

Monitoring Your Network

If you're the unofficial administrator of your home or small office network, I imagine you're already saddled with a fairly long to-do list of network chores: adding and upgrading network devices, configuring your router, adding and maintaining users, creating passwords, adding shared folders, setting permissions, and on and on. The last thing you probably need is yet another set of chores tacked on to that list. Well, sorry, but I'm afraid I'm going to do just that in this chapter as I show you how to monitor three aspects of your network: performance, shared folders, and users.

The good news is that none of the monitoring tasks you learn about in this chapter are activities you need to do very often. In all cases, in fact, you may need to perform the monitoring chores only once in a while, or on an as-needed basis. For example, you might want to check your network performance now to get a baseline for comparison, then you might want to check it again only if the network feels slow or if you upgrade your equipment.

Remember, however, that even a network with just a few computers is still a fairly large and unwieldy beast that requires a certain amount of vigilance to keep things running smoothly. Therefore, it's worth it to keep an eye on the network to watch for things going awry.

- Monitoring Network Performance
- Monitoring Shared Folders
- From Here

Monitoring Network Performance

By far the most important aspect of your network that you should monitor is the network's performance. A network's job is to transfer data, and if your data is getting transferred at a rate that's substantially slower than it should be, you and your users won't be happy or productive.

The easiest way to check network performance is to check the current status of wired and wireless network connections (see Figure 17.1). I explained how to do this in Chapter 5, "Working with Vista's Basic Network Tools and Tasks." In particular, you want to look at the Speed value: If it says, for example, that you have a 100Mbps connection but you thought you were using Gigabit Ethernet equipment, you need to check that equipment.

- To learn how to view the status of a network connection, see "Viewing the Current Network Status," p. 123.

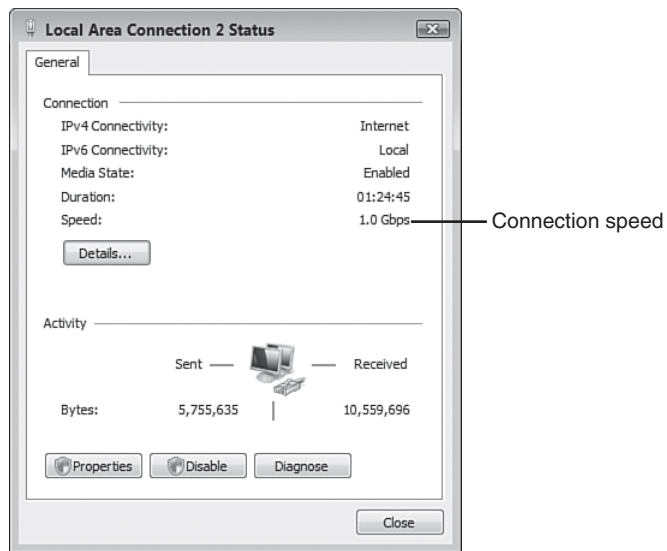


FIGURE 17.1

In the Status dialog box for your network connection, check the Speed value to ensure your connection is operating at the correct rate.

Monitoring Network Performance with Task Manager

The Task Manager utility is excellent for getting a quick overview of the current state of the system, and it offers a couple of tools that help you monitor your network.

To get Task Manager onscreen, follow these steps:

1. Press Ctrl+Alt+Delete. Vista displays its security window.
2. Select Start Task Manager.

If your network feels sluggish, it could be that the remote computer you're working with is sharing data slowly or that network traffic is exceptionally high. To see whether the latter situation is the cause of the problem, you can check out the current *network utilization* value, which is the percent of available bandwidth that your network adapter is currently using.

To check network utilization, display Task Manager's Networking tab, shown in Figure 17.2. Use the graph or the Network Utilization column to monitor the current network utilization value. Notice that this value is a percentage. This means that the utilization is a percentage of the bandwidth shown in the Link Speed column. So, for example, if the current network utilization is 10% and the Link Speed value is 1Gbps, the network is currently using about 100Mbps bandwidth.

The Network Utilization value combines the data sent by the computer and the data received by the computer. If the utilization is high, it's often useful to break down the data stream into the separate sent and received components. To do that, select View, Network Adapter History, and then select Bytes Sent (which displays as a red line on the graph) or Bytes Received (which displays as a yellow line on the graph).

