method of securely communicating the key. In home and small business environments, this can often be done by verbally transmitting the key, but in larger organizations, it can be a significant problem. Overall, WEP provides additional security, but it does not completely address all potential vulnerabilities.

Using Wi-Fi Protected Access

The goal of the Wi-Fi Protected Access (WPA) protocol is to provide for increased security over that of the WEP standard. WPA is generally seen as a replacement for the less secure WEP protocol, but WEP is still supported in operating systems such as Windows Vista for backward compatibility with devices that do not support it.

Like WEP, you generally configure WPA security on a wireless router or access point. To enable WPA, the network adapter and operating system must also support it. When creating a new connection, users are prompted to provide the appropriate WPA key (you'll look at the specific steps later in this chapter).

NOTE Recommending wireless devices

Customers rely on your advice as a Consumer Support Technician when selecting wireless networking products. Most retail stores provide a wide array of options for adapters, routers, and other devices. When recommending products to use with Windows Vista, you should look for the Works with Windows Vista logo for the product. This information can help you determine that the product includes support for new features and standards used in the operating system. It also helps assure you that your customers will be able to get technical support and updated drivers if problems should arise.

Using Service Set Identifiers

When working with wired networks, it's often easy to tell to which network you're connecting. In a home or small-business environment, there is typically only one available network, and all of the connections enable computers to communicate (assuming that they have the proper

permissions). In the world of wireless networking, it's possible for several different wireless networks to be available for access from a given location. For example, in a typical home environment, it might be possible to connect to neighbors' wireless networks.

The Service Set Identifier (SSID) is designed to assist users with finding and connecting to wireless networks that are available. The SSID is a name that is continually broadcast by a wireless access point device. The name of the wireless network (which you usually define when you initially configure an access point) is provided, along with details about whether the network requires security credentials. When a wireless network adapter is present in a computer, Windows Vista can automatically detect the available networks and identify them based on their SSID. Users can then choose to which network they want to connect (and, optionally, to provide security information).

NOTE Configuring SSIDs for usability and security

As a Consumer Support Technician, you'll likely need to answer customers' questions about setting up SSIDs. Most wireless network device vendors use a default SSID that does not contain descriptive information. Ideally, the wireless network name should be descriptive to the intended users of the network as well as unique. For example, "Office" might not be unique enough for a small-business network using office space that is shared with other businesses. Customers might also be tempted to disable SSID broadcasting as a method of increasing security. This practice is often known as "security through obscurity" and is generally not recommended. Nonbroadcast networks can still be detected but are more difficult for even authorized users to find (because they must know the exact name of the device). Overall, it is far better to rely on wireless encryption standards such as WPA to keep data secure.

Configuring Wireless Networks

In the past, end users have often found the process of connecting to wireless networks too complicated and unreliable. To address these issues, Windows Vista includes several different tools and methods for connecting to wireless networks. The goal is for these tools to remain consistent, regardless of the specific wireless protocols, security methods, and brands of network devices that are being used. In most cases, you can use the wireless network features to create a connection quickly, using minimal effort. In this section, you'll learn how to connect to a wireless network and manage wireless network settings. The content of this section assumes that you are already familiar with creating and managing standard network connections as described in Lesson 1 of this chapter.

Connecting to a Wireless Network

Unlike wired network connections, the process of connecting to a wireless network does not require a physical action such as plugging in a cable. Instead, users must choose to which wireless network they would like to connect from those that are within range. When you have

installed and configured a wireless network adapter on the computer, the Network And Sharing Center shows the connection in the display. If the adapter is not currently connected to a specific wireless network, you can click the Connect To A Network link. The resulting dialog box (shown in Figure 9-17) shows all of the available wireless network connections within range, along with their signal strength.

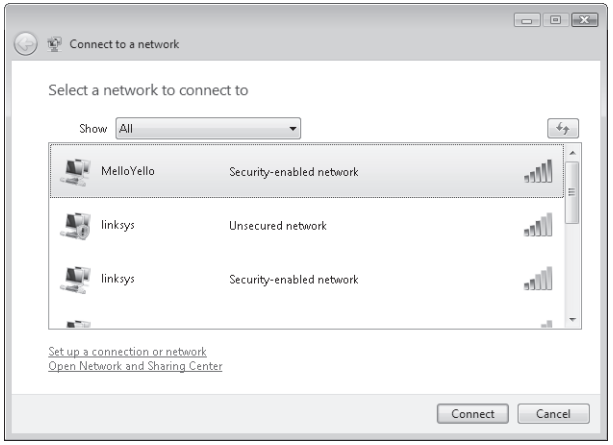

Figure 9-17 Viewing a list of available wireless networks

The details also show whether the network is security-enabled or unsecured. You can click Connect to connect to a particular wireless network. If security information is required for the network (and it has not yet been stored on the local computer), Windows Vista prompts you to provide the necessary details (see Figure 9-18). Optionally, it is possible to provide network configuration information that is stored on a USB drive (if available).