If you're feeling ambitious or curious, you can view much more information than what you see in the default Networking tab. Follow these steps to add one or more columns to the view:

1. Select the View, Select Columns command. Task Manager displays the Select Columns dialog box, as shown in Figure 17.3. This dialog box offers a long list of networking measures that you can monitor.

tip To bypass the security window, either press Ctrl+Shift+Esc or right-click an empty section of the taskbar, and then click Task Manager.

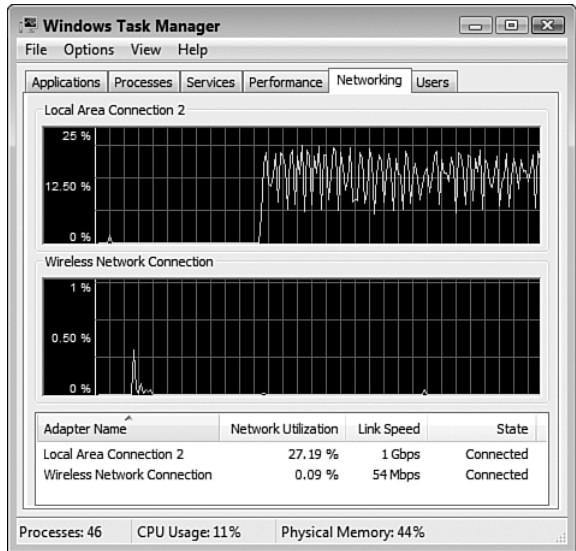


FIGURE 17.2
Use Task Manager’s Networking tab to check the current network utilization percentage.

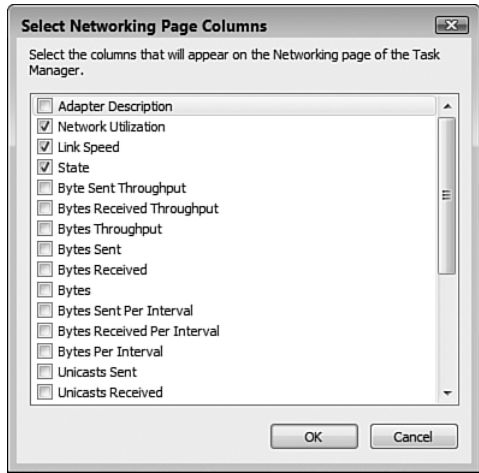


FIGURE 17.3
Use the Select Columns dialog box to choose which values you want to monitor in the Networking tab.

2. Activate the check box of a value that you want to monitor.
3. Repeat step 2 for each value you want to add to the networking tab.
4. Click OK.

tip By default, the Networking tab doesn't collect data when you're viewing some other Task Manager tab. If you prefer that the Networking tab always collect data, select Options, Tab Always Active.

Here's a summary of some of the more useful columns you can add:

Adapter Description	This column shows the description of the network adapter.
Network Utilization	This is the network utilization value.
Link Speed	This value shows the network adapter's connection speed.
State	This column displays the general state of the adapter.
Bytes Sent Throughput	This value shows the percentage of connection bandwidth used by traffic sent from Windows Vista.
Bytes Received Throughput	This value shows the percentage of connection bandwidth used by traffic received by Windows Vista.
Bytes Throughput	This value shows the percentage of connection bandwidth used by traffic both sent from and received by Windows Vista.
Bytes Sent	This column tells you the total number of bytes sent from Windows Vista over the network adapter during the current session (that is, since the last boot).
Bytes Received	This column tells you the total number of bytes received by Windows Vista over the network adapter during the current session.
Bytes	This column tells you the total number of bytes sent from and received by Windows Vista over the network adapter during the current session.
Bytes Sent Per Interval	This value shows the total number of bytes sent from Windows Vista over the network adapter during the most recent update interval. (For example, if the Update Speed value is set to Low, the display updates every 4 seconds, so the Bytes Sent Per Interval value is the number of bytes sent during the most recent 4-second interval.)

Bytes Received Per Interval	This value shows the total number of bytes received by Windows Vista over the network adapter during the most recent update interval.
Bytes Per Interval	This value shows the total number of bytes sent from and received by Windows Vista over the network adapter during the most recent update interval.

On your small network, you can use these measures to watch out for extreme values. That is, with normal network traffic, the values should never be either really small or really large for long periods. If you notice small (or zero) values for long periods, it could indicate that your computer isn't able to send or receive data; if you notice high values (particularly on the various "Throughput" measures, where "high" means values near 100%) for an extended time, it could indicate a software problem where a rogue application is bombarding your computer with data.