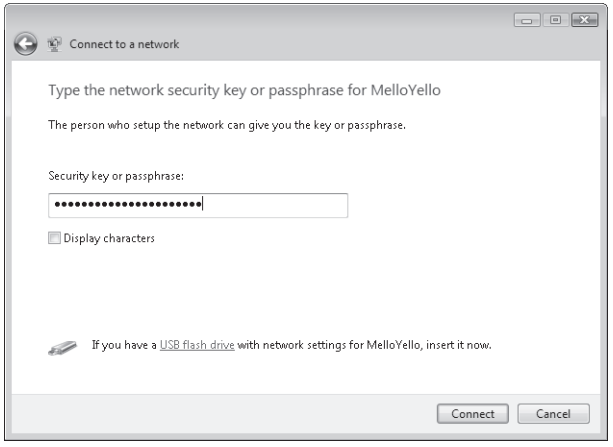

Figure 9-18 Providing network security information when connecting to a wireless network

If the connection is successful, you have the option to save the network settings. This option stores the security settings on the local computer running Windows Vista so that you do not need to provide the security details again in the future. If you save these settings, you can enable the option to connect automatically to this network connection when the computer is within range. If you enable this option, the user does not need to access the Network And Sharing Center manually to connect to the network when it is available.

It is also possible to access wireless network settings by right-clicking the wireless network icon in the system tray (if it is available) and choosing the Connect or Disconnect option. The Connect option automatically displays the wireless network connection screen. This method is useful if multiple wireless networks are available, and you would like to change connections quickly.

Configuring Wireless Ad Hoc Network Connections

It's most common in home and small-business environments to use a wireless router or access point for creating network connections. Often, these devices also provide access to other resources such as the Internet or computers that are located on other wired or wireless segments of the network. In some cases, however, it might be helpful for two or more computers to connect directly with each other to share files or perform sharing functions. Ad hoc wireless networks are designed to meet this need.

An ad hoc wireless network is connected directly between several different wireless-enabled computers without the use of a wireless access point. To create a new ad hoc wireless network, users can click Set Up A Connection Or Network in the Network And Sharing Center and choose the Set Up A Wireless Ad Hoc (Computer-To-Computer) Network option (see Figure 9-19).

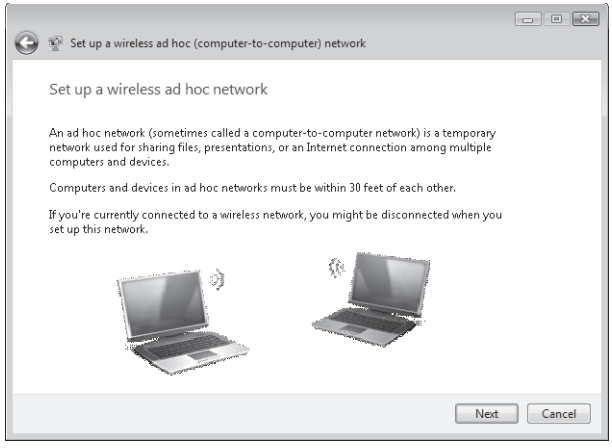

Figure 9-19 Creating an ad hoc wireless network connection

As indicated in the dialog box, it is not possible for the same wireless adapter to connect simultaneously to a standard wireless network and an ad hoc wireless network. Figure 9-20 shows the options that are available when setting up the new network.