Monitoring Network Performance with Performance Monitor

For more advanced performance monitoring, Windows Vista offers the Performance Monitor tool, which you display by following these steps:

1. Select Start, Control Panel to open the Control Panel window.
2. Select System and Maintenance to open the System Maintenance window.
3. Select Administrative Tools to open the Administrative Tools window.
4. Double-click Reliability and Performance Monitor. The User Account Control dialog box appears.
5. Enter your UAC credentials to continue. Windows Vista displays the Reliability and Performance Monitor.

The Reliability and Performance branch displays the Resource Monitor, which is divided into six sections:

- **Resource Overview.** This section shows graphs of the data in the CPU, Disk, Network, and Memory sections.
- **CPU.** This section shows the percentage of CPU resources that your

tip You can also open the Reliability and Performance Monitor by pressing Windows Logo+R (or selecting Start, All Programs, Accessories, Run) to open the Run dialog box, typing **perfmon**, clicking OK, and then entering your UAC credentials when prompted. (Alternatively, select Start, type **perfmon** in the Search box, and then click **perfmon** in the search results.)

system is using. Click anywhere on the CPU bar to expand the section and show the percentage of resources that each running process is using.

- **Disk.** This section shows the total hard disk input/output transfer rate (disk reads and writes in kilobytes per second). Click anywhere on the Disk bar to expand the section to see the files involved in the current disk I/O operations.
- **Network.** This section shows the total network data-transfer rate (data sent and received in kilobits per second). Click anywhere on the Network bar to expand the section to see the remote computers and other processes involved in the current network transfers, as shown in Figure 17.4.

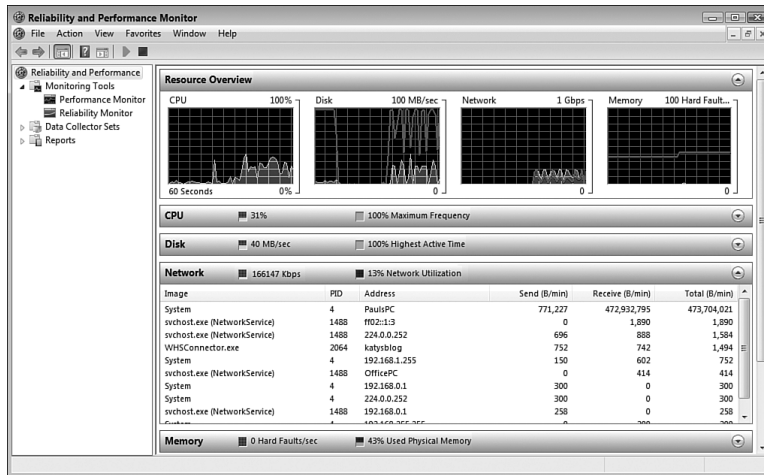


FIGURE 17.4

The new Reliability and Performance Monitor enables you to monitor various aspects of your system.

- **Memory.** This section shows the average number of hard memory faults per second and the percentage of physical memory used. Click anywhere on the Memory bar to expand the section to view the individual processes in memory.
- **Learn More.** This section contains links to the Reliability and Performance Monitor help files.

For more detailed network performance monitoring, select the Reliability and Performance Monitor, Monitoring Tools, Performance Monitor branch. The Performance Monitor appears, as shown in Figure 17.5.

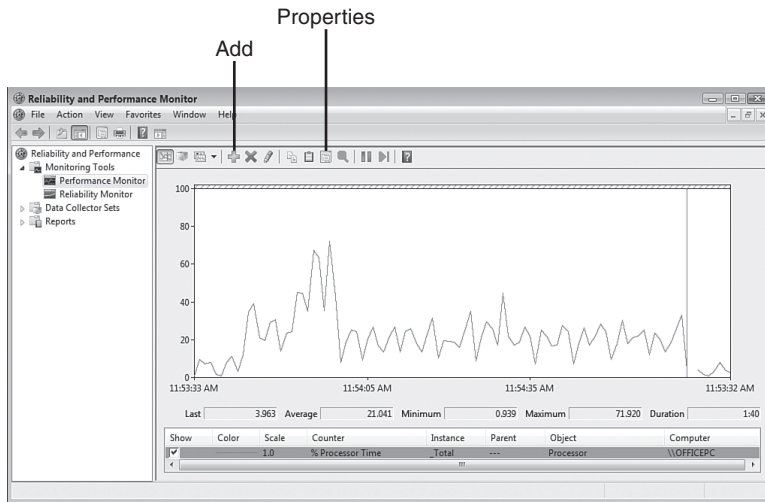


FIGURE 17.5

You can use Performance Monitor to keep an eye on your network performance.