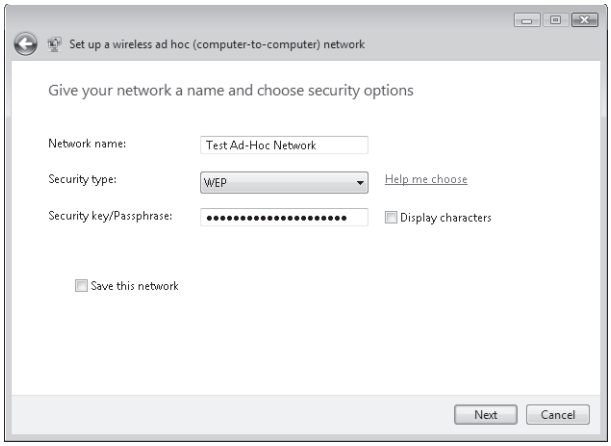

Figure 9-20 Providing details and security settings for an ad hoc wireless network

After you create the network connection, other users can connect to it as long as they are within range.

Viewing Wireless Network Connection Status Details

The speed of a wired connection is generally constant after a connection is made. With wireless connections, a variety of factors such as distance from the access point and the strength of the signal affect the performance of the connection. You can view the immediate status of the connection by clicking the appropriate View Status link in Network And Sharing Center. Figure 9-21 shows the details that are shown for a wireless connection.

The information that is unique to wireless connections includes the SSID, the speed of the connection, and the signal quality. Additionally, clicking Wireless Properties enables the user to set automatic connection and security-related settings for the connection (see Figure 9-22).

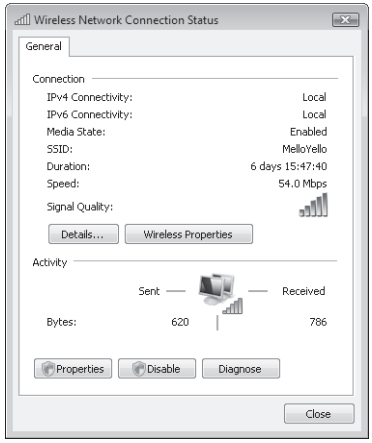

Figure 9-21 Viewing status details for a wireless network connection

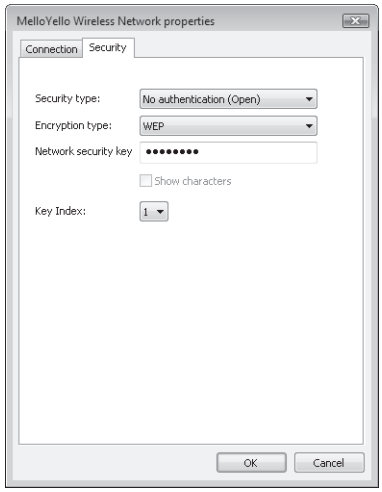

Figure 9-22 Configuring security settings for a wireless network

Managing Wireless Network Connections

For most portable computers, it's common to work with wireless networks in several different environments. For example, a customer might use his or her laptop to connect to wireless networks at home, in a hotel, and at his or her office. Although the user could manually connect to each of these networks when they are in range, Windows Vista can simplify the process by storing the details of the connections on the local computer.

To manage settings for wireless networks, you can click Manage Wireless Connections in Network And Sharing Center. The management utility (shown in Figure 9-23) shows details about which wireless networks are currently configured on the local computer. The list shows the

order of preference for wireless networks. Windows Vista tries to connect to networks that are listed higher in the list before attempting connections to the lower items. You can modify the preference order by selecting the item and using the Move Up or Move Down button.

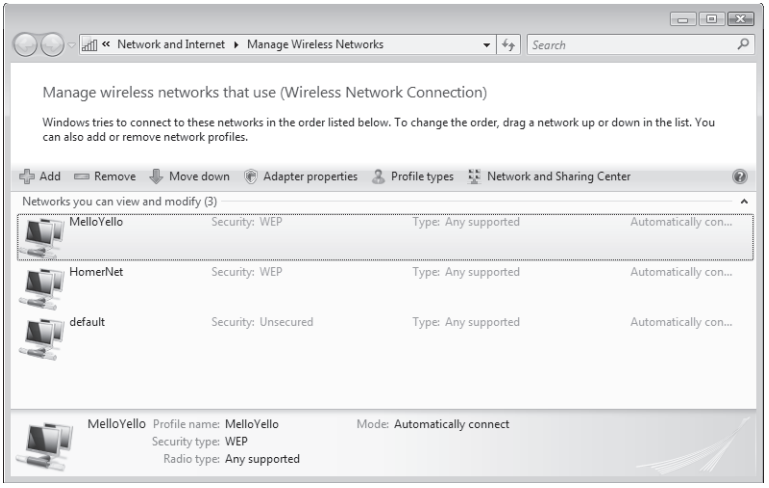

Figure 9-23 Using the Manage Wireless Networks dialog box

You can remove existing network connections if you no longer want the computer to connect to the network automatically. You can also add new wireless networks, using the Add button. Figure 9-24 shows the available options. If the wireless network you want to add is currently within range and is broadcasting its SSID, the first option is easiest.