Performance Monitor's job is to provide you with real-time reports on how various system settings and components are performing. Each item is called a *counter*, and the displayed counters are listed at the bottom of the window.

Windows Vista shows just one counter at first—the % Processor Time, which tells you the percentage of time the processor is busy. However, as you see in the next section, you can add more counters to monitor what you want. Each counter is assigned a different colored line, and that color corresponds to the colored lines shown in the graph. Note, too, that you can get specific numbers for a counter—the most recent value, the average, the minimum, and the maximum—by clicking a counter and reading the boxes just below the graphs.

tip By default, Performance Monitor samples the performance data every second. To change the sample interval, right-click Performance Monitor and then select Properties. (You can also press Ctrl+Q or click the Properties button in the toolbar, pointed out in Figure 17.5.) In the Performance Monitor Properties dialog box, display the General tab, and modify the value in the Sample Every X Seconds text box. Click OK to put the new sample interval into effect.

The idea is that you should configure Performance Monitor to show the processes you're interested in (such as current network bandwidth) and then keep Performance Monitor running while you perform your normal chores. By examining the Performance Monitor readouts from time to time, you gain an appreciation of what is typical on your system. Then, if you run into performance problems, you can check Performance Monitor to see whether you've run into any bottlenecks or anomalies.

Adding Performance Counters

To add another setting to the Performance Monitor window, follow these steps:

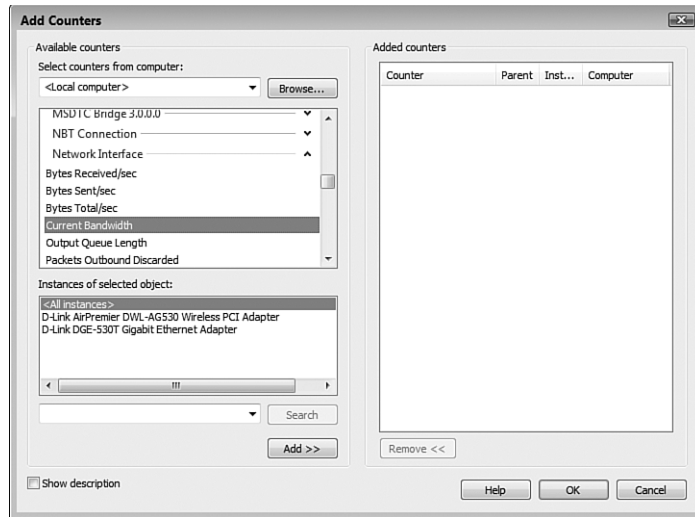
1. Right-click Performance Monitor and then click Add Counters. (You can also press Ctrl+I or click the Add button in the toolbar; see Figure 17.5.)

The Add Counters dialog box appears

2. Double-click the counter category you want to work with.
3. Select the counter you want. If you need more information about the object, activate the Show Description check box.
4. If the counter has multiple instances (see Figure 17.6), select the instance you want from the Instances of Selected Object List. (For example, if you choose Network Interface as the performance object and your system has multiple network interface cards, you need to choose which NIC you want to monitor. You can also usually select <All Instances> to monitor the total of all the instances.)
5. Click Add. Performance Monitor places the counter in the Added Counters list.
6. Repeat steps 2–5 to add any other counters you want to monitor.
7. Click OK.

tip The graph is only useful if you can see the results properly. Unfortunately, sometimes the scale of the graph isn't appropriate for the numbers generated by a particular counter. The default scale is from 0 to 100; so if a counter regularly generates numbers larger than 100, all you'll see is a straight line across the top of the graph. Similarly, if a counter regularly generates very small numbers, the counter's graph will be a straight line across the bottom of the graph.

To fix this, you can change the scale used by the Performance Monitor graph. Right-click Performance Monitor, and then select Properties. (You can also press Ctrl+Q or click the Properties button in the toolbar.) In the Performance Monitor Properties dialog box, display the Graph tab and modify the values in the Maximum and Minimum text boxes. I also find that activating the Horizontal Grid check box helps you to interpret the graph. Click OK to put the new settings into effect.

**FIGURE 17.6**

Use the Add Counters dialog box to add more counters to Performance Monitor.