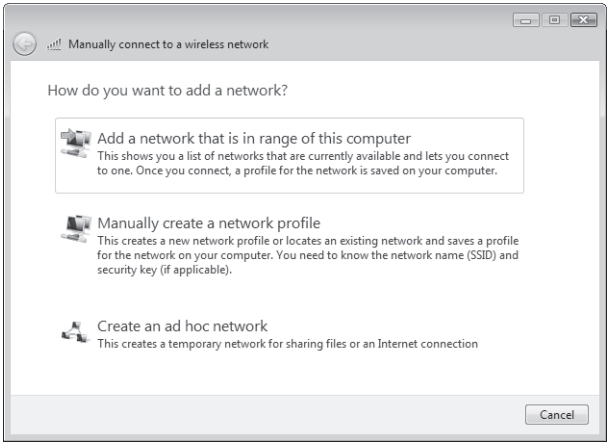

Figure 9-24 Adding a new wireless network

In cases in which the wireless network is not within range or the SSID is not being broadcast, you can use the Manually Create A Network Profile option. Figure 9-25 shows the details that you must provide.

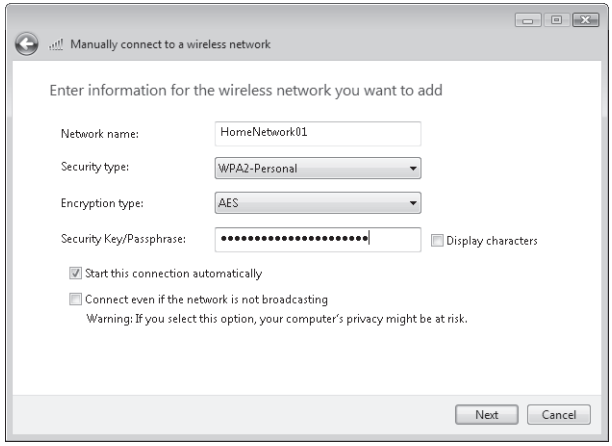

Figure 9-25 Manually connecting to a wireless network

Managing User Profile Types

In configurations through which multiple users regularly access the same computer, it might be helpful to control which users can connect to which networks. The Manage Wireless Networks dialog box provides the ability to configure the type of profile that Windows Vista uses for new wireless network connections. Figure 9-26 shows the available options.

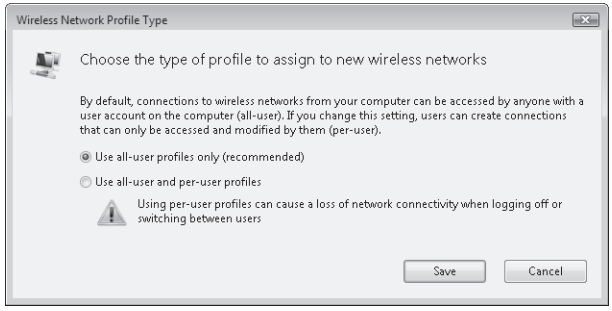

Figure 9-26 Configuring default profile type settings for new wireless network connections

The Use All-User Profiles Only (Recommended) option is preferred, which specifies that all users on the computer share the same set of wireless network connection settings. If this is not desired for security reasons, you can enable per-user profiles, using the second option. When Windows Vista creates per-user profiles, users can create new network connections for only their own user accounts.

Troubleshooting Wireless Connections

Wireless networking technology does not always work flawlessly, and users might encounter issues with lost connections or intermittent problems. The general troubleshooting steps presented in Lesson 1 apply equally to wireless networks. For example, Windows Vista includes the ability to diagnose and repair wireless connections automatically. If the computer is not using a valid IP address for the network, the operating system can automatically attempt to obtain a new address through DHCP.

In addition to standard protocol-level troubleshooting, common wireless problems are related to the strength of the wireless network connection. Earlier in this lesson, you saw how to view the details in the Properties dialog box of the network connection. A quicker way to determine signal strength is to hover the mouse pointer over the wireless networking icon in the system tray. The resulting display (shown in Figure 9-27) shows currently connected networks, along with the quality of the connection.