Understanding Network Performance Counters

In the Add Counters dialog box, the Network Interface category has the network performance counters you want to work with. There are quite a few here, some of which monitor the same things as the Task Manager statistics I mentioned earlier. Fortunately, only a few of the performance objects are truly useful for your Windows Vista network, and in most situations you need only track a few counters to monitor the network performance. Here's my list of the most useful Network Interface counters:

- Current Bandwidth** This counter tells you the current network bandwidth, in bits per second. For example, a 1Gbps connection shows as 1,000,000,000,000.
- Bytes Total/Sec** This counter tells you the total number of bytes received and bytes sent over the network connection per second. (This is the sum of the Bytes Received/Sec and Bytes Sent/Sec values.) Multiply this value by 1,024 to calculate the number of bits per second that are passing through the adapter. Under load (say, while streaming media), the result should be close to the Current Bandwidth value. If it's substantially less, you have a network bottleneck.

Packets Outbound Errors	This counter shows the number of network packets that could not be sent because of errors. Errors are normally rare, so if you're seeing packet errors, it could indicate a problem. You may need to update the remote computer's NIC device driver, or it could mean that the NIC has a problem and needs to be replaced.
Packet Received Errors	This counter shows the number of network packets that could not be received because of errors. Seeing errors here may mean that you need to update your computer's NIC device driver, or it could mean that your NIC needs to be replaced.

Monitoring Shared Folders

Windows Vista comes with a snap-in tool called Shared Folders that enables you to monitor various aspects of the folders that you've shared with the network. For example, for each shared folder, you can find out the users who are connected to the folder, how long they've been connected, and the files they have open. You can also disconnect users from a shared folder or close files that have been opened on a shared folder. The next few sections provide the details.

Launching the Shared Folders Snap-In

To get started, you need to open the Shared Folders snap-in. Here are the steps to follow:

1. Press Windows Logo+R (or select Start, All Programs, Accessories, Run) to open the Run dialog box.
2. In the Open text box, type `fsmgmt.msc`.
3. Click OK. The User Account Control dialog box appears.
4. Enter your UAC credentials. Windows Vista opens and the Shared Folders snap-in appears.

note A snap-in is a component that works with Vista's Microsoft Management Console (MMC) program. This program creates a console into which different mini-programs can be "snapped in." If you want to take a look at MMC, press Windows Logo+R (or select Start, All Programs, Accessories, Run) to open the Run dialog box, type `mmc`, and click OK. In the Console window that appears, select File, Add/Remove Snap-in (or press Ctrl+M) to see the list of available snap-ins.

5. Select the System Tools, Shared Folders branch.

tip Another way to launch the Shared Folders snap-in is to select Start, type **fsmgmt.msc** in the Search box, and then click fsmgmt in the search results.

Viewing the Current Connections

To see a list of the users connected to any Windows Vista shared folder, select Shared Folders, Sessions. Figure 17.7 shows an example. For each user, you get the following data:

User	The name of the user.
Computer	The name of the user's computer. If Windows Vista doesn't recognize the computer, it shows the machine's IP address, instead.
Type	The type of network connection. Windows Vista always shows this as Windows (even if the user is connected from a Mac or from Linux).
Open Files	The number of open files in the shared folders.
Connected Time	The amount of time that the user has been connected to the remote computer.
Idle Time	The amount of time that the user has not been actively working on the open files.
Guest	Whether the user logged on using the Guest account.

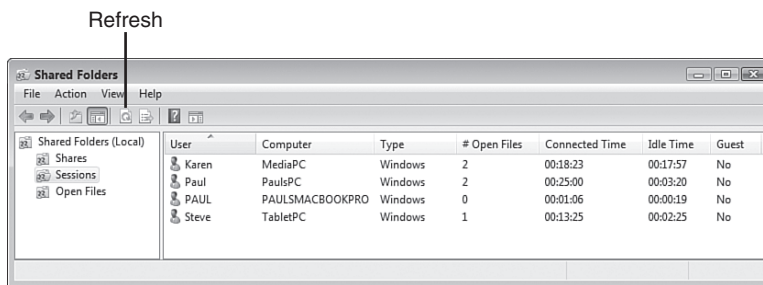


FIGURE 17.7

The Sessions folder shows the users currently connected to shared folders on the remote computer.