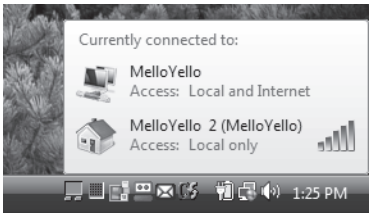

Figure 9-27 Viewing signal strength for a wireless connection, using the system tray

Quick Check

1. Which wireless security protocol provides the greatest level of security?
2. How would you connect to a wireless network that is not configured to broadcast its SSID?

Quick Check Answers

1. The Wi-Fi Protected Access (WPA) protocol provides increased security over the previous standard, Wired Equivalent Privacy (WEP).
2. Wireless networks that are not broadcasting SSID information can be connected to manually by using the Manage Network Connections list in Network And Sharing Center.

Practice: Managing Wireless Network Settings

In this practice, you will set up a new wireless network connection on a computer running Windows Vista. The exercise assumes that you currently have an active and functioning

wireless network connection and that you have the appropriate information (including any security keys) required to connect to the network.

▶ Practice: Connect to a Wireless Network

In this practice, you disconnect from your current wireless network and then walk through the steps of adding the wireless network connection to the computer.

1. Right-click the icon for the current wireless network connection and click Network And Sharing Center.
2. In the Network And Sharing Center, click View Status to view information about the connection. Make a note of the SSID that the current connection is using, and then click Close to return to the Network And Sharing Center.
3. Click Disconnect next to the wireless network connection.
4. Next, click Manage Wireless Networks in the Network And Sharing Center. If the SSID that you recorded in step 2 is present in the list, right-click it and select Remove Network. Click OK to confirm the removal.

   This prevents Windows Vista from automatically connecting to the network when it is available.
5. Close the Manage Wireless Networks dialog box.
6. To create a connection to the wireless network, click Connect To A Network in the Network And Sharing Center.
7. Select the name of the SSID that you recorded in step 2, and then click Connect. Windows Vista attempts to connect to the network.
8. If prompted for security information for the connection, type in the security key or passphrase for the wireless network, and then click Connect.
9. If you would like Windows Vista to connect automatically to this wireless network connection in the future, select both check boxes in the final step of the connection process. If not, you can clear the Start This Connection Automatically and Save This Network check boxes. Click Close to return to Network And Sharing Center.
10. Open Internet Explorer and browse to a Web site to verify that the connection is working properly.
11. When finished, close Internet Explorer and close Network And Sharing Center.

Lesson Summary

- Wireless network connections typically involve the use of a wireless network adapter and a wireless router or access point.
- There are various wireless networking protocols available, each with a different combination of range and performance.

- The primary security protocols for wireless networks are Wired Equivalent Privacy (WEP) and the more secure Wi-Fi Protected Access (WPA).
- Ad hoc wireless networks are created between computers without requiring a wireless router or access point.
- Wireless networks can be created and managed using the Network And Sharing Center.
- Wireless network connection profiles can be created for all users or on a per-user profile basis.

Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 2. The questions are also available on the companion CD if you prefer to review them in electronic form.

NOTE Answers

Answers to these questions and explanations of why each answer choice is correct or incorrect are located in the "Answers" section at the end of the book.

---

1. You are a Consumer Support Technician assisting a customer with configuring a wireless network. Specifically, the wireless network settings are working properly in her home environment. However, when she takes her notebook computer to her office, Windows Vista automatically connects to the incorrect wireless network. How can she resolve this problem?
   - **A.** Reinstall the drivers for the wireless network adapter.
   - **B.** Enable the wireless network adapter.
   - **C.** Change the preferred network connection order, using the network map in the Network And Sharing Center.
   - **D.** Configure the network connection order, using the Manage Wireless Networks option in the Network And Sharing Center.
2. Which of the following methods enable you to view the current signal strength for a wireless network connection? (Choose all that apply.)
   - **A.** View the status of a wireless network in the Network And Sharing Center.
   - **B.** Generate a network map in the Network And Sharing Center.
   - **C.** Click Set Up A Connection in the Network And Sharing Center.
   - **D.** Click the system tray icon for the wireless network connection.