Viewing Connections to Shared Folders

The Shared Folders snap-in also makes it possible for you to view the connections to Windows Vista by its shared folders. To get this display, select Shared Folders, Shares. As you can see in Figure 17.8, this view provides the following information:

Share Name	The name of the shared folder. Note that the list includes the Windows Vista hidden shares.
Folder Path	The drive or folder associated with the share.
Type	The type of network connection, which Windows Vista always shows as Windows.
# Client Connections	The number of computers connected to the share.
Comment	The description of the share.

note To ensure that you're always viewing the most up-to-date information, regularly select the Action, Refresh command or click the Refresh toolbar button (pointed out in Figure 17.7).

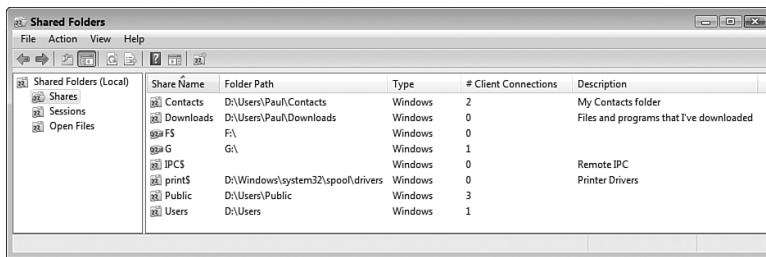


FIGURE 17.8

The Shared Folders snap-in can display a server's connections by its shared folders.

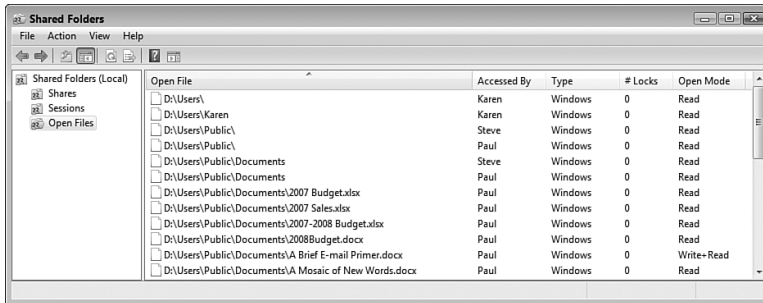
Viewing Open Files

The Shared Folders snap-in can also display the files that are open on the Windows Vista shares. To switch to this view, select System Tools, Shared Folders, Open Files. Figure 17.9 shows the result. Here's a summary of the columns in this view:

Open File	The full pathname of the file.
Accessed By	The name of the user who has the file open.

tip You can also use the Shares branch to work with the shared folders. For example, select a share and then select Actions, Open to display the folder. You can also select Action, Properties to modify the share name, description, and permissions of the selected share. Finally, you can also select Action, Stop Sharing to turn off sharing on the selected folder.

Type	The type of network connection, which Windows Vista always shows as <i>Windows</i> .
# Locks	The number of locks on the file.
Open Mode	The permissions the user has over the file.

**FIGURE 17.9**

The Shared Folders snap-in can also display a remote computer's open files in its shared resources.

Closing a User's Session or File

Although in the interest of network harmony you'll want to let users connect and disconnect as they please, at times you might need to boot someone off a machine. For example, you might see that someone has obtained unauthorized access to a share. To disconnect that user, follow these steps:

1. In the Shared Folders snap-in, select Shared Folders, Sessions.
2. Right-click the name of the user you want to disconnect.
3. Click Close Session. Windows Vista asks you to confirm.
4. Click Yes.

Similarly, you'll usually want to let users open and close files themselves so that they don't lose information. However, you might find that a user has a particular file open and you would prefer that the user not view that file (for example, because you want to work on the file yourself or because the file contains information you

caution If you have a file in a shared folder and you don't want other users to see that file, it makes more sense to either move the file to a protected folder or change the permissions on the file's current folder.

don't want the user to see). To close a file opened by a user, follow these steps:

1. In the Shared Folders snap-in, select Shared Folders, Open Files.
2. Right-click the name of the file you want to close.
3. Click Close Open File. Windows Vista asks you to confirm.
4. Click Yes.

note The remote user doesn't see a warning or any other indication that you're closing the file. For example, if the user is playing a music file, that file just stops playing and can't be started again (except by closing all open shared files and folders and starting a new session).

From Here

- To learn how to view the status of a network connection, see "Viewing the Current Network Status," p. 123.
- For the details on sharing folders, see "Sharing Resources with the Network," p. 184.
- If you detect a problem with your network, you'll need to do some troubleshooting; see Chapter 18, "Troubleshooting Network Problems," p. 441.