Chapter Review

To further practice and reinforce the skills you learned in this chapter, you can perform the following tasks:

- Review the chapter summary.
- Review the list of key terms introduced in this chapter.
- Complete the case scenarios. These scenarios set up real-world situations involving the topics of this chapter and ask you to create a solution.
- Complete the suggested practices.
- Take a practice test.

Chapter Summary

- The Next Generation TCP/IP stack of Windows Vista supports both IPv4 and IPv6.
- Computers that are using IPv4 can be configured to use a DHCP-assigned address. Users can also manually set the IP address, subnet mask, default gateway, and DNS server address(es) for the computer.
- Windows Vista includes built-in tools for connecting to wireless networks and managing wireless network functionality.
- Windows Vista supports the Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) wireless security standards.

Key Terms

Do you know what these key terms mean? You can check your answers by looking up the terms in the glossary at the end of the book.

- ad hoc wireless network
- default gateway
- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- Internet Protocol v4 (IPv4)
- Internet Protocol v6 (IPv6)
- IP address
- local area network (LAN)

- Service Set Identifier (SSID)
- subnet mask
- Wi-Fi Protected Access (WPA)
- Wired Equivalent Privacy (WEP)

Case Scenarios

In the following case scenarios, you apply what you've learned about configuring Windows Vista networking. You can find answers to these questions in the "Answers" section at the end of this book.

Case Scenario 1: Adding a New Computer to a Network

You are a Consumer Support Technician assisting a customer with configuring a new wired network connection in his home. In the past, you assisted him with setting up a home network connection. The network currently does not have any method of automatically assigning network addresses. The IPv4 information you used on the original computer includes the following:

- IPv4 Address: 10.10.0.120
- Subnet Mask: 255.255.255.0
- Default Gateway: 10.10.0.1
- DNS Server Address (Primary): 10.10.0.1

The other computer is working properly and can access the Internet. He would like the new computer to be able to access the Internet and to be able to communicate with the other computer. There are no other computers on the network.

1. What IP address should you assign for the new computer?
2. What value should you use for the subnet mask of the new computer?
3. How can you manually configure the network settings for the TCP/IPv4 protocol on the new computer?
4. How can you simplify the process of managing network address information for future computers that are added to the network?

Case Scenario 2: Managing Wireless Network Connections

You are a Consumer Support Technician assisting a customer with configuring a wireless connection for use in multiple scenarios. The customer states that she frequently travels between multiple locations and wants to use the features of Windows Vista to connect to wireless networks quickly and easily when they are available. Examples of typical locations include the customer's home, her local office, coffee shops, airports, and hotel rooms. In some locations, such as her local office, multiple wireless network connections are available, but the customer would like to connect automatically to only one of these. Occasionally, she will share her laptop computer with a co-worker who already has an account on the computer.

1. For security reasons, the customer would like to be prompted for a key or passphrase whenever she connects to a new wireless network. How can you configure this?
2. How can you specify an order of preference for wireless network connections that are available at the customer's local office?
3. How can the customer configure some connections to connect automatically for only her user account?

Suggested Practices

To help you successfully master the exam objectives presented in this chapter, complete the following tasks.

Managing Network Connections in Windows Vista

The following practices help you become familiar with various methods of working with wired and wireless network connections in Windows Vista.

- **Practice 1: Configure Network Connections** Choose several different computers running Windows Vista and examine their network configurations. If possible, attempt to connect new computers to a test wired or wireless network and keep track of the settings that you have decided to use. Use the Network Map feature of the Network And Sharing Center to gain an overview of all of the available computers in the environment.
- **Practice 2: Troubleshoot Network Problems** Choose a computer running Windows Vista that has either a wired or wireless network connection. Manually make various changes to TCP/IPv4 settings, such as the IP address, subnet mask, default gateway, and DNS servers. Choose values that might not be compatible with the current network. Then, use the Diagnose and Repair options to try to troubleshoot the problems automatically. Additionally, use command-line tools such as IPCONFIG, PING, and NETSH to help determine the source of problems and to correct them.

Take a Practice Test

The practice tests on this book's companion CD offer many options. For example, you can test yourself on just one exam objective, or you can test yourself on all of the 70-623 certification exam content. You can set up the test so that it closely simulates the experience of taking a certification exam, or you can set it up in study mode so that you can look at the correct answers and explanations after you answer each question.

MORE INFO Practice tests

For details about all the practice test options available, see the "How to Use the Practice Tests" section in this book's introduction.
